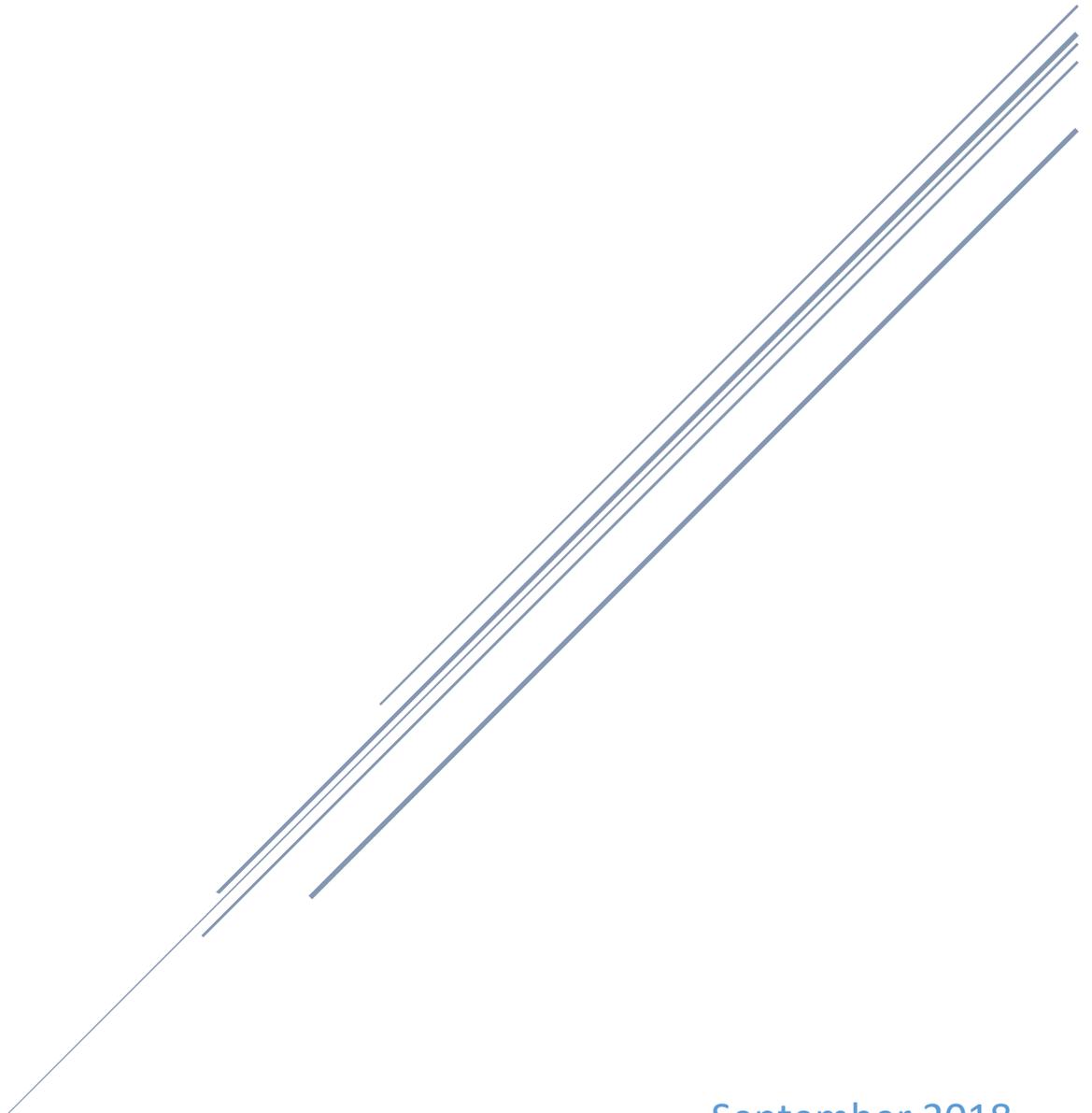


PUBLIC AWARENESS AND TRAINING WORKING GROUP STRATEGIC PLAN

Chair: Stephen A. Key | Co-Chair: Robert E. Dittmer



September 2018
Indiana Executive Council on Cybersecurity

Public Awareness and Training Working Group Strategic Plan

Contents

Committee Members	4
Introduction.....	6
Executive Summary	8
Research.....	10
Deliverable: Statewide Cybersecurity Public Relations Plan	13
General information	13
Implementation Plan	15
Evaluation Methodology	19
Supporting Documentation	21
ACS Cyberseucrity Guide.....	22
Deloitte-NASCIO Cybersecurity Survey	95
Global Cyber Security Capacity Centre Cyber Security Awareness Campaigns “Why do they fail to change behavior?” Draft Working Paper	132
IECC Public Awareness and Training Working Group Public Relations Plan 2018-2020	171
ITU Cybersecurity Index.....	228
Pew Research Center What Americans Know About Cybersecurity	307

Committee Members

Committee Members

Name	Organization	Title	Committee/ Workgroup Position	IECC Membership Type
Stephen A. Key	Hoosier State Press Association	Executive Director	Chair	Voting
Robert E. Dittmer	REDCOM Public Relations Consulting	President	Co-Chair	Voting Proxy
David Hosick	IN Dept. of Homeland Security	Communications Director	Full Time	Advisory
Nicole Needham	IN Office of Technology	Security Awareness Manager	Full Time	Advisory
Graig Lubsen	IN Office of Technology	Director of Communications	Full Time	Advisory
Julie A. Vincent	IUPUI	Public Relations Lecturer	Full Time	Advisory
Brian O'Hara	InfraGard	Past - President	As Needed	Advisory
Greg Ellis	Indiana Chamber of Commerce	VP, Energy and Environmental Policy	As Needed	Advisory
Dave Arland	Indiana Broadcasters Association	Executive Director	As Needed	Advisory
Kathleen Johnston	NA	Media Freelancer	Full Time	Advisory
David Woodward	Indiana Department of Education	Director, Building Security and Safety	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
 - The Public Awareness and Training Working Group (PATWG) has submitted questions to all IECC committees/work groups to help determine the needs of those units. PATWG received a proposal from Julie Vincent’s J428 Public Relations Strategic Planning and Research class at IUPUI with outreach plan for citizens and high school students. PATWG also reviewed a study released by the PEW Research Center on March 2017, which is titled “What Americans Know About Cybersecurity.

- **Research Findings**
 - Comprehensive plan for public awareness and training will have two distinct components: one geared toward the public at large and another tailored for the specific needs of other IECC committees and work groups. Any plan will require the state to commit resources for implementation.

- **Working Group Deliverable**
 - Statewide Cybersecurity Public Relations Plan

- **Additional Notes**
 - Next step for PATWG is to reach out personally to other committees/work groups through script prepared by co-chair Bob Dittmer to supplement written responses to work group’s questions. The needs analysis will help PATWG create the comprehensive plan.

- **References**
 - [No Response]

Research

Research

- 1. What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
 - a. There has essentially been no coordinated statewide effort to educate the general public about cybersecurity efforts. Individual industries and individual state agencies have conducted various programs focused generally in areas of their responsibility. The Indiana Attorney General has conducted a limited campaign, and the Indiana Office of Technology (IOT) has extensive training opportunities available and has worked in a limited fashion to promote cybersecurity awareness. Department of Revenue (DOR) has worked to educate taxpayers on fraud prevention.
- 2. What (or who) are the most significant cyber vulnerabilities in your area?**
 - a. The greatest vulnerability is the general lack of both awareness and knowledge among the general public on how best to protect themselves from cyber attacks.
- 3. What is your area's greatest cybersecurity need and/or gap?**
 - a. Public knowledge gap.
- 4. What federal, state, or local cyber regulations is your area beholden to currently?**
 - a. None.
- 5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
 - a. Very few. Virginia has done some work in this area and will be used as an initial model. However, they have no cohesive, comprehensive plan.
- 6. What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
 - a. PEW Research Center study: "What Americans Know About Cybersecurity." Conducted June 2016; Published March 2017.
 - b. "ACS Cybersecurity: Threats, Challenges, Opportunities." Australian Computer Society, November 2016.
 - c. "Cyber Security Awareness Campaigns: Why do they fail to change behavior?" draft working paper, Global Cyber Security Capability Center, July 2015.
 - d. IUPUI student survey (convenience sample) conducted of Indiana residents, November 2017.
- 7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
 - a. Governor's Association and selected (few) states. Individual Indiana state agencies with limited perspectives and individually focused activities.

- 8. What does success look like for your area in one year, three years, and five years?**
- a. One year:
 - i. Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
 - ii. Achieve active Cybersecurity activities by Hoosiers to 25 percent.
 - iii. Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
 - b. Three years:
 - i. Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
 - ii. Achieve 50 percent active cybersecurity protective measures by Hoosiers.
 - iii. Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
 - c. Five years:
 - i. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
 - ii. Achieve 75 percent active cybersecurity protective measures by Hoosiers.
 - iii. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
- 9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
- a. N/A
- 10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
- a. N/A
- 11. What do we need to do to attract cyber companies to Indiana?**
- a. N/A
- 12. What are your communication protocols in a cyber emergency?**
- a. N/A. See procedures for Indiana Joint Operations Center and Joint Information Center.
- 13. What best practices should be used across the sectors in Indiana? Please collect and document.**
- a. From a public awareness and training perspective, there are none. See Supporting Documentation.

Deliverable: Statewide Cybersecurity Public Relations Plan

Deliverable: Statewide Cybersecurity Public Relations Plan

General information

1. What is the deliverable?

- a. The PAT working group will create an initial public communication plan for execution in two phases. The first phase will educate Hoosiers about cybersecurity and high schools students about cybersecurity careers. The second phase will be focused on supporting awareness and cyber defense for specific industries and businesses (working with all other committees and working groups).

2. What is the status of this deliverable?

- a. 100% Complete

3. Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See [Executive Order 17-11](#) for further context.

- Establish an effective governing structure and strategic direction.
- Formalize strategic cybersecurity partnerships across the public and private sectors.
- Strengthen best practices to protect information technology infrastructure.
- Build and maintain robust statewide cyber-incident response capabilities.
- Establish processes, technology, and facilities to improve cybersecurity statewide.
- Leverage business and economic opportunities related to information, critical infrastructure, and network security.
- Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. Which of the following categories most closely aligns with this deliverable (check ONE)?

- Research – Surveys, Datasets, Whitepapers, etc.
- Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
- Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
- Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
- Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
- Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. What is the resulting action or modified behavior of this deliverable?

- a. Initial deliverable will be a complete cybersecurity public awareness campaign plan that is designed to increase public awareness and knowledge about methods to protect individuals and systems from cyberattack. A second level plan will target businesses and industries to build awareness and knowledge. Both will include communication planning to change physical behaviors to enhance cybersecurity by individuals and employees/businesses.

6. What metric or measurement will be used to define success?

- a. A series of measurable awareness, knowledge and behavior traits will be used for measurement.

7. What year will the deliverable be completed?

- a. 2018
- b. Note: the plan will be delivered in 2018. However, execution will be a multi-year activity.

8. Who or what entities will benefit from the deliverable?

- a. All Hoosiers and Hoosier businesses.

9. Which state or federal resources or programs overlap with this deliverable?

- a. While there are some individual and limited state departments promoting good cybersecurity habits, research would suggest there is no entities taking a holistic approach to the problem. This will be that approach.

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

- a. We will be working with all other committees and working groups to develop the second phase of the communication plan targeting behaviors of employees and businesses.

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

- a. Federal agencies: none
- b. State agencies: perhaps all, perhaps none. Most likely, however, IOT and Department of Homeland Security (DHS) along with the Governor's office.
- c. Associations: Probably many industry and trade associations will need to be involved.
- d. Non-profit organizations: Unknown at this time.

12. Who should be main lead of this deliverable?

- a. Governor's office or identified lead agency. Could be IDHS or IOT.

13. What are the expected challenges to completing this deliverable?

- a. If the deliverable is the plan, none. However, implementation will require funding and/or staffing.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

- a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Plan	Working Group	100%	May 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

- a. Yes
- b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
At least one	At least one	Senior Public Relations Professional	Appropriated	None	At least one very experienced public relations professional working from the Governor's office with overall responsibility for plan execution, public representation, and coordination among key agencies. Will also oversee activities and budget for advertising agency.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Advertising and creative agency	Advertising portion of the campaign plan requires development of print, online and broadcast advertising	SWAG: \$250,000.00	SWAG: \$250,000			
Purchase of advertising space	Support of campaign; broad reach; message consistency	Incl.	Incl.			

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

- a. Principle benefit is a coordinated approach to increasing public awareness of the need for cybersecurity awareness, knowledge, and activity across all key constituent groups, but especially the general public.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

- a. The more active the public is in defending personal and business systems from cyberattack, the less risk to individuals, businesses, and the state’s critical infrastructure.

19. What is the risk or cost of not completing this deliverable?

- a. The risk is status quo: where there is measurable ignorance of cybersecurity and even less individual cyber defense activity exposing the State’s people and infrastructure to potential compromise.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

- a. Metrics are included in the plan. Principle baseline of measurement is a Pew Center Study from 2016.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

- a. No
- b. **If Yes, please list states/jurisdictions**
 - i. Not recommended. Measure against a national standard (Pew Study).

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

- a. Yes
- b. **If Yes, please list states/jurisdictions**
 - i. Every state. But, not recommended.
 - ii. We can examine using Ohio or Illinois or Kentucky. The challenge will be conducting sufficient research to measure their lack of activity and results.
 - iii. In this case, it is more important to measure against a national standard (the Pew Study) than comparing to individual states.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

- a. Budget availability
- b. Personnel availability

24. Does this deliverable require a change from a regulatory/policy standpoint?

- a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

- a. Continued support for qualified personnel and a supportive budget.

26. Who has the committee/working group contacted regarding implementing this deliverable?

- a. Currently working with the Cybersecurity Program Director.

27. Can this deliverable be used by other sectors?

- a. Yes
- b. **If Yes, please list sectors**
 - i. It is intended to continue this planning process to include activities support each of the other sectors as their operational plans become more defined. This planning will likely take place during the first phase (year 1) of the plan and be executed in the second phase (years 2-3).

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

- a. Cybersecurity Council
- b. Governor
- c. Senior agency leadership

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. N/A

Evaluation Methodology

Objective 1: The IECC Public Awareness and Training Working Group complete a statewide public relations cybersecurity campaign plan by June 2018.

Type: Output Outcome

Evaluative Method:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Completion | <input type="checkbox"/> Peer Evaluation/Review |
| <input type="checkbox"/> Award/Recognition | <input type="checkbox"/> Testing/Quizzing |
| <input type="checkbox"/> Survey - Convenient | <input type="checkbox"/> Benchmark Comparison |
| <input type="checkbox"/> Survey – Scientific | <input type="checkbox"/> Qualitative Analysis |
| <input type="checkbox"/> Assessment Comparison | <input type="checkbox"/> Quantifiable Measurement |
| <input type="checkbox"/> Scorecard Comparison | <input type="checkbox"/> Other |
| <input type="checkbox"/> Focus Group | |

Objective 2: IECC will implement an IECC public relations micro-plan on year one efforts by September 2018.

Type: Output Outcome

Evaluative Method:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Completion | <input type="checkbox"/> Peer Evaluation/Review |
| <input type="checkbox"/> Award/Recognition | <input type="checkbox"/> Testing/Quizzing |
| <input type="checkbox"/> Survey - Convenient | <input type="checkbox"/> Benchmark Comparison |
| <input type="checkbox"/> Survey – Scientific | <input type="checkbox"/> Qualitative Analysis |
| <input type="checkbox"/> Assessment Comparison | <input type="checkbox"/> Quantifiable Measurement |
| <input type="checkbox"/> Scorecard Comparison | <input type="checkbox"/> Other |
| <input type="checkbox"/> Focus Group | |

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- ACS Cybersecurity Guide
- Global Cyber Security Capacity Centre: Cyber Security Awareness Campaigns “Why do they fail to change behavior?” Draft Working Paper
- Deloitte NASCIO Cybersecurity Survey
- IECC Public Relations Plan
- ITU Cybersecurity Index 2017
- Pew Research Center – What Americans Know About Cybersecurity

ACS

Cybersecurity Guide

November 2016



November 2016



Cybersecurity

Threats
Challenges
Opportunities



“It is only when
they go wrong
that machines
remind you
how powerful
they are.”

Clive James

Contents

01

Foreward	1
Executive summary	4

02

A brave new world	5
Cyber speak!	6
What is cybersecurity?	7
And the weakest link is...	9
A world without cybersecurity	11

03

Threats in the information age	13
The nature of threats	14
The Internet of Things (IoT)	16
Botnet armies	17
When security is an afterthought	18
Autonomous systems	19
Driverless cars and transport	19
ATMs and Point of Sale	21
What about wearables?	22
Cyberwarfare	24
Automated attacks	24
Energetic Bear	24
Cyberattacks on infrastructure	26
When software kills	28
Data manipulation	29
Backdoors and espionage	29
Cloud concerns	29
Blast from the past	30
Virtualised threats	32
Industry and the individual	33
Ransomware and Cryptoware	33
Multi-vector attacks	33
Identity theft	34
The world we live in	34



04

The future in our hands	35
The 100% secure computer	37
Opportunities	38
The data-driven economy	38
Technology as wealth creation	39
Cybersecurity as job growth	39
Leveraging technology talent	39
Challenges	40
Leadership	40
Learning from history	40
Collaboration	41
Education and awareness	41
You are what you do	43
Legal and regulatory	43
Services and privacy	43
Perception and practicality	44

05

Looking to the road ahead	45
State of the nation	46
What role can you play?	47
Government	47
Education and research	50
Business and industry	50
You, the individual	50
The five pillars of cybersecurity readiness	51
Online resources	52
Through the looking glass	53
Fast facts	55
Glossary	57
References	59



Protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

Foreword

You've seen documents like this pass your desk before, but we hope this one is a little different. You can gloss over it, seeking the diamonds in the rough, but take the time to delve into the information presented here and you will walk away with a different appreciation of the laptop on your desk, the car that you drive, and the phone that you carry.

Not to mention the planes you fly, the banks that hold your money, the hospitals that keep you alive and the very infrastructure that makes our cities run. In short: the basis of our modern lives.

It can be hard to not overuse a word that's become popular thanks to public awareness, but 'cyber' is now firmly entrenched in our language and our mindset, by virtue of the fact that our society today depends so much on technology.

So we're going to talk about cyber with respect to security, as the two are intimately intertwined. In this guide we aim to break down what is sometimes a large and complex issue into an easy to read and digestible summary that should – if we've done our job well – give you the tools to both talk confidently about the issues, as well as equip you with the core information required to make decisions around cybersecurity.

Because, despite the technical nomenclature, the issue of cybersecurity is as vital to our way of life as technology itself. In fact, they can't be separated: our economic health, our national security, and indeed the fabric of our society is now defined by the technology we depend on every day.

What's left unsaid here, however, is the assumption that this technology will continue to work as we intend – but this is only true if we can protect it from being hacked, manipulated, and controlled.

Logically, then, protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

Which is to say, all of us.

If you are part of government, this primer serves as a guide to the greater sphere of cybersecurity and how it relates to our national security, our national interest, and our economic prosperity.

If you are an executive, board member, business leader, or IT professional this is an opportunity to verse yourself in the language and the ecosystem, the threats and the opportunities, and to better communicate the issues and responsibilities around cybersecurity within your organisation.

And if you are simply an individual interested in understanding more about the nature of our digitally-driven world, this guide will provide the basics and a clear overview of how cybersecurity relates to you.

At the ACS we welcome every opportunity to educate and assist. If you have any questions, or would like more information, please feel free to contact me at: anthony.wong@acs.org.au.

Enjoy this guide. We hope it will make a difference to you.

Anthony Wong
President, ACS



SECURING AUSTRALIA'S FUTURE

At ACS we are passionate about the ICT profession being recognised as a driver of productivity, innovation and business – able to deliver real, tangible outcomes.

This year ACS celebrates 50 years of advancing ICT in Australia. Our founders and pioneers worked on the first innovative computers in government, academia and industry, and our members now work at the coalface of technology development across every industry.

In 2011, ACS brought together its own Cyber Taskforce from our 23,000 members to respond to the Federal Government's new cyber discussion paper, 'Connecting with Confidence', where we highlighted the need to develop co-ordination and a focus on the pipeline of cyber professionals.

To play our part in securing Australia's future, we continue to perform the role of trusted advisor to government, and deliver

services to identify and certify ICT professionals you can trust, including through the Professional Standards Scheme that assures professionals have the specialist skills business can rely upon.

ACS is part of the global federation of professional ICT societies, the International Federation for Information Processing (IFIP), and the first professional body to receive accreditation under the International Professional Practice Partnership (IP3) – providing a platform for accreditation for ICT professionals and mutual recognition across international boundaries. The ACS currently chairs IP3 and plays a leading role in the professionalism of the ICT workforce.

IP3 has since gained global attention after successful engagements at the World Summit on the Information Society (WSIS) Forum in Geneva and the United

Nations in New York, where the importance of ICT professionalism was acknowledged by the UN General Assembly President in 2015.

In May 2016 the President of IFIP participated in the European Foresight Cyber Security Meeting where he advocated that professionalism of the ICT workforce is "a key element in building trustworthy and reliable systems" and that it is important to ensure that "cyber security and cyber resilience is also a duty of care of the individual ICT professional".

As we move forward another 50 years, ACS will be there at the forefront meeting the challenges and opportunities of ICT, and supporting the growth and potential of ICT professionals in Australia.



01

Executive summary

As technology continues to evolve so also do the opportunities and challenges it provides. We are at a crossroads as we move from a society already entwined with the internet to the coming age of automation, Big Data, and the Internet of Things (IoT).

But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyberattacks. Therefore, protecting it is of paramount priority.

This guide looks at some of the concerns facing us in the near future that include:

- Attack vectors such as botnets, autonomous cars and ransomware.
- Threats including data manipulation, identity theft, and cyberwarfare.
- Tangential issues such as data sovereignty, digital trails, and leveraging technology talent.

Additionally, it provides some background to the nature of digital ecosystems and the fundamentals of cybersecurity.

Critically, this document clarifies the importance for Australia to take responsibility for its own cybersecurity, especially with regards to essential infrastructure and governance.

On the flip side – and as one of the fastest growth industries globally – developing our own cybersecurity industry is also an opportunity for economic growth, job creation, and education – ensuring Australia is well positioned for a future as a digitally advanced nation.

Finally, we look at some of the challenges that countries worldwide are currently dealing with in regards to cybersecurity, including:

- The need for more collaboration in order to mitigate threats.
- Education and awareness; and
- The balance between privacy and security.

Our aim is that this document provides an informative primer on the relevant issues facing Australia in relation to cybersecurity, to generate discussion and debate, and to raise awareness with regards to a fundamental building block of the technologically-dependent society which we have already become.

As you will read in the following pages, cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And – through education, awareness, and proactive change – we can all play a part in securing our future.

A brave new world

You're reading this document written with, laid out by, and printed using computers. From start to finish it existed as 0s and 1s – the binary blood of our modern world.

In fact, our lives today are codified by data: almost everything we do, and everything we depend on, involves data and the technology that uses it – there are scant few areas not touched by this revolution we call the **information age**.



CYBER SPEAK!

Every industry has its own lexicon, and the cyber world is no different. While built on technological foundations that we all know – computers, the internet, smartphones, and similar – as you delve deeper into the subject you start to encounter acronyms and technical concepts that you may not be familiar with.

And, if we're all to communicate on the subject of cybersecurity – across all sectors of government, business, industry, and academia – then it can help to familiarise yourself with the nomenclature associated with this diverse and compelling subject.

To this end we've included a Glossary on page 57. Feel free to flick back and forth as you read to ensure you get the most out this document, spending more time expanding your knowledge and less time scratching your head!

And so it follows that in order to keep our way of life – and to continue to prosper through technology – we must ensure that it always operates and works for us as intended.

And for the most part it does, until it's hacked. In the hands of less than favourable individuals, organisations, and governments, technology and the data it depends on can be turned against us.

When you read yet another report of a multimillion-dollar bank theft, yet another million usernames and passwords leaked on the web, or yet another scam milking millions from vulnerable people – what you are reading about is the lack of cybersecurity: a failure to protect systems, processes, or data and thereby enabling exploitation. Sometimes the end result is just an embarrassment for a company or

individual; at other times it can cause significant financial or operational harm. At its worst, loss of life can be a result.

Cybersecurity, then, is not optional. As our world transitions more products and services online, and we in turn depend on them, protecting this technological infrastructure has become a fundamental building block for information systems globally. It must underpin every technology, every gadget, every application, and anywhere data is stored.

To help understand the risks, this document will explore the threats Australia faces in this digital age: to our economy, our sovereignty, and ultimately, our way of life.

It will also cover the opportunities as a burgeoning industry – one that is projected to be worth \$US639

billion¹ globally in the next seven years alone – and the possibility for Australia to establish itself as a leader, pioneering new technologies and exporting cybersecurity products to the rest of the world.

We are more than just the lucky country. We are early adopters. We are tenacious innovators. We are a nation with the skills and talent to lead the world in cybersecurity – and with the right mix of leadership and commitment from government, industry, and academia, we can make it happen.

What part will you play?

46%
OF THE WORLD'S
POPULATION
IS CONNECTED
TO THE
INTERNET

What is cybersecurity?

As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain.

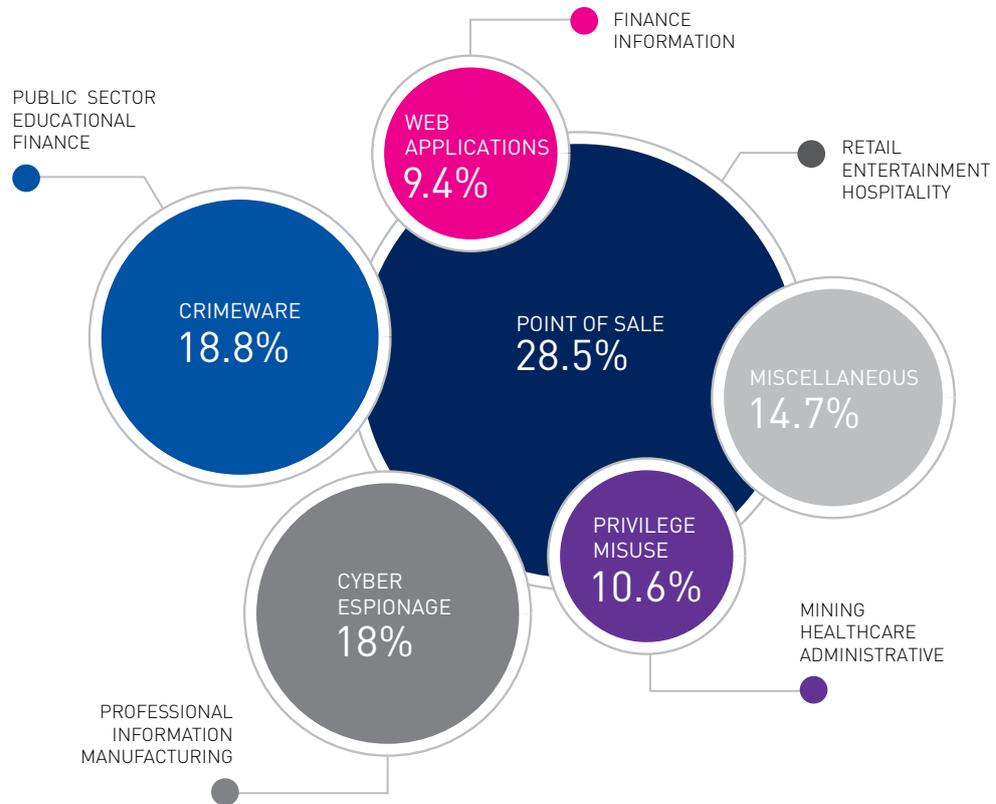
Despite the threat of viruses and malware almost since the dawn of computing, awareness of the security and sanctity of data with computer systems didn't gain traction until the explosive growth of the internet, whereby the exposure of so many machines on the web provided a veritable playground for hackers to test their skills – bringing down websites, stealing data, or committing fraud. It's something we now call **cybercrime**.

Since then, and with internet penetration globally at an estimated 3.4 billion users (approximately 46% of the world's population²), the

THREAT VECTORS BY INDUSTRY

The vectors by which industries are compromised.

Source: Verizon 2015 Data Breach Investigations Report



opportunities for cybercrime have ballooned exponentially.

Combating this is a multi-disciplinary affair that spans hardware and software through to policy and people – all of it aimed at both preventing cybercrime occurring in the first place, or minimising its impact when it does. This is the practice of **cybersecurity**.

There is no silver bullet, however; cybersecurity is a constantly evolving, constantly active process just like the threats it aims to prevent.

What happens when security fails? While what frequently makes the news are breaches of user accounts and the publication of names and passwords – the type that the Ashley Madison hack publicly exemplified – it's often financial gain, or the theft

of critical business or government intelligence, that drives the cyber underworld.

One fact remains clear: it's only going to increase. As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defences we employ to stop them through the education and practice of cybersecurity.

The increasing prevalence and severity of malicious cyber-enabled activities... constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat.

Barack Obama,
President of the United States, 2015³



LAST TO KNOW

MORE THAN
90%
OF BREACHES
ARE DISCOVERED
BY EXTERNAL
PARTIES



WHAT'S THE PASSWORD?

63%
OF BREACHES ARE
CAUSED BY WEAK,
DEFAULT, OR STOLEN
PASSWORDS

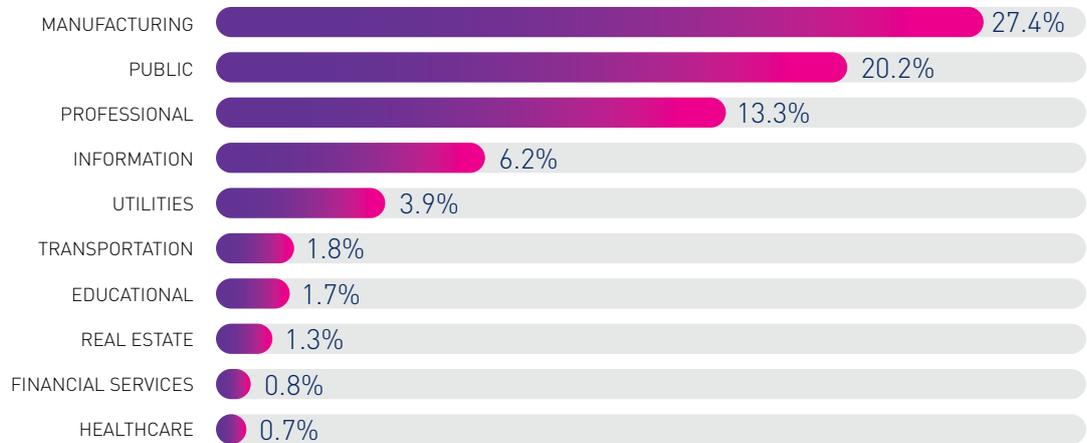
EASY HACKS, EASY BREACHES

Source: Verizon 2016 Data Breach Investigations Report

TOP 10 ESPIONAGE TARGETED INDUSTRIES

The most targeted industries in 2015.

Source: Verizon 2015 Data Breach Investigations Report



AND THE WEAKEST LINK IS...

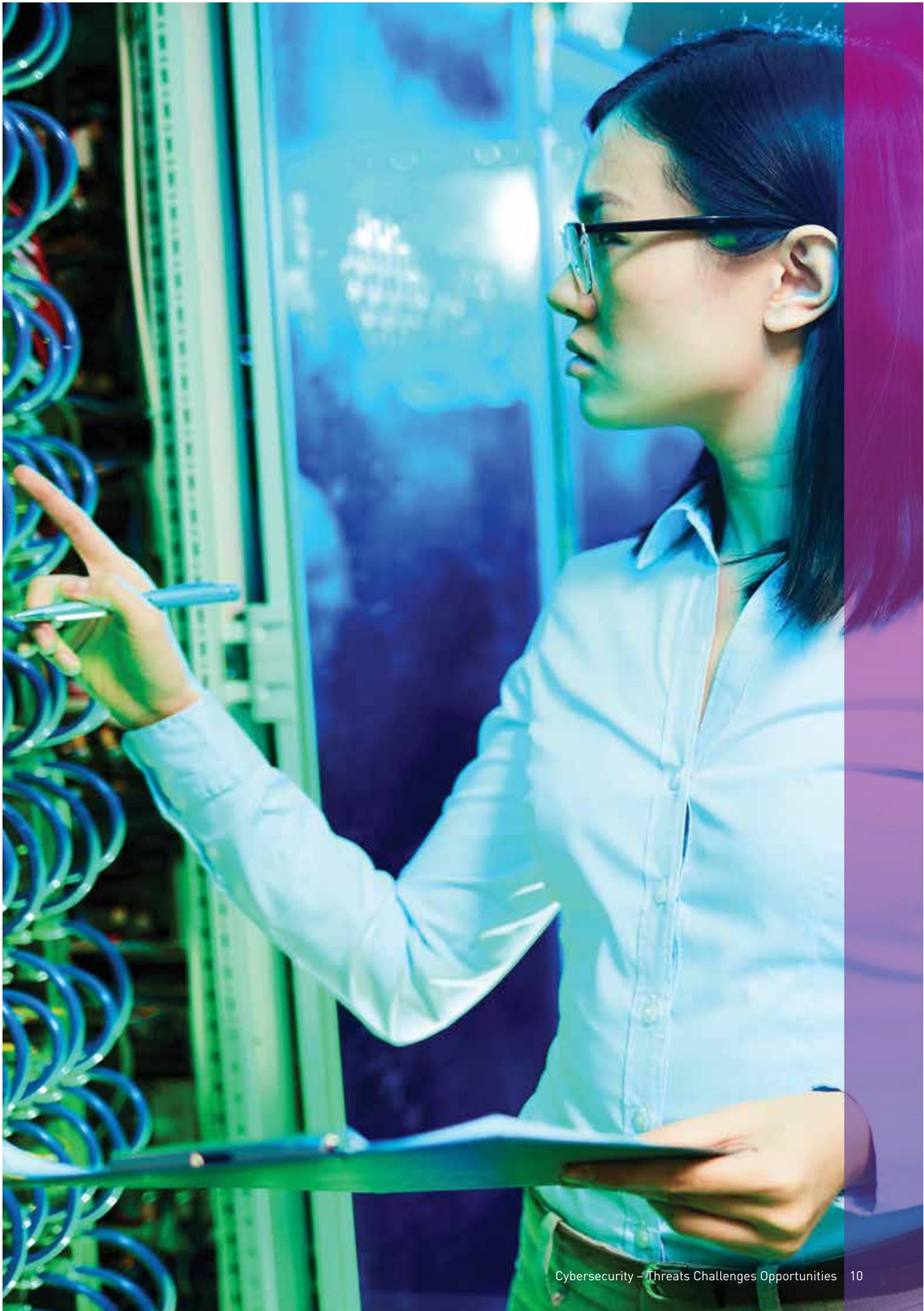
Humans are inherently complex and multi-faceted creatures with our own agendas, influences, faults, beliefs, and priorities.

Sometimes we're also simply just too trusting.

Even the most hardened system can be breached through **social engineering** – the 'hacking' of people. No amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link, or being convinced to give up login details over the phone by someone pretending to be from the IT department.

In fact a recent study by researchers at the Friedrich-Alexander University of Erlangen-Nuremberg, Germany, revealed that just over 50% of people click on links in emails from strangers, **even when they were aware of the risks.**⁴

And so, as a result, cybersecurity isn't just about technological defences: it's also about people. From the home user through to industry and government, everyone needs a basic understanding of cyberthreats and how to recognise them – something which comes under the umbrella of **digital literacy**.



A world without cybersecurity

One the most damaging targets for a society embroiled in cyberwarfare is infrastructure.

Our reliance on automation focuses single points of failure that can have dramatic consequences if directed at power stations, communication networks, transport and other utilities.



93% OF CASES HACKERS TOOK JUST MINUTES TO BREACH WHILE COMPANIES TOOK WEEKS OR MONTHS TO DISCOVER



SHOW ME THE MONEY 95% OF WEB ATTACKS ARE FINANCIALLY MOTIVATED



EMPLOYEE MISTAKES LOST ASSETS 100x TIMES MORE PREVALENT THAN THEFT



NEARLY 30% OPEN PHISHING EMAILS 12% DO CLICK THE LINK OR OPEN ATTACHED FILES

SIMPLE MISTAKES, COSTLY LOSSES

Source: Verizon 2016 Data Breach Investigations Report

By way of example, and to draw from the emerging technology of driverless cars gaining popularity now, is the following example of what might happen if we continue to create products and services without cybersecurity in mind:

Thirty years from now our society runs on automated cars, buses and trains. Planes still require human authority – for now – and drones line the sky. On the one hand, this advance in technology has brought much greater efficiency: traffic jams eliminated, pollution lowered, cheaper cost of transport and more. It's a golden age.

Then a cyberattack compromises the central network. The systems that co-ordinate all transport shut down, bringing the city of Sydney – now 7 million people – to an abrupt halt.

No cars, no buses, no trains.

Workers can't get to and from work, and productivity stops. Life-saving medicine doesn't arrive and people die. Essential services begin to fail, and chaos ensues. The economic and social fallout is immense: a city held hostage by an external force – be it

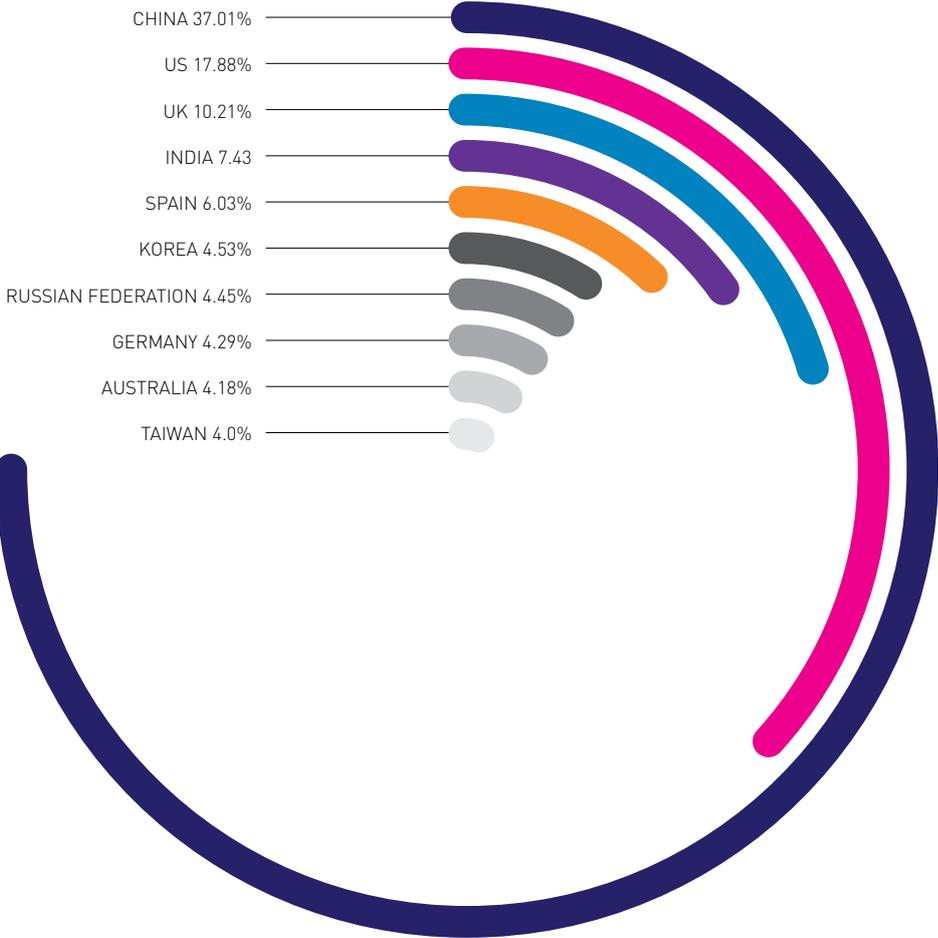
terrorist, criminal, or foreign power. Australia invaded without the invader ever stepping on our shores.

It's a stark example, but it demonstrates the Achilles heel the inter-connected society that we are heading for right now, and the reason cybersecurity must be part of all technology from the outset.

Consider this: the internet has enabled entirely new business models that have already shaped our planet. But the Googles and Facebooks and Amazons of this world are not the most profitable organisations that conduct business over the internet today – that crown belongs to cybercrime. It speaks volumes that the most lucrative business on the internet today is fraud.⁹

Q2 2015 saw one of the highest packet rate attacks recorded... which peaked at 214 million packets per second (Mpps). That volume is capable of taking out Tier 1 routers, such as those used by Internet service providers (ISPs).

Akamai, State of the Internet Q2 2015 Report¹⁰



TOP 10 SOURCE COUNTRIES FOR DDOS ATTACKS, Q2 2015

Top sources of mitigated DDoS attacks on Akamai's network.
Source: Akamai State of the Internet Report, Q2 2015

Threats in the information age

Every minute, we are seeing about half a million attack attempts that are happening in cyberspace.

Derek Manky,
Fortinet Global Security Strategist⁵



500,000 ATTACKS
AGAINST FORTINET
EVERY MINUTE

Thousand

To understand just how technology becomes vulnerable to cybercrime, it helps to first understand the nature of threats and how they exploit technological systems.

You might first ask why technology is vulnerable at all, and the answer is simple: trust. From its inception, the protocols that drive Internet, by and large, were not designed for a future that involved exploitation – there was little expectation at its birth that we might need to one day mitigate against attacks such as a **distributed denial of service** (DDoS), or that a webcam you buy off the shelf might need security protocols to prevent it being hacked and used to spy on you.

There is much greater awareness today, but even so you can still buy devices that connect to the internet that have poor security measures or no security at all built-in, because up until recently this simply wasn't part of the design scope. In many cases, the idea that a device might be used

for nefarious purposes isn't even considered.

And the result is that today cybercrime almost exclusively leverages the lack of security-focused design in everything from your smartphone and web browser through to your credit card and even the electronic systems in your car.

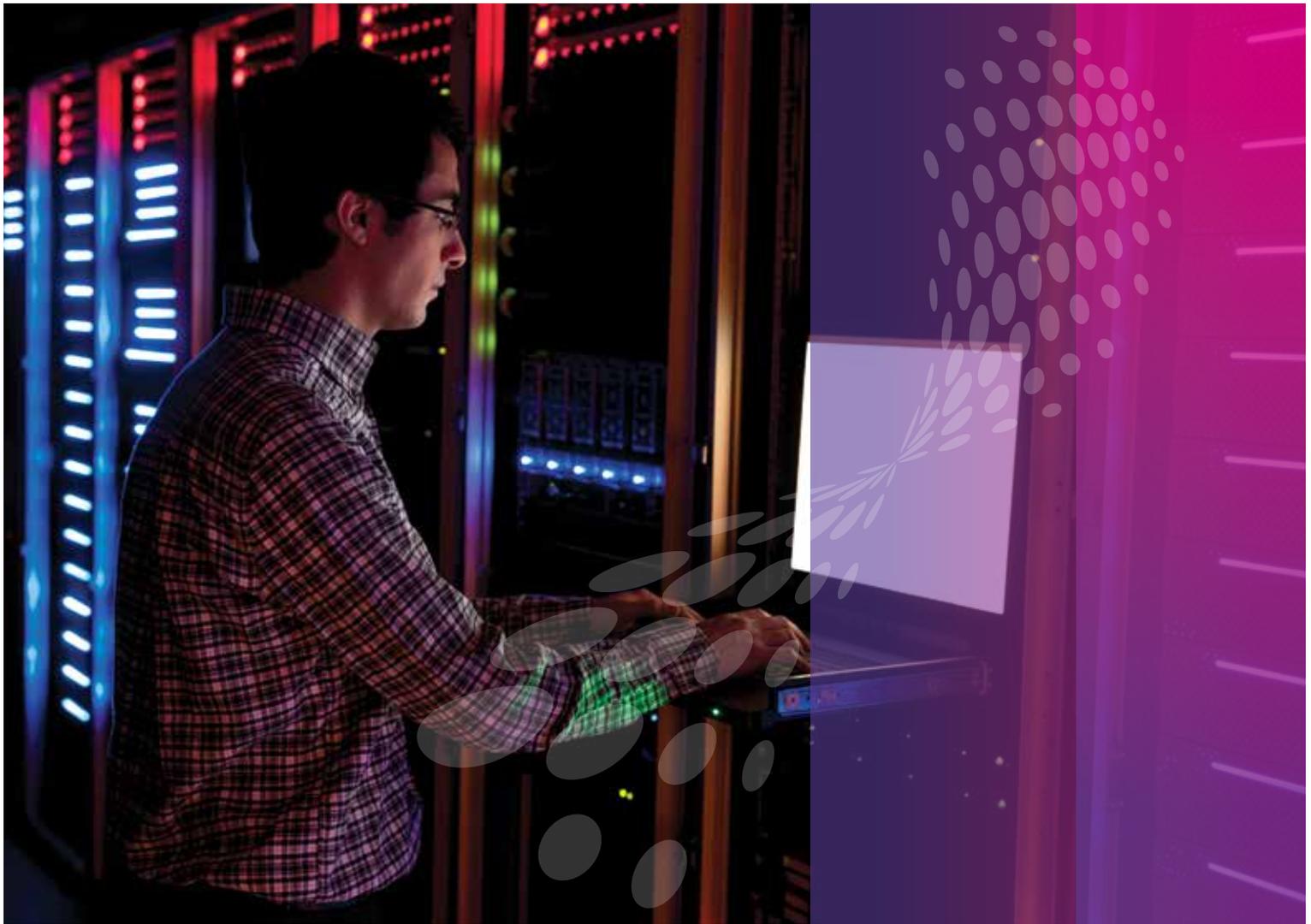
The nature of threats

Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransomware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers).

It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what's known as the **attack surface**: the size of the vulnerability presented

by hardware and software. That is, if a hacking exploit works on Apple iPhones for example, and everyone in your organisation has one, then by definition the attack surface could range in the dozens to the thousands depending on the size of your company. Or, looking at it another way, if anyone with an iPhone is vulnerable, the attack surface worldwide totals in the hundreds of millions.

This is further compounded by the fact that hardware and software may provide multiple vectors for attacks, such that – and using the above example again – an iPhone might have multiple different vulnerabilities, each of them a possibility for exploitation. In some cases, multiple exploits can be used in tandem to hack a device, as the FBI recently demonstrated when it gained access to the San Bernardino shooter's iPhone (yes, the good guys can hack you, too...)



There were 19 distributed denial-of-service (DDoS) attacks that exceeded 100 Gbps during the first three months of the year, almost four times more than in the previous quarter. In some cases attackers don't even have to deliver on their threats. Researchers from CloudFlare reported that an extortion group earned \$100,000 without ever launching a single DDoS attack.

Lucien Constantin,
Network World, 2016²⁸

03

And this is to say nothing of embedded systems the type that of which power our infrastructure including transport, electricity, and communications. Here, attacks are often more targeted – even down to specific to systems in a particular plant – but the repercussions are also considerably more dangerous. Shutting down an electrical grid, for example, can have life-threatening consequences.

What you also don't see – because it's hidden in the millions of fibre-optic networks and routers that form the internet – is that attacks are happening constantly all around the world, even as you read this. Your modem at home that gives you access to the internet is constantly fending off queries to see if your IP address has any open ports (the virtual addresses that allow software to communicate to and from your computers and network).

According to network security and services company Fortinet, 500,000 attacks occur against its networks every minute⁵. And that's just one service provider.

The bottom line is this: almost anything controllable by technology will have a weak spot. In the past year we've seen everything from cars ("Hackers remotely kill jeep on highway"⁶) to medical devices ("Hackers can send fatal dose to drug pumps"⁷) to toys ("Hackers hijack Hello Barbie Wi-Fi to spy on children"⁸) succumb to anyone with a little knowledge, time, and opportunity.

To appreciate the scope of the challenge that lies ahead – the new types of threats that we are starting to see emerge now – and thus the importance of cybersecurity for the government, industry, and the individual, the following section delves into our predictions of where cybercrime is heading, and the type of attacks we can expect to see.

The Internet of Things (IoT)

For \$6 in Bitcoin, I can rent time on a DDoS tool and bring down most websites. Better yet, if I send just the right type of packet to their web servers, I can crash the site for free.

A Thief's Perspective (interview), Intel Security, 2015¹⁸

Perhaps the most recognised buzzword of the moment, the Internet of Things (IoT) encompasses the many and varied devices currently on the market, or soon to be on the market, that will connect to and stay connected to the internet 24/7.

Typically this includes products like webcams, smart TVs, and even the much touted internet-connected fridges. But IoT actually encompasses a broad range of products most of which you won't actually see – electronics, sensors, actuators and software soon to be built into everything from your car to your home: technology to unlock your door and turn on the lights when you arrive home; technology to allow cars to talk to other cars and traffic lights to prevent accidents; technology to let entire cities regulate air-quality, manage energy distribution, and regulate water supply all in real-time from thousands of buildings, each with thousands of sensors, all communicating through a city-wide network.

Sound like fantasy? There is already a development in the UK by River Clyde Homes and the Hypercat Consortium to build a Smart Neighbourhood in Scotland by installing hundreds of IoT devices to monitor everything from temperature and local weather through to carbon monoxide levels, potential gas leaks, lift maintenance, smoke detection and communal lighting to name a few. All of these talk to each other to provide an overall real-time knowledge base for the operating of neighbourhood services, and to minimise health and safety risks.

But this is just the beginning. IoT has the potential to encompass a lot more – heart monitoring implants, pathogen monitoring for food, transponders for animals on farms, environmental waste monitoring, field devices for police to detect threats, feedback sensors for firefighters in search and rescue and much, much more.

Perhaps the best way to imagine IoT is – and to borrow a phrase from a research paper at the Social Science Research Network – is to think of IoT as an “inextricable mixture of hardware, software, data and service”¹¹. Which of course is to say that the potential is close to limitless.

According to the CEO of Cisco, Chuck Robbins, the IoT industry is expected to be worth \$US19 trillion globally by 2020¹². Closer to home, Frost & Sullivan is tipping the Australian market for IoT – just in terms of home devices, such as in security or energy management – to be worth \$200M by 2020.¹³

Taken together, this means is that in the near future just about everything you use, and everywhere you go, devices will be hooked up to each other communicating, sharing data, and enabling a future that once was the realm of science-fiction. The potential boon for society is immense, but so too are the risks.

As barriers to entry drop we will see an uptake of IoT, creating a future where attack vectors are everywhere.

Source: IoT Alliance Australia



Considerably more devices will be connected to each other and the internet: Intel predicts there will be as many as 200 billion devices by 2020.¹⁴

And if you remember our primer at the start of this document, that is one very large, very vulnerable attack surface. It should go without saying that the threat potential from IoT is beyond vast, and therefore cybersecurity practices must form part of IoT development from the ground up. For example, car manufacturers need to build security protocols into the sensors in smart cars to ensure they can't be turned against the driver to cause injury or death. Something which, unfortunately, is currently not the case (see next section, **Autonomous systems**).

Although a successful attack on industrial IoT devices with an installed base of hundreds of millions would likely cause havoc, one device at a key point in a critical infrastructure control system could be far more devastating.

McAfee Labs 2016
Threats Predictions¹⁵

Botnet armies

Somewhat related are botnets. A bot (sometimes called a 'zombie') is a remotely-controlled and compromised – unbeknownst to the owner – computing device that's connected to the internet. This could be a desktop computer or a laptop, but it can also be a webcam, a modem, or a Wi-Fi router, all of which almost everyone has in their home today. Unfortunately, again, poor security design sees devices like these come with only basic security that can be easily bypassed, allowing cybercriminals to install malware and control the device remotely.

Collect enough bots and you have a botnet, and with a botnet you can launch a distributed denial-of-service (DDoS) attack. In large enough numbers, such an attack can take down websites and knock services offline – something we saw first-hand earlier this year when the Australian Bureau of Statistics eCensus website was very publicly attacked.

This is to say nothing of what happens when IoT devices take part in a DDoS, which we know they already do. In fact, the world's largest DDoS occurred in August of this year knocking out French internet service provider OVH, suffering an attack that transmitted a record-breaking 1Tbps¹⁷. To put this into perspective, a 1Gbps attack is sufficient to knock most businesses anywhere in the world offline, and this attack was 1000 times stronger. It was only earlier in 2016 that the previous record came in at 579GBps. That is, we have already seen almost a doubling of capability in less than a year, and at a volume so high that very few very large players –

the Googles and Akamais of this world – are able to withstand.

Analysis of the attack on OVH revealed it consisted of some 145,000 devices, the majority of which belonged to internet-connected CCTV cameras and DVRs (digital video recorders) typically used in business and home surveillance.

Such products make ideal bots because their limited functionality provides less scope for security software; they're often headless, meaning a user doesn't have a display or other means to interact with them to monitor activity. They almost always come with a default administrator password that nobody changes because it requires effort and a bit of technical know-how – allowing cybercriminals to walk through the front door and take it over.

This is a great example of how lack of security design enables cybercrime – who would think to hack a CCTV? But that's the line of thinking that engenders security flaws. And once a flaw is out there, it often can't be fixed: the cost of updating the devices could be ruinous for a company if they need to be recalled, as not every device supports the ability to be updated remotely.

Prevention, then, is better than cure.

Recently, cybercriminal botnet operators have moved to self-sustaining botnets that continually find new devices to infect and add to the flock, even while others may be taken offline¹⁶. This has led to cybercriminals to sub-lease access to their botnets on the cheap, meaning anyone with a grudge and \$50 can bring down a website.

TABLETS



2015 – 248 MILLION



2019 – 269 MILLION

WEARABLE DEVICES



2015 – 200 MILLION



2019 – 780 MILLION



IOT DEVICES



2015 – 15 BILLION



2020 – 200 BILLION

GLOBAL PUBLIC CLOUD MARKET SIZE



2015 – \$97 BILLION



2020 – \$159 BILLION

MORE DEVICES, MORE THREATS

The growth in user-centric mobile and IoT devices will see greater exploitation of personal data.

Source: McAfee 2016 Threats Predictions

WHEN SECURITY IS AN AFTERTHOUGHT

One of the most potent botnets to date is **Lizardstresser**, by the infamous Lizard Squad DDoS group. In 2015 the group released the source code, allowing others to make their own. This has resulted in copy-cat groups and a stark increase in botnets-for-hire.

Lizardstresser relies on cheap IoT hardware to build large botnet armies, using shell scripts (simple text-based scripted programs) to scan IP ranges and to attempt access using hardcoded usernames

and passwords (usually all related to administrator logins).

It's so successful because many IoT devices are manufactured with the same default login credentials. Additionally, these same devices are also often simply plugged in and turned on, and have unfettered access to the internet through whatever corporate or home networks they are connected to. This makes them easy targets to enslave into botnets.¹⁹

Attacks on automobile systems will increase rapidly in 2016 due to the rapid increase in connected automobile hardware built without foundational security principles.

McAfee Labs 2016
Threats Predictions¹⁵

Autonomous systems

As technology continues to permeate our lives, we move from operating technology to integrating with it. This is especially true of autonomous systems that are by definition designed to blend in with our society, becoming second nature.

By the same token however, reliance on such systems makes the outcome of their abuse potentially more damaging. Typically, these technologies also integrate into critical infrastructure, such as payment systems and – in the case of autonomous cars – the transport network, making protecting them from a cybercrime a pivotal focus for cybersecurity.

Driverless cars and transport

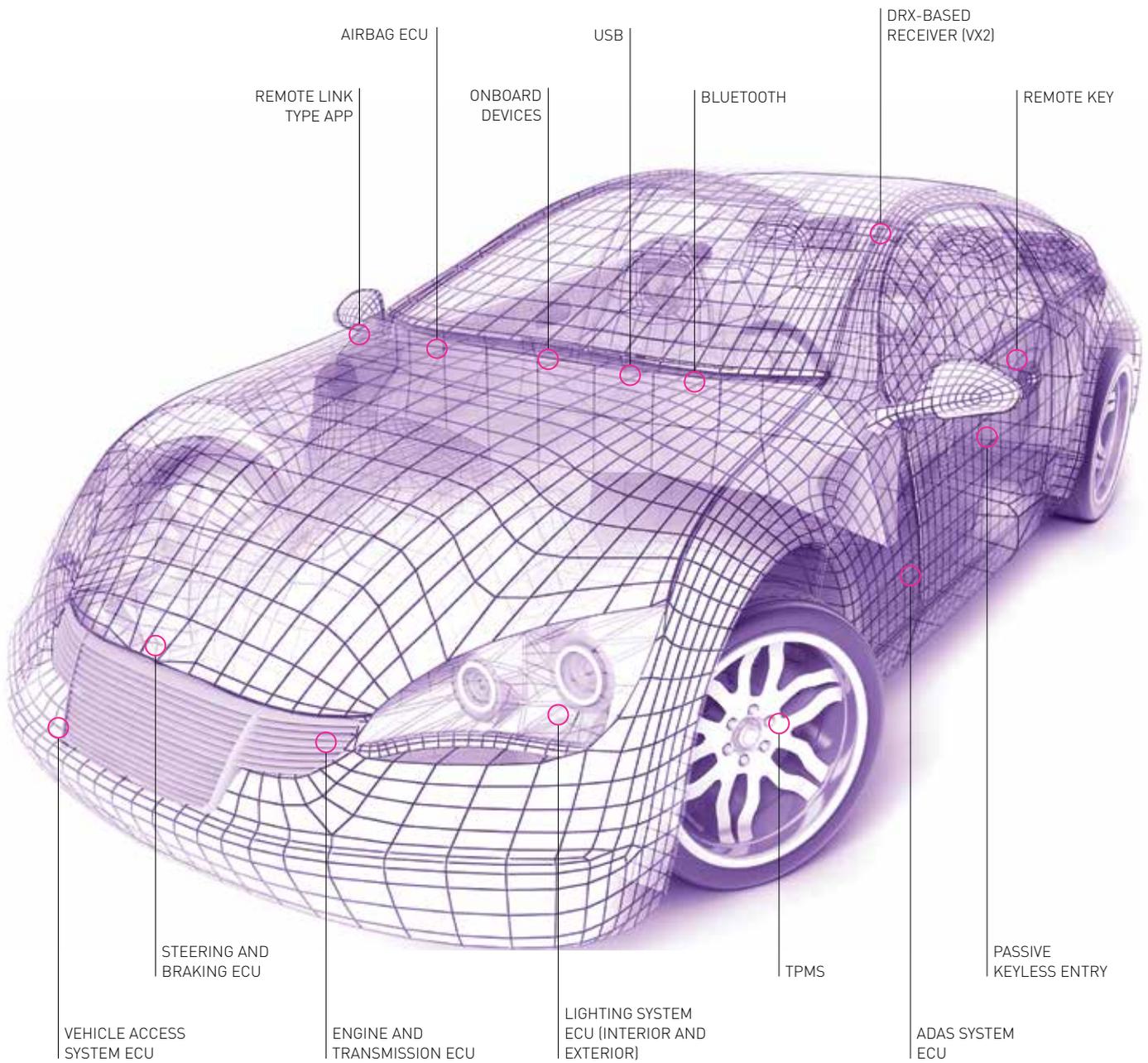
At the moment, driverless cars are stealing the limelight of autonomous systems. While so far there have been no documented cases of wilful misuse, it's already been demonstrated that autonomous cars can be remotely controlled.

In 2015, 1.4 million Jeep Cherokees were recalled after hackers demonstrated that the cars could be taken over remotely through the entertainment system.⁶

Similar abuse of access has also been demonstrated with cars from Mercedes, BMW, Toyota, Audi and Fiat – all due to poor security in the design process.^{20 21 22}

It's not hard to see that in the wrong hands such abuse could result in cars being used as weapons to maim or kill pedestrians – or even the occupants themselves – on the road. According to Business Insider in its Connected-Car Report, there will be 220 million autonomous cars on the road by 2020.²³

McAfee's 2016 Threats Predictions Report notes that "poorly secured driverless cars and smart highways will further expose drivers and passengers in 2017 and beyond, likely resulting in lost lives...", and that "recent vehicle hacks are a great example... selectively modifying communications and commands so they can take control or affect what the vehicle does. This has a potentially terrifying result."¹⁵



THE ATTACK SURFACE OF A MODERN CAR

Many car systems have not been designed with security in mind, making it possible to hack into a car via smartphone or laptop.
 Source: McAfee 2016 Threats Predictions



BIRTH AND REBIRTH OF A DATA BREACH

An example of how one breach can lead to another (in this case, harvesting payment data of consumers after first breaching a POS vendor).

Source: Verizon 2016 Data Breach Investigations Report

They'd been inside our network for a long period, about two years. And the way it was described to us was they're so deep inside our network it's like we had someone sitting over our shoulder for anything we did.

Daryl Peter, IT Manager,
NewSat 2012-2014⁸⁵

ATMs and Point of Sale

Credit cards have long been the target of fraudsters, spurring the development of RFID chips and other protective technology in the banking ecosystem. However, security is an arms race and threats such as skimming is now a global phenomenon that allows data from cards to be read and transmitted wirelessly in real time from ATM machines and point of sale devices.

Indeed, point of sale systems as a whole are their own a sub-category of cybercrime infiltration, being the weakest point of the payment

processing system, and so it's not uncommon to find malware specifically designed to pull data from embedded systems in POS terminals (see 'Birth and re-birth of a data breach' diagram, above.)

Now, of course, the technology has progressed further with contactless pay systems from the likes of Apple (Apple Pay) and Google (Android Pay), as well as players like Samsung (Samsung Pay, of course) that allow consumers to pay simply by waving their smartphone over a device – which presents yet another attack surface for cybercrime.



WHAT ABOUT WEARABLES?

Wearables are rapidly gaining popularity with smartwatches such as the Apple Watch and Samsung Gear, as well as exercise wearables like those from FitBit and Jawbone. According to ABI Research, an estimated 780 million wearable devices will be in circulation by 2019.

Now you might be wondering just what would be so bad about hacking a fitness wearable? This is exactly the line of thinking that allows cybercrime to occur.

Wearables are tracking all sorts of personal information including GPS location, blood pressure, heart rate, and anything else you feed them such as weight or diet. Such personally identifiable information could be used as a base to target you for spear-phishing, or aid in identity theft. But the real opportunity is these devices linking to your smartphone, where phone numbers, more personally identifiable information, emails, web logins etc. could theoretically be compromised.



Cyberwarfare

Most modern countries now are treating cyberspace as another military domain, in addition to land, air and sea.

Dmitri Alperovitch, Cybersecurity industry executive²⁵

Once the domain of science fiction, cyberwarfare is now very real, with most superpowers now having dedicated cyberwarfare divisions of the military. And while there have been few known, co-ordinated cyberattacks on physical targets, we don't need a crystal ball to predict the future: they will only increase.

It's telling that we are now in an age where governments, political groups, criminals and corporations can engage in cyberespionage, cyberwarfare, and cyberterrorism. The Prime Minister, Malcolm Turnbull, announced at the Australia-US Cyber Security Dialogue in September that Australia is well equipped to both defend against and carry out cyber-operations.

We now live in a world where warfare can be conducted entirely virtually – though the consequences will almost always have repercussions in the physical world.

Automated attacks

Much of what we talk about with regards to 'hacking' is a function of people at keyboards finding and abusing weak links in security. It is a skilled and time-consuming process.

However, in the ever-evolving arms race between subversive elements and cybersecurity, a move to automating such attacks would have clear benefits: whereas exfiltration may have taken days by skilled personnel, automated attacks can reduce this to hours – infiltrating, searching for a payload, gobbling it

ENERGETIC BEAR

One of the more well-known nation-state sponsored tools of cyberwarfare currently active is Energetic Bear. First uncovered in 2012, and believed to be sponsored by Russia, Energetic Bear used the Havex Trojan to gain access to company networks, particularly those in the energy sector, though it has also been found

in manufacturing, construction, health care and defence companies.

Primarily designed for cyberespionage, when the threat was first mapped in 2014 by security firm Kaspersky Labs, it identified nearly 2,800 victims worldwide, affecting countries including the US, Spain, Japan and Germany.⁴⁴



Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years.

Critical Infrastructure Readiness Report, Aspen Institute and Intel Security, 2015²⁵

up, encrypting it, and sending it out over the network before the host machine's security personnel even knows what's happened.

The defence to which, of course, is to automate security to combat automated attacks – computer software fighting computer software, all without human intervention. And while this sounds like a sci-fi movie, the reality is it's already here – in August this year the world's first automated cyber-hacking contest was held at DARPA (Defence Advanced Research Projects Agency), which saw supercomputers battle it out for a \$2 million prize, the win going to a perhaps appropriately named machine called 'Mayhem'.⁴⁵

30,000

PEOPLE LOST
POWER WHEN
30 SUB-STATIONS
IN WESTERN
UKRAINE WERE
SHUT DOWN
VIA A REMOTE
ATTACK

Cyberattacks on infrastructure

As societies around the world depend ever more heavily on technology, the ability to shut down or destroy infrastructure, take control of machines and vehicles, and directly cause the loss of life has become a reality. To date, some of the more well-known examples of cyberattacks on infrastructure include:

- In 2008 when Russia sent tanks into Georgia, the attack coincided with a cyberattack on Georgian government computing infrastructure. This is thought to be one of the first land and cyber coordinated attacks.³⁹
- Also in 2008, Stuxnet – a computer worm purportedly jointly designed by the US and Israel – crippled

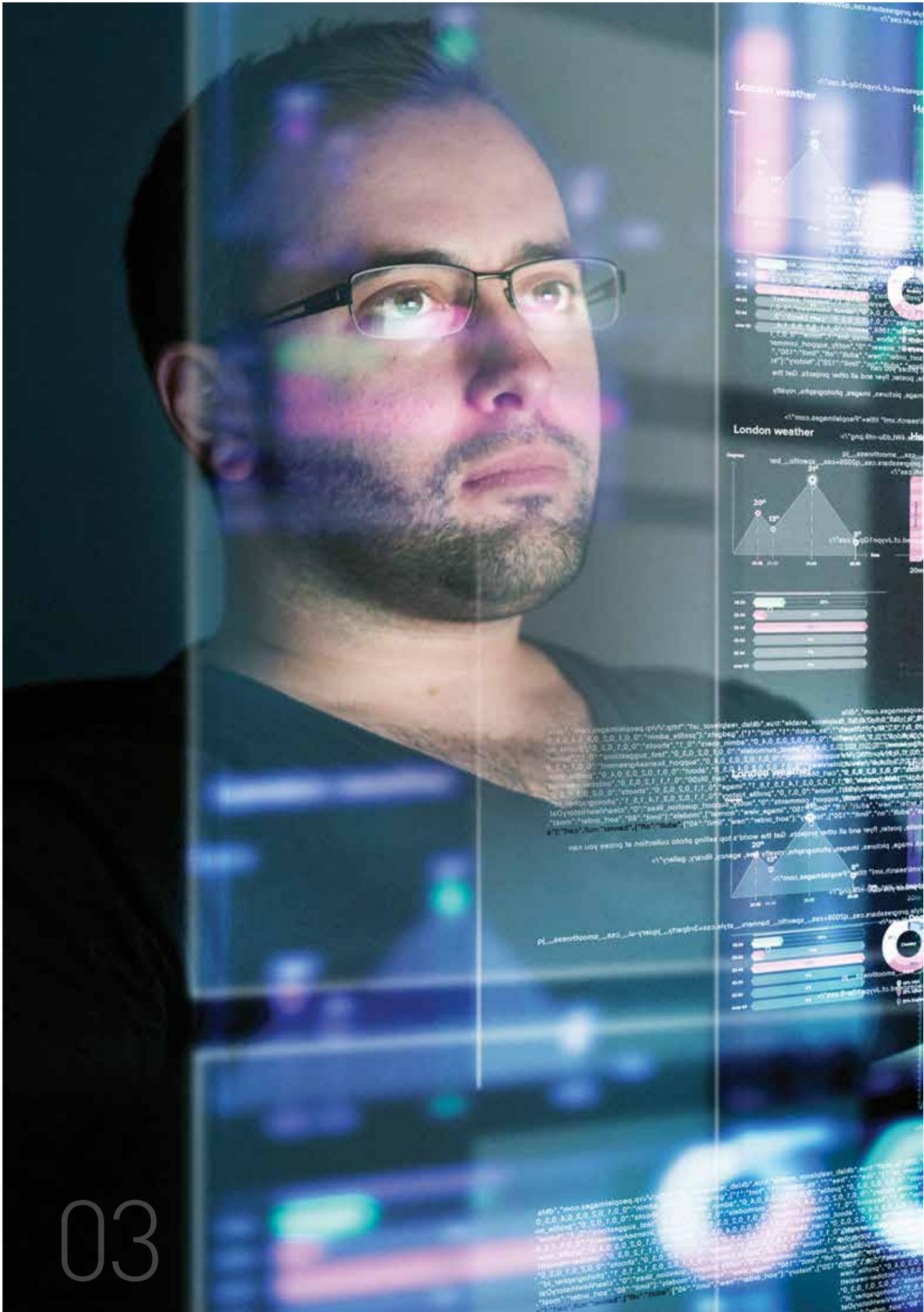
Iran's nuclear-enrichment program by sabotaging centrifuges.⁴⁰

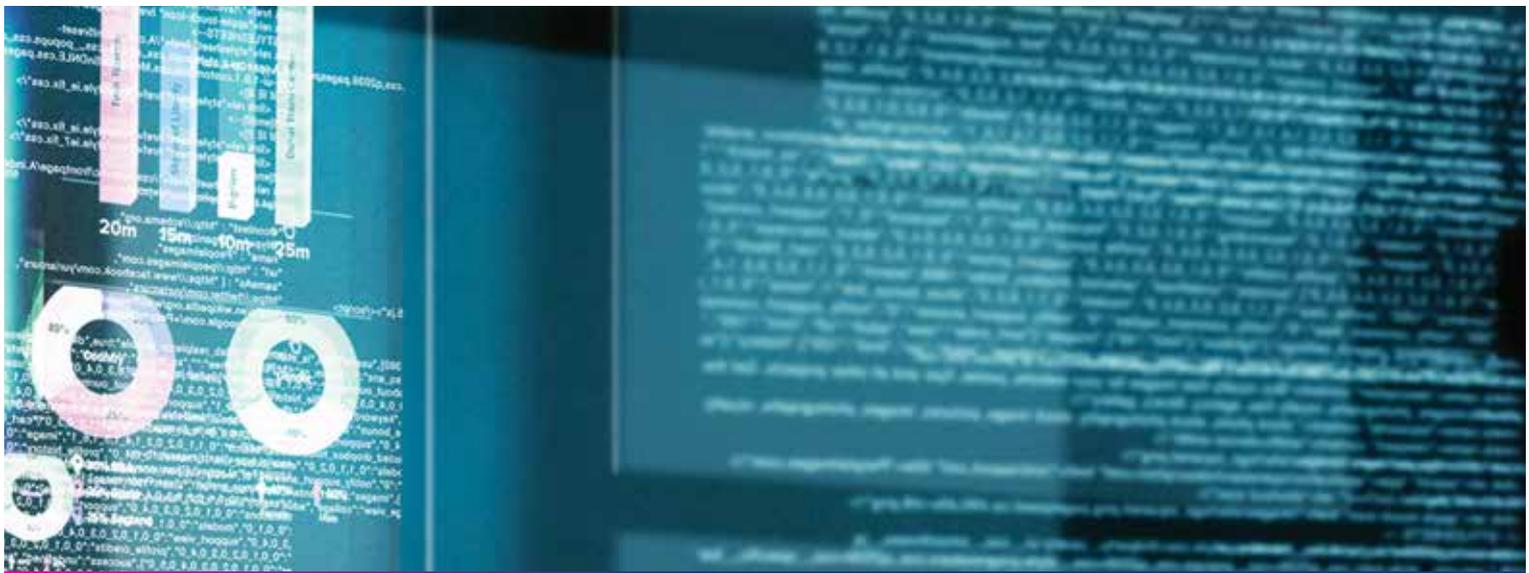
- In 2014 a German steelworks was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down.⁴¹
- In 2015, with an attack strongly suspected to have originated from Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack. Operators at the Prykarpattiaoblenergo control centre were even locked out of their systems during the attack and could only watch it unfold.⁴²

In all of these, and as an indication of how the landscape of war is changing, the weapon of choice for these attacks wasn't guns or bombs – it was a keyboard.

French Coldwell, Chief Evangelist at governance, risk, and compliance apps company Metricstream, at a cybersecurity summit earlier this year noted that "this is the canary in the coalmine. Much more of this will come."⁴³

We can expect governments around the world to strengthen their cyberattack and defence capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But here the results could be much more subtle – as noted in the McAfee 2016 Threats Predictions report, "they will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyberwarfare."¹⁵





America's top spies say the attacks that worry them don't involve the theft of data, but the direct manipulation of it, changing perceptions of what is real and what is not.

Patrick Tucker, Defense One²⁷

WHEN SOFTWARE KILLS

It's easy to forget that computers can have life-threatening consequences. Here are some well-known examples of what happens when technology fails due to small mistakes in computer code.

Therac 25

This is so well known that it's now taught in computer science curriculums. Therac 25 was a Canadian medical machine designed to help save lives by administering targeted doses of radiation to kill cancer. Instead, a rare software glitch saw patients receiving 100 times the necessary dose. In a period from 1985-1987 five patients died, while many others were seriously injured.²⁹

Patriot missile

During the Gulf War in 1991 a Patriot missile failed to intercept a Scud missile due to a software fault, resulting in the death of 28 US soldiers and injuring 100 others.³⁰

Toyota's ETCS

Toyota recalled 8 million vehicles worldwide starting in 2009 after faults with the Electronic Throttle Control System resulted in the death of 89 people.³¹

Tesla's autopilot

In July 2016 a man died while relying on the autopilot function of his Tesla Model S when it failed to detect a trailer, crashing into it.³²

These are examples of unintended software faults, but subtle manipulation of data could intentionally result in loss of life, and remain undetected until this occurs. Military officials in the US have even raised concerns that Chinese hackers known to have infiltrated defence contractors over the last decade could have already altered code for weapon systems, sitting dormant until the next major conflict.³³

Data manipulation

The biggest threats in cybersecurity today are around the large scale proliferation of targeted attacks – from breach and email distribution of socially engineered ransomware to potentially harmful attacks on critical infrastructure like energy networks.

Rodney Gedda,
Senior Analyst, Telsyte⁵³

Not all attacks are about theft or destruction. A more sinister cause is the manipulation of data in place – such that machines can be controlled – or the wrong information reported to human operators without their knowledge.

It's clear if a cybercriminal releases stolen usernames and passwords on the web. It's much less clear if data belonging to a business has been modified – with those who own the data none the wiser. As no destruction is caused such intrusions here can be harder to detect, if they're detected at all. Yet even the smallest alterations can have serious consequences and implications.

James Clapper, Director of US National Intelligence, said it succinctly when he stated, "Decision making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."²⁷

Backdoors and espionage

Backdoors are particularly concerning because they can be both hard to discover and provide unfettered access to a system or entire network.

A compromised system can provide cybercriminals or a nation-state the ability to spy on data, or alter the data in place. And for as long as a system is compromised, abuse of privilege will be ongoing.

By way of example, in 2015 Juniper Networks announced it had discovered multiple backdoors in its firewall operating system code installed with its products – the same products used to protect corporate and government systems around the world. These backdoors had been active for at least three years.

One of the backdoors gave remote control of the firewall to an outside user, while another disturbingly allowed for the decryption of traffic running through a Juniper Networks firewall, allowing traffic to be eavesdropped. The sophistication and nature of this breach points to a nation-state as the culprit.³⁴

Cloud concerns

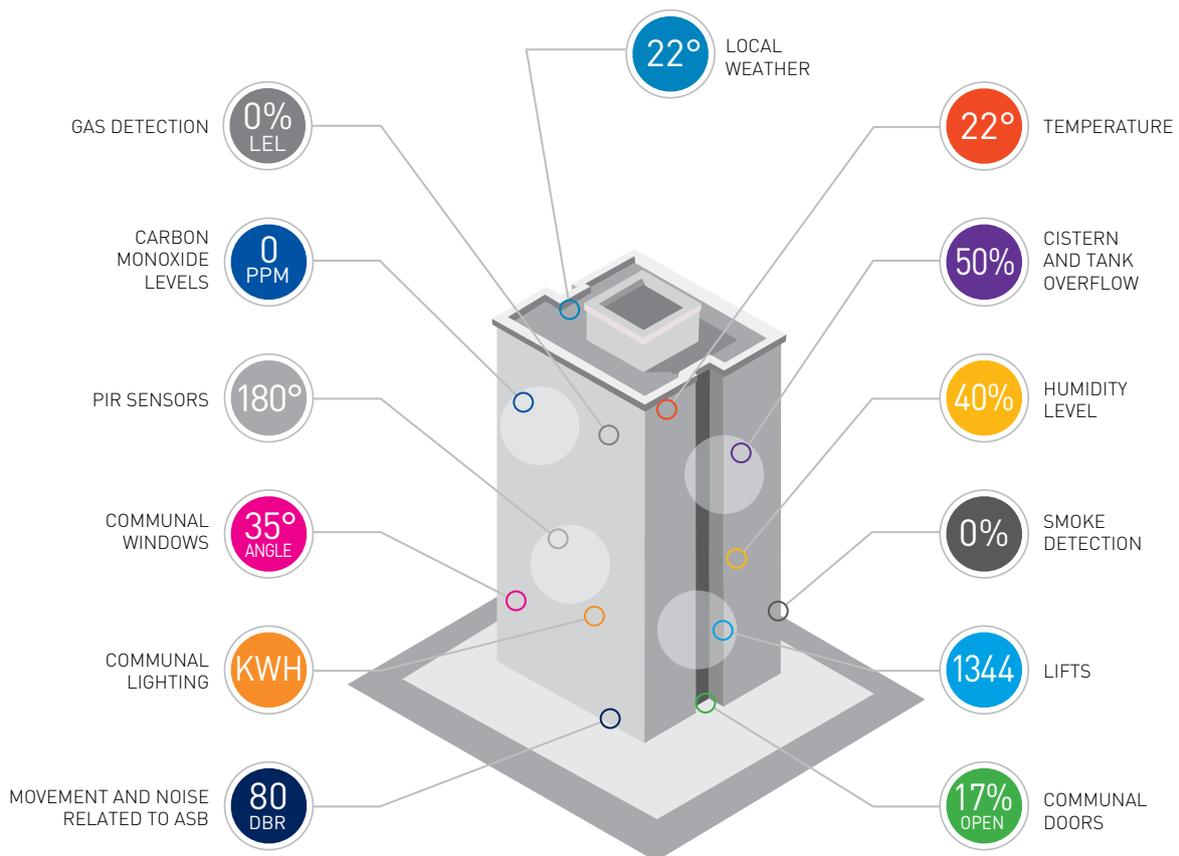
As with any successful technology, the more popular it becomes the larger a target it also becomes. Cloud is now well entrenched as a concept and a service offering, and indeed many businesses now rely on cloud services to operate.

On the one hand this can make security easier for companies outsourcing their data to lie on a cloud service where the cost of security is carried by the vendor, but on the other it centralises cloud services as highly viable targets for attack.

BLAST FROM THE PAST

Perhaps one of the more prominent examples of cyberwarfare – even before the internet became ubiquitous – comes from the cold war in 1982 when a Siberian oil pipeline exploded, creating at the time one of the largest non-nuclear explosions in history, so large

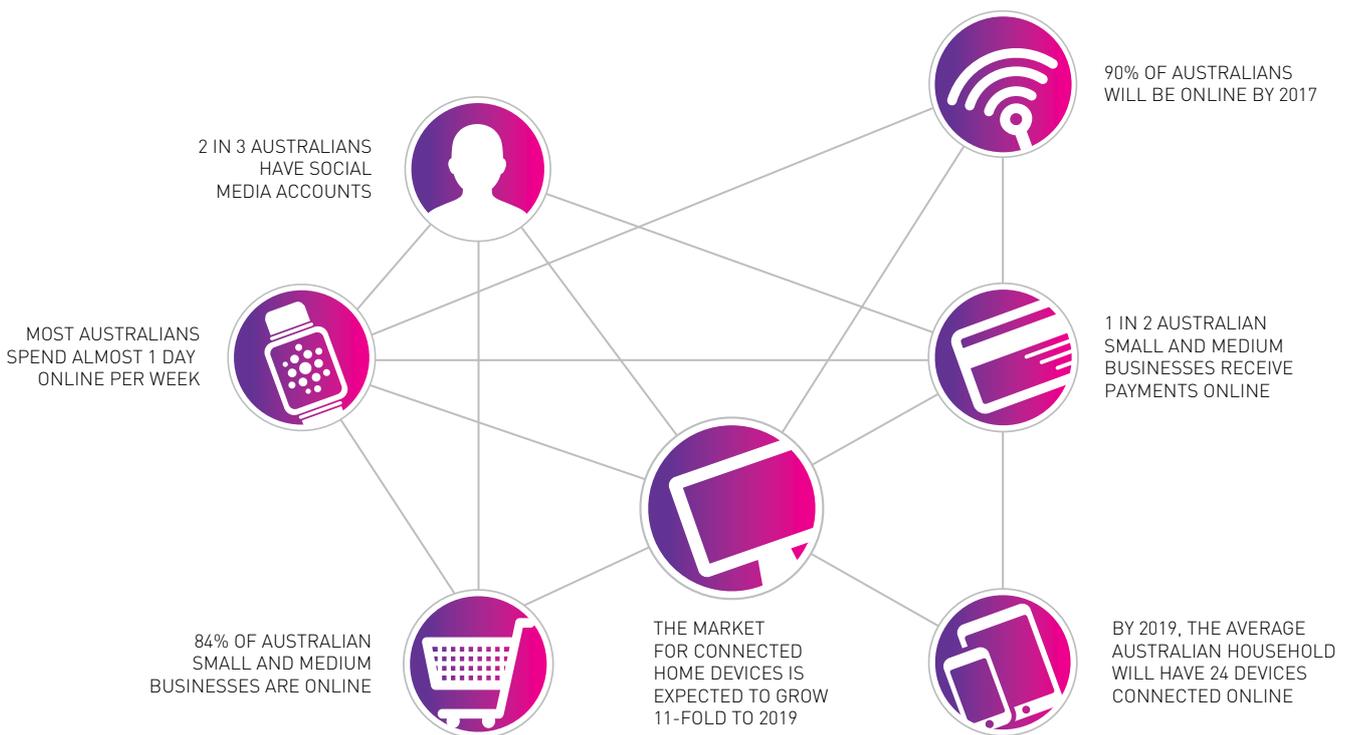
it was visible from space. Later the cause was revealed to be a Trojan horse implanted by the US in pipeline equipment sold from a Canadian company on to Russia. End result: economic sabotage facilitated by computer software.



SMART CITIES – BRITAIN'S NEIGHBOURHOOD@BROOMHILL PROJECT

A small sample of the types of IoT sensors in a smart city apartment block.

Source: IoT Alliance Australia



AUSTRALIANS ARE BECOMING INCREASINGLY CONNECTED ONLINE

As Australia becomes ever more connected, cybersecurity becomes ever more important. Source: Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy.

Nation-state cyberwarfare will become an equaliser, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s.

McAfee Labs 2016 Threats Predictions¹⁵

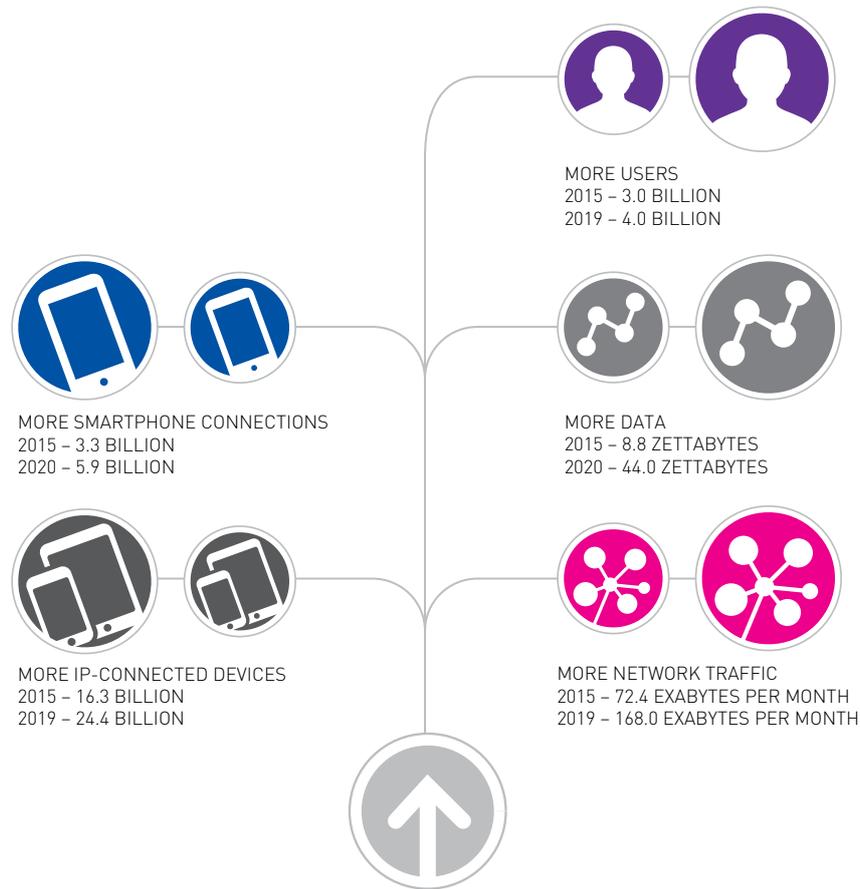
But there's also a less obvious concern here: sovereignty.

Security of cloud data is not just about encryption, but also the sovereignty of access when data is physically located in an overseas jurisdiction. The internet may have no borders, but data itself still lies within traditional real-world boundaries and in turn may be bound by the laws of a foreign nation.³⁵

Further, even if we trust in the laws of a foreign nation there's no guarantee they won't change, and data that was previously protected could be subpoenaed, accessed by government departments, or shared with third parties without consent.

A good example of how the landscape can change is the news earlier this year that in Russia, ISPs are now required to store both the metadata and content of communications, and hand over encryption keys for any encrypted data³⁶. Any cloud data passing through an ISP can become readable by Russia's government and intelligence services. This had the immediate fallout of some popular VPNs closing their Russian nodes, and in at least one known case³⁷ servers were seized from the VPN provider under this law.

With cloud expected to grow by around 18% through 2016³⁸, concerns around the sanctity and sovereignty of cloud data are only going to increase.



THE GROWING CYBERATTACK SURFACE

More devices, more users, more data – every year.
Source: McAfee 2016 Threats Predictions

Virtualised threats

As a result of the growth in cloud services, there has been an explosion in the use of virtual machines for business, making these prime targets for cybercrime.

Fortinet notes, “growing reliance on virtualisation and both private and hybrid clouds will make these kinds of attacks even more fruitful for cybercriminals.”⁵

And, as the McAfee’s 2016 Threats Predictions report notes, “how do you accurately track and attribute an attack, with all of the obfuscation possible with clouds and virtualisation?”¹⁵ It goes on to state, “if we keep our stuff in the cloud and access it from a phone, tablet, kiosk, automobile, or watch (all of which

run different operating systems and different applications), we have substantially broadened the attack surface.”

Indeed, the use of apps that rely on the cloud will also allow mobile devices running compromised apps as a way for hackers to remotely attack and breach public and private corporate networks.⁵

Finally, there’s one other consideration: cybercriminals can use cloud services themselves, providing powerful resources for processing power and storage, and the ability to appear and disappear at the click of a button.

Industry and the individual

Malware is still very popular and growing, but the past year has marked the beginnings of a significant shift toward new threats that are more difficult to detect, including file-less attacks, exploits of remote shell and remote control protocols, encrypted infiltrations, and credential theft.

McAfee Labs 2016
Threats Predictions¹⁵

While large security breaches make the news, the majority of cybercrime involves fraud targeting businesses and individuals. Here, a mixture of malware and social engineering can see financial fraud resulting in the loss of thousands, all the way up to millions, of dollars.

And, it's also some of the hardest crime to combat – largely due to the sheer scope of attack surfaces which can range from desktop computers through to laptops, tablets and smartphones.

Sometimes, the vector is simply a phone: using social engineering through an employee to gain access to a network, or con an individual out of money – as in the classic **technical support scam**, of which the Government has a great summary at www.scamwatch.gov.au (also a great site to learn about other online scams).

Ransomware and Cryptoware

The ease with which amateur cybercriminals can get their hands on tools to extort money is increasing. So far in 2016 we've seen a prevalence of cryptoware targeting both enterprise and individuals, requiring the payment of a ransom to unlock encrypted files.

The most well-known of these was Cryptolocker, said to have earned its creators \$US3 million before it was shut down by a consortium involving the US, the UK, and a number of security vendors and researchers.

While in an ideal world these ransoms would never be paid – and thus not

encourage extortion as a business model – with victims opting to restore data from backups instead, the reality is that this isn't always practical. This is especially true for companies, where the downtime or lost productivity from denied access to the data can be higher than the price of the ransom.

Recently, however, the ante was upped with the appearance of ransomware that claims to have encrypted files and asks for payment for the decryption key, but in fact the files have simply been deleted unbeknownst to the owner.⁴⁶ Known as **Ranscam**, the one upside to this change in tactics is that if it becomes the prevalent form of ransomware, it will destroy the trust – or what little there is – between the criminal and the victim that the data will be recoverable. No honour among thieves, it seems.

Multi-vector attacks

Taking advantage of multiple concurrent attack mechanisms, a single attacker may try to penetrate an organisation on multiple levels in order to access different data, such as targeting the CFO with social engineering, with the aim to secure financial information while using spear-phishing targeted at office staff to get malware installed.

Utilising the cumulative bandwidth available to these IOT devices, one group of threat actors has been able to launch attacks as large as 400Gbps.

Arbor Networks on LizardStresser¹⁹



THE WORLD WE LIVE IN

Facebook CEO, Mark Zuckerberg, has been observed in a promotional photo for Instagram with his laptop in the background sporting tape covering both the camera and the microphone – the implication being he doesn't trust his own machine is secure from cyberespionage.²⁴

If the CEO of one of the world's technology innovators can't necessarily trust his own computer, what does that mean for the rest of us?

One of the largest known (considering not all companies like to own up to having been scammed) scams to date resulted in the loss of €40 million from Leoni AG²⁴ in August of this year, facilitated by tricking a financial officer into transferring funds to the wrong account.

Importantly, success with one method can lead to exploitation of others, such as an employee clicking on a macro within an email which in turn downloads a program, which then automatically pulls down targeted malware to access network resources (this is sometimes known as 'weaponised email attachments').

The Aspen Institute's Critical Infrastructure Readiness Report notes "the analysis of this year's data led to an interesting new revelation – nearly 70% of attack victims are

targeted for the purpose of advancing a different attack against another victim. For instance, an attacker may hack a website to serve malware to visitors with the intentions of infecting its true target."²⁵

A common adage in cybersecurity is that while defence must consider every possible attack vector, attackers only need to find one weak point. An attack only needs to be successful once.

Identity theft

Identity theft is the crime no one thinks will happen to them until it does.

According to Javelin Strategy and Research, some \$US16 billion was stolen from 12.7 million consumers in the US alone during 2014 due to identity theft.²⁶

However, identity theft is more than just financial fraud, it's a central pillar for all manner of cybercrimes: once you can impersonate an individual, you can gain access to their accounts, commit multiple types of fraud in their name, steal information only they have access to, and much more.

As we share more of our lives online, we open ourselves to being exploited further. In McAfee's 2016 Threats Predictions report the authors note that "the growing value of personal data... is already more valuable than payment card information and will continue to climb."¹⁵

The future in our hands

Asia-Pacific is rapidly emerging as a potential market for cybersecurity solution providers, driven by emerging economies such as China, India and South-East Asian countries.

Cybersecurity Ventures⁴⁸

A large, stylized graphic of the number '639' with a dollar sign '\$' to its left. The characters are filled with a vertical gradient from purple at the top to bright pink at the bottom. The '6' is the largest, followed by the '3', and then the '9'. The dollar sign is also in the same gradient and is positioned to the left of the '6'.

Billions

ESTIMATED WORTH OF
THE CYBERSECURITY
INDUSTRY BY 2023

It should be clear by now that we live in a world reliant on technology, and that this technology can also be vulnerable if it's not designed with security in mind. While some products and services are, many more are not, and to this end the development of cybersecurity tools, skills, and education is essential to protecting both our infrastructure and way of life.

Globally, the industry is worth \$US106 billion with estimates projecting its value at \$US639 billion by 2023¹. As a nascent industry, there is a real opportunity for Australia to become a centre of cybersecurity excellence with the right leadership and investment.

Additionally, as cybersecurity must underpin the design of almost any technology product that comes to market, it goes without saying that if we don't develop our own cybersecurity products and services then we need to purchase them from overseas.

However, there is real value in producing cybersecurity products and services locally, not the least of which is control over the source code – ultimately, you must trust an overseas vendor that there are no backdoors or mechanisms in their software and firmware that would allow either exploitation by a foreign nation's government departments (such as intelligence agencies), or exploitation by cybercriminals discovering these vulnerabilities.

Particularly when it comes to national cyber defence, it would be preferable to utilise home-grown products. Not doing so is, in the words of Alex Scundurra, CEO of fintech hub Stone & Chalk, "like outsourcing our defence force to someone else."⁵⁶

Achieving any kind of growth for a local cybersecurity industry will require support of the government, private sector, and academia. We know that as we depend more and more on technology the demand for qualified cybersecurity specialists, products, and services is only going to increase – so it's in our best interests to work towards developing and harnessing our own cybersecurity sector.

THE 100% SECURE COMPUTER

When it comes to security you can never completely eliminate risk, you can only minimise and mitigate it – there is no such thing as the 100% secure system.

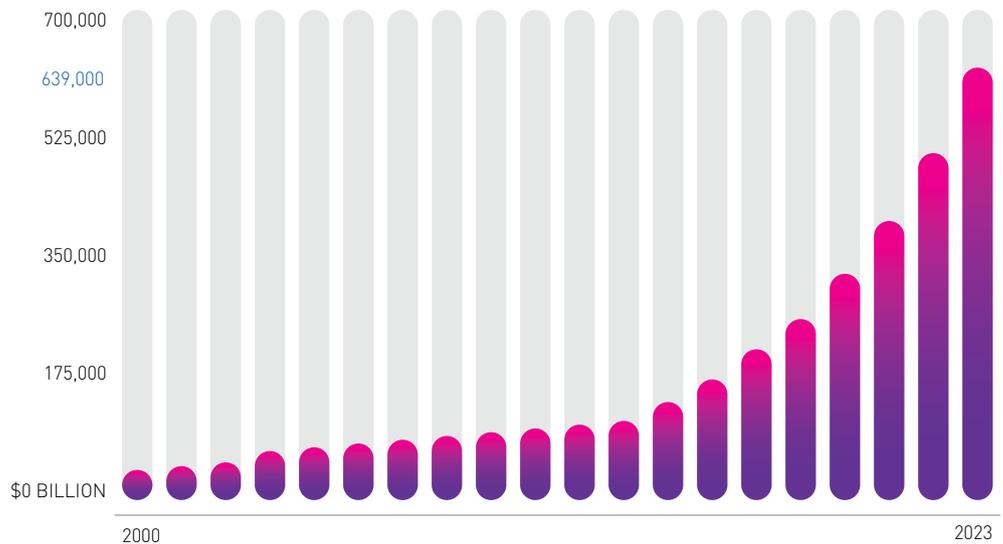
The adage goes that the only **truly** secure computer is locked in a lead box, buried fifty feet underground, sealed with concrete, with no wired or wireless connections in or out.

And turned off.

Which is to say, not a very useful computer.

Ultimately, for the majority of cases, security is about making the cost of entry higher than the value of the assets being protected.





ESTIMATED GLOBAL CYBERSECURITY SPENDING TO 2023

An estimated ten-fold increase in spending as cybercrime becomes a pivotal focus.
Source: IT-Harvest

Opportunities

Cyberattacks are costing global businesses as much as \$500 billion per year... The banking and financial sectors have led the way as top targets for cyberattacks in the last five years, with IT and telecom, defence, and the oil and gas sectors following behind.

Cybersecurity Ventures⁴⁸

The threats are many and varied, but so are the opportunities – technology constantly teases us with new ideas, new products, and new ways of living our lives. It also presents new economic opportunities, new ways of doing business, and new ways to make a difference.

The data-driven economy

If there's one prediction we can make about the next decade it is this: data will be king. From machine-learning AI to the Internet of Things, the accumulation and analysis of data from every aspect of our lives will drive entirely new insights and products.

We already have advanced local information system industries to support this, including the emerging FinTech sector (where already nine Australian FinTech businesses are listed in the world's top 100 FinTech companies⁴⁷).

But the opportunities for products and services involving data are going

to increase exponentially – already we are creating new ways to mine data and produce new services (right down to robot lawyers⁸⁶). Combined with the Internet of Things, there is tremendous economic opportunity for Australian technology companies to innovate and produce products for the world stage.

But all of these will also require cybersecurity as a fundamental building block. Regardless of the level of investment or development in Australian technology businesses, we will need a vibrant cybersecurity sector to support innovation and guarantee the economic prosperity of technology initiatives.

Security is as much about software as it is about awareness. It takes sophisticated coding to develop ransomware, but only one click to activate it.

Rodney Gedda,
Senior Analyst, Telsyte⁵³

Technology as wealth creation

The benefits of technology have created tremendous wealth over the last decade – you only need to look at household names like Google, Apple, or Facebook for examples.

As we move to a world populated by internet-connected devices – from your car to your fridge, your children’s toys and even the clothes you wear – there are still Googles and Apples and Facebooks to be discovered.

This alone represents tremendous opportunities for Australia’s ICT sector, but for any of this to be possible, the gadgets and the networks they communicate on must be secure, and this means cybersecurity will need to form the basis of every new technology going forward.

The end result, as it happens, is that good cybersecurity is good for the bottom line. There is an inherent interest for companies to implement good cybersecurity strategies to ensure their profitability is protected, and this in turn will require cybersecurity products and skilled cybersecurity professionals in the workforce.

The economic opportunity for Australia then for a strong cybersecurity sector is clear.

Cybersecurity as job growth

According to SEEK, cybersecurity roles are already in demand, having grown 57% in the last year.⁵⁰ This includes jobs like Security Analyst, Security Architect, Security Engineer, and Chief Information Security Officer, all of which represent the new type of opportunities that are developing in the workforce.

We have the skills and talent in Australia to support and capitalise on this growth, which will only see more demand as the importance of cybersecurity in the development of new technologies and products continues to grow.

There are lessons to be learned from Israel’s high proportion of security vendors here: moving from a high proportion of agricultural exports some 50 years ago, one of Israel’s primary exports is now software. Government support for a startup culture and the belief that technology is the backbone of a strong economy has seen Israel now lead the world in cybersecurity, second only to the US globally.

Currently there are some 228 cybersecurity vendors in Israel, and only 15 in Australia. Israel has one third the population of Australia.

Meanwhile in the UK, and since the British government published its cybersecurity strategy in 2011, the cybersecurity sector in the UK has almost doubled from £10 billion to £17 billion and is now responsible for employing 100 thousand people.⁴⁹

Australia can galvanise its own cybersecurity industry with government and private-sector support – but part of this involves addressing the need for more trained scientists, mathematicians, engineers, and ICT workers. As a nation we need a scientifically literate community capable of engaging in a national conversation on vital technology issues like cybersecurity.

Leveraging technology talent

Which leads us to the talent we already have – Australia has some of the world’s top universities, but as a previously resource-driven economy we currently lack a technology focus, the type of which Israel recognised as essential for a data-driven future.

Collaboration of government, industry and research organisations to incentivise new developments and monetise research to bring products and services to market will be key. This includes interacting with incubators and accelerators, sharing key learnings from innovation, and encouraging entrepreneurial thinking.

Diversity is also a critical component in order to meet demand for skilled ICT workers. This includes utilising a greater proportion of our aged workforce, and galvanising interest in ICT with women, who are currently underrepresented in the technology sector (just 28% of ICT roles are held by women⁵⁰) and represent a large untapped resource.

Challenges

Many of these devices are always on, always listening, and always communicating... raising concerns about transparency and privacy. With homeowners unprepared and ill-equipped to detect and remediate most security threats, some highly successful attacks will collect personal info on an ongoing basis.

McAfee Labs 2016
Threats Predictions¹⁵

While the opportunities are clear for ICT in Australia and the nation as a whole, there are a number of challenges we need to address. Ideally, all sectors from government and industry, to enterprise and academia, need to play a part in the development and promotion of cyber education, skills and products.

Leadership

Lack of leadership is a key challenge, if only because it takes a concerted effort to both recognise and take action on what is clearly a vital function in today's technologically savvy world.

This is true across government, the private sector, education and academia – the rate at which technology adoption occurs in Australia far outstrips our ability to predict the implications of technology, particularly when it comes to the results of cybercrime.

The foundation of any society is trust, as well as the foundation for security itself. Security helps build trust between people and technology. If we cannot protect for example personal data, it will have negative consequences for technology adoption and the ICT industry as a whole.

As a result, leadership is required to tackle issues around cybersecurity, governance, private-sector support and education to ensure we can adequately protect the foundation of trust upon which we all depend.

LEARNING FROM HISTORY

In 1958 when the National Defense Education Act was signed into law in the US, the goal was to provide funding to education institutions at all levels. The impetus was Russia beating the Americans to space, and a national feeling that America was falling behind. Over a period of four years \$USD1 billion was spent on science education.⁵⁷

Today we face a similar situation where we are already in a skills shortage for ICT in Australia, and if we are to create a blossoming cybersecurity ecosystem we will first need a strong emphasis on and promotion of STEM-based skillsets for Australians throughout the educational pathway.

695K

THE DEMAND FOR SKILLED ICT WORKERS WILL INCREASE FROM 638K TODAY TO 695K BY 2020

Collaboration

If there's one lesson to learn from cybercriminals it is this: collaboration is king. Analysis of attacks over the years has revealed that cybercriminals work together exceptionally well: sharing knowledge of exploits, selling stolen data in an open market, and working together to develop new hacking techniques for infiltration.

By contrast, compare this with the other side of the coin – those of us who defend against cyberattacks: siloed security vendors with competing products, little co-operation between government and industry, and companies afraid to share that they've been hacked for fear of impacting share price.

The latter is particularly important: knowledge is power, as we know, and so keeping a breach secret only helps the attackers – if an exploit isn't made public, it can be used

on the next company, and the next. In order to stop it, free sharing of information among business and enterprise, cybersecurity professionals, and security software vendors is essential. As Ron Moritz of TrueBit Cyber Partners notes, "while industry remains separate, the bad guys will always be ahead."⁵²

Therefore, developing the knowledge and software to protect against cyberattacks cannot happen in a vacuum. No one company or security vendor is able to withstand the collective might of an opponent who collaborates. This is a key lesson many in the private sector will have to learn if we are to keep pace in the cyber arms race.

Education and awareness

According to **Australia's Digital Pulse**, a report commissioned by the ACS, the demand for skilled ICT workers will increase from 638K today to 695K by 2020, with ICT university graduates meeting only 1% of this demand.⁵⁰ Additionally, there has been a 35% drop in enrolment rates for ICT subjects at universities since 2001.⁵⁰

As we move to a knowledge economy, we will need more scientists, mathematicians, engineers and programmers. Promotion and support of STEM subjects in schools, expanded degrees specific to cybersecurity disciplines at university, and an increased emphasis on entrepreneurial business skills will all help get Australians on track for roles in a cybersecurity industry as well as ICT at large.

It's interesting to note that professionals like lawyers and doctors are seen as prestigious, yet the skills and knowledge required to be a cybersecurity professional doesn't demand quite the same esteem. However, we are already at a stage where skilled cybersecurity professionals are essential to the operation of most industries in Australia. Can we generate a profession that garners a similar level of respect as other highly-skilled career paths?

Education also includes embedding cybersecurity in current workplace practice: as noted earlier, the weakest link is often people so good cybersecurity policies and



Infrastructure has always been considered a legitimate target. In WWII we bombed and destroyed the electrical infrastructure of our enemies. Now we have the ability, through a cyberattack, to just shut the grid down.

General Michael Hayden,
former CIA & NSA director⁸⁵

YOU ARE WHAT YOU DO

The famous adage 'you are what you eat' has an interesting parallel in the digital world – it's easy to forget that almost anything you do online involves data, and that this data tells a story about who you are and where you have been. From web browsing to smartphones, you and everyone you know is tracked, logged, and the data shared among a variety of services.

Whether it's a connection from your IP address in a application's log, or cookies about a website stored on your computer, every day you leave a trail – often called your **digital exhaust** or **data exhaust**.

While much is for analytics, once it's out there you have no control over it, let alone ownership (most applications and programs will prompt you to sign over your permission on first use). Even Microsoft's latest Windows 10 comes with 'mandatory' data collection about your use of the operating system.

McAfee's 2016 Threats Predictions report notes that "within the next five years, the volume and types of personal information gathered and stored will grow from a person's name, address, phone number, email address,

and some purchasing history to include frequently visited locations, 'normal' behaviours, what we eat, watch, and listen to, our weight, blood pressure, prescriptions, sleeping habits, daily schedule, and exercise routine."¹⁵

The more information that is out there about you, the greater the risk there is for it to be abused. Not just by cybercriminals seeking to develop correlations that can be used in fraud such as identity theft, but also intentional or unintentional misuse by companies or government services.

We're entering this world where everything is catalogued and everything is documented and companies and governments will be making decisions about you as an individual based on your data trail. If you want to be considered an individual and not just a data point, then it's in your interest to protect your privacy.

Josh Lifton, CEO of Crowd Supply⁵⁵

procedures are as essential to the operation of any business. If you are in an organisation that currently does not have policies and procedures in place to both prevent and mitigate cybercrime, now is a good time to start.

Finally, perhaps the biggest hurdle here is educating the sector, particularly among CEOs and Boards. There is a dearth of knowledge among decision makers on cybersecurity risks and the investment required to manage them.

According to a survey by The Economist Intelligence Unit, IT and security leaders in Australia think cybersecurity is the #1 issue at present – but less than 6% of C-Suite executives agree. There is a large disconnect between the reality of threats and awareness of them at the executive level.⁵⁸

Legal and regulatory

While collaboration is key, the good guys do have some hurdles the bad guys don't. For one, there may be legal or regulatory limitations, particularly where the sharing of

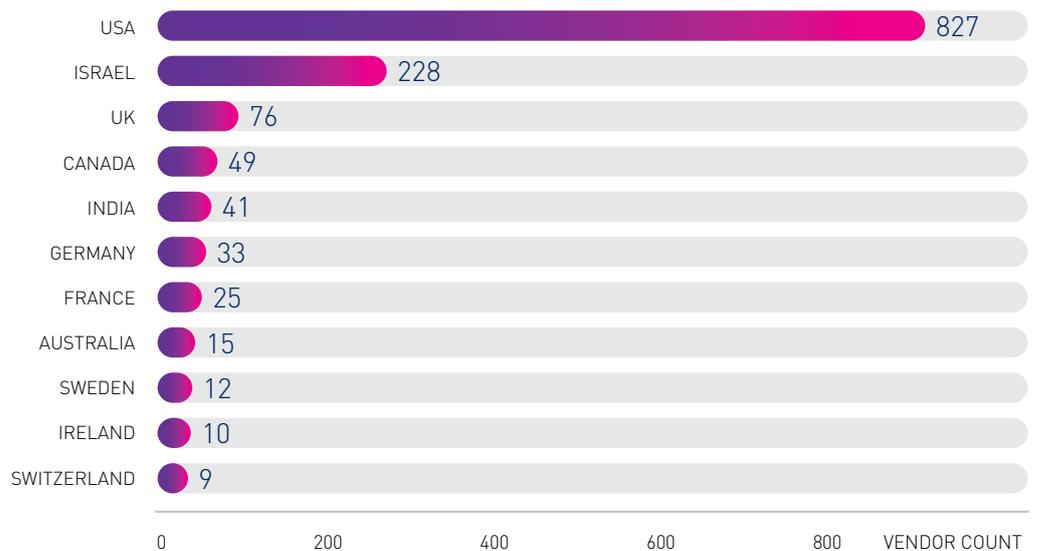
information could breach privacy laws. Where necessary, reviewing laws and regulations to facilitate better communication and collaboration for the purposes of cybersecurity may be required.

Services and privacy

Increasingly in our digital world services come at the cost of privacy. There is an inherent trade-off, and while we accept some encroachment of privacy over data we share, it nonetheless remains a fundamental building block of our society and must factor into any solutions.

We now know there is no such thing as a 100% secure system, any personal data stored on any server be it government, enterprise, or otherwise has the possibility of being breached and personal information being made public.

It's also important to note how the type and volume of data stored also acts as a target for cybercrime, in cases of identity theft, for example. The trend today for many companies is to capture as much personal information as possible, all the better



CYBERSECURITY VENDORS BY COUNTRY AS AT 2016

USA and Israel currently lead cybersecurity research and products.

Source: IT-Harvest

to mine for advertising or other products, but as more breaches come to light this trade-off of personal data for services will come under increased scrutiny.

This has implications for mass surveillance and the storage of metadata. As Jill Slay, Director of the Australian Centre for Cyber Security, and Greg Austin, Professor Australian Centre for Cyber Security, succinctly noted, “you cannot demand mass surveillance and metadata retention without there being costs that make us much less safe. Metadata retention is retrospective – it won’t predict or stop crimes, but it will open up breaches that bad actors can waltz through.”⁵⁴

The DDoS against the Australian Bureau of Statistics eCensus servers in August this year demonstrated just how easily a service can be knocked offline and, typically, DDoS attacks can often hide secondary attacks aimed at breaching a system. Any large database such as census data is a prime target for cybercriminals as it’s a jackpot for identity theft. McAfee’s Threats Predictions report

for 2016 notes that “Government identity records such as birth/death, taxes, and national insurance IDs; and banking accounts and ATM transactions will also be targeted.”¹⁵

Increasingly, as governments and corporations turn to big data, it will become paramount that this data be de-identified when possible to limit the damage from data breaches as well as preserve privacy of individuals.

Perception and practicality

Finally, there is a perception that Australia is not currently a technology leader – not just in cybersecurity, but as a whole. The current view with technological products is that it’s better if it comes from overseas.⁵⁶

This is a perception that needs to change. We have all the ingredients to create world-class products and services in Australia, particularly in relation to ICT and cybersecurity.

Pioneers like Atlassian and WiseTech Global demonstrate we have the

capability to create highly successful companies and products that compete on the world stage.

Changing this perception will involve, in part, the promotion of the value of home-grown ICT and raising awareness of Australian technological solutions.

Practically, it also helps for the private sector and the ICT industry as a whole to seek Australian products when canvassing for solutions.

It’s a market economy... the price of a compromised system of \$5 shows you exactly how far down the road we are of the cybersecurity story.

Tim Wellsmore, Former Manager, Fusion Special Intelligence 2013-16⁸⁵

Looking to the road ahead

It's clear cybersecurity is pivotal to both the economic future of Australia and indeed the fabric of our society. As we develop and embrace more and more technology, this will become ever more important.



For all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the cooperation and creativity of academia and industry. Indeed, government needs to be challenged by academia and industry.

Malcolm Turnbull,
Prime Minister of Australia.
September 2016

Helping ensure a secure and successful environment ultimately comes down to every government, business, academic institution and individual around the world. All three are the targets of cybercrime and any government department, corporate network, or the smartphone in your pocket could be used as a vector for attack.

That's not to say we should all stop using technology because the risks are too high – it's all about process and procedure. Good government regulation, skilled and qualified IT staff in an organisation, and education about common scams and how to avoid them, can dramatically shrink the surface of exposure and minimise or prevent data breaches, cybercrime, and many of the threats covered here.

So what are other parts of the world doing, and what are we doing here in Australia?

State of the nation

Economies of scale aside, the US administration, under Obama and now Trump, allocated \$US14 billion to cybersecurity spending in the 2016 budget³, and has asked for \$US19 billion for the 2017 fiscal year.⁶⁰

In the UK the British Government has allocated £860 million over a five-year period from 2011-2016, and is increasing this to £1.9 billion to 2021.⁵¹ The UK also conducts three exercises each month to test cyber resilience and response, and has a joint program with the US to prepare for a cyber-enabled terrorist attack on nuclear power stations. UK Chancellor George Osborne has called it "one of the greatest challenges of our lifetime".⁵⁴

Elsewhere in Europe, the European Parliament in June imposed security and reporting obligations for industries such as "banking, energy, transport and health and on digital operators like search engines and online marketplaces."⁸⁷

While in Japan the Japanese Government in August announced plans for a government institute, as part of Japan's Information Technology Promotion Agency (IPA), to train and educate employees to recognise and counter cyberattacks.⁸⁸

So where are we now in Australia? In September this year Prime Minister Malcolm Turnbull addressed the Australia-US Cybersecurity Dialogue at the Center for Strategic and International Studies, in which he reiterated the importance of cybersecurity and noted "for all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the cooperation and creativity of academia and industry. Indeed, government needs to be challenged by academia and industry."

On the 21st April, the Federal Government's Cyber Security Strategy⁵⁹ was launched and encompassed:

- A national cyber partnership between government, researchers and business including regular meetings to strengthen leadership and tackle emerging issues.

At the end of the day this really is about stewardship for us as a country. It's really about them, about the next generation. Bear in mind that they are only entrusting us with their future for a little while longer, because they're coming, and they're coming with or without us.

Adrian Turner, CEO, Data 61⁹³

- Strong cyber defences to better detect, deter and respond to threats and anticipate risks.
- Working with international partners through the new Cyber Ambassador and other channels to champion a secure, open and free internet while building regional cyber capacity to crack down on cyber criminals and shut safe havens for cybercrime.
- Help Australian cybersecurity businesses to grow and prosper, nurturing our home-grown expertise to generate jobs and growth, and support new business models, markets and investment.
- Create more Australian cybersecurity professionals by establishing Academic Centres of Cyber Security Excellence in universities, fostering skills throughout the education system and raising awareness of cybersecurity.

Additionally, initiatives like the Australian Centre for Cyber Security, (now in its second year), and an injection of \$30 million to establish an industry-led Cyber Security Growth Centre – charged with creating business opportunities for Australia's cybersecurity sector – as part of the National Innovation and Science Agenda further establishes the government's commitment to cybersecurity development in Australia.

Meanwhile, the CyCSA national Cyber Security Challenge (www.cyberchallenge.com.au) encourages students to participate in a cybersecurity competition. It's now in its fourth year.

What role can you play?

We know cybersecurity isn't just about technological defences; it's also about people and the way we handle data in the workplace, the emails we click or the sites we browse, and how good we are at identifying social engineering and other scams and tricks.

Good cybersecurity needs both good technological solutions and good people solutions. And, it requires all of us to participate.

In which case – whatever your responsibilities – what role can you play to make a difference?

Government

If you work in government, Prime Minister Malcolm Turnbull has already laid out in his address at the Australia-US Cyber Security Dialogue that leaders at government levels must know that “cyber is one of their essential functions” and to question what barriers can government “continue to remove, either through deregulation or positive action” to ensure the adoption of cybersecurity practices.

Regardless of your role in government, you can raise the conversation around cybersecurity and how it fits into your sector, and what the next steps are in bringing the government's cybersecurity strategy to fruition.



SHAKEN AND STIRRED

In security parlance a threat agent (not the 'James Bond' type) is an attack source combining motivation and capability. In general, threat agents can be categorised from benign to critical. To the right is a breakdown of common threat agent categories and their typical vectors:²⁵

THREAT LEVEL	THREAT AGENT	THREAT VECTOR
CRITICAL	Nation state	Espionage, theft, sabotage, product alteration
	Competitor	Espionage, theft, product alteration
	Organised crime	Espionage, fraud, theft
	Terrorist	Sabotage, violence
HIGH	Activist/hacktivist	Espionage, data theft, sabotage
	Disgruntled employee	(All of the below)
	Reckless, untrained or distracted employees	Accidental breach or misuse of data
MEDIUM	Thief	Physical theft, espionage, fraud
	Irrational individual	Physical theft or sabotage
	Vendor or partner	Accidental leak, but also intentional fraud or theft
LOW	Outward sympathiser	Deliberate data leak or misuse of data



Education and research

If you work in academia, university, research or other educational institutions you have a great opportunity to see how cybersecurity principles can either be applied to your work, or considered in the application and delivery of your work.

Educational institutions from pre-school through to university all play a vital part in the promotion of STEM-based skills upon which disciplines such as cybersecurity are based. And, as we've noted in this guide, we are already in a shortage of skilled cybersecurity professionals. What you can do to promote this challenging and rewarding career pathway is of benefit not just to your students but Australia as a whole.

Within research and academic institutions the results of your work may be critical in any number of ways, and so if not already the access to and handling of data needs to be guided by solid cybersecurity principles in order to minimise or prevent any loss through a cyberattack.

Business and industry

In your workplace, the single most important step you can take is to draw attention to cybersecurity – or the lack of it – within your company. Write a cybersecurity report card looking at your organisation's policies, training and awareness programs, technical controls, management processes and general security culture.

Every business plays its part just as every one of us plays a part. The smartphone in your pocket could act as a vector for the theft of your own personal data, or as a vector of

attack in the company you work for. It's in everyone's best interests to be informed, prepared, and responsible. Remember, cybersecurity is not just a safety risk, it's a business risk.

If you are an executive, it is incumbent on management to be well-versed in cybersecurity language and the realities of cybersecurity threats to your business. If not already, appoint a CISO (Chief Information Security Officer) or CSO (Chief Security Officer) and ensure they have a place in board-level decision making. Also ensure clear and easy lines of communication between security, IT staff and upper management – these employees are your front line of defence.

Remember that just as your business does not operate in a vacuum, the same is true for cybersecurity. You may have all the best policies and procedures in the world but be vulnerable through a third party such as suppliers or distributors with which you do business. It is important to ensure they, too, have adequate cybersecurity preparations and resources to protect themselves and the businesses they work with – and you can help them.

Finally, it's important to ensure your IT staff and security specialists are trained with up-to-date qualifications, as well as ensuring they have the necessary skills and expertise, and are certified to a recognised standard.

You, the individual

Because we all use a variety of devices every day, cybersecurity isn't just about protecting corporate networks or organisational assets.

Each of us has plenty of data – personal information – that should remain personal and not be used against us for extortion, identity theft, or as part of a scam.

It's telling that we lock our doors when leave home, or lock our cars when we arrive at work, and yet don't consider the safety of the data on our computers when we browse the web or install an application.

And there's actually a lot you can do to help ensure your data remains yours. There are plenty of guides online, but a good summary includes:

- Use complex passwords over simple ones, and don't re-use passwords between sites and services. If you find passwords hard to remember, use a password manager.
- When on offer, use two-factor authentication. This is becoming more common now with various services to ensure others can't log in as you, even if they manage to attain your passwords.
- Learn to recognise phishing emails – listen to that nagging voice in your head: if it sounds suspicious, it is. Banks, government services, and reputable companies won't ask for your login details over email.
- Don't open files from someone you don't know, and don't download or install any files delivered through pop-ups or pop-unders during web browsing.
- Keep your operating system and your applications up-to-date with the latest patches.

There's plenty more to learn. See the Online Resources on page 52 for a good place to start.

The five pillars of cybersecurity readiness

As the peak body for ICT professionals in Australia, the ACS considers the following to be the five core pillars of cybersecurity readiness.

1

Education and Awareness

First and foremost, it's essential that cybersecurity forms part of the conversation in every organisation, from the lunch room to the boardroom. Only through keeping cybersecurity front of mind can it form part of the decision-making process, infrastructure investment, and regulatory and governance requirements.

Additionally, as people can themselves be an attack vector through social engineering, everyone within an organisation ultimately shares responsibility in ensuring best-practice cybersecurity processes are carried out. This requires staff education with regular updates to material as new threats arise. In fact, parallels have been drawn between cybersecurity and healthcare – everyone needs some form of cybersecurity education.

Finally, the employment of qualified cybersecurity professionals or certified training for key staff both in IT and management should form part of any cybersecurity readiness.

2

Planning and Preparation

A cybersecurity incident isn't an 'if' but a 'when', and to that end, preparation is essential. This can include management systems, best practice policies, IT auditing, and dedicated staff responsible for cybersecurity operations.

Good cybersecurity readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cybersecurity threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, has incident response plans in place in the event of a breach, and clear business continuity plans to minimize any loss.

Typically, many of the above responsibilities belong to the CISO (Chief Information Security Officer) or equivalent, though other stakeholders such as senior leadership, legal and communications staff, and public relations may also need to have preparations in the event of an incident.

3

Detection and Recovery

When a breach happens, the quicker it is detected and responded to, the greater the chance of minimising loss – be it financial, reputational, or otherwise.

How quickly can your organisation identify and respond to the theft of data or the disabling of key services? How fast can affected servers or workstations be quarantined for forensic analysis? How quickly and easily can lost or corrupted data be restored? What is the incident response plan and who are the stakeholders that need to be notified immediately?

Importantly, the preservation and analysis of logs that can help identify how the breach happened, and thus how it can be closed, is part of the recovery process. It's not enough just to close the hole; an understanding of how the breach occurred can lead to preventing other, similar, breaches.

4

Sharing and Collaboration

As we've covered in this guide, collaboration is essential to mitigating current and future risks.

Sharing the results of your breach analysis with government and industry can help stop a known attack vector hitting other organisations. In turn, your company may be able to prevent an exploit by learning from a breach that another organisation shared.

Also consider joining or providing information to an ISAC (Information Sharing and Analysis Centers, www.nationalisacs.org) if there is an equivalent for your industry.

In some cases, your organisation may be bound by legislative requirements to report an incident. At a minimum, a breach should be reported to government or organisations such as AusCERT (www.uscert.org.au) and the Australian Centre for Cyber Security (www.acsc.gov.au).

5

Ethics and Certification

It may initially seem a less practical pillar, but the difference between a 'white hat' hacker and 'black hat' hacker is mindset.

In any company or organisation, ethics plays a role and should be of particular concern when it comes to cybersecurity. While some sectors, such as defence, will have their own means to vet credentials, for an industry as diverse and skilled as ICT it helps if professionals can demonstrate adherence to a code of ethics through membership of a professional institution.

Many professional organisations hold their members to standards that ensure the reputation and respectability of a profession is preserved. ACS, for example, has a code of ethics all Certified Professionals must abide by, in addition to other requirements such as demonstrating continued education and personal development in their chosen professional field of expertise.

ONLINE RESOURCES

For further reading and more information, visit the following websites:

- Australia's Cybersecurity Strategy cybersecuritystrategy.dpmc.gov.au
- Australian Center for Cyber Security www.acsc.gov.au
- Australian Computer Emergency Response Team (AusCERT) www.uscert.org.au
- Australian Cybercrime Online Reporting Network (ACORN) www.acorn.gov.au
- Australian Internet Security Initiative www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative
- Australian Signals Directorate – Top 4 Mitigation Strategies www.asd.gov.au/infosec/mitigationstrategies.htm
- Australian Signals Directorate – CyberSense Videos www.asd.gov.au/videos/cybersense.htm
- Australian Government – Stay Smart Online www.staysmartonline.gov.au
- ACCC – Scam Watch www.scamwatch.gov.au
- Australian Computer Society (ACS) www.acs.org.au

Through the looking glass

The following is a snapshot – just a sample – of the stories that made the news during the production of this guide. These headlines give you an insight to the ongoing, every day, occurrences of what happens in the absence of cybersecurity.

'LINKEDIN USER?
YOUR DATA MAY BE
UP FOR SALE'⁶¹

'EASYDOC
MALWARE ADDS
TOR BACKDOOR
TO MACS
FOR BOTNET
CONTROL'⁶³

'LIZARDSTRESSER BOTNETS
USING WEBCAMS, IOT
GADGETS TO LAUNCH
DDOS ATTACKS'⁶⁵

'DDOS ATTACK
TAKES DOWN
US CONGRESS
WEBSITE FOR
THREE DAYS'⁶⁷

'HACKERS FIND 138
SECURITY GAPS IN
PENTAGON WEBSITES'⁶⁹

'HACKER STEALS 45
MILLION ACCOUNTS FROM
HUNDREDS OF CAR, TECH,
SPORTS FORUMS'⁷¹

'10 MILLION
ANDROID
DEVICES
REPORTEDLY
INFECTED
WITH CHINESE
MALWARE'⁷³

'THIEVES GO HIGH-TECH
TO STEAL CARS'⁷⁵

'CROOKS ARE
WINNING THE
'CYBER ARMS
RACE', ADMIT
COPS'⁷⁷



The US government has increased its annual cybersecurity budget by 35%, going from \$14 billion budgeted in 2016 to \$19 billion in 2017. This is a sign of the times and there's no end in sight. Incremental increases in cybersecurity spending are not enough. We expect businesses of all sizes and types, and governments globally, to double down on cyber protection.

Cybersecurity Ventures⁴⁸

'A HACK WILL KILL SOMEONE WITHIN 10 YEARS AND IT MAY HAVE ALREADY HAPPENED'⁷⁹

'CHINA HACKED US BANKING REGULATOR'⁸¹

'APPLE DEVICES HELD FOR RANSOM, RUMOURS CLAIM 40M ICLOUD ACCOUNTS HACKED'⁶²

'RESEARCHERS DISCOVER TOR NODES DESIGNED TO SPY ON HIDDEN SERVICES'⁶⁴

'RESEARCHERS FOUND A HACKING TOOL THAT TARGETS ENERGY GRIDS ON THE DARK WEB'⁶⁶

'CITING ATTACK, GOTOMYPC RESETS ALL PASSWORDS'⁶⁸

'POLITICAL PARTY'S VIDEO CONFERENCE SYSTEM HACKED, ALLOWED SPYING ON DEMAND'⁷⁰

'ONLINE BACKUP FIRM CARBONITE TELLS USERS TO CHANGE THEIR PASSWORDS NOW'⁷²

'ANDROID RANSOMWARE HITS SMART TV'S'⁷⁴

'HACKERS CAN USE SMART WATCH MOVEMENTS TO REVEAL A WEARER'S ATM PIN'⁷⁶

'IDENTITY FRAUD UP BY 57% AS THIEVES 'HUNT' ON SOCIAL MEDIA'⁷⁸

'WHY YOU SHOULD DELETE THE ONLINE ACCOUNTS YOU DON'T USE ANYMORE – RIGHT NOW'⁸⁰

'MASSIVE DDOS ATTACKS REACH RECORD LEVELS'²⁸

'HACKER DEMONSTRATES HOW VOTING MACHINES CAN BE COMPROMISED'⁸⁹

'FTC WARNS CONSUMERS OF RENTAL CAR DATA THEFT RISK'⁹⁰

'YAHOO CONFIRMS MASSIVE DATA BREACH, 500 MILLION USERS IMPACTED'⁹¹

Fast facts

It's hard to choose just a handful of facts that highlight the threats and opportunities facing Australia, but here is a sample.

THREATS

IN 2014-15 CERT (COMPUTER EMERGENCY RESPONSE TEAM) AUSTRALIA RESPONDED TO

11,733

INCIDENTS, 218 OF WHICH INVOLVED SYSTEMS OF NATIONAL INTEREST OR CRITICAL INFRASTRUCTURE. OF THESE, ENERGY, BANKING AND FINANCE, AND COMMUNICATIONS WERE THE TOP THREE TARGETS.⁸²

THE AUSTRALIAN GOVERNMENT DEPARTMENT OF COMMUNICATIONS HAS REPORTED THAT THE AVERAGE COST OF A CYBERCRIME ATTACK TO A BUSINESS IS AROUND

\$276,000⁹²

THE WORLD ECONOMIC FORUM'S GLOBAL RISKS 2015 REPORT HIGHLIGHTED CYBERATTACKS AND THREATS AS ONE OF THE MOST LIKELY HIGH-IMPACT RISKS. IN THE UNITED STATES, FOR EXAMPLE, CYBER CRIME ALREADY COSTS AN ESTIMATED

\$US100

BILLION A YEAR.⁵⁰

IOT SENSORS AND DEVICES ARE EXPECTED TO EXCEED MOBILE PHONES AS THE LARGEST CATEGORY OF CONNECTED DEVICES IN 2018, GROWING AT A

23%

COMPOUND ANNUAL GROWTH RATE (CAGR) FROM 2015 TO 2021.⁸³ SOLID CYBERSECURITY POLICY MUST BE IN PLACE FOR THIS FUTURE.

CYBERSECURITY IS A BUSINESS ISSUE, NOT JUST A TECHNOLOGY ONE. IN A SURVEY OF CLOSE TO

4,000

COMPANY DIRECTORS IN AUSTRALIA, ROUGHLY ONLY HALF REPORTED TO BE CYBER LITERATE, AND OF CO-DIRECTORS ONLY

FIFTEEN

PERCENT CLASSED AS CYBER LITERATE. THERE IS A LACK OF KNOWLEDGE ABOUT CYBERSECURITY AT THE EXECUTIVE LEVEL IN MANY BUSINESSES IN AUSTRALIA.¹



OPPORTUNITIES

IN 2003 THE CYBERSECURITY INDUSTRY WAS TAGGED AT

\$US2.5

BILLION TODAY THE GLOBAL CYBERSECURITY MARKET TOTALS MORE THAN \$US106 BILLION. SOME ESTIMATES PEG THE SECTOR WILL BE WORTH \$US639 BILLION BY 2023.¹

BY 2030 IT'S ESTIMATED DATA ANALYTICS, MOBILE INTERNET, CLOUD AND IOT COULD GENERATE \$US625

BILLION

IN SALES PER YEAR IN APAC.¹

THE UK PUBLISHED ITS CYBER-SECURITY STRATEGY IN 2011 – SINCE THEN THE SECTOR ALMOST DOUBLED FROM TEN BILLION POUNDS TO

SEVENTEEN

BILLION POUNDS AND IS NOW RESPONSIBLE FOR EMPLOYING 100K PEOPLE.⁵¹

THERE ARE

1,404

CYBERSECURITY VENDORS IN THE WORLD TODAY. AUSTRALIA SPORTS ONLY FIFTEEN. VENDORS BY COUNTRY: USA 827, ISRAEL 228, UK 76, INDIA 41, AUSTRALIA 15.¹

JOB ADVERTISEMENTS FOR CYBER-SECURITY ALONE HAVE GROWN

57%

IN THE LAST 12 MONTHS ACCORDING TO JOBS WEBSITE SEEK. NETWORK SECURITY CONSULTANTS WERE THE

SIXTH

MOST ADVERTISED ICT OCCUPATION ON LINKEDIN IN 2015.⁵⁰

Glossary

A collection of some common words and phrases you will see used for discussions in and around cybersecurity.

Administrator: Person who administers a computer system or network and has access to the Administrator account.

Black Hat: Programmers who 'hack' into systems to test their capabilities, and exploit vulnerabilities for personal or financial gain. See Cybercrime.

Advanced Persistent Threat: Usually refers to long-term stealth attacks on or infiltration of a system, but can also be used to describe a group, such as a foreign government, with advanced cyberattack capabilities.

CIO/CISO: Chief Information Officer/ Chief Information Security Officer. Executive position responsible for ensuring the security of systems and data in an organisation (can include physical security).

Critical infrastructure: Physical and virtual assets that are vital to the operation of an organisation or nation, for example, the electrical grid.

Cyberattack: An offensive act against computer systems, networks, or infrastructure.

Cybercrime: Computer-facilitated crimes, though frequently can be used to refer to all forms of technology-enabled crimes.

Cyberespionage: The practice and theft of confidential information from an individual or organisation.

Cybersecurity: The discipline and practice of preventing and mitigating attacks on computer systems and networks.

Cyberthreat: A potential threat targeting computer systems and technology, typically from the internet.

Cyberwarfare: Internet-based conflict to attack computer systems to disrupt or destroy. Usually in reference to nation states but can also refer to companies, terrorist or political groups, or activists.

DoS/DDoS: Denial of Service/ Distributed Denial of Service. A common attack involving thousands of devices accessing a site simultaneously and continually to overload its ability to serve web pages.

Hacker/Hacking: While originally in reference to a programmer 'hacking at code', it's now become mainstream to represent individuals who maliciously breach ('hack into') computers and related systems.

ICT: Information and Communications Technology. Overarching term encompassing all forms of computing and telecommunications technology inclusive of hardware, software, and networks.

IoT: Internet of Things. An evolving definition of the wide-variety of internet-connected devices ranging from sensors to smartphones.

Internet security: A general term referring to the security of internet-related technologies, such as web browsers, but also that of the underlying operating system or networks.

Malware: Catch-all term to refer to any type of malicious software, typically used in reference to viruses, ransomware, spyware and similar.

Phishing: Deceptive attempt, usually over email, to trick users into handing over personally identifiable or critical information (such as passwords or credit card numbers). A form of social engineering.

Ransomware: Malware used to hold an individual or organisation to ransom, typically by encrypting files or an entire hard drive and demanding payment to 'unlock' the data. Also known as Cryptoware.

Social engineering: The practice of manipulating human beings to gain access to data or computer systems.

Spear-phishing: Highly-targeted form of phishing towards an individual or business, often utilising social engineering techniques to appear to be from a trusted source.

Spyware: Covert software designed to steal data or monitor people and systems for cybercriminals, organisations, or nation states.

Threat actor: an individual or entity that has the potential to impact, or has already impacted, the security of an organisation.

White Hat: Programmers who 'hack' into systems to test their capabilities, and report vulnerabilities to authorities to be fixed.

References

- 1 Richard Stiennon, Chief Research Analyst, IT-Harvest, National Fintech Cybersecurity Summit 2016
- 2 Internet Users by Country 2016, Internet Life Stats, July 2016
www.internetlivestats.com/internet-users-by-country
- 3 'Cybersecurity Market... Expected To Reach \$170 Billion By 2020', Forbes, Dec 2015
www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020
- 4 'One in two users click on links from unknown senders', Fau.eu, August 2016
www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders
- 5 'Biggest cybersecurity threats in 2016', CNBC, Dec 2015
www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html
- 6 'Hackers remotely kill a jeep on the highway', Wired, July 2015
www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
- 7 'Hackers can send fatal dose to hospital drug pumps', Wired, June 2015
www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps
- 8 'Hackers can hijack Wi-Fi Hello Barbie to spy on your children', The Guardian, November 2015
www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children
- 9 Simi Bajaj, 'Cyber Fraud: A Digital Crime',
www.academia.edu/8353884/cyber_fraud_a_digital_crime
- 10 Akamai's State of the Internet Security Report Q2 2015
media.scmagazine.com/documents/144/q2_2015_soti_security_report_-_35820.pdf
- 11 Contracting for the Internet of Things: Looking into the Nest, Social Science Research Network, February 2016
ssrn.com/abstract=2725913
- 12 'Cisco CEO Pegs Internet of Things as \$19 Trillion Market', Bloomberg Technology, January 2014
www.bloomberg.com/news/articles/2014-01-08/cisco-ceo-pegs-internet-of-things-as-19-trillion-market
- 13 'Aussie IoT in the home spend tipped to top \$200m in 2020', IoT Australia, November 2015
www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020
- 14 A guide to the Internet of Things Infographic, Intel
www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
- 15 2016 Threats Predictions, McAfee Labs, 2016
www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf
- 16 'Lax Security Opens the Door for Mass-Scale Abuse', Imperva Incapsula, May 2015
www.incapsula.com/blog/ddos-botnet-soho-router.html



References continued

- 17 'Hosting company OVH suffers world's largest 1 Tbps DDoS attack', TheTechPortal.com thetechportal.com/2016/09/28/worlds-largest-ddos-attack-ovh-iot
- 18 Dissecting the Top Five Network Attack Methods: A Thief's Perspective, McAfee & Intel Security, 2015 www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf
- 19 'The Lizard Brain of Lizard Stresser', Arbor Networks, June 2016 www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser
- 20 'BMW, Mercedes Vulnerable to Remote-Unlocking Hack', Car and Driver, August 2015 blog.caranddriver.com/researcher-bmw-mercedes-vulnerable-to-remote-unlocking-hack
- 21 'BMW, Audi and Toyota cars can be unlocked and started with hacked radios', The Telegraph UK, April 2016. www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the
- 22 'Fiat Chrysler recalls 1.4 million cars after Jeep hack', BBC News, July 2015 www.bbc.com/news/technology-33650491
- 23 The Connected Car Report, Business Insider, March 2015 www.businessinsider.com.au/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3
- 24 'Mark Zuckerberg covers his laptop camera and you should too', Australian Financial Review, June 2016. www.afr.com/technology/web/security/mark-zuckerberg-covers-his-laptop-camera-and-you-should-too-20160623-gppvwy
- 25 Critical Infrastructure Readiness Report, The Aspen Institute & Intel Security, 2015 www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf
- 26 Identity Theft Prevention – ID Theft Facts and Figures 2016, Kaspersky Lab, May 2016 youtu.be/Fztuohj3Fck
- 27 'The Next Wave of Cyberattacks Won't Steal Data -- They'll Change It', Defense One, September 2015 www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701
- 28 'Massive DDoS attacks reach record levels as botnets make them cheaper to launch', Network World, June 2016 www.networkworld.com/article/3079987/massive-ddos-attacks-reach-record-levels-as-botnets-make-them-cheaper-tolaunch.html
- 29 Therac-25, Wikipedia, 2016 en.wikipedia.org/wiki/Therac-25
- 30 'The Patriot Missile Failure', Douglas Arnold, August 2000 ima.umn.edu/~arnold/disasters/patriot.html
- 31 'Toyota's killer firmware: bad design and its consequences', EDN Network, October 2013 www.edn.com/design/automotive/4423428/Toyota-s-killer-firmware--Bad-design-and-its-consequences
- 32 'Tesla Autopilot Enthusiast Killed In First Self-Driving Car Death', Forbes, June 2016 www.forbes.com/sites/briansolomon/2016/06/30/the-first-self-driving-car-death-launches-tesla-investigation/

- 33 'Chinese cyberattacks hit key US weapons systems. Are they still reliable?', Christian Science Monitor, May 2013
www.csmonitor.com/USA/Military/2013/0528/Chinese-cyberattacks-hit-key-US-weapons-systems.-Are-they-still-reliable
- 34 'Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors', Wired, December 2015
www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors
- 35 'The 10 Commandments of Data Sovereignty', CSO Online, July 2013
www.cso.com.au/article/466539/10_commandments_data_sovereignty
- 36 'Russia Imposes New Data Storage Requirements for Telecoms and ISPs', Hogan Lovells Media, July 2016
www.hlmediacomms.com/2016/07/11/russia-imposes-new-data-storage-requirements-for-telecoms-and-isps
- 37 'We are removing our Russian presence', PrivateInternetAccess.com
www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence
- 38 Image, Cyber Security Trends 2016, Cybernetic Global Intelligence, November 2015
cgi-content-imagesandcode.cyberneticglobal.netdna-cdn.com/wp-content/uploads/2015/11/cyber-predictions-2016-v2.png
- 39 Russo-Georgian War, Wikipedia, 2016
en.wikipedia.org/wiki/Russo-Georgian_War
- 40 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, November 2014
www.wired.com/2014/11/countdown-to-zero-day-stuxnet
- 41 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever', Wired, January 2015
www.wired.com/2015/01/german-steel-mill-hack-destruction
- 42 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, March 2016.
www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid
- 43 French Coldwell, Chief Evangelist, Metricstream, National Fintech Cybersecurity Summit 2016, Sydney
- 44 'Kaspersky report on Energetic Bear', Security Affairs, August 2014
securityaffairs.co/wordpress/27224/cyber-crime/kaspersky-report-energetic-bear.html
- 45 'Mayhem' program wins grand hacking challenge', BBC News, August 2016
www.bbc.com/news/technology-36980307
- 46 'When Paying Out Doesn't Pay Off', Talos Intel, July 2016
blog.talosintel.com/2016/07/ranscam.html
- 47 Fintech 100: Nine Australian companies make the cut
www.home.kpmg.com/au/en/home/media/press-releases/2016/10/the-fintech-100-announcing-the-worlds-leading-fintech-innovators-for-2016.html
- 48 Cybersecurity Market Report, Cybersecurity Ventures, 2016
cybersecurityventures.com/cybersecurity-market-report
- 49 Chancellor's speech to GCHQ on cyber security
www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

References continued

- 50 Australia's Digital Pulse 2016, ACS & Deloitte Access Economics
www.acs.org.au/content/dam/acs/acs-documents/PJ52569-Australias-Digital-Pulse-2016_LAYOUT_Final_Web.pdf
- 51 The UK Cyber Security Strategy 2011-2016, Annual Report, April 2016
www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
- 52 Ron Moritz, TrueBit Cyber Partners, National Fintech Cybersecurity Summit 2016, Sydney
- 53 Email interview, Rodney Gedda Senior Analyst, Telsyte, July 2016
- 54 'The Australian government must take cyber security more seriously',
The Conversation, June 2016
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231
- 55 The dark side of wearables: How they're secretly jeopardizing your security and privacy,
Tech Republic, April 2016
www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/
- 56 Alex Scundurra, CEO Stone & Chalk, National Fintech Cybersecurity Summit 2016, Sydney
- 57 National Defense Education Act, Wikipedia, 2016
en.wikipedia.org/wiki/National_Defense_Education_Act
- 58 'The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise'
www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf
- 59 Australia's Cybersecurity Strategy, Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2016
cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
- 60 'Concerned by cyber threat, Obama seeks big increase in funding', Reuters, February 2016
www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231
- 61 'LinkedIn user? Your data may be up for sale', ZDNet, May 2016
www.zdnet.com/article/linkedin-user-millions-of-users-data-is-up-for-sale
- 62 'Apple devices held for ransom', CSO Online, July 2016
www.csoonline.com/article/3093016/security/apple-devices-held-for-ransom-rumors-claim-40m-icloud-accounts-hacked.html
- 63 'EasyDoc malware adds Tor backdoor to Macs for botnet control', The Register, July 2016
www.theregister.co.uk/2016/07/05/easydoc_malware_adds_tor_backdoor_to_mac_systems_for_botnet_control/
- 64 'Researchers Discover Tor Nodes Designed to Spy on Hidden Services',
Schneier on Security, July 2016
www.schneier.com/blog/archives/2016/07/researchers_dis.html

- 65 'LizardStresser botnets using webcams, IoT gadgets to launch DDoS attacks', SC Magazine, July 2016
www.scmagazineuk.com/lizardstresser-botnets-using-webcams-iot-gadgets-to-launch-ddos-attacks/article/506962
- 66 'Researchers Found a Hacking Tool that Targets Energy Grids on the Dark Web', Motherboard, July 2016
motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum
- 67 'DDoS Attack Takes Down US Congress Website for Three Days', Softpedia News, July 2016
news.softpedia.com/news/ddos-attack-takes-down-us-congress-website-for-three-days-506451.shtml
- 68 'Citing Attack, GoToMyPC Resets All Passwords', Krebs On Security, June 2016
krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords
- 69 'Hackers Find Security Gaps in Pentagon Websites', ABC News, June 2016
abcnews.go.com/Technology/wireStory/hackers-find-security-gaps-pentagon-websites-39945560
- 70 'Political Party's Videoconference System Hacked, Allowed Spying On Demand', Slashdot, June 2016
news.slashdot.org/story/16/06/18/1831235/political-partys-videoconference-system-hacked-allowed-spying-on-demand
- 71 'Hacker steals 45 million accounts from hundreds of car, tech, sports forums', ZDNet, June 2016
www.zdnet.com/article/hacker-steals-45-million-accounts-from-hundreds-of-verticalscope-car-tech-sports-forums/
- 72 'Online Backup Firm Carbonite Tells Users To Change Their Passwords Now', Slashdot, June 2016
it.slashdot.org/story/16/06/21/2032209/online-backup-firm-carbonite-tells-users-to-change-their-passwords-now
- 73 '10 million Android devices reportedly infected with Chinese malware', CNet, July 2016
www.cnet.com/news/malware-from-china-infects-over-10-million-android-users-report-says
- 74 'FLocker Mobile Ransomware Crosses to Smart TV', Trend Micro, June 2016
yro.slashdot.org/story/16/06/13/1845221/android-ransomware-hits-smart-tvs
- 75 'Thieves Go High-Tech to Steal Cars', The Wall Street Journal, July 2016
www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606
- 76 'Hackers Can Use Smart Watch Movements To Reveal A Wearer's ATM PIN', Slashdot, July 2016
news.slashdot.org/story/16/07/06/2132206/hackers-can-use-smart-watch-movements-to-reveal-a-wearers-atm-pin
- 77 'Crooks are winning the 'cyber arms race' admit cops', ZDNet, July 2016
www.zdnet.com/article/crooks-are-winning-the-cyber-arms-race-admit-cops
- 78 'Identity fraud up by 57% as thieves 'hunt' on social media', BBC News, July 2016
www.bbc.com/news/uk-36701297
- 79 'A hack will kill someone within 10 years and it may have already happened', Yahoo News, June 2016
uk.news.yahoo.com/hack-kill-someone-within-10-091800465.html



References continued

- 80 'Why you should delete the online accounts you don't use anymore - right now', Sydney Morning Herald, June 2016.
www.smh.com.au/technology/technology-news/why-you-should-delete-the-online-accounts-you-dont-use-anymore--right-now-20160602-gp9n18.html
- 81 'China Hacked US Banking Regulator From 2010 Until 2013', Slashdot, July 2016
yro.slashdot.org/story/16/07/13/1923215/china-hacked-us-banking-regulator-from-2010-until-2013---and-us-officials-covered-itup-report
- 82 2015 Threat Report, Australian Cyber Security Centre, 2015
www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf
- 83 'Internet Of Things On Pace To Replace Mobile Phones As Most Connected Device In 2018', Forbes, July 2016
www.forbes.com/sites/louiscolombus/2016/07/09/internet-of-things-on-pace-to-replace-mobile-phones-as-most-connecteddevice-in-2018/#468e81846aef
- 84 'One of Europe's Biggest Companies Loses €40 Million in Online Scam', Softpedia
news.softpedia.com/news/one-of-europe-s-biggest-companies-loses-40-million-in-online-scam-507818.shtml
- 85 Cyber War, ABC, 4 Corners, August 2015
www.abc.net.au/4corners/stories/2016/08/29/4526527.htm
- 86 'Robot Lawyers Could Make Time-Consuming, Expensive Court Conflict Thing Of The Past', ABC, July 2016
www.abc.net.au/news/2016-07-06/robot-lawyers-dutch-conflict-resolution-technology-on-its-way/7572488
- 87 'European Union's First Cybersecurity Law Gets Green Light', Bloomberg Technology, July 6
www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light
- 88 'Japanese Government Plans Cyber Attack Institute', The Stack, August 2016
thestack.com/security/2016/08/24/japanese-government-plans-cyber-attack-institute
- 89 'Hacker Demonstrates How Voting Machines Can Be Compromised', CBS News, August 2016
www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines
- 90 'FTC Warns Consumers: Don't Sync To Your Rental Car!', Slashdot, September 2016
tech.slashdot.org/story/16/09/04/0912201/ftc-warns-consumers-dont-sync-to-your-rental-car
- 91 'Yahoo Confirms Massive Data Breach, 500 Million Users Impacted', Slashdot, September 2016
it.slashdot.org/story/16/09/22/095255/yahoo-confirms-massive-data-breach-500-million-users-impacted-updated
- 92 Image, StaySmartOnline.gov.au, October 2015
www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf
- 93 Adrian Turner, CEO, Data 61, National Fintech Cybersecurity Summit 2016, Sydney

ABOUT THE ACS

The Australian Computer Society is the professional association for Australia's Information and Communications Technology sector.

We are passionate about recognising and developing ICT skills and provide more than 60 products and services to our members. We are also the voice of Australian ICT, representing all practitioners in business, government and education.

In everything we do, our goal is to advance ICT in Australia and help our members be the best they can be.

COPYRIGHT NOTICE

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

creativecommons.org/licenses/by-sa/4.0



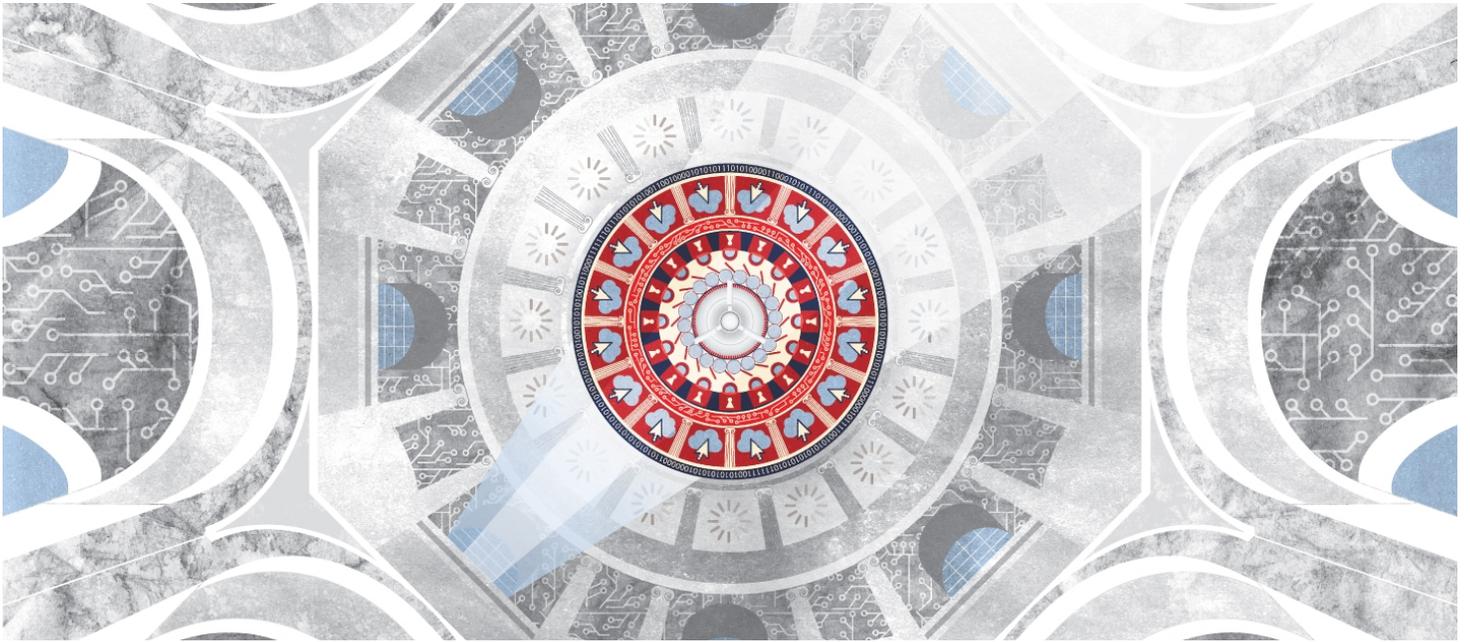


ACS
Level 11
50 Carrington Street
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au

Deloitte-NASCIO Cybersecurity Survey

September 2016



Article

2016 Deloitte-NASCIO Cybersecurity Study

State governments at risk: Turning strategy and awareness into progress

[Doug Robinson](https://dupress.deloitte.com/dup-us-en/authors/r/doug-robinson.html) < <https://dupress.deloitte.com/dup-us-en/authors/r/doug-robinson.html> > , [Srini Subramanian](https://dupress.deloitte.com/dup-us-en/authors/s/srini-subramanian.html) < <https://dupress.deloitte.com/dup-us-en/authors/s/srini-subramanian.html> >

September 20, 2016

For state governments, many challenges of managing cyber risk—in both funding and talent—have persisted over the years. Yet states have also made progress, as governor-level awareness rises

and CISOs make strides in collaborating with other government agencies.

Foreword

Today, no one disputes that state governments need to be concerned with cyber risk. The 2016 Deloitte-NASCIO Cybersecurity Study shows that cyber risk has risen in importance in the eyes of governors and other state executives. For CIOs and CISOs, this governor-level attention is encouraging news and an opportunity to secure resources and support for state cybersecurity programs.

Given its current trajectory, cyber risk in state governments is unlikely to dissipate, and may even grow—largely a result of the increase in innovation and use of technology and data. State governments have rapidly adopted new technology to better serve constituents and reduce dependency on legacy systems that are difficult to maintain. Ironically, the very steps governments have taken to embrace these new innovations add to the cyber risks. This is why we need to begin viewing the management of cyber risk as a core function of running government operations.

Since 2010, Deloitte and NASCIO have been conducting biennial surveys of CISOs and state officials to explore how states are managing cyber risk. In our fourth survey to date, we found that even as the importance of cybersecurity has gained ascendancy, many of the issues CISOs are grappling with are stubbornly persistent. Following are some of the top takeaways from the 2016 survey:

Governor-level awareness is on the rise. The survey results indicate that governors and other state officials are receiving more frequent reports from CIOs/CISOs. Initiatives such as the National Governors Association (NGA) “Call to Action” seem to be helping to maintain the prominence of cybersecurity on executive agendas.

Cybersecurity is becoming part of the fabric of government operations. For the first time, all respondents report having an enterprise-level CISO position. The CISO role itself has become more consistent in terms of responsibilities and span of oversight. CISOs are also focusing their energies more on what they can control.

A formal strategy and better communications lead to greater command of resources . Securing sufficient resources—both funding and talent—remains a top challenge for CISOs. This year, we found evidence that states that take a proactive approach to strategy setting and communication are more likely to see improvements in funding and access to talent.

We believe that, overall, the survey results spell out a clear message for CISOs: **State leaders are paying attention. Take advantage of this focus to make substantial progress.**

Finally, we would like to thank participants in this year’s survey: the 49 CISOs who responded to the longer version of the survey—24 of whom were new to their role—and the 96 state officials who responded to the accompanying state officials survey. Your time and commitment will help states in their efforts to effectively manage

cyber risk and protect citizen data.

The authors of the survey,

Doug Robinson

Executive Director

NASCIO

Srini Subramanian

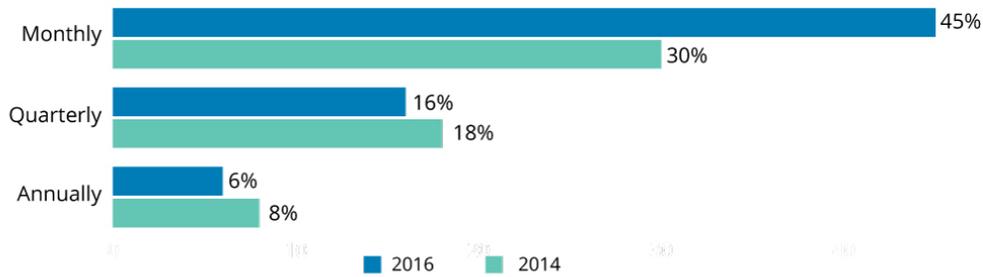
Principal

Deloitte & Touche LLP

Governor-level awareness is on the rise

The critical nature of cybersecurity has not been lost on governors and other state officials. The state officials survey this year shows that over 90 percent say that cybersecurity is important to their state, and over 94 percent say that it is important to their individual agency. Cybersecurity is also a more frequent topic of discussion at state executive leadership meetings (figure 1). More than three-fifths (61 percent) of state officials say that cybersecurity is discussed at executive leadership meetings at least quarterly, if not monthly, compared with less than half (48 percent) in 2014.

Figure 1. How often is the topic of cybersecurity presented or discussed at your agency/office executive leadership meetings?

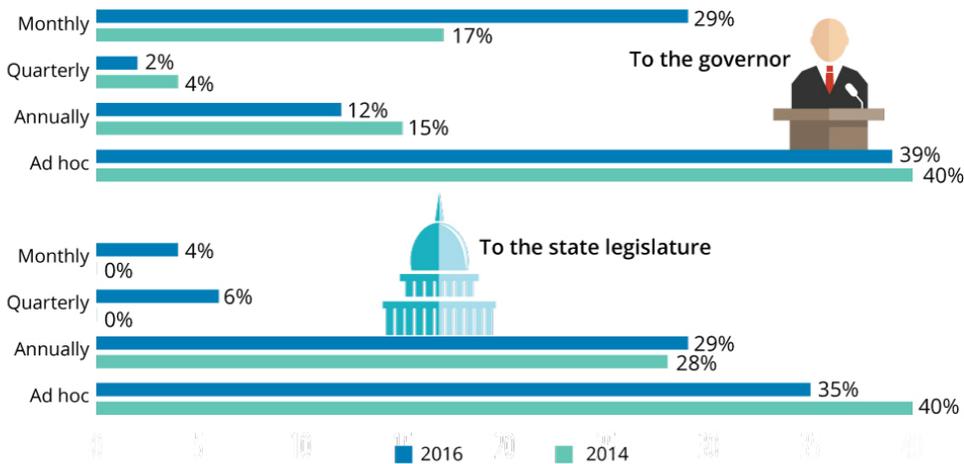


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Governors are receiving more frequent briefings on cybersecurity. Nearly a third (29 percent) of CISOs provide their governors with monthly reports on cybersecurity, compared with only 17 percent in 2014 (figure 2). However, this level of communication has not extended to state legislatures. Nearly a third of respondents say that they never communicate with their legislatures, unchanged from 2014. This is an important consideration, given the legislature’s role in appropriating funds.

Figure 2. To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

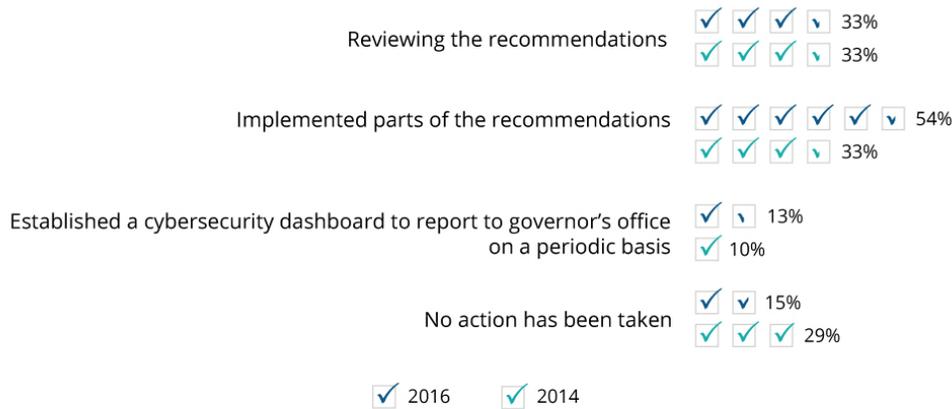
Graphic: Deloitte University Press | DUPress.com

Despite increased executive-level awareness of cybersecurity, there

remains a “confidence gap” in terms of how well CISOs versus state officials think security threats can be handled by their states. For instance, two-thirds (66 percent) of state officials say they are very or extremely confident that adequate measures are in place to protect information assets from externally originating cyber threats, compared with only a quarter (27 percent) of CISOs. These findings, which are similar to those from our 2014 study, indicate that CISOs may need to take a different approach when communicating the severity of cyber threats to state officials.

States are also starting to act and make progress in areas visible to governors. Since the NGA issued its “Act and Adjust: A Call to Action for Governors for Cybersecurity” in 2013, more than half (54 percent) of respondents say that they have implemented at least some of the NGA’s recommendations, compared with only a third (33 percent) in 2014 (figure 3). In fact, governors have launched initiatives ranging from state cyber academies and public-private partnerships to dashboards and preparedness and response plans. ¹

**Figure 3. How do you characterize your state's adoption of NGA's "Act and Adjust" report?
(select all that apply)**



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

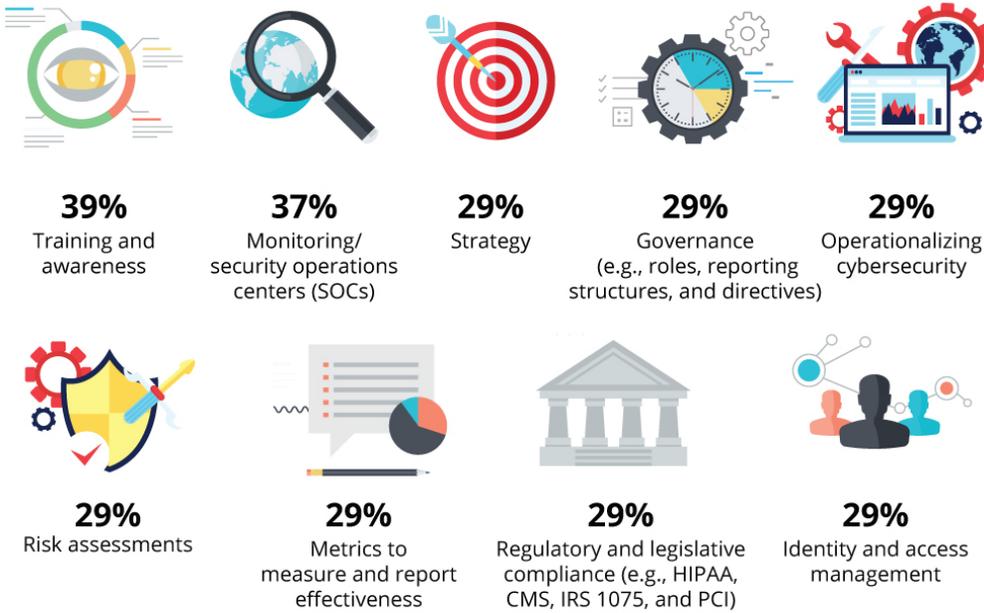
Graphic: Deloitte University Press | DUPress.com

See survey analysis section for more data. [Show more](#)

Cybersecurity is becoming part of the fabric of government operations

CISOs have begun to take a more programmatic approach to managing cyber risk and are starting to concentrate on areas that are in their control (figure 4). Only 45 percent of CISOs cited the "growing sophistication of threats" as a barrier to addressing cybersecurity challenges, down from 61 percent in 2014. CISOs are focusing on areas where they can take proactive steps to better manage risks. Some of the top areas CISOs say are within their purview include audit logs and security event monitoring, strategy and planning, and vulnerability management (figure 5).

Figure 4. Top cybersecurity initiatives for 2016



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 5. Top CISO functions

The survey respondents indicated that the top five functions within the scope of the CISO included:



*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The CISO role itself is now a well-established position in state government. For the first time, all respondents report having an enterprise-level CISO position, an indication that states consider protecting information assets—including citizen data—from cyber threats to be an important government responsibility. CISOs' responsibilities and top priorities have remained consistent over the past two years, a sign that the role is solidifying. This conclusion is

supported by the fact that some 50 percent (24 individuals) are new to the role—yet they say their responsibilities are the same as those who have held their position for several years.

In terms of priorities, three initiatives that made the top five—training and awareness (39 percent), monitoring and SOCs (37 percent), and strategy (29 percent)—were also among the top five in 2014 (figure 4).

The mechanisms by which CISOs’ authority over other organizational entities is established have not changed significantly since 2014. In addition, alignment of cybersecurity initiatives with business initiatives has increased, with 29 percent of respondents reporting appropriate alignment, versus only 14 percent in 2014. However, we continue to see CISOs have challenges in making progress on enterprise-wide initiatives in a largely federated model of governance with the agencies. For example, our results show challenges in operationalizing state-wide identity and access management (IAM) implementations. To overcome these challenges and help close the confidence gap that we continue to see, more will need to be done to elevate the authority and influence of the CISO role. CISOs need to improve communications around risks and metrics to better inform agency business executives and help promote their agendas.

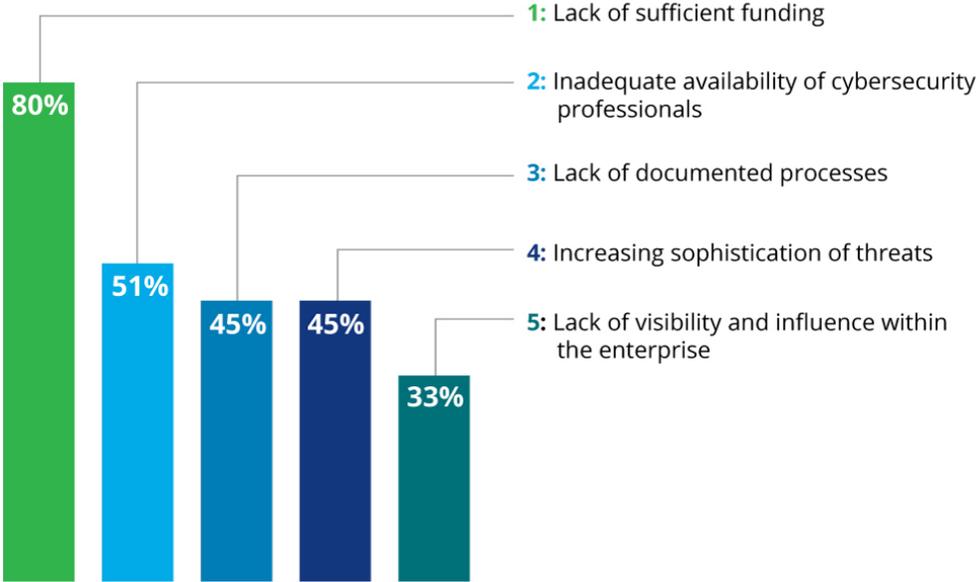
See survey analysis section for more data. [Show more](#)

A formal strategy can lead to more resources

Even as CISOs better define their roles and become an integral part of state government, they continue to face challenges, particularly in securing the resources they need to combat ever-evolving cybersecurity threats. Four-fifths (80 percent) of respondents say inadequate funding is one of the top barriers to effectively address cybersecurity threats, while more than half (51 percent) cite inadequate availability of cybersecurity professionals (figure 6).

Figure 6. Top five barriers in addressing cybersecurity challenges

Funding still remains at the top of the list, with cybersecurity professionals next in line.



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Survey evidence suggests that when CISOs develop and document strategies—and get those strategies approved—they can command greater budgets and attract or build staff with the necessary competencies. A direct correlation can be seen between having an established strategy and obtaining more full-time equivalents (FTEs) dedicated to cybersecurity, as well as year-over-year budget

increases (figure 7). For example, 11 out of 33 states that have an approved strategy also reported they have more than 15 FTEs dedicated to cybersecurity, and 16 out of 33 states with an approved strategy reported they also had an increase in budget. An approved and proactively communicated strategy can also help CISOs overcome another barrier: “lack of visibility and influence in the enterprise,” an ongoing challenge in the largely federated governance model in state government.

Figure 7. Intersection of approved strategy and resources

	More than 15 dedicated FTEs for cybersecurity	Staff has required competencies	Increase in budget	Cyber budget more than 2% of IT budget	Alignment of cyber and business programs
Approved strategy (33 states)	11 (33%)	16 (48%)	16 (48%)	10 (30%)	12 (36%)
No approved strategy (16 states)	1 (6%)	3 (19%)	5 (31%)	0 (0%)	2 (12%)

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

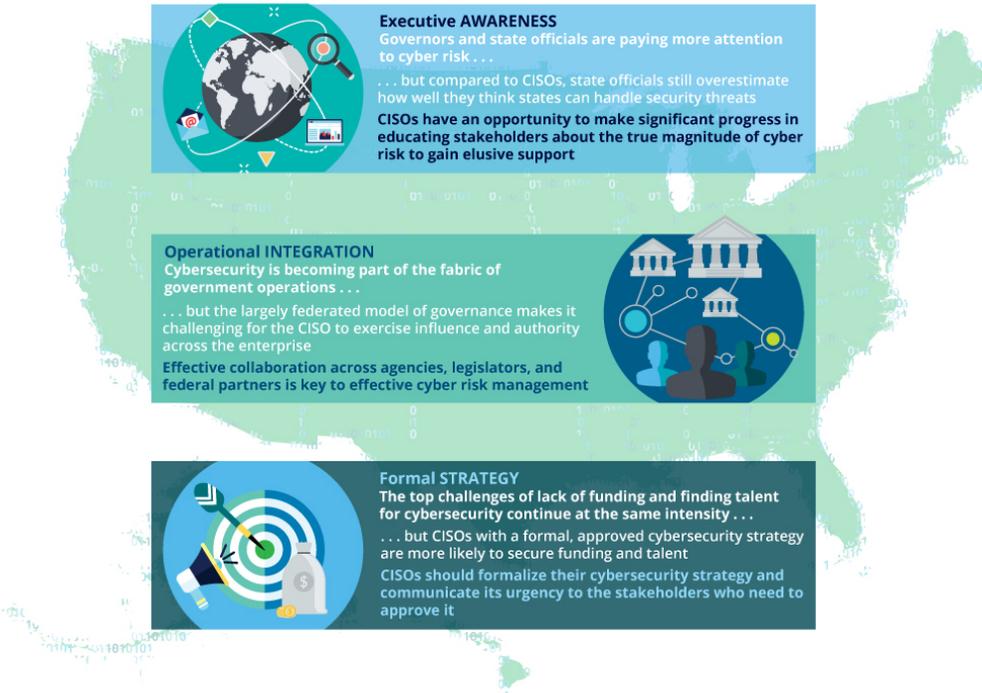
Graphic: Deloitte University Press | DUPress.com

See survey analysis section for more data.

[Show more](#)



Key takeaways overview



Survey data analysis

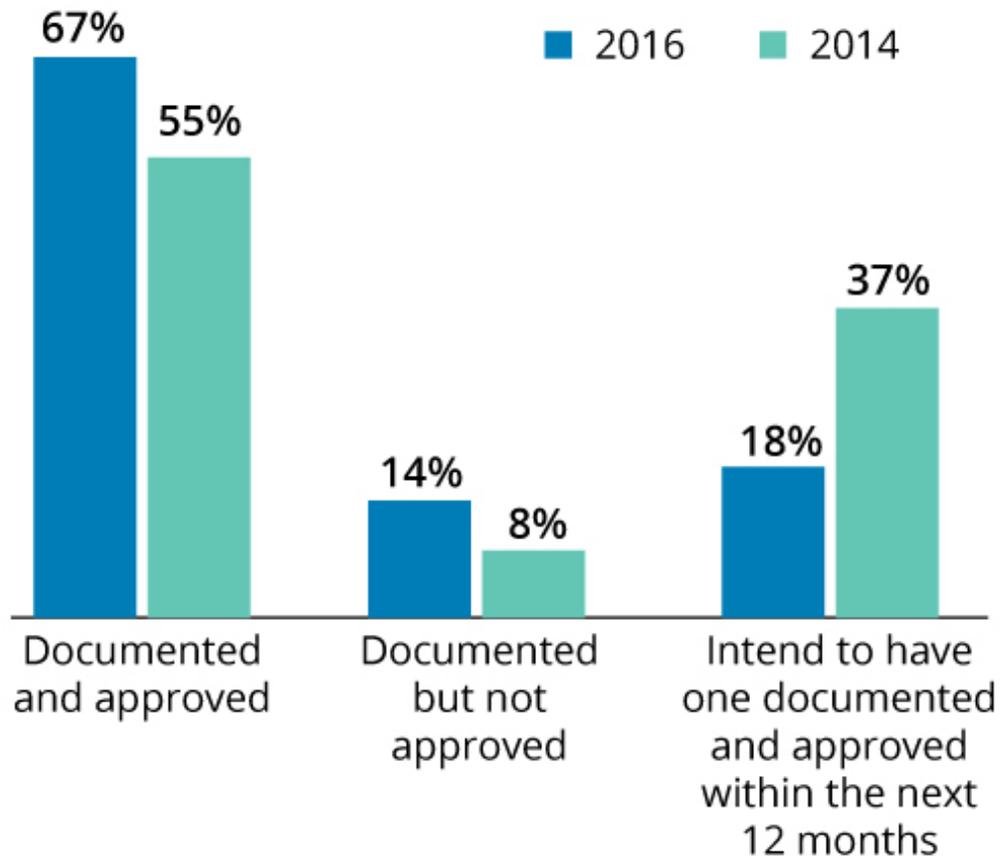
In the following section, we take a detailed look at the survey findings.

STRATEGY AND GOVERNANCE

Strategy is central to driving states' cybersecurity direction, which makes it especially important for CISOs to push for approval of their strategies. This year's survey shows that more CISOs are making

Figure 8. States' progress in maintaining cybersecurity strategy

States are making progress in getting their strategy approved. A third of the states continue to work on getting their strategy approved.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

progress in this regard: Two-thirds (67 percent) had cybersecurity strategies that were both documented and approved, compared with 55 percent in 2014 (figure 8). From a governance perspective, most states' security functions use a largely federated model of governance, which makes it even more important for CISOs to be effective in influencing agency business and technology stakeholders

and getting their buy-in for the strategy.

Strategies continue to involve both lines of business and technology decision makers; however, significant confidence gaps continue from the 2014 study, signifying that improvements need to be made in defining the priorities, risks, and strategies in place. A disconnect can also be seen between senior-level commitment and adequate funding (figure 9).

Collaboration across state lines and with federal agencies is also part of respondents' strategies, and it is an important means of sharing practices for addressing cybersecurity challenges (figure 10). This year, almost all respondents say that they are collaborating with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the United States Department of Homeland Security (DHS) fusion centers.

Figure 9. Senior executive support (governor's office, agency secretary, or CIO) for security projects to effectively address regulatory or legal requirements

State cybersecurity projects continue to have the appropriate level of executive commitment, but lack the required funding.

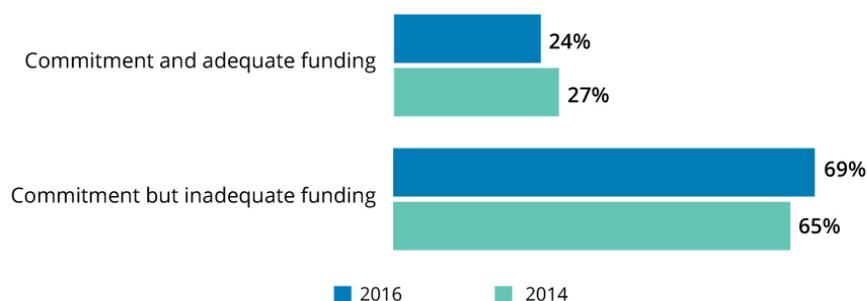
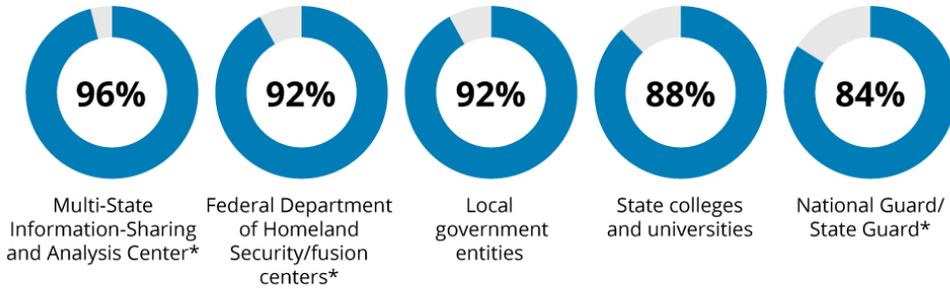


Figure 10. Collaboration trends as part of the states' cybersecurity program

Collaboration is becoming central to state government strategy. Increased collaboration is an area to watch as states establish their security operations centers.



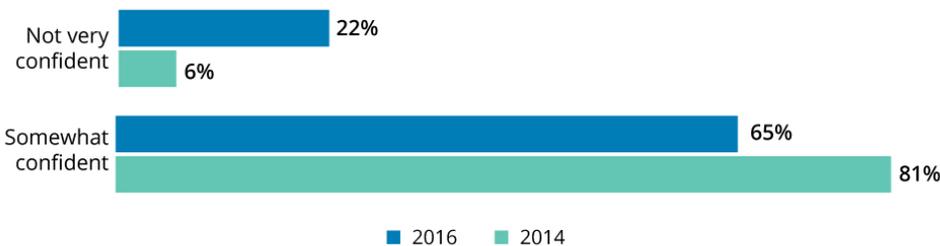
*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CISOs are expressing a growing concern about the security practices of third parties, including those of contractors, service providers, and business partners. Nearly a quarter (22 percent) of CISOs say they are not very confident in this regard (figure 11). CISOs indicate that addressing cybersecurity in the contract is their leading option for managing the cybersecurity practices of third-party organizations (figure 12).

Figure 11. CISOs' confidence levels in cybersecurity practices followed by third parties (contractors, service providers, business partners)

CISOs' confidence level in third-party security management practices continues to be a struggle.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 12. States' leading methods to manage adequacy of third-party (contractors, service providers, business partners, cybersecurity practices)

Ways to manage the adequacy of third-party cybersecurity practices (top five)	2016
Address cybersecurity issues in the contract	84%
Sign confidentiality and/or non-disclosure agreements	80%
Impose enterprise's cybersecurity policy and controls on third party	71%
Where allowed, perform background verification checks on select high-risk third-party employees	61%
Monitor and control third-party access to your systems and data	61%

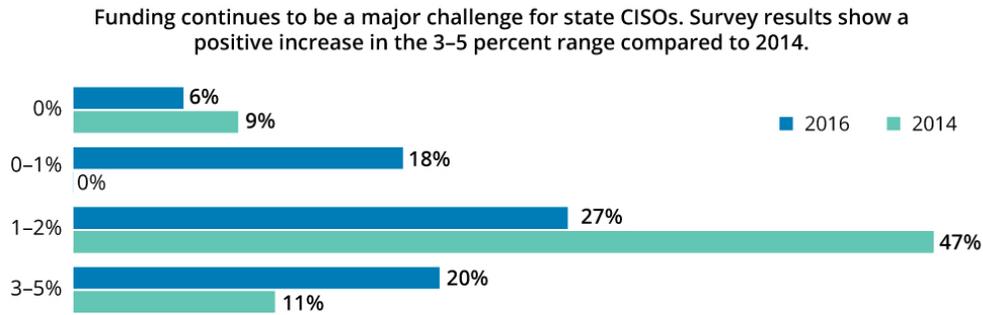
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

BUDGET AND FUNDING

Lack of sufficient funding remained the most significant challenge for CISOs in 2016. The majority of respondents continue to indicate that their cybersecurity budgets were only between 0–2 percent of their state’s overall IT budget (figure 13). The results did show an increase over 2014 in the 3–5 percent range of the state’s overall IT budget. From a year-over-year budget perspective, 33 percent of respondents note that their budgets have remained the same (figure 14). Of the 43 percent of respondents with an increase, most of them noted increases only in the 1–5 percent range. In contrast, the federal cybersecurity budget has seen an increase of 35 percent over the 2016-enacted level. ²

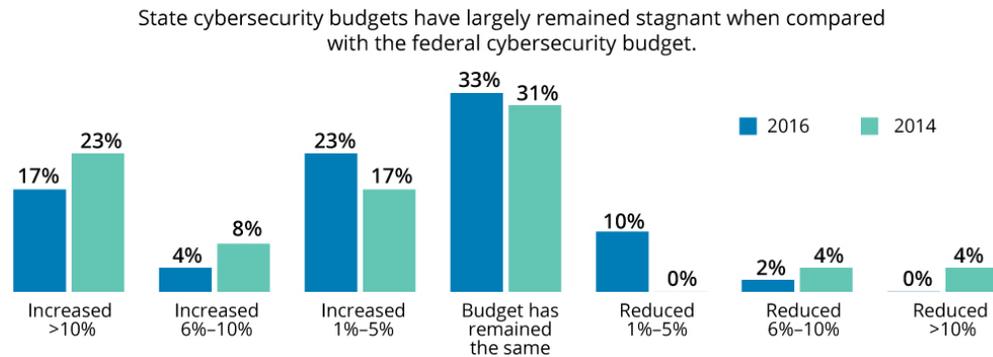
Figure 13. Percentage of state's cybersecurity allocation as part of the overall IT budget



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 14. Year-over-year trending of the state cybersecurity budget for the years 2014-2016



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Looking at the top items covered within a budget, this year's survey shows incident response as the most frequently cited (figure 15). Cybersecurity research and development and audit and certification costs moved up significantly from 2014.

Given cybersecurity's status as a national issue, states are able to tap into a range of state and federal programs and initiatives to secure additional funding (figure 16). Although limited, these are important avenues for CISOs as they build strategies to bridge the funding gap.

Figure 15. Areas covered under the cybersecurity budget

Since 2014, the top areas supported by the cybersecurity budget have changed. Logical access control, research and development, and audit/recertification have made their way into the top five.

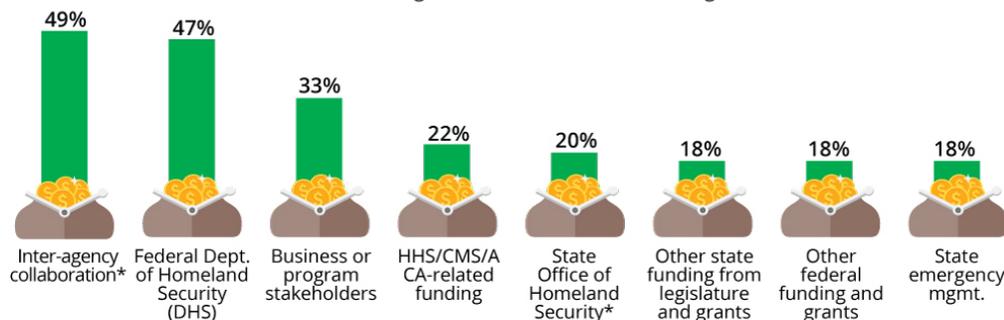
Top areas covered under the cybersecurity budget	2016	2014	Trend
Incident response	83%	69%	↑
Logical access control	79%	51%	↑
Compliance and risk management	69%	74%	↓
Cybersecurity research and development	57%	37%	↑
Audit or certification costs	48%	31%	↑
Infrastructure protection devices	40%	61%	↓
Awareness/communication costs	30%	78%	↓
Security consultants	26%	53%	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 16. Additional funding sources for cybersecurity initiatives

State CISOs have started looking at alternate sources of funding, both inside and outside their states. Inter-agency collaboration and the Department of Homeland Security are their leading sources of additional funding.



*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

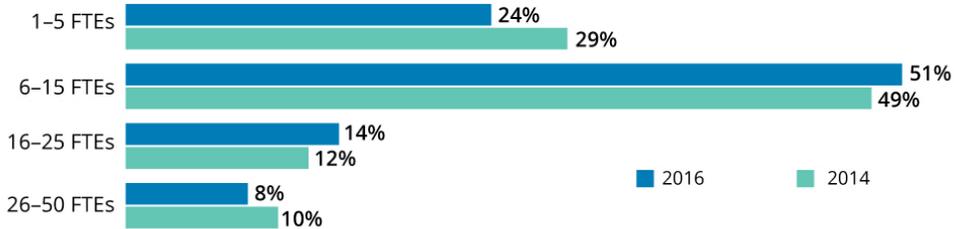
TALENT

In 2016, the cybersecurity talent crisis continues. Overall, the size of state cybersecurity staff moved up slightly, consistent with budgets (figure 17)—but not to the levels seen in the private sector or at federal agencies, which may have well over 100 FTEs handling cybersecurity. CISOs cite the inadequate availability of cybersecurity professionals as one of their biggest challenges, second only to

obtaining sufficient funding, and note salary and competition with the private sector as the top factors negatively impacting their workforce strategies (figure 18).

Figure 17. Dedicated cybersecurity professionals employed by the state's enterprise security office

The majority of states have enterprise cybersecurity teams of between 6 and 15 full-time equivalents (FTEs). Overall team size continues to show a small increase year over year.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

Figure 18. Top three human resources factors that negatively impact the CISO's ability to develop, support, and maintain cybersecurity workforce

State CISOs continue to identify inadequate availability of cybersecurity talent as a top barrier. The ability to attract and retain cybersecurity professionals is impacted by pay grade structures as well as by competition from the federal government and the private sector.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

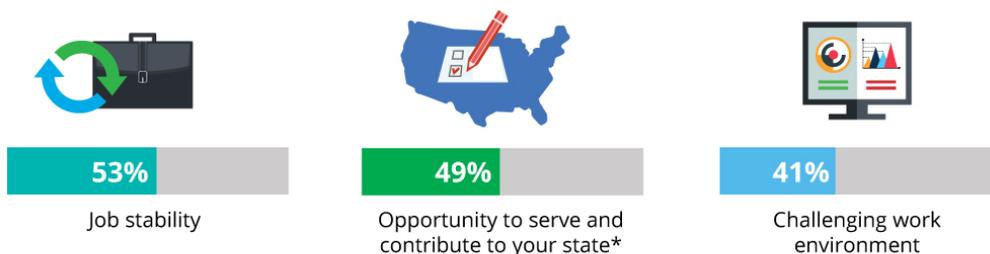
For many CISOs, their challenges are exacerbated by underfunded pension plans and budget constraints that have forced states to change retirement plans for those now entering the workforce. Attractive benefit plans, historically one of the “carrots” of a state government career, are no longer a given, and retirement packages are being restructured to more closely resemble those found in the private sector. ³ In addition, private sector salaries for information

security professionals have risen dramatically in recent years, making state government less competitive on the compensation side.

CISOs are therefore looking for other ways to win the hearts and minds of prospective employees. While more than half say that job stability is one of the top three ways to attract and retain cybersecurity talent, nearly as many point to the opportunity to serve as an important factor as well (figure 19). Promoting the potential to “give back” may be an especially effective way to attract Millennial talent, and should be built into talent acquisition plans.

Figure 19. Top three factors that CISOs employ to attract and retain cybersecurity talent

State CISOs are still grappling with the cybersecurity talent gap. Job stability, the opportunity to serve, and a challenging work environment are the top factors for attracting and retaining talent.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The majority of states (56 percent) see a gap in required competencies (figure 20). To close the cybersecurity competency gap, states are using a range of strategies, including providing training, enlisting outside specialists, and outsourcing certain functional areas (figure 21). Training and awareness, the top initiative reported by states in 2016, has improved since 2014, with more respondents saying that they train a broad range of employees,

from systems administrators and programmers to executives and those handling sensitive information (figure 22).

Figure 20. State internal cybersecurity professional competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements

The majority of states say their staff have gaps in cybersecurity competencies. Training, outsourcing, and staff augmentation are the leading ways that CISOs bridge the talent gap.



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 21. Top outsourced cybersecurity functions

States' leading outsourced functions continue to focus on threat management services.

Outsourced functions (top five)	2016	2014
Cyber threat risk assessments	54%	37%
Forensics/legal support	44%	39%
Cyber threat management and monitoring services	35%	37%
Vulnerability management	27%	18%
Audit log analysis and reports	23%	18%

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 22. Cybersecurity training trends for employees based on job role and function

States have made strides in increasing the breadth of security awareness training.

Provide required training to	Change from 2014 to 2016
Executives	↑
People handling sensitive information	↑
IT application developers and programmers	↑
System administrators	↑
IT infrastructure	↑
Business and program stakeholders	↑
General state workforce	↑
Third-party workforce (vendors, contractors, consultants, business partners)	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

EMERGING TRENDS

Figure 23. Top five barriers to an enterprise IAM approach

Barriers	2016
Complexity of integrating with legacy systems	67%
Competing or higher-priority initiatives*	57%
Decentralized environment of state	47%
Cost of implementation	39%
Inadequate funding to support enterprise deployment*	31%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Identity and access management (IAM)

More states in 2016 (47 percent) than in 2014 (33 percent) have an enterprise IAM solution that covers some or all of the agencies under the

governor’s jurisdiction. However, CISOs continue to face the same barriers to implementing enterprise IAM solutions, including the complexity of integrating with legacy systems, cost, competing or higher-priority initiatives, and the states’ decentralized IT environment (figure 23). Similar to 2014, CISOs are focusing on implementation of multifactor authentication, federated IAM, and privileged identity management solutions. Cloud-based IAM solutions and citizen identity proofing solutions follow closely as leading initiatives (figure 24).

Cyberthreats

Figure 24. States' current IAM initiatives

IAM initiatives	2016
Multifactor authentication	77%
Federated IAM for agency and third party*	48%
Privileged identity management solution	37%
Cloud-based IAM solution	27%
Citizen identity proofing solution*	15%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CISOs view threats targeted at employees—including phishing, pharming, social engineering, and ransomware—as likely to be the most prevalent in the coming year (figure 25). This

is a change from 2014, when attacks exploiting various vulnerabilities and foreign-sponsored espionage topped the list. CISOs continue to be “somewhat confident” in their states’ abilities to protect against cyberthreats (figure 26). They appear most confident in their ability to protect against internal threats and least confident when it comes to threats originating from emerging technologies.

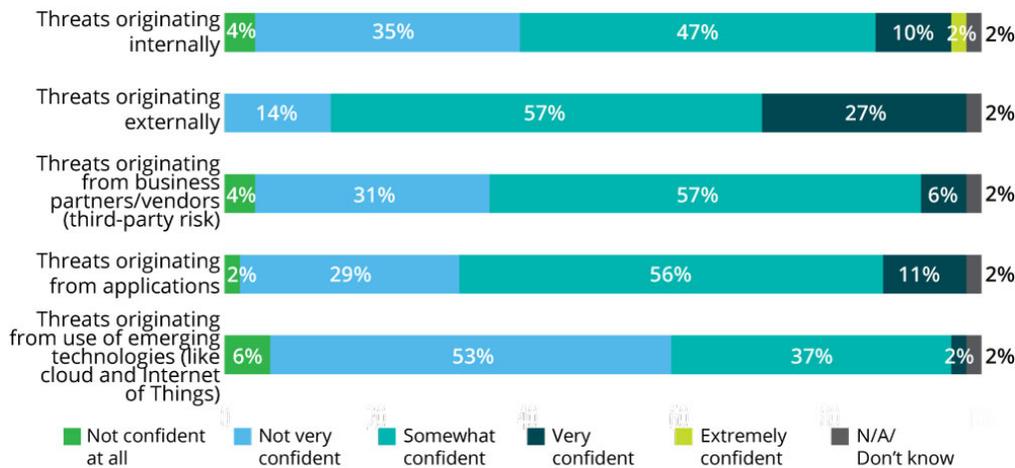
Figure 25. Prevalence of cyberthreats across state governments

	Somewhat higher threat	Very high threat
Phishing, pharming, and other related variants	35%	47%
Social engineering	31%	42%
Ransomware	43%	29%
Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)	51%	14%
Exploits of vulnerabilities from unsecured code	45%	8%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 26. CISOs' confidence levels in protecting their state's information assets from cyber threats



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Assessments

The majority of the states continue to perform ad-hoc assessments to evaluate their cybersecurity posture (figure 27). More frequent assessments could provide a better baseline for determining the effectiveness of cybersecurity controls.

Figure 27. Frequency of cybersecurity assessments

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc
Security code review	6%	2%	0%	8%	63%
Security risk assessment	0%	2%	2%	33%	54%
Internal penetration testing	17%	4%	4%	15%	52%
Application security vulnerability testing	13%	13%	2%	17%	50%
Cyber threat intelligence analytics	35%	2%	0%	2%	48%
External penetration testing	13%	2%	0%	29%	46%
Penetration testing conducted by third party	4%	6%	0%	33%	46%
Privacy impact assessment	0%	0%	2%	13%	44%
Cyber incident simulation or wargaming (to prepare for a cyberattack) and business continuity exercises	2%	6%	10%	33%	33%
Annual disaster recovery exercises and tests	2%	0%	10%	50%	29%
Security events monitoring/security operations center	60%	0%	0%	6%	23%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Cybersecurity technology adoption

More states have adopted traditional cybersecurity solutions, such as firewalls and antivirus software (figure 28). CISOs indicate that security compliance, network behavior analysis, data protection, and IAM solutions lead the next wave of enterprise adoption.

Figure 28. Top emerging technologies

		Plan to fully deploy or pilot within the next 12 months	Currently piloting	Fully deployed
Leading technologies being deployed or piloted in the next 12 months	Security compliance tools	52%	6%	21%
	Multifactor authentication	49%	14%	22%
	Federated identity management	38%	19%	19%
Leading technologies that are currently being piloted	Biometric technologies for user authentication	8%	25%	4%
	Network behavior analysis	29%	21%	27%
	Data loss prevention technology	37%	20%	25%
Leading technologies that are fully deployed	Firewalls	2%	0%	96%
	Antivirus	4%	0%	92%
	Spam filtering solutions	2%	2%	90%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Cyber legislation

Several state legislatures have been active in providing guidance to CISOs regarding implementation of cybersecurity measures—particularly in the areas of data breach reporting and notification. However, most states do not have established cybersecurity legislation in place (figure 29). More than a quarter (29 percent) of states have reported an increase in funding from legislation and grant sources.

Figure 29. Provisions of states' cyber legislation/statutes

	Established and funded	Established and not funded	In progress	Not in place
Cybersecurity incident/data breach reporting and handling	43%	21%	4%	32%
Data breach notification	41%	35%	2%	23%
Role and authority of the enterprise CISO or equivalent	40%	4%	2%	54%
Continuity of government/continuity of operations	35%	13%	4%	48%
Cybersecurity awareness	31%	4%	2%	63%
Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations	27%	21%	2%	50%
State-level cybersecurity program and framework for enterprise risk management	27%	17%	8%	48%
Cybersecurity budget allocation and review	26%	0%	4%	70%
Cyber threat information-sharing program between state agencies, law enforcement, and private entities	21%	10%	6%	63%
Public-private partnerships or council to support the state's cybersecurity programs	13%	2%	4%	81%
Cybersecurity workforce development and training	11%	4%	4%	81%
Cybersecurity legislative council or equivalent to do a periodic review, steer the state's cybersecurity posture, and allocate funding	11%	10%	6%	73%
Role and authority of the enterprise chief privacy officer (CPO) or equivalent	6%	2%	2%	90%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Moving forward

In the past two years, CISOs have moved their states forward in the fight against cyber risk. But the threat environment is so complex and evolving that many challenges remain. States faced with a myriad of priorities and ongoing resource constraints may be hard-pressed to allocate sufficient funding to cybersecurity initiatives. Competition for top talent can make it difficult to attract the professionals needed to effectively combat constantly evolving threats.

But CISOs do have one thing in their favor: State executives, including governors, are starting to pay more attention to the issue of cybersecurity. Those who are able to harness this attention have an opportunity to garner more resources and support for their initiatives. In order to make further progress, CISOs should think about the following:

- **Strategy** : Document and formalize the cybersecurity strategy. Going through the process of socializing the strategy with a broad range of stakeholders has a number of benefits. It ensures input from each of these parties, improving the overall strategy as a result. It strengthens collaborative relationships with other state agencies and departments. It raises awareness of cybersecurity issues. And finally, as our results have shown, it increases the chances of garnering more funding.
- **Funding** : Work with stakeholders to make cybersecurity a significant line item on state IT and business initiative budgets. For most states, cybersecurity is less than 2 percent of the overall IT budget. Cybersecurity is a business risk to state government, and funding should be commensurate with the risk.
- **Communications** : Use metrics and numbers to tell a compelling story about cyber risk. The fact that state officials are significantly more confident than CISOs about their states' ability to protect against cyber risk indicates that the right message still may not be getting across. State officials' lack of insight into the

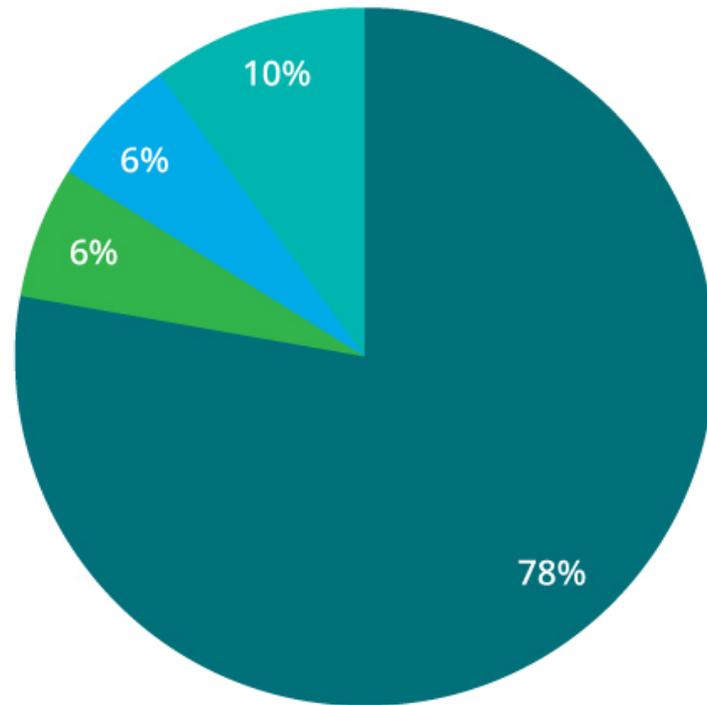
true business risks of cyberthreats could even affect funding. It is important for CISOs to step up the frequency of their communications—especially with agency business executives and legislators—and to communicate the risks more effectively.

- **Talent** : Promote the right benefits, modernize your workplace culture, and better define required skills to attract the right talent. The nature of what states have to offer workers has changed—which can be an advantage if positioned correctly. Millennials are not necessarily attracted by the promise of a secure retirement—something fewer states today are able to offer. Many of them find the prospect of “giving back” to be a more compelling reason to gravitate toward an employer. This, along with a rich training and development program, can serve as the basis for a campaign to recruit Millennial talent.

States should consider these components as they better define their strategy and look to create a higher level of awareness. These approaches can help CISOs continue their progress in combating cyber risks.

Appendix: Survey methodology

Figure 30. CISO survey respondent designation



- Enterprise CISO
- Acting or interim CISO
- Chief information officer
- Others

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CYBERSECURITY STUDY USES SURVEY RESPONSES FROM:

- US state enterprise-level CISOs, with additional input from state agency CISOs and security staff members

- US state (business) officials, using a survey designed to help characterize how the state government enterprise views, formulates, implements, and maintains its security programs

CISO PROFILE

CISO participants answered 59

questions designed to characterize the

enterprise-level

strategy, governance, and

operation of security programs.

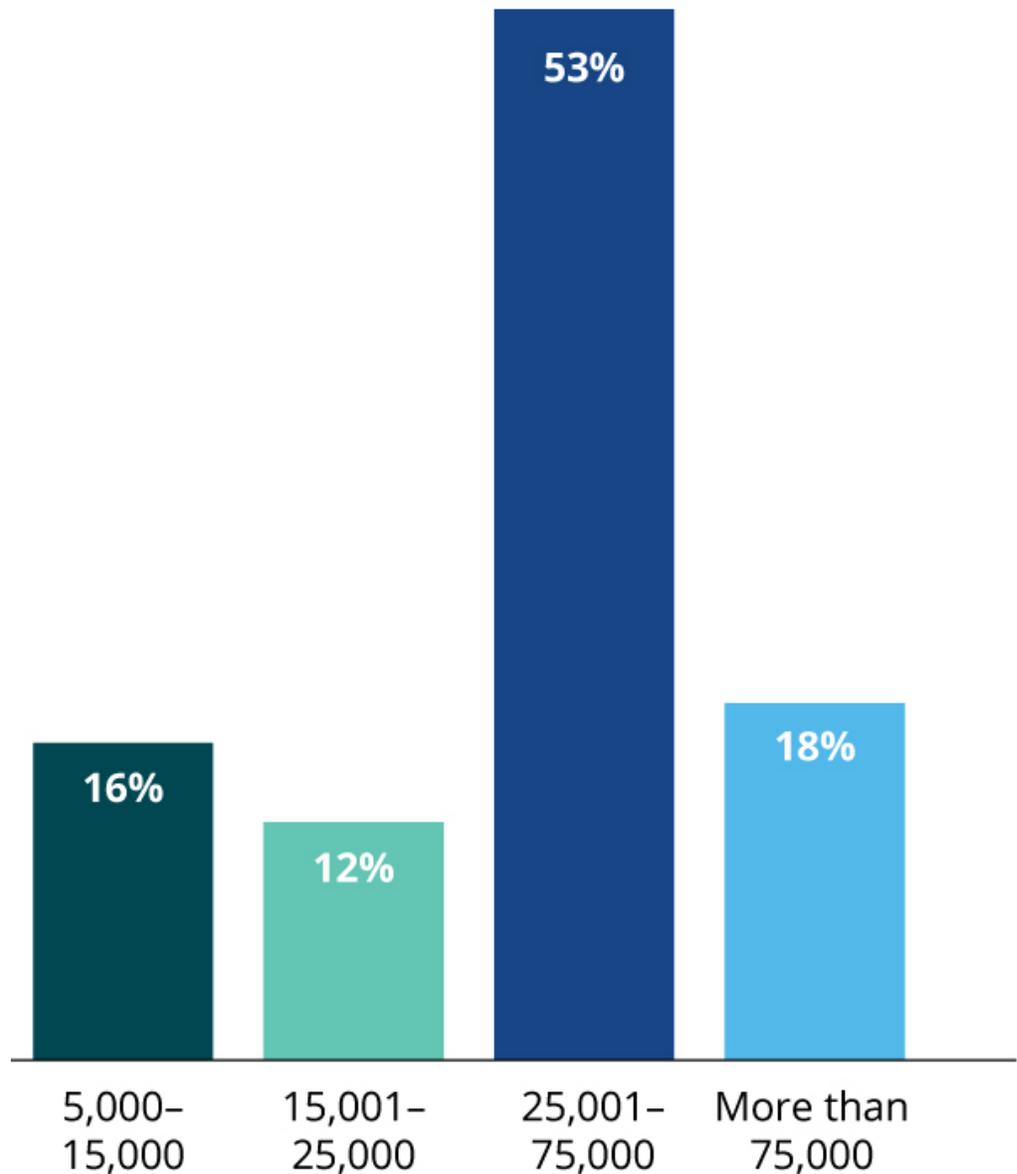
Participation was high:

Responses

were received

from 49

Figure 31. Number of government employees in your state (excluding higher education employees)



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

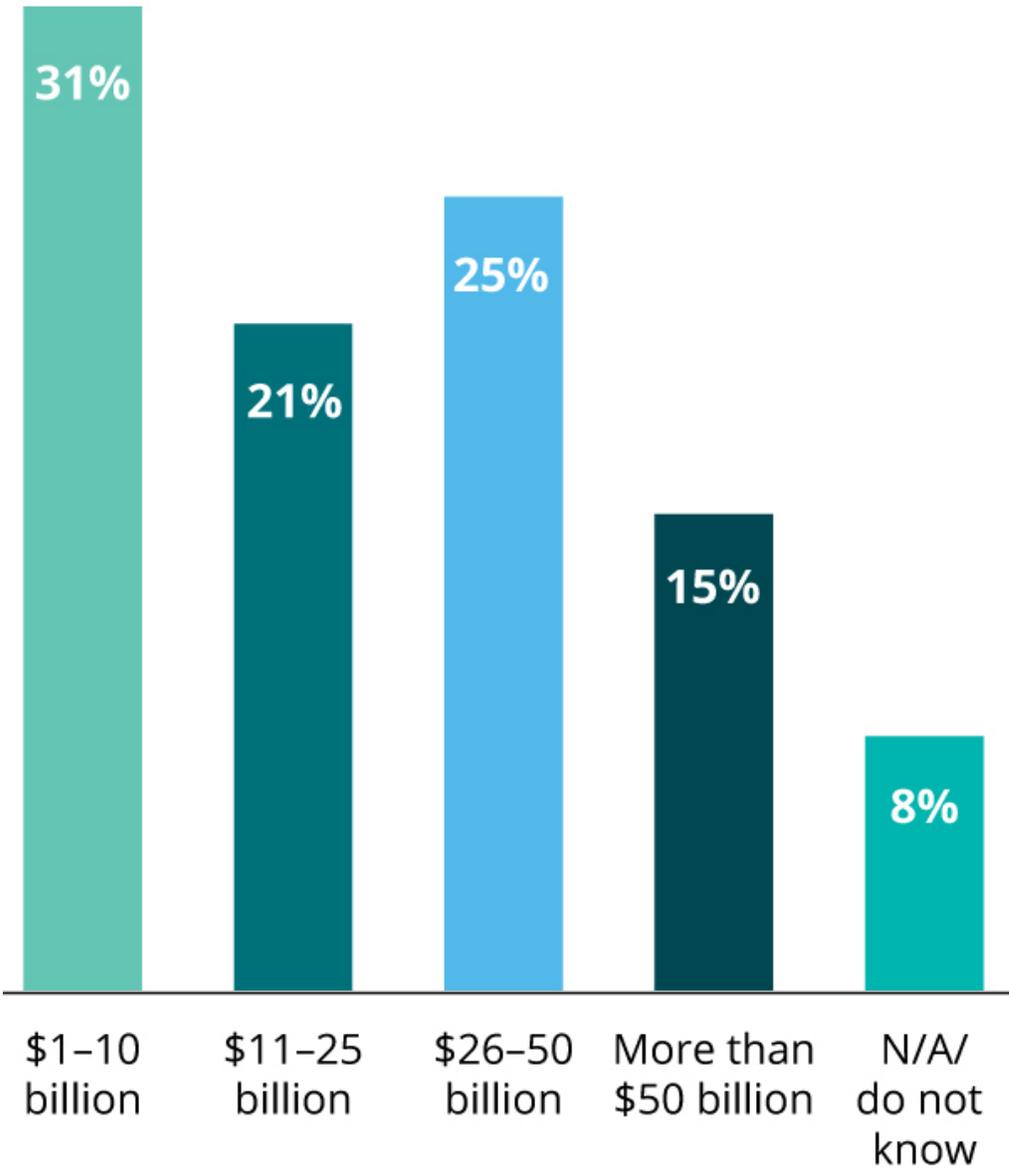
states and territories. Figures 30–32 illustrate the CISO participants' demographic profile.

STATE OFFICIAL PROFILE

Ninety-six state business and elected officials answered 15 questions, providing valuable insight into state business stakeholder perspectives. The participant affiliations included the following associations:

- National Association of State Budget Officers (NASBO)
- National Association of State Auditors, Comptrollers, and Treasurers (NASACT)
- National Association of Attorneys General (NAAG)
- National Association of Secretaries of State (NASS)
- National Association of State Personnel Executives (NASPE)
- National Association of State Chief Administrators (NASCA)
- National Association of State Procurement Officials (NASPO)
- National Association of Medicaid Directors (NAMD)
- National Emergency Management Association (NEMA)
- Federation of Tax Administrators (FTA)
- Governors Homeland Security Advisors Council (GHSAC)
- International Association of Chiefs of Police (IACP)—Division of State and Provincial Police (S&P)

Figure 32. Approximate annual budget of the respondent states (USD)



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The two surveys provided an opportunity for survey respondents to add additional comments when they wanted to further explain “N/A” or “other” responses. A number of participants provided such comments, offering further insight into the analysis.

HOW DELOITTE AND NASCIO DESIGNED, IMPLEMENTED, AND EVALUATED THE SURVEY

Deloitte and NASCIO collaborated to produce the 2016 Deloitte-NASCIO Cybersecurity Study. Working with NASCIO and several

Deloitte Insights: New name, same commitment to delivering insights that matter. [Learn more](#) ✕

questionnaire to probe key aspects of information security within state government. A CISO survey review team, consisting of the members of the NASCIO Cybersecurity Committee, evaluated the survey questions and assisted in further refining the survey questions.

In most cases, respondents completed the surveys using a secure online tool. Respondents were asked to answer questions to the best of their knowledge and had the option to skip a question if they did not feel comfortable answering it. Each participant's response is confidential, and any identifying information was deleted after the preparation of the survey reports.

The data collection and analysis was conducted by DeloitteDEX, Deloitte's proprietary survey and benchmarking service. Results of the survey have been analyzed according to industry-leading practices and reviewed by senior members of Deloitte's Cyber Risk Services practice, the Deloitte Center for Government Insights, and Deloitte's Technology and Human Capital practices. In some cases, in order to identify trends or unique themes, data were also compared to prior surveys and additional research. Results on some charts may not total 100 percent based on answer choices such as

“not applicable,” “do not know,” or “other.”

Due to the volume of questions, and for better readability, this document reports only the data points deemed to be most important at the aggregate level. A companion report, including all questions and benchmarked responses, has been provided individually to the state CISO survey respondents.

Credits

Written By: **Doug Robinson** < <https://dupress.deloitte.com/dup-us-en/authors/r/doug-robinson.html> > , **Srini Subramanian** < <https://dupress.deloitte.com/dup-us-en/authors/s/srini-subramanian.html> >

Acknowledgements

CONTRIBUTORS

We thank the NASCIO and Deloitte professionals who helped to develop the survey and execute, analyze, and create the report.

NASCIO

Doug Robinson, executive director

Meredith Ward, senior policy analyst

Members of the state CISO survey review team

Maria Thompson, State of North Carolina

Agnes Kirk, State of Washington

Marcos Vieyra, State of South Carolina

Erik Avakian, Commonwealth of Pennsylvania

Jim Edman, State of South Dakota

Elayne Starkey, State of Delaware

Deborah Blythe, State of Colorado

Deloitte subject matter specialist contributors

Bharane Balasubramanian, Deloitte & Touche LLP

Bill Eggers, Deloitte Services LP

Art Stephens, Deloitte Consulting LLP

Srini Subramanian, Deloitte & Touche LLP

John O’Leary, Deloitte Services LP

Peter Viechnicki, Deloitte Services LP

Mike Wyatt, Deloitte & Touche LLP

Deloitte survey team, data analysis, and benchmarks

Balaji Kannan, Deloitte & Touche LLP

Pankaj Kamleshkumar, Deloitte Support Services India Private Limited

Marketing

Annette Evans, Deloitte Services LP

Topics in this article

Cyber risk < <https://dupress.deloitte.com/dup-us-en/tags/cyber-risk.html> >
, **State Government** < <https://dupress.deloitte.com/dup-us-en/tags/state-government.html> > , **Public Sector** < <https://dupress.deloitte.com/dup-us-en/tags/public-sector.html> > , **Government** < <https://dupress.deloitte.com/dup-us-en/tags/government.html> >

Endnotes

- 1 National Governors Association, “Resource center for state cybersecurity,” <http://www.nga.org/cms/statecyber> <<http://www.nga.org/cms/statecyber>> , accessed September 10, 2016.

 - 2 ITDashboard.gov, <https://itdashboard.gov/> <<https://itdashboard.gov/>> ; The White House, *President’s IT budget for FY 2017*, https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf <https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf> .

 - 3 Steven Greenhouse, “Pension funds strained, states look at 401(k) plans,” New York Times, February 28, 2011, http://www.nytimes.com/2011/03/01/business/01pension.html?_r=0 <http://www.nytimes.com/2011/03/01/business/01pension.html?_r=0> .
-

© 2017. See [Terms of Use](https://www2.deloitte.com/us/en/legal/terms-of-use.html) <<https://www2.deloitte.com/us/en/legal/terms-of-use.html>> for more information.

Global Cyber Security Capacity Centre
Cyber Security Awareness Campaigns
“Why do they fail to change behavior?”
Draft Working Paper

July 2014



Global
Cyber Security
Capacity Centre

Global Cyber Security Capacity Centre: Draft Working Paper
Cyber Security Awareness Campaigns
Why do they fail to change behaviour?



Dr. Maria Bada

Global Cyber Security Capacity Centre,
University of Oxford

Professor Angela Sasse

Department of Computer Science
Science of Cyber Security Research Institute
University College London

July 2014

Contents

Abstract.....	4
1 Introduction	5
1.1 Scope and purpose.....	5
1.2 Structure of the paper.....	5
1.3 Audience.....	6
2 Theoretical Background	7
2.1. Theory of reasoned action	7
2.2. Theory of planned behaviour	7
2.3. Protection motivation theory.....	8
2.4. Self-efficacy	8
2.5. Expected utility hypothesis	8
3. Information Security Awareness Campaigns	10
4. Persuasion Techniques.....	12
4.1. Behaviour Change	12
4.2. Influence Strategies.....	12
4.3. Factors influencing change.....	14
4.3.1. Personal Factors.....	14
4.3.1.1. Security Fatigue.....	15
4.3.2. Social Factors	15
4.3.3. Environmental Factors	15
4.4. Fear.....	16
4.4.1. Fear as a persuasion approach	16
4.5. Control.....	16
5. Culture.....	18

5.1. Culture and Risk perception.....	19
6. Rewards and Punishments.....	20
7. Media-Framed Messages.....	21
8. Essential Components for a Campaign	22
9. Factors which lead to a Campaign’s failure.....	23
10. Case Studies	24
10.1. Cyber Security Awareness Campaigns in U.K.....	24
10.2. Cyber Security Awareness Campaigns in Australia	29
10.3. Cyber Security Awareness Campaigns in Canada	31
10.4. Cyber Security Awareness Campaigns in Africa.....	31
11. Conclusions	33
References	35

Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Dr. Maria Bada

Global Cyber Security Capacity Centre, University of Oxford, maria.bada@cs.ox.ac.uk

Professor Angela Sasse

Department of Computer Science, Science of Cyber Security Research Institute, University
College London, A.Sasse@cs.ucl.ac.uk

Abstract

The present paper focuses on Security Awareness Campaigns, trying to identify factors which potentially lead to failure of these in changing the information security behaviours of consumers and employees. Past and current efforts to improve information security practices have not had the desired effort. In this paper, we explain the challenges involved in improving information security behaviours. Changing behaviour requires more than giving information about risks and correct behaviours – firstly, the people must be able to understand and apply the advice, and secondly, they must be willing to do – and the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory). We review the suitability of persuasion techniques, including the widely used fear appeals. Essential components for an awareness campaign as well as factors which can lead to a campaign's failure are also discussed.

In order to enact change, the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be identified. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life. Finally, since the vast majority of behaviours are habitual, the change from existing habits to better information security habits requires support. Finally, we present examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1 Introduction

1.1 Scope and purpose

Governments and commercial organizations around the globe make extensive use of information and computing (ICT) systems, and need to keep them secure. To achieve this, they deploy technical security measures, and develop policies that specify 'correct' behaviour of employees, consumers and citizens. There is ample evidence that many people do not comply with specified behaviours - some because do not know the risks or the correct behaviour, but most people who do not comply know the correct behaviour when asked.

The primary purpose of security awareness is to influence the adoption of secure behaviours. In this report, we will identify first what behaviours help to deliver information security, and to what extent they are adopted. We will then examine existing approaches to change information security behaviours through awareness campaigns - what works, and what not, and why.

The aim of this paper is to take a first step towards understanding better the reason why changing information security behaviour is such a challenge. IT requires more than simply telling people what they should and should not do: they need first of all to accept that the information is relevant, secondly understand how they ought to do, and thirdly be willing to do this, in the face of many other demands. In order to enact change, the current sources of influence - whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be found. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life.

Finally: even when people are willing to change, the process of learning a new behaviour needs to be supported.

We discuss components for an awareness campaign as well as factors which can lead to a campaign's failure.

1.2 Structure of the paper

Section 2 of this paper reviews existing knowledge about behaviour and behaviour change in general. Models such as the theory of reasoned action, the theory of planned behaviour, protection motivation theory, as well as the importance of self-efficacy as a personal factor are being presented.

Section 3 reviews current information security awareness campaigns and their effectiveness. In section 4, we examine persuasion techniques used in past campaigns. Many campaign designers use fear to encourage people to adopt better practices. Psychological research findings show the importance of fear in attitude and / or behavior change Influence strategies. Also factors which influence change, such as personal, social and environmental factors, are described.

In Section 5 we consider the importance of cultural differences as a factor which influences or prohibits behavioural change. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient.

Section 6, discusses rewards and punishments as a method of influencing people in order to follow a desired behaviour. Section 7, presents the importance of message framing and their persuasiveness.

Section 8, summarises the essential components for a campaign, and section 9 presents the factors which can lead to a campaign's failure.

The last part of this paper, section 10, presents examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1.3 Audience

This paper is written primarily for experts on awareness campaigns, influence strategists as well as experts on education and training.

2 Theoretical Background

In order to change behaviour, there has to be a change in attitudes and intentions. These antecedents of behaviour change are key indices of a person's mental readiness for action and are described in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory).

2.1. Theory of reasoned action

The theory of reasoned action (Ajzen & Fishbein, 1980) proposes an internal decision mechanism in which the formation of intention of behavior is immediately preceding the same behavior and mediates between that and the impact of other variables. According to this theory, the psychological requirements of intended behavior are attitudes and perceived social norms.

Overall, the model supports a linear process in which changes in behavior and normative beliefs of an individual will ultimately affect the actual behavior. Perceived control, the sense one has that he/she can drive specific behavior has been found to affect the intention of behavior but also the real behavior.

2.2. Theory of planned behaviour

The theory of planned behaviour (TPB) was developed by Ajzen in 1988. The theory proposes a model which can measure how human actions are guided. It predicts the occurrence of a particular behaviour, provided that behaviour is intentional.

The theory was intended to explain all behaviours over which people have the ability to exert self-control. The key component to this model is behavioural intent. Behavioural intentions are influenced by the attitude about the likelihood that the behaviour will have the expected outcome and the subjective evaluation of the risks and benefits of that outcome.

The TPB states that behavioural achievement depends on both motivation (intention) and ability (behavioural control). It distinguishes between three types of beliefs - behavioural, normative, and control. The TPB is comprised of six constructs that collectively represent a person's actual control over the behaviour.

1. Attitudes - refer to the degree to which a person has a favourable or unfavourable evaluation of the behaviour of interest. It entails a consideration of the outcomes of performing the behaviour.
2. Behavioural intention - refers to the motivational factors that influence a given behaviour where the stronger the intention to perform the behaviour, the more likely the behaviour will be performed.
3. Subjective norms - refer to the belief about whether most people approve or disapprove of the behaviour. It relates to a person's beliefs about whether peers and people of importance to the person think he or she should engage in the behaviour.
4. Social norms - refer to the customary codes of behaviour in a group or people or larger cultural context. Social norms are considered normative, or standard, in a group of people.

5. Perceived power - refers to the perceived presence of factors that may facilitate or impede performance of a behaviour. Perceived power contributes to a person's perceived behavioural control over each of those factors.
6. Perceived behavioural control.

2.3. Protection motivation theory

Protection motivation theory was originally developed to explain the influence of fear invocations on attitudes and health behaviors (Rogers, 1975).

Protection motivation theory is organized around two cognitive processes: the process of threat assessment and the process of handling assessment.

Based on only one factor of protection motivation theory, vulnerability, we can say that many other factors prevent people to appreciate properly the possibilities of a result. It is important to note that the final threat assessments and handling reflections will react through measurements of intent and behavior.

2.4. Self-efficacy

According to theory of Self-efficacy (Bandura 1977), the adoption of a preventive health behavior, depends on three factors:

- the realization that the person is at risk,
- the expectation that behavior change will reduce this risk and
- the expectation that the person is capable enough to adopt preventive behavior or to refrain from risky health behavior.

It is not simply a matter of how capable is someone but how capable he/she considers to be. Bandura (1977), successfully showed that people with different levels of self-efficacy perceive the world differently. Individuals with a high sense of self-efficacy are generally of the opinion that they have absolute control over their lives. That their personal actions and decisions shape their lives. In contrast, individuals with low sense of self-efficacy feel that their lives do not depend on them.

Our beliefs about self-efficacy, affect the way we think and of course affect our emotional reactions.

2.5. Expected utility hypothesis

In economics, game theory, and decision theory the expected utility hypothesis refers to a hypothesis concerning people's preferences with regard to choices that have uncertain outcomes (gambles). This hypothesis states that if certain axioms are satisfied, the subjective value associated with a gamble by an individual is the statistical expectation of that individual's valuations of the outcomes of that gamble (Bernoulli, Daniel, 1954).

According to the expected utility approach, behavioural change can be explained because individuals perceive it as a 'useful' decision. In the presence of risky outcomes, a decision maker could use the expected value criterion as a rule of choice: higher expected value investments are simply the preferred ones. This hypothesis has proved useful to explain some popular choices

that seem to contradict the expected value criterion (which takes into account only the sizes of the pay-outs and the probabilities of occurrence), such as occur in the contexts of gambling and insurance.

3. Information Security Awareness Campaigns

There is a need to move from awareness to tangible behaviours. Governments and Organizations need to secure their information assets and systems, and develop policies that specify the expected, 'correct' behaviours for their employees. Governments encourage citizens to transact online – and dispense advice on how to do so. But there is ample evidence that major cyber events continue to occur (Kirlappos & Sasse, 2012, Kirlappos, Parkin, & Sasse, 2014). Training as conceived is not working. Caputo, et al., (2013) having spear phishing as an example showed that framing had no significant effect. The study suggested that effective embedded training must take into account not only framing and security experience but also perceived security support, information load, preferred notification method and more.

The fact is that people know the answer to awareness questions but they do not act accordingly to their real life (ISF, 2014, NIST, 2003). The Coventry, et al., report (2014, Government Office for Science, UK) proposes that it is essential for security and privacy practises to be designed into a system from the very beginning. A system difficult to use will eventually lead users to make mistakes and avoid it.

The primary purpose of security awareness is to render people amenable to change (Winkler, I. & Manke, S, 2013). Influence strategists need to identify vital behaviours, meaning behaviours which they wish to change before they start trying to change them. Equally important is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011).

Awareness is defined in NIST Special Publication 800-16 (Wilson and Hash, 2003) as follows: *“Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.*

Questions rise on what exactly is not working and the majority of security awareness campaigns cannot secure the human element. The most recent ISF report (2014), identifies the following reasons:

1. Solutions are not aligned to business risks
2. Neither progress nor value are measured
3. Incorrect assumptions are made about people and their motivations
4. Unrealistic expectations are set
5. The correct skills are not deployed
6. Awareness is just background noise

Persuasiveness of recommendations for health, among other things, is a function of assessing the cost of the recommended behaviour - such as money, time, effort and discomfort - and the reaction efficiency, defined as the probability that compliance with the recommendation will lead to the desired goal.

Various behavioural theories consider the cost and efficiency of a reaction and have independent effects on persuasion. Among health messages, more effective are those tailored to the

individual's needs (Simons-Morton, et. Al., 1997). However, even when the design of the message is taken into account, there is a big gap between the recognition of the threat and the manifestation of the desired behaviour at regular intervals. The attempt to change a certain behaviour is much more difficult when the person is bombarded by a large number of messages about certain issues.

Naturally, an individual who is faced with so many warnings and advice, may be tempted to abandon all efforts to protect himself, and not worry about any danger (Fisher & Rost, 1986). Threatening or intimidating messages are not particularly effective, for the reason that they increase the stress of the individual to such an extent that the individual may even be repulsed or deny the existence of any problem.

An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise. An awareness and training program can be effective, if the material is interesting and current. Any presentation that "feels" impersonal and so general as to apply to any audience, will be filed away as just another obligatory session (NIST, Wilson and Hash, 2003).

Briefly, a persuasive message must have four characteristics: First, it needs to attract attention, secondly, it must be understood, thirdly, it must relate to a matter worthy processing and fourthly, its contents will need to be stored and recalled easily from memory.

Research findings show that it is better to present the arguments on both sides. In that case the recipient is able to autonomously decide which of the two would believe. If only convinced by the arguments in favour of a view and then opposing arguments are presented, then it is likely that the initial convictions falter and weaken.

Findings of studies on persuasion, highlighted the existence of an important phenomenon, called "retardant effect of persuasion", which refers to persuasion brought about the desired results after a long time later. This phenomenon occurs when the initial belief of a message is changing, and the recipient cannot remember what caused the change (Cook & Flay, 1978).

4. Persuasion Techniques

4.1. Behaviour Change

Persuasion can be defined as an “*Attempt to change attitudes or behaviors or both (without using coercion or deception)*” (Fogg, 2002). There are basically two ways of thinking about changing behaviour (Dolan, et al., MINDSPACE, 2010). The first is based on influencing what people consciously think about, rational or cognitive model. This model suggests that citizens and consumers will analyse the various pieces of information from various sources, the numerous incentives offered to them and act in their best interests. The second model of shaping behaviour focuses on the more automatic processes of judgment and influence. This shifts the focus of attention away from facts and information, and towards altering the context within which people act, the context model. The context model recognises that people are sometimes seemingly irrational and inconsistent in their choices, often because they are influenced by surrounding factors. It focuses more on ‘changing behaviour without changing minds’. This route has received rather less attention from researchers and policymakers.

Three factors are particularly useful for understanding controversy around behaviour change (Dolan, et al., MINDSPACE, 2010).

1. **Who the policy affects.** Any behaviour change that will affect a group in particular is likely to require careful justification—there may be particular controversy if the behaviour concerned is seen as integral to a group’s identity or culture.
2. **What type of behaviour is intended.** If the harm is seen to be more distant from the individual, it may be seen as a less pressing case for changing behaviour. Making the desired behaviour change clear, salient and justified can balance out people’s tendency to care less about “distant” harms. The availability and prestige of evidence and experience may be crucial factors in doing so.
3. **How the change will be accomplished.** MINDSPACE effects depend at least partly on automatic influences on behaviour. This means that citizens may not fully realise that their behaviour is being changed – or, at least, how it is being changed.

4.2. Influence Strategies

Messages which are most concerned on persuading us, are found in advertising, public relations and advocacy. These “persuaders” use a variety of techniques to grab our attention, to establish credibility and trust, to stimulate desire for the product or policy, and to motivate us to act (buy, vote, give money, etc.).

We call these techniques the “language of persuasion”.¹ They’re not new. Aristotle wrote about persuasion techniques more than 2000 years ago, and they’ve been used by speakers, writers, and media makers for even longer than that. The basic persuasion techniques include:

- Fear

¹ Media Literacy Project, Language of Persuasion, Retrieved from <http://medialiteracyproject.org/language-persuasion>

- Association
- Beautiful people (a way to attract attention)
- Experts
- Explicit claims (So are specific, measurable promises about quality, effectiveness, or reliability)
- Humour
- Intensity (comparatives, exaggeration)
- Testimonial
- Repetition

Intermediate persuasion techniques include:

- Nostalgia
- Rhetorical questions
- Scientific evidence
- Symbols. Symbols are words or images that bring to mind some larger concept, usually one with strong emotional content

Advanced persuasion techniques include:

- Analogy (an analogy compares one situation with another)
- Denial
- Group dynamics
- Majority belief
- Scapegoating
- Timing (Sophisticated ad campaigns commonly roll out carefully-timed phases to grab our attention, stimulate desire, and generate a response).

Clearly, lecturing and other attempts at verbal persuasion haven't managed to effect all of the change we need. Usually, single-source strategies are rarely the answer to complex problems (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

People do not just follow advice or instructions even if they come from a person of authority. Especially, security education is a field that requires background and experience in the varied subject areas within the security environment that are only accomplished through learning over time (Roper et al., 2006).

In many of the cases listed above, end users do know about the dangers. Security experts have warned them, confused them, and filled them with fear, uncertainty and doubt. People base their conscious decisions on whether they have the ability to do what is required and whether the effort will be worth it².

² Robinson A., The SANS Institute, 2013. <https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385>

4.3. Factors influencing change

The increased availability of information has significant effects, most of them positive. But providing information per se often has surprisingly modest and sometimes unintended impacts when it attempts to change individuals' behaviour (Dolan, et al., MINDSPACE, 2010).

A considerable amount of money is being spent by Governments on influencing behaviour, and the success in doing so will be maximised if they draw on robust evidence of how people actually behave. Dolan et al., (MINDSPACE, 2010) outline nine robust influences on human behaviour and change.

1. **Messenger** (who communicates information)
2. **Incentives** (our responses to incentives are shaped by predictable mental short cuts, such as strongly avoiding losses)
3. **Norms** (what others do strongly influences us)
4. **Defaults** (we follow pre-set options)
5. **Salience** (what is relevant to us draws our attention)
6. **Priming** (our acts are often influenced by sub-conscious cues)
7. **Affect** (emotional associations can powerfully shape our actions)
8. **Commitments** (we seek to be consistent with our public promises, and reciprocate acts)
9. **Ego** (we act in ways that make us feel better about ourselves)

To really enact change, we must find the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

Personal motivations refer to feelings associated with an action, while social motivations come from peer pressure and interactions with others in a group. Environmental motivations can be coming either from the physical environment or the ways the culture of an organization rewards and punishes certain activities (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

4.3.1. Personal Factors

The individuals and their knowledge, skills and understanding of cybersecurity as well as their experiences, perceptions, attitudes and beliefs are the main influencers on behaviour (Coventry, et al., 2014, Government Office for Science, UK). Personal motivation and personal ability, are the most powerful sources of influence (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). Awareness professionals can tap into the source of motivation by linking people's actions to their values. By giving people an image of their best selves, and showing them how to stay true to that image, enacting "secure" behaviours can be made inherently satisfying (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). When values align with actions, people are more excited to work and be more productive (Meyerson, 2011).

In many cases, people will have to overcome existing patterns in order to form new habits. If asked, the conscious mind will invent stories to rationalize these things that the unconscious mind is telling them to do (Hogan, 2005). The desire to behave consistently will drive people to honour a previous commitment to an ideal or an activity (Cialdini, 2009). As users begin to think of themselves as people who are security-conscious, they then begin to act in accordance with this image.

In many cases, these behavioural changes can lead to attitudinal changes. In order people to change their behaviour they have to start by doing something (Hogan, 2005). If a security practitioner is trying to sell an idea or a behaviour, then first he has to present users with a more difficult, more unpleasant or more expensive behaviour.

Changing the emotion associated with an activity is a powerful way to motivate this change in behaviour (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). “Vicarious experience”, using vivid stories that allow the listener to become a participant by identifying with the characters, is a powerful technique for affecting this emotional change (Hogan, 2005).

4.3.1.1. Security Fatigue³

People can sometimes get tired of security procedures and processes, especially if the perception is that security is an obstacle, disturbing them all the time. It can also be stressful to remain at a high level of vigilance and security awareness. These feelings can be a sign of Security Fatigue and they can be hazardous to the overall health of an organization or society.

In the security world there is something called the Security vs. Usability Triangle. The basic premise behind the triangle is that you are trying to create a balance between security and usability. If the triangle leans too far in either direction, then this can lead to a super secure system that no one can use, or an insecure system that everyone can use, even hackers. Therefore, there has to be a balance. Security fatigue becomes an issue when the triangle swings too far to the security side.

If security fatigue sets in at an organizational level, it could cause users and administrators to become lax and could open up the doorways for hackers and malicious social engineers.

4.3.2. Social Factors

Another powerful influence source available to security awareness professionals is peer pressure. The majority of people will conform to the social norm. Leadership is a key component of security culture (Coventry, et al., 2014, Government Office for Science, UK). Influential leaders derive their power from four perceptions (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008):

- They are knowledgeable and continue learning
- They have others’ best interests at heart
- They are generous with their time and well connected
- They speak their minds directly

4.3.3. Environmental Factors

To change behaviour, the easiest thing to do may often be to change the environment and make the desired behaviour easier to achieve. Environmental influencers reflect the design of the

³ O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from:
<http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm>

environment, the physical environment such as the workplace, and the technology, but also the economic factors (Coventry, et al., 2014, Government Office for Science, UK).

4.4. Fear

A meta-analysis (Sutton, 1982) research conducted on communication invoking fear held between 1953 and 1980, showed that increases in perceived level of fear led to increases in the acceptance of the proposed adjustment or behavioural intention.

4.4.1. Fear as a persuasion approach

The invocation of fear is "*a persuasive message designed to scare the world, describing the terrible things that will happen if they do not do what the message recommends*» (Witte, 1992). Surveys have shown that fear can be a quite persuasive tactic to specific situations or counterproductive tactic in other (Ahluwalia, 2000). Psychological research findings show the importance of fear in attitude and / or behaviour change (Levanthal, 1970; Girandola, 2000).

Various theoretical approaches have been used to explain the effect of fear persuasion e.g. The Drive Model-Janis, (1967), The Parallel Reaction Model (Levanthal, 1970) and the Protection Motivation Theory (Rogers, 1975; 1983).

Culturally sensitive interventions have been found to cause more effective changes in behaviour in high-risk populations, such as adolescents. This finding suggests that interventions based on major theoretical knowledge to change behaviour (e.g., social learning theory or the theory of self-efficacy) take into account the cultural beliefs and attitudes, and are more likely to succeed (Arthur, Quester, 2004).

O'Keefe (1990), makes an important distinction between the two definitions of fear invocations (message content - public reactions) and he notes that messages with horrible content may not cause fear and that fear may be caused without frightening contents. However, the majority of research on invoking fear have combined both definitions to handle fear invocations.

When researchers refer to a strong condition of fear invocation, usually they mean that the message represents a big threat and the recipient perceived a big threat. Typically, the invocations of fear offer recommendations that are as efficacious in preventing the threat. Thus, the three central structures in fear invocations is fear, threat and efficacy.

4.5. Control

"Perceived Control" is a core construct that can be considered as an aspect of empowerment (Eklund, & Backstrom, 2006). It refers to the amount of control that people feel they have, as opposed to the amount of "Actual Control" that they have. In contrast, "Vicarious Control" and "Vicarious Perceived Control" refer to the amount of control that outside entities have over the subject.

The positive effects of perceived control mainly appear in situations where the individual can improve its condition through its own efforts. Also, the greater the actual threat, the greater the

value that perceived control can play. When we apply this theory to information security, we could assume that home computer users often experience high levels of actual control over their risk exposure. They can choose which websites to visit, whether to open email attachments and whether to apply system updates. In contrast, employees in big organisations, lack the sense of control, since IT experts control every aspect of security (More Josh, 2011).

Ajzen (2002), introduced a new concept concerning the relationship between self-efficacy and perceived behavioral control. He argued that "*the central concept of perceived behavioral control consists of two factors: self-efficacy (on the ease / difficulty of performing a behavior) and the ability to control (the extent to which performance depends entirely on the person).*"

5. Culture

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004).

The role of culture in the persuasion process is until now under research. How can cultural factors impact the persuasion process? Is persuasiveness of a message determined by the cultural background of the message recipient and its framing in order to be congruent with culturally divergent motivational styles?

Cultural systems shape a variety of psychological processes. Motivational orientation is one potential process behind cultural differences. Messages that match regulatory focus can “feel right” and this feeling leads us to an evaluation of the content of the message, which increases persuasiveness (Uskul, A. et. al., 2009).

Messages are more persuasive when there is a match between the recipient’s cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual’s ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

The Regulatory focus theory (Higgins, 1998), proposes that in a promotion-focused mode of self-regulation, individuals’ behaviours are guided by a need for nurturance, the desire to bring one’s actual self into alignment with one’s ideal self, and the striving to attain gains. In a prevention-focused mode of self-regulation individual’s behaviours are guided by a need of security, the need to align one’s actual self with one’s ought self by fulfilling one’s duties and obligations and the striving to ensure non-losses.

The values that distinguish country cultures from each other could be categorised into four groups (Hofstede et al., 2010)⁴. The Hofstede dimensions of national culture are a) Power Distance (PDI) b) Individualism versus Collectivism (IDV) c) Masculinity versus Femininity (MAS) and d) Uncertainty Avoidance (UAI). Culture can be only used meaningfully by comparison. The forces that cause cultures to shift tend to be global or continent-wide. This means that they affect many countries at the same time, so if their cultures shift, they shift together and their relative positions remain the same. Exceptions to this rule are failed states and societies in which the levels of wealth and education increase very rapidly.

In Western more individualistic cultures, people tend to define themselves in terms of their internal attributes such as goals, preferences and attitudes. Individuals tend to focus on their personal achievements and tend to favour promotion over prevention strategies focusing on positive outcomes that they hope to approach, rather than the negative outcomes they hope to avoid (Lockwood, Marshall, & Sadler, 2005). Providing messages that fit the dominant regulatory focus of individuals may lead to a “feeling right” experience and thus to an increased persuasion (Cesario et al., 2004).

⁴ <http://geert-hofstede.com/national-culture.html>

In Eastern more collectivist cultures, individuals tend to define themselves in terms of their relationships and social group memberships (Triandis, 1989). In this cultural context, individuals tend to avoid behaviours that cause social disruptions and they favour prevention over promotion strategies focusing on the negative outcomes which they hope to avoid rather than the positive outcomes they hope to approach (Lockwood et al., 2005).

5.1. Culture and Risk perception

Risk perception refers to people's responses to questions regarding the riskiness of their decisions and actions (Weber E. & Hsee Ch., 2000). Perception of risk can be a collective phenomenon (Douglas, M., & Wildavsky, A., 1982). Each culture selects some risks for attention and chooses to ignore others.

Cultural differences in risk perceptions are explained in terms of their contribution to maintaining a particular way of life. There are different patterns of interpersonal relationships such as archical, individualist, egalitarian, fatalist and hermitic. Risk is also seen as the other side of trust and confidence, as the result of the way in which the theory see risk perception as being imbedded in social relations (Douglas, M., & Wildavsky, A., 1982).

6. Rewards and Punishments

Rewards and punishments can be used in order to influence people follow a desired behaviour. Both rewards and punishments, however, can have unintended consequences⁵. Rewarding people for an activity that they already enjoy makes that activity less desirable, while the receiver of the reward begins to question the intrinsic value of the activity (Kohn, 1994). Even honouring certain employees that follow the new standards may backfire, causing others to feel resentful (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

This process is called, "Incentivized Awareness Programs" (Winkler & Manke, 2013)⁶. That better represents what we are talking about, as a comprehensive awareness program does not limit itself to a single tool. With incentivized awareness (Gamification), you create a reward structure that incentivizes people to exercise the desired behaviours, which could include seeking out additional training. The incentives ideally make demonstrating or learning about awareness behaviours fun.

Rewarding people for doing the right behaviours makes them more security conscious. In general, extrinsic rewards should not be the first strategy. They could be used them only in conjunction with motivational strategies that encourage intrinsic satisfaction and social support (Kohn, 1994). Short-term goals need to be created and small improvements in those vital behaviours can be celebrated.

Economists argue that we are more inclined to avoid actual loss than to strive for conditional benefits. This tendency is called loss aversion and it refers to not setting the stakes too high.

⁵ Robinson A., Using influence strategies to improve security awareness programs, The SANS Institute, 2013.
Retrieved from: <https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385>

⁶ Winkler & Manke (2013).

1. 7. Media-Framed Messages

Media constructions often serve as a heuristic for citizens, whose understanding of issues is powerfully shaped by the values involved (Domke D. et al., 1998). Prevention messages typically try to convey either the benefits of performing a behaviour (gain-framed messages) or the costs associated with failing to perform a health-promoting behaviour. Gain-framed messages are usually more persuasive when they are used to promote prevention behaviours. Messages which are congruent with a person's predominant motivational orientation are more effective than messages that are not congruent.

Most studies on framing have compared the persuasive power of messages emphasizing the benefits of performing a behaviour, to messages highlighting the cost of not performing a behaviour (similar framing effects). The distinction between positive and negative messages, with respect to either the presence or absence of pleasant or unpleasant results seem to be a useful conceptual tool for studying the role of pre-existing perceptions about safety issues. Broemer, P. (2002), states that the framework would be relevant even when given only negative results.

2. 8. Essential Components for a Campaign

In order a Campaign to be successful, there are several essential components which need to be taken into consideration (Winkler Ira and Manke Samantha, 2013)⁷.

1. **Communication.** A significant part of a campaign is communication. This can be accomplished by collateral, internally distributed materials. These are things like newsletters, blogs, and other internal communications. Also, posters are a very crucial method of raising awareness. While some people believe they are old-fashioned and outdated, they can be very effective when they are well designed.
2. **Computer Based Training.** CBT is the most omnipresent component of security awareness programs, as it is the most clearly accepted method of achieving compliance.
3. **Events.** Well-executed events bring the Security Awareness program, and the whole security effort for that matter, to life.
4. **Security Portal.** An internal security portal provides several functions. It provides a Knowledge base that can provide a huge return on investment with includes information on security related topics. It is also important to include information on home and personal security strategies, such as protecting children online and securing social media accounts.
5. **Behavioural Testing and Teachable Moments.** Phishing, USB drive drops, and Social Engineering tests require some care, but are important components to give your employees a "teachable moment."
6. **Teaching New Skills Effectively.** What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). As teachers, security awareness professionals must break down complex goals in short, clear achievable steps.

⁷ Winkler & Manke (2013).

3. 9. Factors which lead to a Campaign's failure

In order a Campaign to be successful, there are several factors which need to be avoided (Winkler and Manke, 2013)⁸.

1. **Not understanding what security awareness really is.** Information must be provided in a way that relates to how people think and behave. There must be a personal association of how knowledge would impact their actions. There is also a difference in providing an individual information on a one time basis, and delivering information in different formats over the course of time to effect change.
2. **Compliance.** In short, saying your awareness program is compliant does not necessarily equate to create the desired behaviours.
3. **Illustrate that awareness is a unique discipline.** A good security awareness professional will have good communication ability, be familiar with learning concepts, understand that awareness is more than a check the box activity, knowledge of a variety of techniques and awareness tools, and an understanding that there is a need for constant reinforcement of the desired behaviours.
4. **Lack of engaging and appropriate materials.**
5. **Not collecting metrics.** By collecting regular metrics, you can adjust your program to the measured effectiveness. By determining what is working and what is not, you can tailor future programs based upon lessons learned. The appropriate metrics also allow for the determination of which components are having the desired impact. They should be taken prior to starting any engagement effort, at least once during the engagement, and also post-engagement.
6. **Unreasonable expectations.** No security countermeasure will ever be completely successful at mitigating all incidents. There will always be a failure.
7. **Arrange multiple training exercises.** Focusing on a specific topic or threat does not offer the overall training needed.

⁸ Winkler & Manke (2013).

4. 10. Case Studies

10.1. Cyber Security Awareness Campaigns in U.K.

10.1.1. GetSafeOnline Campaign⁹

This campaign focuses on users at home and businesses. Get Safe Online is a jointly funded initiative between several Government departments and private sector businesses. It provides practical advice on how to protect yourself, your computers and mobile devices and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site – including safe online shopping, gaming and dating. The site also keeps you up to date with news, tips and stories from around the world. Unfortunately, there is too little information regarding cyberbullying and how to act when you are a victim.

The site offers easy access by listing information. All information appears on the home page. Also a question tag and possibility to apply your own question.

Message: The positive message of “get safe online” again gives the responsibility to users for staying safe.

The campaign covers, topics such as:

- Protecting Your Computer
- Protecting Yourself
- Smartphones & Tablets
- Shopping, Banking & Payments
- Safeguarding Children
- Social Networking
- Businesses

The campaign offers a repository of threats and how-to advice but its tone and approach is based on essential fear tactics. As previously discussed, messages with horrible content may not cause fear and that fear may be caused without frightening contents. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. Messages also can be more persuasive when there is a match between the recipient’s cognitive, affective or motivational characteristics and the content of framing of the message.

⁹ www.getsafeonline.org

10.1.2. The 'Cyber Streetwise' campaign¹⁰

This campaign focuses on users at home and businesses. The campaign advises home users to use social media responsibly, to keep a child's identity safe. In short, this campaign presents users as the weakest links in the cyber security chain.

The new Home Office Cyber Streetwise site advises businesses to adopt five basic measures. These include, using strong, memorable passwords, installing antivirus software on all work devices, checking privacy settings on social media, checking the security of online retailers before loading card details and patching systems as soon as updates are available. The service will be of particular use to small and medium-sized businesses.

A survey of FTSE 350 companies by the Department for Business, Innovation and Skills last month revealed that only 14 per cent are regularly considering cyber threats, with a significant number not receiving any intelligence about cyber criminals.

It is a campaign which tries to cause a behavioural change by providing tips and advice on how to improve online security.

- It urges businesses to get online
- To take control of their online behaviour
- Suggests to companies that a well-designed site provides a sense of security and business reliability.
- Suggests that the good reputation of a company for safety and security online will lead to business growth and will boost sales.

Message: The campaign uses a positive message method to influence the behaviour of users. *“In short, the weakest links in the cyber security chain are you and me”*. This campaign represents several advances on past government-supported efforts:

1. The campaign targets specific demographic groups: based on Experian's MOSAIC product of UK demographics, X target users groups have been identified by age, gender and education/profession: small and medium businesses, seniors, middle aged men who know it all, etc.). Specific cyber threats, and how to protect against them been designed by communication professionals, is visually appealing and engaging, and avoids the 'scare factor'. It also presents the materials in the context of everyday tasks that people recognise: banking
2. The effect of targeted campaigns is measured through a set of Key Performance Indicators (KPI) for secure online behaviours.

The campaign covers, topics such as:

1. Passwords
2. Bank safely online / on your mobile
3. Common shopping scams
4. Computer health
5. Identity theft

¹⁰ www.cyberstreetwise.com

6. Operating system and software updates
7. Online payment options
8. Online shopping
9. Phishing
10. Social media
11. Smart phone health
12. Wireless network security

These are the main advice suggestions on security for users. The advice usually comes from security experts and service providers, who monotonically repeat suggestions such as ‘use strong passwords’. That advice pushes responsibility and workload for issues that should be done by the service providers and product vendors onto users, not caring that following this advice would be a near-full-time job for those who can understand it.

One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed. Security awareness, education and training cannot just ‘fix’ security problems (Coventry, et al., 2014, Government Office for Science, UK). If security is difficult to use, too complex, too effortful, people will not do it. Perceived control, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012).

10.1.3. Webwise Campaign¹¹

This campaign focuses mainly on parents and home users. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign urges users to “*Make the most of being online*”. It offers an online course, whereas basic technology is used.

The campaign covers, topics such as:

- Home
- Your computer
- Using the web
- Email & sharing
- Living & interests
- Safety & privacy
- Glossary

¹¹ <http://www.bbc.co.uk/webwise/0/>

1.1.4. Good to know Google's¹²

This campaign targets the general public but mainly families. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign uses a more collective/collaborative message “*Working together to stay safe online*”. It is friendly to users with a step by step guide.

The campaign covers, topics such as:

- Manage your privacy and security
- Prevent cybercrime
- Getting started
- Explore with confidence
- Manage your online reputation

Google launched the “*Good to Know*” campaign promoting online safety in association with the Citizens Advice Bureau (CAB).

10.1.5. Behind the Screen¹³

Behind the Screen is a hub of free computing resources for your GCSE students, complete with lesson plans and mark schemes. The resources are developed with industry to provide authentic projects mapped to computing, ICT and computer science qualifications.

The Behind the Screen projects and resources are currently free to use for all UK schools. There are eight projects live on the site. Projects are developed with key industry partners who provide the real life business cases and ideas for each, and supply industry resources and software for students to use. Projects are presented as problems through a brief, and students are guided through to their solution. All resources they need to achieve the outcomes are provided. Projects take from 6 to 15 hours to complete, depending on the route taken. Extension activities are also provided.

Projects are supported with lesson plans, guides, mapping to current Key Stage 4 qualifications, and presentations to support delivery. Assessment is through a Student Log, and teachers are provided with an exemplar to make assessment straightforward.

10.1.6. Cyber Security Challenge UK¹⁴

Cyber Security Challenge UK is helping to fill the cyber security skills gap by tapping into untapped talent. It is a not-for-profit organisation which operates primarily through sponsorship. Its main role is to run a national programme of competitions which are designed to attract and inspire new talent into the UK cyber security profession.

¹² <https://www.google.co.uk/goodtoknow/>

¹³ <http://www.behindthescreen.org.uk/>

¹⁴ <http://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx>

Sponsored by over 50 organisations from government, industry and academia and leading sponsor Government Communications Headquarters (GCHQ), the Challenge sets competitions that test existing cyber security skills, runs cyber camps to help individuals develop new skills, and provides information through networking events on cyber security career changes.

CESG have produced two posters for the Palace of Westminster to help raise IA awareness which can be customised with your own logo for use in your own government department (or supporting industry partner).

10.1.7. The Devil's In Your Details¹⁵

In the first campaign of its kind involving both the private and public sectors, The Devil's in Your Details campaign brings together Action Fraud, The Telecommunications UK Fraud Forum (TUFF) and Financial Fraud Action UK - the name under which the financial services industry coordinates its fraud prevention activity, in a powerful demonstration of what can be achieved when industry and government work together.

The National Fraud Authority backed campaign is raising awareness of the importance of protecting personal information and aims to remind the public to check that who they share their details with is genuine. The Devil's In Your Details campaign encourages consumers to suspect anyone or anything they are uncertain about, to keep asking questions and to challenge or end an engagement if it feels uncomfortable. As an introduction to a wider campaign against fraud, this awareness activity aims to increase reporting of fraud, making it harder for fraudsters to target consumers in the future.

The campaign includes professional videos which are very well presented. But it scared less experienced people away from online transactions, which is not what government intends to achieve. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined. It is crucial to decide the target group of a campaign and try to match a cultural theme of the message recipient but also match the recipient's cognitive, affective or motivational characteristics with the content of framing of the message.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, instead of using fear invocations often leading to pure avoidance of the suggestion.

10.1.8. VOME¹⁶ Visualisation and Other Methods of Expression

VOME is a three year collaborative research project bringing together researchers from the Information Security Group (ISG) at Royal Holloway, University of London, Salford and Cranfield Universities, working with consent and privacy specialists at Consult Hyperion and Sunderland City Council, to explore how people engage with concepts of information privacy and consent in on-line interactions.

¹⁵ <http://www.actionfraud.police.uk/thedevilsinyourdetails>

¹⁶ <http://www.vome.org.uk/>

The purpose of VOME (Visualisation and Other Methods of Expression) is to explore how user communities engage with concepts of information privacy and consent in on-line interactions. The aim is to develop alternative conceptual models of on-line privacy which enable users to make clearer on-line disclosure choices. These decision making models will facilitate a better dialogue between the designers of privacy and consent functionality and their customers.

This project offers benefits to on-line service providers, the manufacturers of technology used to deploy on-line services, as well as the general public. To date there has been considerable interest in this project from each of these communities.

This is a more innovative approach to raising awareness including games, theatre and other methods of expression.

10.2. Cyber Security Awareness Campaigns in Australia

10.2.1. Stay Smart Online¹⁷

This is a one-stop shop providing information for Australian Internet users on the simple steps they can take to protect their personal and financial information online. The site has informative videos, quizzes and a free Alert Service that provides information on the latest threats and vulnerabilities.

10.2.2. ThinkUKnow - Internet Safety Program¹⁸

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia. Users will need to subscribe to the site to gain access to its tools and resources.

10.2.3. Tagged (CyberSmart) - ACMA¹⁹

Developed by the ACMA's Cybersmart program, Tagged has received acclaim for its realistic depiction of teenagers and the problems they can face in a digital world. Since its launch in September 2011, Tagged has become a popular resource for Australian teachers and parents. More than 10,000 copies of the film and posters have been distributed nationwide and it has attracted nearly 50,000 views on YouTube.

10.2.4. Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)²⁰

By using social networking environments to target children and young people directly, the SOSO initiative educates children and young people about the dangers that exist online and on how they can manage their personal safety.

¹⁷ <http://www.staysmartonline.gov.au/>

¹⁸ <http://www.thinkuknow.org.au/site/>

¹⁹ <http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx>

²⁰ <http://napcan.profero.com.au/soso>

10.2.5. Make cyberspace a better place - KIDS Helpline²¹

Kids Helpline campaigns to help children enjoy the freedom and fun of using the Internet and to help make cyberspace a fun and safe place.

10.2.6. The Alannah & Madeline Foundation - Keeping children safe from violence²²

This national charity aims to protect children from violence and its devastating impact. The website provides a range of information and resources for parents and children, including an evidence-based educational program ([eSmart Schools](#)), and a variety of other resources about bullying and cybersafety.

Some campaigns are delivered in collaboration with a wide variety of public and private agencies. As a result, there is a large degree of crossover in the material of various contributors presented across the websites. Furthermore, initiatives may target a specific issue (such as cyberbullying), or they may be delivered as part of a broader social awareness campaign (child protection).

10.2.7. Who's chatting to your kids? - Queensland Police Resource²³

A brochure published by the Queensland Police Service's Task Force Argos. This brochure provides information to parents on Internet safety for children and young people. It discusses social networking, mobile phones, webcams and online gaming, and provides information about the types of things to look out for that may indicate that children could be at risk.

Some of the more popular social networking sites provide information specifically tailored to help parents understand their child's use of the site.

10.2.8. Keep it Tame²⁴

Keep it Tame Campaign tries to Promote Online Safety and Measure Behaviour Change in Young People. This is an online campaign targeting Australian teenagers, drawing attention to the consequences of thoughtless and hurtful use of social media and empowering them to act with respect online.

Unique to the campaign is the application of an innovative digital tracking methodology which – in conjunction with a cohort study that will survey and interview young people over time – will measure its impact on behaviour change.

The campaign guides teenagers through a series of mock social media posts. As things turn nasty, an animated creature slowly becomes more grotesque, highlighting the hurtful effects of the online exchanges and ultimately encouraging people to act with respect. The Keep it Tame

²¹ <http://www.kidshelp.com.au/teens/get-info/cyberspace/>

²² <http://www.amf.org.au/bullying/>

²³ <http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/>

²⁴ <http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour-change-young-people/>

campaign is the first in a series of campaigns to come out of the Young and Well CRC's Safe and Well Online project, a five-year study of the most effective ways to design, deliver and evaluate online social marketing campaigns aimed at improving safety and wellbeing.

This project is an initiative of the Young and Well CRC and is led by the University of South Australia in conjunction with the University of Western Sydney, Zuni and the Queensland University of Technology. Safe and Well Online builds upon the original Smart Online Safe Offline initiative developed by NAPCAN.

10.3. Cyber Security Awareness Campaigns in Canada

10.3.1. Get Cyber Safe²⁵

Get Cyber Safe is a national public awareness campaign created to educate Canadians about Internet security and the simple steps they can take to protect themselves online. The campaign's goal is to bring together all levels of government, the public and private sectors, and the international community, to help Canadians be safer online.

The campaign is an important component of [Canada's Cyber Security Strategy](#), which is dedicated to securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.

The campaign is being led by Public Safety Canada on behalf of the Government of Canada.

10.3.2. Stop Hating Online²⁶

Stop Hating Online is the Government of Canada's anti-cyberbullying public awareness campaign. It focuses on cyberbullying in terms of social impacts and potential legal consequences. As a comprehensive resource for parents and youth, GetCyberSafe.ca provides information, advice and tools to prevent and stop hate, cyberbullying and the non-consensual distribution of intimate images that can take place online, including through social networks and mobile messages. The campaign encourages everyone to stand up against cyberbullying.

10.4. Cyber Security Awareness Campaigns in Africa

10.4.1. ISC Africa²⁷

A coordinated, industry and community-wide effort to inform and educate Africa's citizens on safe and responsible use of computers and the internet so that we can minimise the inherent risks and increase consumer trust.

²⁵ <http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx>

²⁶ <http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx>

²⁷ <http://iscafrica.net/#home>

10.4.2. Parents corner²⁸

The effort is intended to co-ordinate the work done by government, industry and civil society. Its objectives are to protect children, empower parents, educate children and create partnerships and collaboration amongst concerned stakeholders. Parents' Corner tips for a safer internet include:

1. People aren't always who they say they are.
2. Think before you post.
3. Likewise, children need to think before they respond to things that other people have posted.
4. It's not just about computers. Many parents don't understand that the Internet their children can access via their cell phones is the same Internet accessed via a computer.
5. Finally, just as they would in real life, friends must protect friends.

²⁸ <http://www.parentscorner.org.za/>

11. Conclusions

The ISF report (February 2014), proposes that simple transfer of knowledge is not enough. Knowledge and awareness is a prerequisite to change behaviour but not necessarily sufficient and this is why it has to be implemented in conjunction with other influencing strategies. It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, and a part of an organisation's information security culture. One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed.

Moreover, the advice usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords'. But, security awareness, education and training cannot just 'fix' security problems. If security is difficult to use, too complex, too effortful, people will just not accept it (Coventry, et al., 2014, Government Office for Science, UK). Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012). Behaviour change in an information security context could be measured through risk reduction, but not through what people know, what they ignore or what they do not know.

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004). Messages also can be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual's ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

As previously discussed while reviewing existing awareness campaigns fear invocations are often used, as influence strategies. But, fear invocations are proved insufficient to change behaviour. They cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are not combined. As previously discussed, messages with horrible content may not cause fear and fear may be caused without frightening contents.

Following that rationale of the expected utility approach, perhaps increasing the 'perceived utility' of cybersecurity could be one additional factor to improve the effectivity of awareness campaigns. Also, perceived control and personal handling ability, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. A campaign should use simple consistent rules of behaviour that people can follow. This way, their perception of control will lead to better acceptance of the suggested behaviour.

We suggest that the following factors can lead to more sufficient awareness campaigns:

1. Awareness has to be professionally prepared and organised in order to work.
2. Causing feelings of fear to people is not an effective tactic, since it will put off people who can least afford to take risks. To make the internet accessible, risks should not be exaggerated.
3. Awareness alone is not enough. Usually all it does is catch attention.

4. Security education has to be more than providing information to people - it needs to be targeted, actionable, and doable. At the moment, what is correct behaviour is far too difficult and complex. We need simple consistent rules of behaviour that people can follow.
5. Once people are willing to change, training and feedback is needed to sustain them through the change period.

References

- Ajzen, I. (1988). Attitudes, personality, and behaviour. Dorsey Press, Chicago.
- Bernoulli, Daniel, "Exposition of a New Theory on the Measurement of Risk". Originally published in 1738, translated by Dr. Louise Sommer. (January 1954). *Econometrica* (The Econometric Society) **22** (1): 22–36. doi:[10.2307/1909829](https://doi.org/10.2307/1909829).
- Caputo, D., Lawrence Pfleeger, Sh., Freeman, D.J., Johnson, E.M. Going Spear Phishing: Exploring Embedded Training and Awareness, *IEEE Security & Privacy*, vol. 12, no. 1, pp. 28-38, Jan.-Feb. 2014, doi:10.1109/MSP.2013.106.
- Cesario, J., Grant, H., & Higgins, T.E. (2004). Regulatory fit and persuasion: Transfer from "feeling right". *Journal of Personality and Social Psychology*, *86*, 388-404.
- Cook, T., & Flay, B. (1978). The temporal persistence of experimentally induced attitude change: An evaluative review. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 11). New York: Academic Press.
- Coventry, D.L., Briggs, P., Blythe, J., Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Government Office for Science, London, UK. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf
- Dolan P., Hallsworth, M., Halpern, D., King, D., Vlaev, I. MINDSPACE Influencing behaviour through public policy, Institute for Government, Cabinet Office, 2 March 2010. Retrieved from: <http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf>
- Domke David, Shah V. Dhavan and Wackman B. Daniel (1998). Media Priming Effects: Accessibility, Association and Activation. *International Journal of Public Opinion Research*, *1*(1), 51-74.
- Douglas, M., & Wildavsky, A. (1982). *Risk and culture: An essay on the selection of technological and environmental dangers*. Berkeley: University of California Press.
- Eklund, M., & Backstrom, M. (2006). The role of perceived control for the perception of health by patients with persistent mental illness. *Scandinavian Journal of Occupational Therapy*, *13*, 249-256.
- Fogg, B. J. (2002). *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann.
- Fisher, E.B., & Rost, K. (1986). Smoking cessation: A practical guide for the physician. *Clinics in Chest Medicine*, *7*, 551-565. Hofstede, G., Hofstede, J.G., Minkov, M. *Cultures and Organizations: Software of the Mind*. 3rd Edition, McGraw-Hill USA, 2010.
- Higgins, E.T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *Advances in Experimental Social Psychology*, *30*, 1-46.
- Information Security Forum (ISF). From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. Retrieved from: <https://www.securityforum.org/shop/p-71-170>
- Kirlappos, I., Sasse, M. A. (2012). [Security Education against Phishing: A Modest Proposal for a Major Rethink](#). *IEEE Security and Privacy Magazine* *10*(2), 24-32

Kirlappos, I., Parkin, S., Sasse, M. A. (2014). Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security. *Workshop on Usable Security* Kreuter, M. W., & McClure, S. M. (2004). The role of culture in health communication. *Annual Review of Public Health, 25*, 439-455.

Lapowsky I (2013). Reward vs. Punishment: What Motivates People More? Retrieved from: <http://www.inc.com/magazine/201304/issie-lapowsky/get-more-done-dont-reward-failure.html>

Lockwood, P., Marshall, T., & Sadler, P. (2005). Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models. *Personality and Social Psychology Bulletin, 31*, 379-392.

Media Literacy Project, Language of Persuasion, Retrieved from <http://medialiteracyproject.org/language-persuasion>

More Josh (2011). Measuring Psychological Variables of Control In Information Security, - January 12, Retrieved from <http://www.sans.org/reading-room/whitepapers/awareness/measuring-psychological-variables-control-information-security-33594>

NIST, National Institute of Standards and Technology. Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory. October 2003. Retrieved from: <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from: <http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm>

Palmer, C.G.S. (1996). Risk perception: An empirical study of the relationship between worldview and the risk construct. *Risk Analysis, 16*, 717-724.

Robinson Alyssa, Using influence strategies to improve security awareness programs, The SANS Institute, 2013. Retrieved from: <https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385>

Roper, C., Fischer, L., Grau, J. Security Awareness, Education and Training, Elsevier Inc. UK, 2006. ISBN-13: 978-0750678032.

Simons-Morton, B.G., Donohew, L.C., Aria, D. (1997). Health communication in the prevention of alcohol, tobacco and drug use. *Health Education and Behaviour, 24*, 544-554.

Triandis, H.C. (1989). The self and social behaviour in differing cultural contexts. *Psychological Review, 96*, 506-520.

Uskul K. Ayse, Sherman K. David, Fitzgibbon John (2009). The cultural congruency effect: Culture, regulatory focus, and the effectiveness of gain- vs. loss- framed health messages. *Journal of Experimental Social Psychology, 45*, 535-541. doi: 10.1016/j.jesp.2008.12.005

Weber U. Elke, Hsee K. Christopher (2000). Culture and Individual Judgement and Decision Making. *Applied Psychology: An International Review, 49(1)*, 32-61.

Winkler Ira and Manke Samantha (2013). 7 Reasons for Security Awareness Failure, CSO Magazine, July 10. Retrieved from <http://www.csoonline.com/article/2133408/network-security/the-7-elements-of-a-successful-security-awareness-program.html>

Winkler Ira and Manke Samantha (2013). 6 essential components for security awareness programs. Retrieved from <http://www.csoonline.com/article/2133971/strategic-planning-erm/6-essential-components-for-security-awareness-programs.html>

Winkler Ira and Manke Samantha (2013). How to create security awareness with incentives. Retrieved from <http://www.csoonline.com/article/2134189/strategic-planning-erm/how-to-create-security-awareness-with-incentives.html>

Links to Campaigns in U.K.

1. **The 'Cyber Streetwise' campaign** www.cyberstreetwise.com
2. **GetSafeOnline Campaign** www.getsafeonline.org
3. **Webwise Campaign** <http://www.bbc.co.uk/webwise/0/>
4. **Good to know Google's** <https://www.google.co.uk/goodtoknow/>
5. **Behind the Screen** <http://www.behindthescreen.org.uk/>
6. **Cyber Security Challenge UK**
7. <http://www.cesg.gov.uk/awaresstraining/Pages/Cyber-Security-Challenge-UK.aspx>
8. **The Devil's In Your Details** <http://www.actionfraud.police.uk/thedevilsinyourdetails>
9. **VOME Visualisation and Other Methods of Expression** <http://www.vome.org.uk/>

Links to Campaigns in Australia

1. **Stay Smart Online** <http://www.staysmartonline.gov.au/>
2. **ThinkUKnow - Internet Safety Program** <http://www.thinkuknow.org.au/site/>
3. **Tagged (CyberSmart) – ACMA**
<http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx>
4. **Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)** <http://napcan.profero.com.au/soso>
5. **Make cyberspace a better place - KIDS Helpline** <http://www.kidshelp.com.au/teens/get-info/cyberspace/>
6. **The Alannah & Madeline Foundation - Keeping children safe from violence**
<http://www.amf.org.au/bullying/>

7. **Who's chatting to your kids? - Queensland Police Resource**
8. <http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/>
9. **Keep it Tame** <http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour-change-young-people/>

Links to Campaigns in Canada

1. **Get Cyber Safe** <http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx>
2. **Stop Hating Online** <http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx>

Links to Campaigns in Africa

1. **ISC Africa** <http://iscafrica.net/#home>
2. **Parents corner** <http://www.parentscorner.org.za/>

**IECC Public Awareness and Training
Working Group
Cybersecurity Public Relations Plan**

June 2018



Indiana Executive Council on Cybersecurity

Public Awareness and Training Plan

2018-2020

Public Awareness and Training Working Group

June 2018

TABLE OF CONTENTS

<u>TITLE</u>	<u>PAGE</u>
EXECUTIVE SUMMARY	3
INTRODUCTION	4
PURPOSE AND BACKGROUND	5
RESEARCH	6
CAMPAIGN GOALS	13
KEY PUBLICS	14
PLAN: PHASE 1	15
PLAN: PHASE 2	36
PLAN: PHASE 3	45
BUDGET	54

EXECUTIVE SUMMARY

This cybersecurity plan is developed by the Public Awareness and Training Working Group in support of the Indiana Executive Council on Cybersecurity's (Council) mission. It is designed to increase public awareness, knowledge and positive cybersecurity behaviors by Hoosiers over a five-year period. Additionally, it promotes cybersecurity as a career field for young people and has elements informing the Indiana public about the activities of the Council.

Extensive secondary research demonstrates that similar campaigns to impact public awareness fail. Research has identified that there are 13 key knowledge points (Pew) the public should know and use, and that positively framed messaging is more effective than negatively framed (fear) messaging for influencing behaviors.

Based on the research, a five-year, three-phased plan has been developed to affect behavior change in Hoosier's use of the internet and in their awareness and knowledge of cybersecurity.

A series of overarching goals are established to achieve these changes. Five key publics (audiences) were identified to be reached via a variety of messaging strategies. In each case (publics), measurable objectives are established. Based on the 13 key knowledge points, the public (as organized into the five categories) will be targeted with strategic communication messages to increase awareness and knowledge of cybersecurity practices, and to increase positive behaviors in cybersecurity protection and defense.

Activities will be measured at the conclusion of each phase of the campaign, and the subsequent phase adjusted to reflect that learning.

Two additional goals are established: one to increase knowledge and awareness among high school students about the potential for cybersecurity as a career field, and a second to inform the Indiana public about the activities of the Cybersecurity Council.

The Working Group continues to research and address the career field and training challenges and expects to provide additional materials to support this effort.

This plan is the result of approximately a year of effort on behalf of the Working Group to develop. The Group will continue to work on projects in support of the overall Cybersecurity Council mission, including development of training options, and providing advice and counsel to other committees and working groups as needed. It will also serve as an advisory group during the implementation of this campaign plan as needed.

**Indiana Executive Council on Cybersecurity
Public Awareness and Training Plan
2018-2020
July 2018**

INTRODUCTION

This cybersecurity plan is presented in partial fulfillment of the Public Awareness and Training Working Group's mission. It includes a detailed research summary, a detailed set of goals and objectives, and a three-phased campaign plan to increase awareness, knowledge and positive cybersecurity behaviors among five key publics in Indiana.

This plan is the result of approximately a year of effort on behalf of the Working Group to develop. The Working Group anticipated that execution of this campaign plan would be the responsibility of state government agencies, either directly or with a third-party agency (advertising/public relations contractor), and under the direction of a state official.

The Group will continue to work on projects in support of the overall Council mission, including development of training options, and providing advice and counsel to other committees and working groups as needed. It will also serve as an advisory group during the implementation of this campaign plan as needed.

It should be noted that the plan addresses Indiana residents in four categories. In one category, the intent is to inform Indiana residents about the activities of the Council. That function is addressed in the plan, but not fully developed. It is anticipated a separate plan will be developed via the Governor's office, IOT, Homeland Security and others to address that goal in greater detail.

Additionally, we did not address the need to properly "brand" the Council's efforts. However, the Working Group strongly recommends that take place to support the effort and to separate the state's work and messages from others. Branding also identifies the state's efforts to do so via this campaign.

PURPOSE

The Public Awareness and Training Working Group of the Indiana Executive Council on Cybersecurity (Council) has been charged by Governor Holcomb to create an executable plan to communicate cybersecurity awareness and knowledge to citizens of Indiana. The Council was established by Executive Order #17-11 dated January 9, 2017.

The Council's mission:

The Council shall develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.

Working Group Mission:

In order to protect the security and economy of the State, it is appropriate and necessary for state government to establish and lead a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana's cybersecurity.

The working Group established three principle goals for its work. The goal specifically addressed by this plan is:

Develop a comprehensive plan to provide information and training to the public in general and specific sectors of the Indiana economy to protect its electronic data from criminal or terroristic attempts to breach electronic databases and what to do if a breach does occur.

BACKGROUND

The Public Awareness and Training Working Group (PATWG) was established and chartered in August 2017. Since that time, a number of projects have been completed leading to the development of this plan. The PATWG has an established charter and has conducted a series of planning meetings. In addition, the group has conducted research on the topic and has engaged with a student team from IUPUI to develop an initial public awareness campaign in Indiana.

RESEARCH

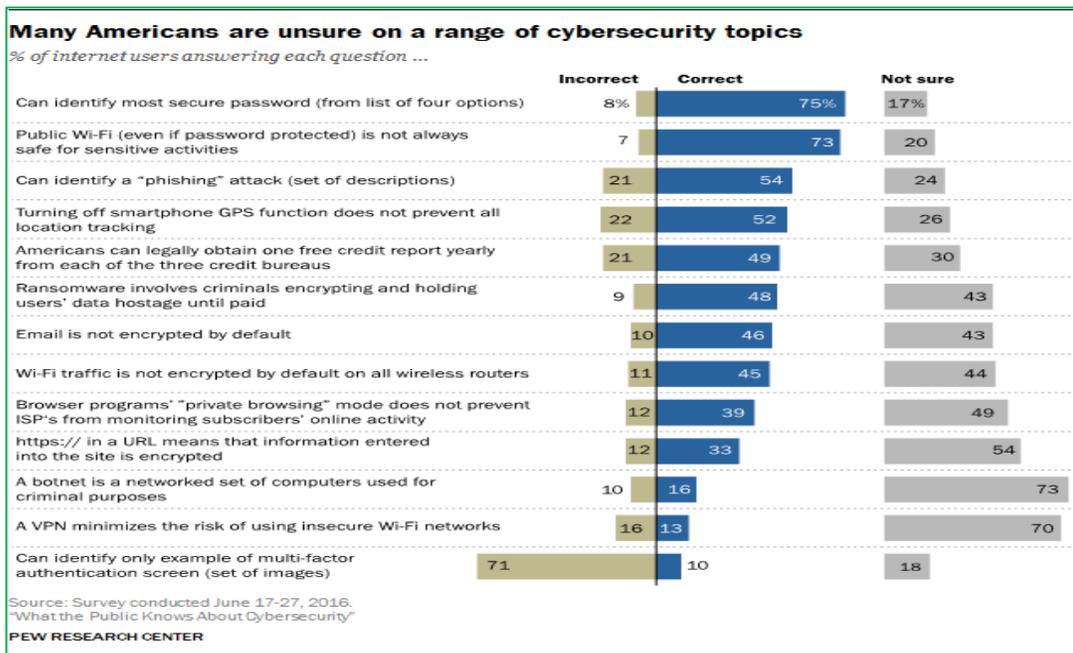
Summary

What research is available demonstrated that the greatest vulnerability is general lack of both awareness and knowledge among the general public on how best to protect themselves from cyberattacks. There is a significant public awareness and knowledge gap.

Research has established that there has essentially been no coordinated statewide effort to educate the general public about cybersecurity efforts. Individual industries and individual state agencies have conducted various programs focused generally in areas of their responsibility. The Indiana Attorney General has conducted a limited campaign focused primarily on identity theft, and IOT has extensive training opportunities available and has worked in a limited fashion to promote cybersecurity awareness. The Indiana Department of Revenue also has worked to educate taxpayers on fraud prevention over the past three years.

Specific Research Studies

1. PEW Research Center study: “What Americans Know About Cybersecurity.” Conducted June 2016; Published March 2017. We anticipate that the findings from this survey of Americans can be generalized to Indiana residents.
 - a. US nationwide survey of 1,055 adult internet users
 - b. 13-question survey
 - c. Observations:
 - i. Typical respondent answered only 5 of 13 correctly!
 - ii. Only 1 percent answered all 13 correctly!
 - iii. Majority answered only 2 correctly!
 - iv. Only 4 questions correctly answered by 50% or better

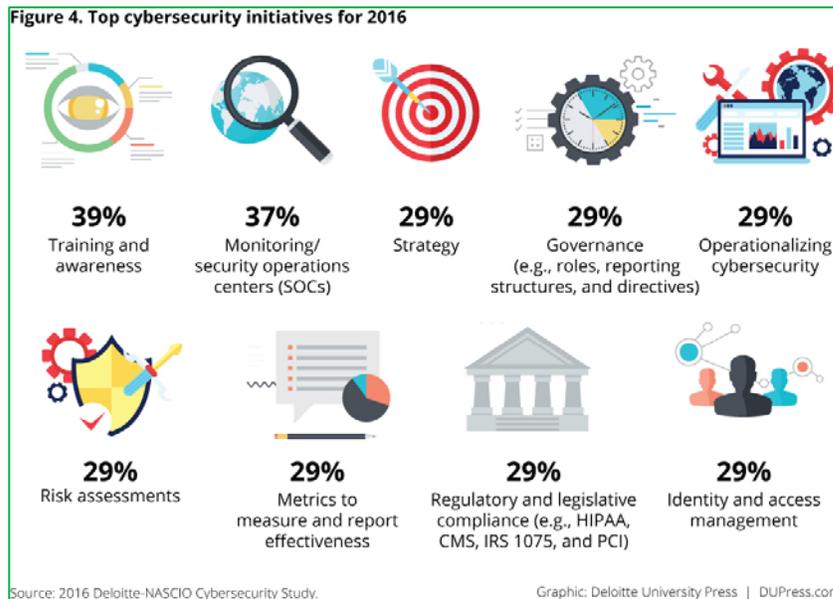


- d. Operational Findings:
 - i. Broad differences in knowledge by educational attainment
 - Significant differences between college and non-college respondents
 - ii. Modest differences in knowledge by age
 - Younger = more knowledgeable
 - Older = less knowledgeable

2. “ACS Cybersecurity: Threats, Challenges, Opportunities.” Australian Computer Society, Nov. 2016. This Australian association report provides a chapter dedicated to “Looking at the Road Ahead.” It principally notes that there are few efforts worldwide to combat cybersecurity attacks. It notes that Japan has recently established and funded efforts to educate and train cybersecurity techniques in government, industry and with individuals. The report also identifies all the standard techniques for cybersecurity defense for businesses and industries. Perhaps most key in this report is the acknowledgement that the tools exist, we just need to educate and use them. As such, it places “education and awareness” as its number one priority out of five.
 - a. Here are resources provided by this report (all Australian):
 - Australia’s Cybersecurity Strategy - cybersecuritystrategy.dpmc.gov.au
 - Australian Center for Cyber Security - www.acsc.gov.au
 - Australian Computer Emergency Response Team (AusCERT) - www.uscert.org.au
 - Australian Cybercrime Online Reporting Network (ACORN) - www.acorn.gov.au
 - Australian Internet Security Initiative - www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative
 - Australian Signals Directorate – Top 4 Mitigation Strategies - www.asd.gov.au/infosec/mitigationstrategies.htm
 - Australian Signals Directorate – CyberSense Videos - www.asd.gov.au/videos/cybersense.htm
 - Australian Government – Stay Smart Online - www.staysmartonline.gov.au
 - ACCC – Scam Watch - www.scamwatch.gov.au

 - b. Some key facts from the report:
 - The world economic forum’s global risks 2015 report highlighted cyberattacks and threats as one of the most likely high-impact risks. In the United States, for example, cybercrime already costs an estimated \$100 billion a year.
 - IOT Sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018, growing at a 23% compound annual growth rate from 2015 to 2021.

- Cybersecurity is a business issue, not just a technology one. In a survey of close to 4,000 company directors in Australia, roughly only half reported to be cyber literate, and of co-directors, only 15 percent classed as cyber literate. There is a lack of knowledge about cybersecurity at the executive level in many businesses in Australia.
 - There are 1,404 cybersecurity vendors in the world today. Vendors by country: USA 827; Israel 228; UK 76; India 41; Australia 15.
 - Job advertisements for cybersecurity alone have grown 57% in the last 12 months according to jobs website Seek. Network security consultants were the 6th most advertised occupation on LinkedIn in 2015.
3. International Telecommunications Union (ITU) Global Cybersecurity Index 2017. This annual assessment of global (national and regional) cybersecurity efforts places the United States very high compared to most other regions and countries and observes that the National Governor’s Association leads the way with its resource Center for State Cybersecurity.
 4. Deloitte NASCIO Cybersecurity Study, Doug Robinson and Srin Subramanian, published September 20, 2016. This article examined state government efforts in cybersecurity protection and activity.
 - a. One observation was that states are now taking a much more active role in cybersecurity defense. The figure below (extracted from the study) identifies the efforts now (2015) underway in comparison to other efforts in the cybersecurity arena. Note that Training and Awareness is the top area of priority and activity.



- b. The study noted a positive trend in training of employees. All education and training trends are up across the board (between 2014 – 2016) except for third-party workforce.



- 5. “Cyber Security Awareness Campaigns: Why do they fail to change behavior?” draft working paper, Global Cyber Security Capability Center, July 2015.
 - a. This early research paper by academics in UK studies the nature of awareness and behavior change campaigns conducted to increase cybersecurity awareness and the adoption of new defensive behaviors.
 - b. Of particular note is the identification of six (6) “Essential Components for a Campaign:”
 1. Communication. A significant part of a campaign is communication. This can be accomplished by collateral, internally distributed materials. These are things like newsletters, blogs, and other internal communications. Also, posters are a very crucial method of raising awareness. While some people believe they are old fashioned and outdated, they can be very effective when they are well designed.
 2. Computer Based Training. CBT is the most omnipresent component of security awareness programs, as it is the most clearly accepted method of achieving compliance.
 3. Events. Well-executed events bring the Security Awareness program, and the whole security effort for that matter, to life.

4. Security Portal. An internal security portal provides several functions. It provides a Knowledge base that can provide a huge return on investment with includes information on security related topics. It is also important to include information on home and personal security strategies, such as protecting children online and securing social media accounts.

5. Behavioral (sic) Testing and Teachable Moments. Phishing, USB drive drops, and Social Engineering tests require some care, but are important components to give your employees a "teachable moment."

6. Teaching New Skills Effectively. What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). As teachers, security awareness professionals must break down complex goals in short, clear achievable steps.

c. The authors also identified seven (7) key factors that lead to campaign failure:

1. Not understanding what security awareness really is. Information must be provided in a way that relates to how people think and behave. There must be a personal association of how knowledge would impact their actions. There is also a difference in providing an individual information on a one-time basis, and delivering information in different formats over the course of time to effect change.

2. Compliance. In short, saying your awareness program is compliant does not necessarily equate to create the desired behaviors.

3. Illustrate that awareness is a unique discipline. A good security awareness professional will have good communication ability, be familiar with learning concepts, understand that awareness is more than a check the box activity, knowledge of a variety of techniques and awareness tools, and an understanding that there is a need for constant reinforcement of the desired behaviors.

4. Lack of engaging and appropriate materials.

5. Not collecting metrics. By collecting regular metrics, you can adjust your program to the measured effectiveness. By determining what is working and what is not, you can tailor future programs based upon lessons learned. The appropriate metrics also allow for the determination of which components are having the desired impact. They should be taken prior to starting any engagement effort, at least once during the engagement, and also post-engagement.

6. Unreasonable expectations. No security countermeasure will ever be completely successful at mitigating all incidents. There will always be a failure.

7. Arrange multiple training exercises. Focusing on a specific topic or threat does not offer the overall training needed.
- d. Finally, the authors provide five (5) key factors that can lead to more sufficient awareness campaigns:
1. Awareness has to be professionally prepared and organized in order to work.
 2. Causing feelings of fear to people is not an effective tactic, since it will put off people who can least afford to take risks. To make the internet accessible, risks should not be exaggerated.
 3. Awareness alone is not enough. Usually all it does is catch attention.
 4. Security education has to be more than providing information to people - it needs to be targeted, actionable, and doable. At the moment, what is correct behavior is far too difficult and complex. We need simple consistent rules of behavior that people can follow.
 5. Once people are willing to change, training and feedback is needed to sustain them through the change period.
6. IUPUI student survey (convenience sample) conducted of Indiana residents, November 2017. General, small, self-selected sample of Indiana residents (mostly college students). Results generally reflect findings similar to the Pew Center Study.
7. The Working Group also undertook to discover existing resources within state government that could be use in a Cybersecurity campaign and what was available for cybersecurity training to both government personnel as well as industry employees and the general public. Those include:
- The Indiana Office of Technology (IOT) manages a state open website with extensive information and training opportunities for the general public.
 - Find it at <https://www.in.gov/cybersecurity/2494.htm>.
 - Additional tips at <https://www.in.gov/cybersecurity/2571.html>.
 - Additional training and education materials for the public are found at <https://www.in.gov/cybersecurity/2533.htm> and related pages.
 - The Indiana Department of Homeland Security (IDHS) provides information on its website at <https://www.in.gov/cybersecurity/2543.htm>, including a cybersecurity fact sheet for businesses.

- Individual state agencies conduct awareness programs specific to their functions. For example, both the Indiana Department of Revenue (<https://www.in.gov/dor/4794.htm>) and the Indiana Attorney General (<https://secure.in.gov/apps/ag/idtheftprevtoolkit/Login.aspx>) conduct public identity theft education and awareness campaigns annually.
- IOT provides required cybersecurity training for all state employees annually. Some agencies test employees with phishing messages routinely, but this is not consistent across all agencies.

8. Initial, limited plan development.

Opportunity provided the chance to engage with an IUPUI Public Relations Campaigns class and provide a team of students a chance at creating a campaign to increase cybersecurity awareness. Working with members of the working group, the student team identified two key publics to target with two key messages:

- First, the general public was targeted for a general cybersecurity awareness campaign.
- Second, high school students were targeted as a public to receive an awareness campaign focused on cybersecurity as a career field.

The students created a draft campaign plan. This plan was used as a resource for the overarching master campaign plan represented in this document and, as such, has proved to be useful.

5-YEAR CAMPAIGN GOALS

- o Phase 1: After one year:
 - Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
 - Achieve knowledge of cybersecurity protective measures to 25 percent of Hoosiers.
 - Achieve active Cybersecurity activities by Hoosiers to 15 percent.
 - Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
 - Achieve 10 percent awareness of cybersecurity as a career field among high school student.

- o Phase 2: After three years:
 - Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
 - Achieve knowledge of cybersecurity protective measures to 60 percent of Hoosiers.
 - Achieve 45 percent active cybersecurity protective measures by Hoosiers.
 - Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
 - Achieve 40 percent awareness of cybersecurity as a career field among high school student

- o Phase 3: After five years:
 - Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
 - Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.
 - Achieve 60 percent active cybersecurity protective measures by Hoosiers.
 - Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
 - Achieve 70 percent awareness of cybersecurity as a career field among high school student

PUBLICS

1. General Public (all Hoosiers).
 - a. Baby Boomers and Traditionals, ages 54 to 72 and 72 and beyond.
 - b. Gen X (ages 38-53) and Y (ages 23-37).
 - c. Millennials (less than age 22)
 - d. High School students (for careers goal).
2. State government employees.
3. Local Government employees.
4. Industry unique employees. Will be developed in Phase 2 of the working group's planning after close coordination with other committees and working groups.

PHASE 1 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a “phishing” attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users’ data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs’ “private browsing” mode does not prevent ISP’s from monitoring subscribers’ online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	OPT	OPT	
Credit Reports	OPT	OPT	
Ransomware	OPT	OPT	
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	OPT	
Https	OPT	REQ	REQ
Botnet	OPT	OPT	
VPN	OPT	OPT	
Multi-factor Auth	OPT	REQ	REQ

1. **Awareness** equals correct answers to the 3 required questions and correct answers on at least 2 others.
2. **Knowledgeable** equals correct answers to the 7 required questions and at least one other.

3. **Action** will be measured via both survey and behavioral testing. To be considered “active” a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 1 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Evaluation results will be used to validate the target objectives for Phase 2.

PHASE 1

Phase 1 includes the initial year of the campaign from launch date (TBD) to one year later. It also includes an evaluation period at the end of the year. The evaluation data will be used to fine tune objectives for Phase 2.

PHASE 1 GOALS (after one year)

Goals:

1. Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 25 percent of Hoosiers.
3. Achieve active Cybersecurity activities by Hoosiers to 15 percent.
4. Achieve 10 percent awareness of cybersecurity as a career field among high school student.
5. Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.

GOAL 1: ACHIEVE AWARENESS OF CYBERSECURITY PROTECTIVE MEASURES TO 50 PERCENT OF HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

OBJECTIVE 1-1: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," "How Can You...", "You are part of the Solution," and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
- b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
- c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
- d. Develop television media partners in each major market for cybersecurity messaging.
- e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
- f. Develop special Facebook site to support social media messaging on this platform.
- g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.

Public: Gen X and Gen Y, ages 23-53.

OBJECTIVE 1-2: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: Millennials (less than age 22)

OBJECTIVE 1-3: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: State government employees

Objective 1-4: Achieve 50 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” and others similar are appropriate.

Tactics:

Continue current activities via IOT.

Public: Local government employees

Objective 1-5: Achieve 50 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” and others similar are appropriate.

Special Tactics:

- a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
- b. Require all local government employees to take the training annually.
- c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives. Communication should include the following:
 1. Monthly email messages
 2. Monthly Print feature stories
 3. Monthly website postings for intranets

GOAL 2. ACHIEVE KNOWLEDGE OF CYBERSECURITY PROTECTIVE MEASURES TO 25 PERCENT OF HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 2-1: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," "How Can You...", "You are part of the Solution," "You can...", and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
- b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
- c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
- d. Develop television media partners in each major market for cybersecurity messaging.
- e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
- f. Develop special Facebook site to support social media messaging on this platform.
- g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.

Public: Gen X and Gen Y, ages 23-53

Objective 2-2: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” “You can...,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: Millennials (less than age 22)

Objective 2-3: Achieve 25 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” “You can...,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: State government employees

Objective 2-4: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” “You can...,” and others similar are appropriate.

Tactics:

Continue current activities via IOT.

Public: Local government employees

Objective 2-5: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: “Did You Know,” “How Can You...,” “You are part of the Solution,” “You can...,” and others similar are appropriate.

Special Tactics:

- a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
- b. Require all local government employees to take the training annually.
- c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives.

Communication should include the following:

1. Monthly email messages
2. Monthly Print feature stories
3. Monthly website postings for intranets

GOAL 3. ACHIEVE 15 PERCENT OF HOOSIERS ACTIVE IN CYBERSECURITY ACTIVITIES.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 15 percent active personal cybersecurity actions among Indiana Boomers/Traditionals one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a "call to action" step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: "To be part of the solution...", "How Can You...", "You can protect yourself...", "You can help by...", and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
 - b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
 - c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
 - d. Develop television media partners in each major market for cybersecurity messaging.
 - e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
 - f. Develop special Facebook site to support social media messaging on this platform.
 - g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.
-

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 15 percent active personal cybersecurity actions among Indiana Generation X'ers one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a “call to action” step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: “To be part of the solution...,” “How Can You...,” “You can protect yourself...,” “You can help by...,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: Millennials (less than age 22)

Objective 3-3: Achieve 15 percent active personal cybersecurity actions among Indiana Millennials one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a “call to action” step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: “To be part of the solution...,” “How Can You...,” “You can protect yourself...,” “You can help by...,” and others similar are appropriate.

Tactics:

- a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
 - b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
 - c. Develop special Facebook site to support social media messaging on this platform.
 - d. Develop special Instagram site to support social media messaging on this platform.
 - e. Develop special Snapchat site to support social media messaging on this platform.
 - f. Develop special Twitter site to support social media messaging on this platform.
 - g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.
-

Public: Indiana state government employee

Objective 3-4: Achieve 15 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Tactics:

Continue current activities via IOT.

Public: Local government employees

Objective 3-5: Achieve 15 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Strategy: Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a “call to action” step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: “To be part of the solution...,” “How Can You...,” “You can protect yourself...,” “You can help by...,” and others similar are appropriate.

Special Tactics:

- a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
- b. Require all local government employees to take the training annually.
- c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives. Communication should include the following:
 1. Monthly email messages
 2. Monthly Print feature stories
 3. Monthly website postings for intranets

GOAL 4. ACHIEVE 10 PERCENT AWARENESS OF CYBERSECURITY AS A CAREER FIELD AMONG HIGH SCHOOL STUDENTS.

Public: Indiana high school students

Objective 4-1: Achieve 10 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (An awareness test for cybersecurity careers will be created for evaluation purposes.)

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook. A secondary effort will approach key influencers like guidance counselors and technology teachers via conferences, direct mail, and the provision of collateral materials that promote the career field and provide information about its various elements and higher education opportunities and scholarships.

Message Strategy: Awareness is built initially via both informative and persuasive messages framed positively. To build awareness, messaging should include a focus on informing students about cybersecurity opportunities and persuading them to think positively about cybersecurity as a potential career field and field of study. Thus, messages should include statistics about open opportunities, salary information, educational opportunities, career advancement, scholarship opportunities, etc. Additionally, persuasive messaging should also be used to engage students. Thus, success stories and testimonials are appropriate.

Tactics:

- a. Develop special website with key Information about cybersecurity career opportunities for high school that can be used in conjunction with media outreach. Site should host detailed information, feature stories, in-state education opportunities, scholarship opportunities, etc. that can support a social media campaign.
- b. Create state-wide social media advertising campaign with a focus on opportunities for careers in cybersecurity to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
- c. Develop special Facebook site to support social media careers messaging on this platform.
- d. Develop special Instagram site to support social media careers messaging on this platform.
- e. Develop special Snapchat site to support social media careers messaging on this platform.
- f. Develop special Twitter site to support social media careers messaging on this platform.

- g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity career and education and features that highlight those opportunities.
- h. Create an outreach program for technology instructors/teachers in high schools that provides them information to share with students about cybersecurity careers and educational opportunities.
 - 1. Working with industry groups, create a cybersecurity speakers' bureau of cybersecurity professionals who can speak at high schools around the state.
 - 2. Promote the speakers' bureau to high school technology teachers.
 - 3. Create key collateral materials including a brochure, fact sheets, etc. that can be provided to technology teachers and speakers'.
 - 4. Work with university programs that offer cybersecurity education and training to integrate their efforts in the campaign.
 - 5. Use direct mail (printed) and email to communicate with technology teachers the opportunities for both careers and speakers'. Message at least monthly during school year.

GOAL 5. ACHIEVE 20 PERCENT AWARENESS OF STATEWIDE CYBERSECURITY PROTECTIVE ACTIVITIES BY GOVERNMENT AND INDUSTRY AMONG HOOSIERS.

Public: all Hoosiers

Objective 5-1: Achieve 20 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 3 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (Evaluation tool to be created.).

Strategy: This very broad public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana. The secondary approach will be social media, primarily Facebook and LinkedIn. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy:

Tactics:

- a. Establish a key public affairs position in the governor's office responsible for coordinating public information about cybersecurity state-wide, including overall coordination with Council and key departments (such as IOT, IDHS, State Police, others).
- b. Conduct a new conference upon completion of initial Cybersecurity Plan featuring the Governor and key Council leadership – especially industry partners. Support with news release and media kit. Consider this an annual event.
- c. Distribute monthly news release to all state media with key activities conducted during past month on a monthly basis.
- d. Conduct an annual cybersecurity conference and publicize heavily.
- e. Offer cybersecurity interviews routinely (at least quarterly) to key media, including business media, public affairs television shows, editorial boards of key newspapers, etc.

KEY OVERALL MESSAGES FOR PHASE 1

- Cybersecurity awareness is everyone's business.
- Cybersecurity knowledge is important to protect individuals and critical infrastructure.
- Cybersecurity activities are important to the defense of our identities, our computers, and our critical infrastructure networks.
- Cybersecurity training is free and available.
- Cybersecurity is a profession (targeted to high school students).
- The Cybersecurity Council's activities in helping defend Indiana from cyberattack. (this includes efforts by industries and sectors in the state via the C/WGs)
- Additional, very specific key messages:
 1. Effective and secure passwords are at least x characters long and include letters, numbers and symbols.
 2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
 3. A "phishing" attack is an effort to gain access to your personal information by getting you to reveal your logon and password information.
 4. Turning off smartphone GPS function does not prevent all location tracking.
 5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
 6. Ransomware involves criminals encrypting and holding users' data hostage until paid.
 7. Email is not encrypted by default.
 8. Wi-Fi traffic is not encrypted by default on all wireless routers.
 9. Browser programs' "private browsing" mode does not prevent ISP's from monitoring subscribers' online activity.
 10. [Https://](https://) in the URL means that information entered into the site is encrypted.
 11. A botnet is a networked set of computers used for criminal purposes.
 12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
 13. Using multi-factor authentication significantly enhances your personal online security.

GOALS PHASE 2: AFTER THREE YEARS (YEAR 2 & 3 OF THE CAMPAIGN):

Note: These outcomes, and the development of their appropriate strategies and tactics, will be updated using data/results from the evaluation of Phase 1 goals and objectives.

PHASE 2 GOALS

1. Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 60 percent of Hoosiers.
3. Achieve 45 percent active cybersecurity protective measures by Hoosiers.
4. Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
5. Achieve 40 percent awareness of cybersecurity as a career field among high school student

PHASE 2 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a “phishing” attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users’ data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs’ “private browsing” mode does not prevent ISP’s from monitoring subscribers’ online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	OPT	OPT	OPT
Credit Reports	REQ	REQ	REQ
Ransomware	REQ	REQ	REQ
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	OPT	OPT
Https	OPT	REQ	REQ
Botnet	OPT	OPT	OPT
VPN	OPT	REQ	REQ
Multi-factor Auth	REQ	REQ	REQ

4. **Awareness** equals correct answers to the 6 required questions and correct answers on at least 2 others.
5. **Knowledgeable** equals correct answers to the 10 required questions and at least one other.
6. **Action** will be measured via both survey and behavioral testing. To be considered “active” a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 2 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Evaluation results will be used to validate the target objectives for Phase 3.

GOAL 1. ACHIEVE 80 PERCENT AWARENESS OF CYBERSECURITY PROTECTIVE MEASURES BY HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 1-1: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: 2-Gen X and Gen Y, ages 23-53.

Objective 1-2: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: Millennials (less than age 22)

Objective 1-3: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: State government employees

Objective 1-4: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: Local government employees

Objective 1-5: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

GOAL 2. ACHIEVE KNOWLEDGE OF CYBERSECURITY PROTECTIVE MEASURES TO 60 PERCENT OF HOOSIERS.

Public: Traditionals

Objective 2-1: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: Gen X and Y

Objective 2-2: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: Millennials

Objective 2-3: Achieve 60 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: State government employees

Objective 2-4: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: Local government employees

Objective 2-5: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

GOAL 3. ACHIEVE 45 PERCENT ACTIVE CYBERSECURITY PROTECTIVE MEASURES BY HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 45 percent active personal cybersecurity actions among Indiana Boomers/Traditionals three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 45 percent active personal cybersecurity actions among Indiana Generation X'ers three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: Millennials (less than age 22)

Objective 3-3: Achieve 45 percent active personal cybersecurity actions among Indiana Millennials three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: state government employees

Objective 3-4: Achieve 45 percent active cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Strategy:

Tactics:

Public: Local government employees

Objective 3-5: Achieve 45 percent active cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Strategy:

Tactics:

GOAL 4. ACHIEVE 40 PERCENT AWARENESS OF CYBERSECURITY AS A CAREER FIELD AMONG HIGH SCHOOL STUDENT

Public: Indiana High School students

Objective 4-1: Achieve 40 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (Create awareness test for cybersecurity careers. Will recruit some help here.)

GOAL 5. ACHIEVE 50 PERCENT AWARENESS OF STATEWIDE CYBERSECURITY PROTECTIVE ACTIVITIES BY GOVERNMENT AND INDUSTRY AMONG HOOSIERS.

Public: All Hoosiers

Objective 5-1: Achieve 50 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 4 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (evaluation tool to be created).

Strategy:

Tactics:

GOALS PHASE 3: AFTER FIVE YEARS:

Note: These outcomes, and the development of their appropriate strategies and tactics, will be updated using data/results from the evaluation of Phase 2 goals and objectives (at the end of year three of the campaign).

GOALS

1. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.
3. Achieve 60 percent active cybersecurity protective measures by Hoosiers.
4. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
5. Achieve 70 percent awareness of cybersecurity as a career field among high school student

PHASE 3 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a “phishing” attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users’ data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs’ “private browsing” mode does not prevent ISP’s from monitoring subscribers’ online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	REQ	REQ	REQ
Credit Reports	REQ	REQ	REQ
Ransomware	REQ	REQ	REQ
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	REQ	REQ
Https	OPT	REQ	REQ
Botnet	OPT	REQ	REQ
VPN	REQ	REQ	REQ
Multi-factor Auth	REQ	REQ	REQ

7. **Awareness** equals correct answers to the 8 required questions and correct answers on at least 1 other.
8. **Knowledgeable** equals correct answers to the 10 required questions and at least two others.
9. **Action** will be measured via both survey and behavioral testing. To be considered “active” a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 3 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Goal 1. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 1-1: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: 2-Gen X and Gen Y, ages 23-53.

Objective 1-2: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: Millennials (less than age 22)

Objective 1-3: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: State government employees

Objective 1-4: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: Local government employees

Objective 1-5: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Goal 2. Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.

Public: Baby Boomers/Traditionals

Objective 2-1: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Gen Xers and Gen Yers

Objective 2-2: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Millennials

Objective 2-3: Achieve 80 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: State government employees

Objective 2-4: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Local government employees

Objective 2-5: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Goal 3. Achieve 60 percent active cybersecurity protective measures by Hoosiers.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 60 percent active personal cybersecurity actions among Indiana Boomers/Traditionals one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 60 percent active personal cybersecurity actions among Indiana Generation X'ers one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Millennials (less than age 22)

Objective 3-3: Achieve 60 percent active personal cybersecurity actions among Indiana Millennials one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Indiana state government employees

Objective 3-4: Achieve 60 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Public: Local government employees

Objective 3-5: Achieve 60 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Goal 4. Achieve 70 percent awareness of cybersecurity as a career field among high school students.

Public: Indiana high school students

Objective 4-1: Achieve 70 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (Create awareness test for cybersecurity careers. Will recruit some help here.)

Goal 5. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.

Public: all Hoosiers

Objective 5-1: Achieve 75 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 5 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (evaluation tool to be created.).

Outline Budget

Cybersecurity Public Awareness Plan: Phase 1 (first year) only
 Activities drawn from Tactics for Phase 1 Goals and Objectives

This outline budget is applicable to the Phase 1 activities identified in this plan. It is based on best estimates for all of the strategies and tactics recommended. It is also expected, however, that this budget will be fine-tuned as agents are assigned for plan execution, and as selected tactical activities are either selected or rejected in the normal process of plan execution.

It assumes that one or more persons be hired to manage the campaign overall with either assistance from multiple state agencies, and/or with assistance from a third-party vendor – an advertising or public relations firm.

It is also important to note that this budget does not address training management nor the cost of obtaining and delivering cybersecurity training to local government employees or others.

Additionally, while we have recommended the Cybersecurity program be properly “branded,” the cost of that effort is not included in this budget.

Activity	Description	Agent	Cost	Notes
Cybersecurity Public Relations Director	Per recommendation, hire a senior public relations professional to take overall responsibility for the campaign and also serve as overall spokesperson on cybersecurity issues.	New Hire; locate in Governor’s office with appropriate directive authority.	\$119,000	Estimated based on a hire at \$85,000 plus benefits (@40%).
Website	Develop and maintain a website designed specifically for the public to provide information on cybersecurity protective measures and education/training opportunities	State: IOT (continue and expand current site; rebrand away from IOT	\$0	Assume this rebranding and build/maintain can be accomplished in-house using collective assets
Earned Media	Monthly feature release on cybersecurity methods to print and broadcast media	CS PR Director	\$0	In-house activity
PSAs	Create and distribute monthly PSAs to radio outlets around the state matching news release feature messages.	CS PR Director	\$12,000*	This may be handled in-house if technology and distribution can be managed. Otherwise, contract to external agency. \$1,000 per month.
Media Partners	Develop relationship with at least one television partner in each major market to help distribute information on cybersecurity	CS PR Director	\$0	Expect this activity can be handled in-house. Results will vary as will actual activities.

Activity	Description	Agent	Cost	Notes
Advertising Campaign	Create state-wide advertising campaign (print, radio, television, social media) to deliver cybersecurity messages on a consistent monthly basis.	External agency supervised by CS PR Director	\$5,000	Initial campaign development
			\$1,500	Monthly creative
			\$10,000	Monthly ad buy
			Total: \$143,000	
Social media	Create new Facebook, Instagram, Twitter, Snapchat, LinkedIn sites/pages focused on Cybersecurity and branded appropriately.	In house managed by CS PR Director and executed via identified agencies in coordination.	\$0	In house
Speakers' Bureau	Develop, promote and maintain a speakers' bureau to provide speakers to civic and other organizations on Cybersecurity.	Directed by CS PR Director using a volunteer state agency to manage. <u>Alternative:</u> hire entry level PR professional to manage. Use qualified volunteers for speakers.	\$0	Development and maintenance.
			\$42,000	Alt: PR Coordinator: \$30,000 plus benefits. <u>Note:</u> if hiring, this coordinator also can assume other cybersecurity communication responsibilities for this program reducing reliance on other agencies who would perform these duties as collateral responsibility.
			\$12,000	Travel and expenses for speakers at \$1,000 monthly
Local Government Training Program	Develop and support local government employee training program meeting the same standards as state government employees.	Managed locally and operated via IOT Training.	\$???	
Local government direct email	Consistent with features and web materials, promotion monthly via email directly to all local government employees`	CS PR Director ICW local governments	\$0	In-house; will require close coordination with local government entities. Probably simplest to provide copy to key contacts for redistribution.
Local government feature stories and web postings	Materials produced and provided to local governments for use and promotion via email.	Direction: CS PR Director Action: Shared responsibility with key agencies	\$0	Assumed that materials produced for state distribution can be repackaged for local government distribution.
Total (low estimate)			\$286,000	Local training costs not included
Total (high estimate)	Recommended		\$328,000	Local training costs not included

Activity	Description	Agent	Cost	Notes
Option:	Understanding that this campaign may need to be implemented earlier than a solid budget can be allocated, one way to reduce the cost is to defer the paid advertising program to Phase 2 (second two years). That would save \$143,000 this initial first-year budget.		\$185,000	Local training costs not included
Note:	Training management and coordination			This budget does not include provision for a central training manager to coordinate available training assets for delivery to various publics, including local government employees.

ITU Cybersecurity Index

2017



Global Cybersecurity Index (GCI) 2017



Global Cybersecurity Index 2017

Acknowledgments

This report has been produced by the International Telecommunication Union (ITU) with the support of Michael Minges. The Cybersecurity Team of the ITU would like to express its appreciation to Dr. Sherif Hashem (NTRA Egypt), Michaela Saisanna and Hedvig Norlen (Joint Research Centre of the European Commission) as well as the Rapporteurs of the Study Group 2 Question 3 Rozalin Al-Balushi (Oman) and Eliot Lear (USA) for their input to the Global Cybersecurity Index (GCI) work and report.

The online questionnaire preparation, secondary data collection, data validation and report elaboration have been carried out with the support of Mohaamed Ahmed Yousef Aly, Ahmed Abd Allah Abd El- Latif, Tymoteusz Kurpeta, Benjamin Lim, Daniela Toma, Grace Rachael Acayo, and Lena Lattion.

If you have any comments, please contact the ITU Cybersecurity Team: cybersecurity@itu.int

ISBN

978-92-61-25061-4 (paper version)

978-92-61-25071-3 (electronic version)

978-92-61-25081-2 (EPUB version)

978-92-61-25091-1 (Mobi version)



Please consider the environment before printing this report.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

The global community is increasingly embracing ICTs as key enabler for social and economic development. Governments across the world recognize that digital transformation has the power to further the prosperity and wellbeing of their citizens. In supporting this transformation, they also recognize that cybersecurity must be an integral and indivisible part of technological progress.



In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world.

First launched in 2014, the goal of the Global Cybersecurity Index (GCI) is to help foster a global culture of cybersecurity and its integration at the core of ICTs. This second iteration of the GCI measures the commitment of ITU Member States towards cybersecurity in order to drive further efforts in the adoption and integration of cybersecurity on a global scale.

The GCI reaffirms ITU's commitment to build confidence and security in the use of ICTs. This report on the second iteration of the GCI continues to show the cybersecurity commitment of ITU Member States around the world, and I am pleased to note that the overall picture shows improvement and strengthening of the global cybersecurity agenda.

I wish to thank Member States for their contribution to this effort.

The collection of information for the GCI is an ongoing process, and I therefore invite all ITU Member States to continue sending and updating information on their cybersecurity efforts so that we can effectively share experiences, views and solutions in order to make the digital world a more secure and safe environment for all citizens.

A handwritten signature in blue ink, appearing to read 'Brahima Sanou'.

Brahima Sanou

Director, Telecommunication Development Bureau

Executive Summary

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected.

One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein cover all 193 ITU Member States.

The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible. The level of development of the different pillars varies from country to country in the regions, and while commitment in Europe remains very high in the legal and technical fields in particular, the challenging situation in the Africa and Americas regions shows the need for continued engagement and support.

In addition to providing the GCI score, this report also provides a set of illustrative practices that give insight into the achievements of certain countries.

Table of Contents

Foreword	iii
Executive Summary	v
1 Introduction	1
2 GCI Scope and Framework	3
2.1 Background	3
2.2 Reference model	3
2.3 Conceptual framework	4
3 Methodology	9
4 Key Findings	13
4.1 Heat Map of National Cybersecurity Commitments	13
4.2 GCI Groups	13
5 Global Outlook	17
5.1 Noteworthy figures	17
5.2 Comparing GCI with other indices	19
6 Regional Outlook	25
6.1 Africa	26
6.2 Americas	28
6.3 Arab States	30
6.4 Asia and the Pacific	32
6.5 Commonwealth of Independent States	34
6.6 Europe	36
7 Illustrative practices by pillar	39
7.1 Legal	39
7.1.1 Cybercrime legislation	39
7.1.2 Cybersecurity regulation	39
7.1.3 Cybersecurity training	39
7.2 Technical	40
7.2.1 National CERT/CIRT/CSIRT	40
7.2.2 Government CERT/CIRT/CSIRT	40
7.2.3 Sectoral CERT/CIRT/CSIRT	40
7.2.4 Cybersecurity standards implementation framework for organizations	41
7.2.5 Child online protection	41
7.3 Organizational	41
7.3.1 Strategy	41
7.3.2 Public consultation	42
7.3.3 Responsible agency	42
7.3.4 Cybersecurity metrics	42
7.4 Capacity building	42
7.4.1 Standardization bodies	42
7.4.2 Good practice	42

7.4.3	Cybersecurity research and development programmes	43
7.4.4	Public awareness campaigns	43
7.4.5	Cybersecurity professional training courses	43
7.4.6	National education programmes and academic curricula	43
7.4.7	Incentive mechanisms	43
7.4.8	Home-grown cybersecurity industry	44
7.5	Cooperation	44
7.5.1	Bilateral agreements	44
7.5.2	Multilateral agreements	44
7.5.3	Participation in international fora	44
7.5.4	Public-private partnerships	45
7.5.5	Interagency partnerships	45
8	Conclusion	47
	Abbreviations	49
	Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region	51
	Annex 2 – GCI 2017 Score	59

List of Tables, Figures and Boxes

Tables

Table 3.1: Numbers of responses received from all Members States regionally	10
Table 5.1: Top ten most committed countries, GCI (normalized score)	17
Table 6.1.1: Top three ranked countries in Africa	26
Table 6.2.1: Top three ranked countries in the Americas	28
Table 6.3.1: Top three ranked countries in the Arab States	30
Table 6.4.1: Top three ranked countries in Asia and the Pacific	32
Table 6.5.1: Top three ranked countries in Commonwealth of Independent States	34
Table 6.6.1: Top three ranked countries in Europe	36

Figures

Figure 2.3.1: GCI pillars and sub-pillars	5
Figure 2.3.2: GCA tree structure illustrating all pillars (simplified)	6
Figure 2.3.3: GCI tree structure illustrating Legal pillar	7
Figure 4.1.1: GCI Heat Map	13
Figure 4.2.1: GCI Tiers	14
Figure 5.1.1: Cybersecurity strategy and training commitments	18
Figure 5.1.2: Computer emergency response teams and metrics	18
Figure 5.1.3: Home-grown industry and international participation	19
Figure 5.2.1: Global comparison GCI and IDI	20
Figure 5.2.2: Comparison GCI and IDI in the Africa region	20
Figure 5.2.3: Comparison GCI and IDI in the Americas region	21
Figure 5.2.4: Comparison GCI and IDI in the Arab States	21
Figure 5.2.5: Comparison GCI and IDI in the Asia and the Pacific region	22
Figure 5.2.6: Comparison GCI and IDI in the Commonwealth of Independent States	22
Figure 5.2.7: Comparison GCI and IDI in the Europe region	23
Figure 6.1: Average pillar scores by region	25
Figure 6.1.1: Top three ranked countries in Africa and global ranked of all countries in Africa	26
Figure 6.1.2: Africa region scorecard	27
Figure 6.2.1: Top three ranked countries and an average score of all the Americas	28
Figure 6.2.2: Americas region scorecard	29
Figure 6.3.1: Top three ranked countries and an average score of the Arab States	30
Figure 6.3.2: Arab States scorecard	31
Figure 6.4.1: Top three ranked countries and an average score of all Asia and the Pacific	32
Figure 6.4.2: Asia and the Pacific Region Scorecard	33
Figure 6.5.1: Top three ranked countries and an average score of all CIS	34
Figure 6.5.2: CIS region scorecard	35
Figure 6.6.1: Top three ranked countries and an average score of all Europe	36
Figure 6.6.2: Europe region scorecard	37

1 Introduction

The information and communication technologies (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half the world used the Internet (3.5 billion users)¹ and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020². Yet, just as in the real world, the cyber world is exposed to a variety of security threats that can cause immense damage.

Statistics on threats to computer networks are sobering and reflect a shift from the relatively innocuous spam of yesteryear to threats that are more malicious. A security company tracking incidents in 2016 found that malicious emails became a weapon of choice for a wide range of cyberattacks during the year used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One-in-131 emails sent were malicious, the highest rate in five years.

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to USD 1 077, up from USD 294 a year earlier³. The scale of cybercrime makes it critical for governments to have a robust cybersecurity ecosystem in place to reduce threats and enhance confidence in using electronic communications and services.

It is therefore clear that there is a direct cause-effect principle between the growth of ICTs and their illicit and malicious use. To counter this effect, cybersecurity is becoming more and more relevant in the minds of countries' decision makers, and cybersecurity related doctrines have been established in almost all countries in the world.

However, there is still an evident gap between countries in terms of awareness, understanding, knowledge and finally capacity to deploy the proper strategies, capabilities and programmes to ensure a safe and appropriate use of ICTs as enablers for economic development.

In this context, ITU, together with international partners from private-public and private sector as well as academia, has established the GCI with the key objective of building capacity at the national, regional and international level, through assessing the level of engagement of countries on cybersecurity, and, with the data gathered, producing a list of good practices that can be used by countries in need.

¹ www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

² www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

³ www.symantec.com

2 GCI Scope and Framework

2.1 Background

The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. Specifically, Member States are invited “to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors”.

A first iteration of the GCI was conducted in 2013-2014 in partnership with ABI Research¹, and the final results have been published².

Following feedback received from various communities, a second iteration of the GCI was planned and undertaken. This new version was formulated around an extended participation from Member States, experts and industry stakeholders as contributing partners (namely World Bank and Red Team Cyber as new GCI partners joining the Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet & Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica and UNODC) who all provided support with the provision of secondary data, response activation, statistical analysis, qualitative appreciation amongst other.

The data collected via GCI 2017 for ITU-D Study Group 2 Question 3 (SG2Q3) surveys have been analysed by the Rapporteur and co-Rapporteur for inclusion in the SG2Q3 final report. GCI partners have been active in providing expertise and secondary data as appropriate, while the UN office of ICT (New York) has also initiated collaborative work. ITU is also working in a multi-stakeholder collaboration led by the World Bank to elaborate a toolkit on “Best practice in Policy/Legal enabling Framework and Capacity Building in Combatting Cybercrime”. ITU is providing support on the component on capacity building from a cybersecurity perspective based on GCI 2017 data.

An enhanced reference model was thereby devised. Throughout the steps of this new version, Member States were consulted using various vehicles including ITU-D Study Group 2 Question 3/2, where the overall project was submitted, discussed and validated.

2.2 Reference model

The GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. These pillars form the five pillars of GCI.

The main objectives of the GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- the progress in cybersecurity commitment of all countries from a global perspective;
- the progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

¹ <https://www.abiresearch.com/>

² <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx>

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering, a global culture of cybersecurity.

2.3 Conceptual framework

The five pillars of the GCI are briefly explained below:

1. **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. **Capacity Building:** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Figure 2.3.2 below represents all the five pillars from GCA with their indicators.

Figure 2.3.2: GCA tree structure illustrating all pillars (simplified)

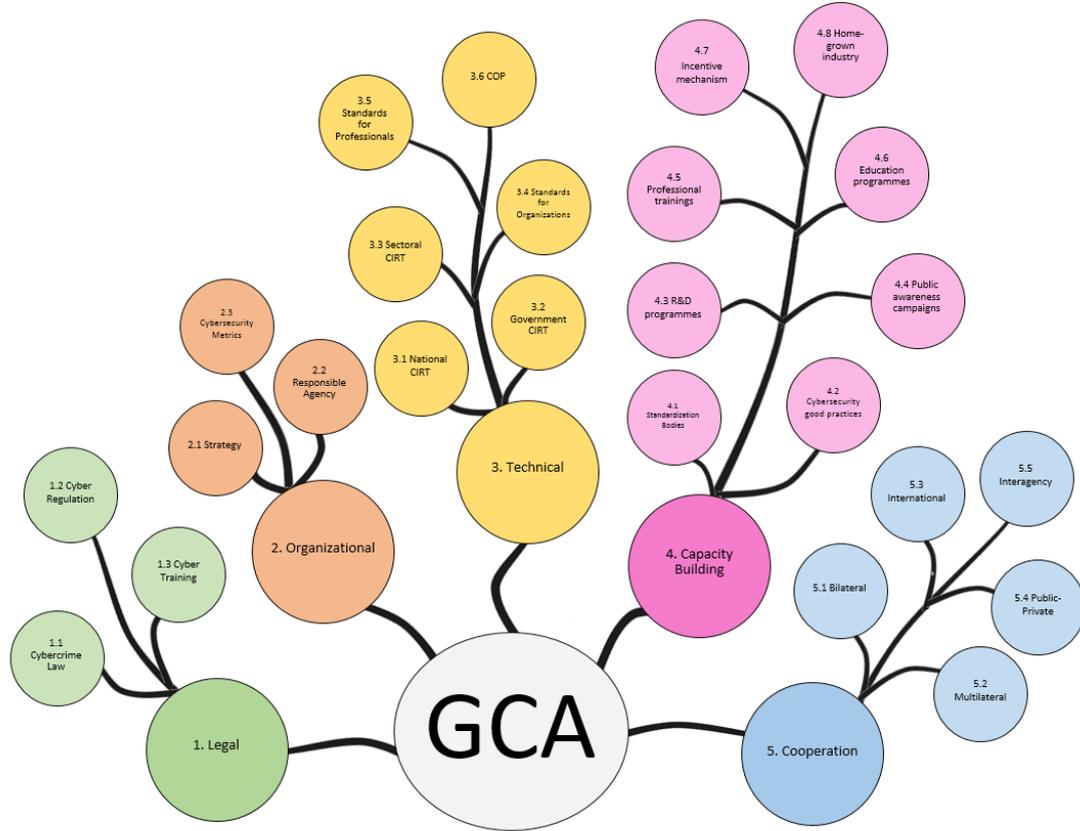
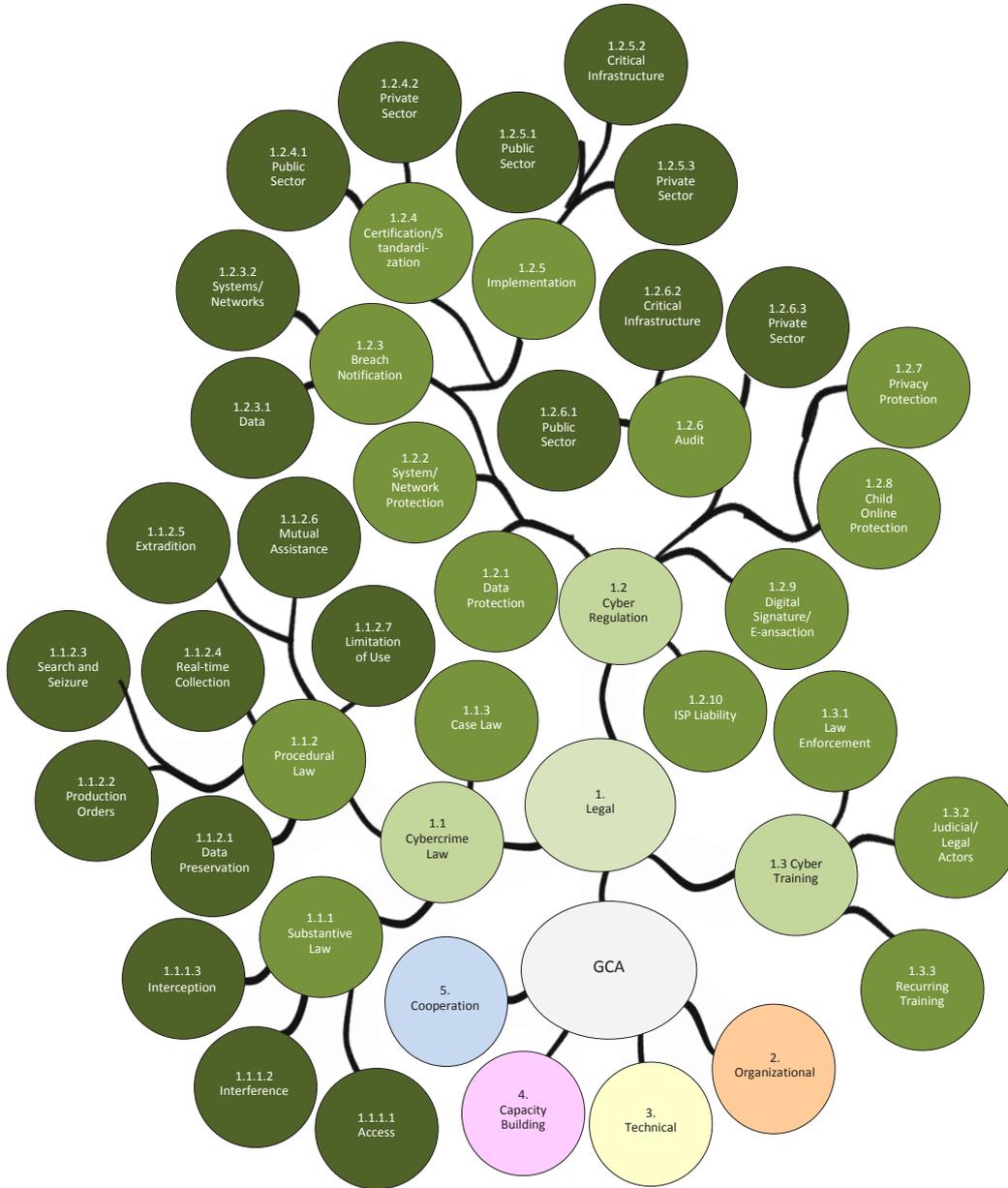


Figure 2.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 2.3.3: GCI tree structure illustrating Legal pillar



3 Methodology

The GCI includes 25 indicators and 157 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- relevance to the five GCA pillars and in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.

The whole concept of a new iteration of the GCI is based on a cybersecurity development tree map and binary answer possibilities.

The tree map concept, which is illustrated in Figures 2.3.2 and 2.3.3, is an example of different possible paths that might be taken by countries in order to enhance their cybersecurity commitment.

Each of the five pillars are associated with a specific colour. The deeper the path taken, indicating a more developed level of commitment, the deeper the colour depicting it becomes.

The various levels of cybersecurity development among countries, as well as the different cybersecurity needs reflected by a country's overall ICT development status, were taken into consideration. The concept is based on the assumption that the more developed cybersecurity is, the more complex the solutions observed will be. Therefore, the further a country goes along the tree map by confirming the presence of pre-identified cyber solutions, the more complex and sophisticated the cybersecurity commitment is within that country, allowing it to obtain a higher score with the GCI.

The rationale behind using binary answer possibilities is the elimination of opinion-based evaluation and of any possible bias towards certain types of answers.

Moreover, the simple binary concept will allow quicker and more complex evaluation as it will not require lengthy answers from countries. This, in turn, is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm the presence or lack of certain pre-identified cybersecurity solutions. An online survey mechanism, which was used for gathering answers and uploading all relevant materials, enabled the extraction of good practices.

The key difference in methodology between GCI 2014 and GCI Version 2017 is the use of a binary system instead of a three-level system. The binary system evaluates the existence or absence of a specific activity, department or measure. Unlike GCI Version 2014, it does not take 'partial' measures into consideration. The facility for respondents to upload supporting documents and URLs is a way of providing more information to substantiate the binary response. Furthermore, a number of new questions have been added in each of the five pillars in order to refine the depth of research.

The GCI 2014 and GCI 2017 are not directly comparable due to a change in methodology. While the 2014 index used a simple average methodology, the 2017 index employs a weighting factor for each pillar.

The questionnaire, made available through an online survey from January to September 2016, was administered to the 193 ITU Member States (plus State of Palestine) in the regions of Africa, Americas, Arab States, Asia and the Pacific, the Commonwealth of Independent States, and Europe. 134 countries responded to the online survey while 59 countries did not provide primary data.

Table 3.1: Numbers of responses received from all Members States regionally

Region	Africa	Americas	Arab States	Asia and the Pacific	CIS	Europe	Global
Responses	29	23	16	25	7	34	134
Non-responses	15	12	5	13	5	9	59
Total of participants	44	35	21	38	12	43	193

The data collection process was implemented as follows:

1. A **Letter of Invitation** was sent by the ITU Secretariat to all Member States, informing them on the initiative and requesting the identification of a country level GCI focal point with whom ITU could liaise and who would be responsible for collecting all relevant data for completing the online GCI questionnaire. A guideline to the online questionnaire which provided explanations and examples for each question, was attached to the letter¹.
2. **Primary data collection** (for countries who responded to the questionnaire):
 - Verification of the responses received by the specific Member State to identify possible missing elements (no or missing responses, no or missing supporting documents, no or missing links, etc.).
 - For instance, if a Member State answered “No”, ITU researched to prove that they do not have any documents in the ITU database or online.
 - If a Member State answered “Yes”, ITU researched to verify that answers provided were correct and corresponded to the question.
 - The focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
 - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.
 - Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.
3. **Secondary data collection** (for countries that did not respond to the questionnaire):
 - ITU elaborated an initial draft of the response to the questionnaire using publicly available data and online research.
 - The draft was then sent to the concerned Member State for review.
 - The reviewed response received, the focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
 - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.

¹ <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf>

- Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.

The GCI 2017 methodology encompassed the use of a panel of experts, identified according to their specific expertise on the subject, who acted in their personal capacity in order to provide an expert view on the weighting to be used for the scoring.

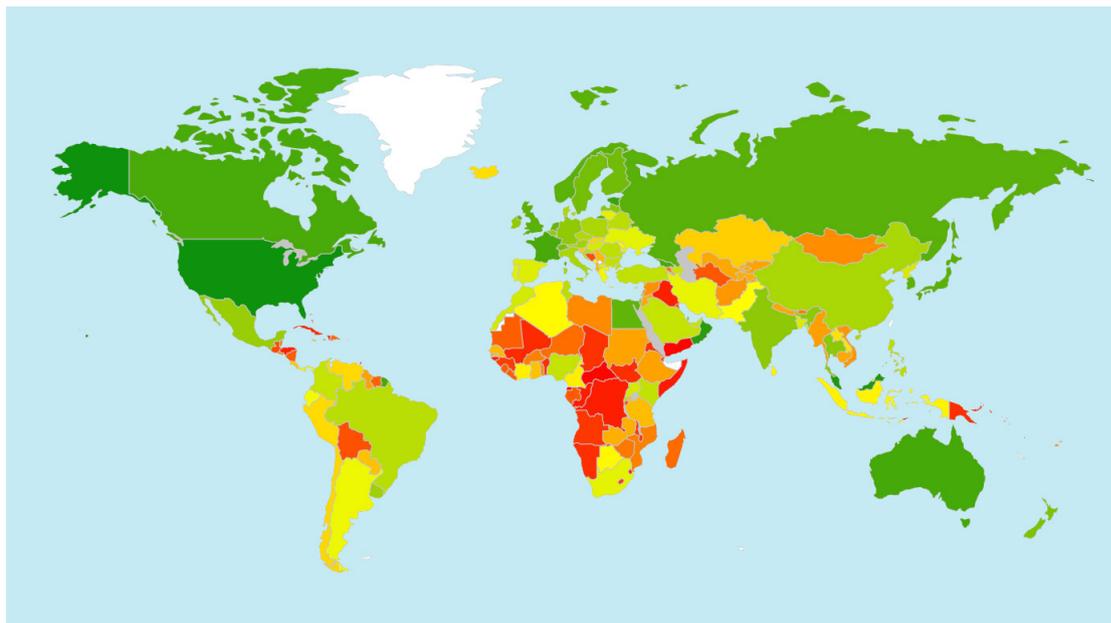
4 Key Findings

4.1 Heat Map of National Cybersecurity Commitments

Out of the 193 Member States, there is a huge range in cybersecurity commitments, as the heat map below illustrates.

Level of commitment: from Green (highest) to Red (lowest)

Figure 4.1.1: GCI Heat Map



4.2 GCI Groups

Member States were classified into three categories by their GCI score (Figure 4.2.1).

- *Initiating stage* refers to the 96 countries (i.e., GCI score less than the 50th percentile) that have started to make commitments in cybersecurity.
- *Maturing stage* refers to the 77 countries (i.e., GCI score between the 50th and 89th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Leading stage* refers to the 21 countries (i.e., GCI score in the 90th percentile) that demonstrate high commitment in all five pillars of the index.

Figure 4.2.1: GCI Tiers

INITIATING		
Afghanistan	Guatemala	Palau
Andorra	Guinea	State of Palestine
Angola	Guinea-Bissau	Papua New Guinea
Antigua and Barbuda	Guyana	Saint Kitts and Nevis
Armenia	Haiti	Saint Lucia
Bahamas	Honduras	Saint Vincent & the Grenadines
Barbados	Iraq	Samoa
Belize	Jordan	San Marino
Benin	Kiribati	Sao Tome and Principe
Bhutan	Kuwait	Seychelles
Bolivia (Plurinational State of)	Kyrgyzstan	Sierra Leone
Bosnia & Herzegovina	Lebanon	Solomon Islands
Burkina Faso	Lesotho	Somalia
Burundi	Liberia	South Sudan
Cambodia	Libya	Sudan
Cape Verde	Liechtenstein	Suriname
Central African Republic.	Madagascar	Swaziland
Chad	Malawi	Syrian Arab Republic
Comoros	Maldives	Tajikistan
Congo	Mali	Timor-Leste
Cuba	Marshall Islands	Togo
Democratic Republic of the Congo	Mauritania	Tonga
Djibouti	Micronesia	Trinidad and Tobago
Dominica	Monaco	Turkmenistan
Dominican Republic	Mongolia	Tuvalu
El Salvador	Mozambique	Uzbekistan
Equatorial Guinea	Myanmar	Vanuatu
Eritrea	Namibia	Vatican
Ethiopia	Nauru	Viet Nam
Fiji	Nepal (Republic of)	Yemen
Gabon	Nicaragua	Zambia
Gambia	Niger	Zimbabwe
Grenada		

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

LEADING		
Australia	Japan	Oman
Canada	Korea	Russian Federation
Egypt	Malaysia	Singapore
Estonia	Mauritius	Sweden
Finland	Netherlands	Switzerland
France	New Zealand	United Kingdom
Georgia	Norway	United States

5 Global Outlook

All of the six ITU regions are represented in the top ten commitment level in the GCI. There are three from Asia and the Pacific, two each from Europe and the Americas, and one from Africa, the Arab States, and the Commonwealth of Independent States.

This suggests that being highly committed is not strictly tied to geographic location.

Table 5.1: Top ten most committed countries, GCI (normalized score)

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

As the GCI shows, there is a wide gulf in cyber preparedness around the globe. This gap exists between and within regions.

Further, cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.

Additionally, cybersecurity is not just a concern of the government but also needs commitment from the private sector and consumers. Thus, it is important to develop a cybersecurity culture where citizens are aware of the trade-off between risks and monitoring when using electronic networks.

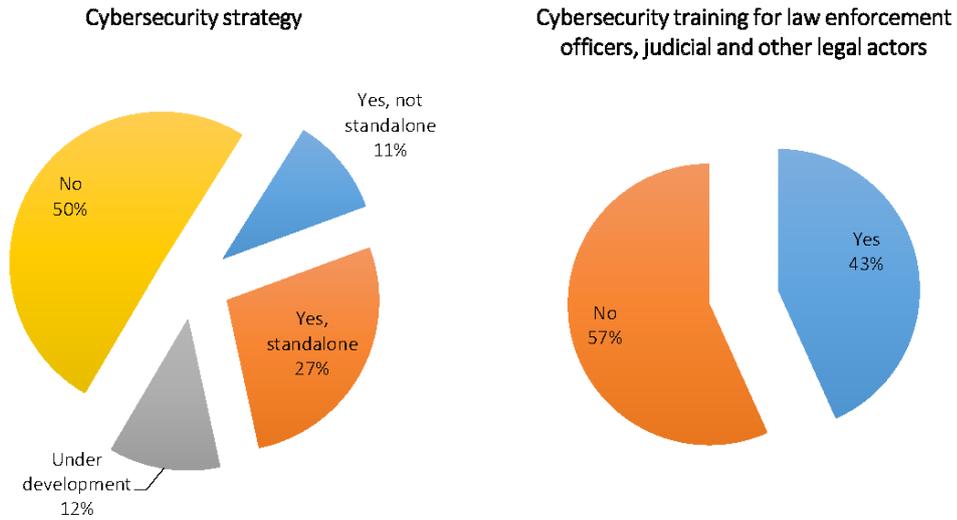
5.1 Noteworthy figures

The GCI consists of 25 different indicators. Some relate to precise commitments that help to concretize the status of specific cybersecurity activities throughout the world.

One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. Only 38% countries have a published cybersecurity strategy and only 11% have a dedicated standalone strategy (Figure 5.1.1, left); another 12% have a cybersecurity strategy under development.

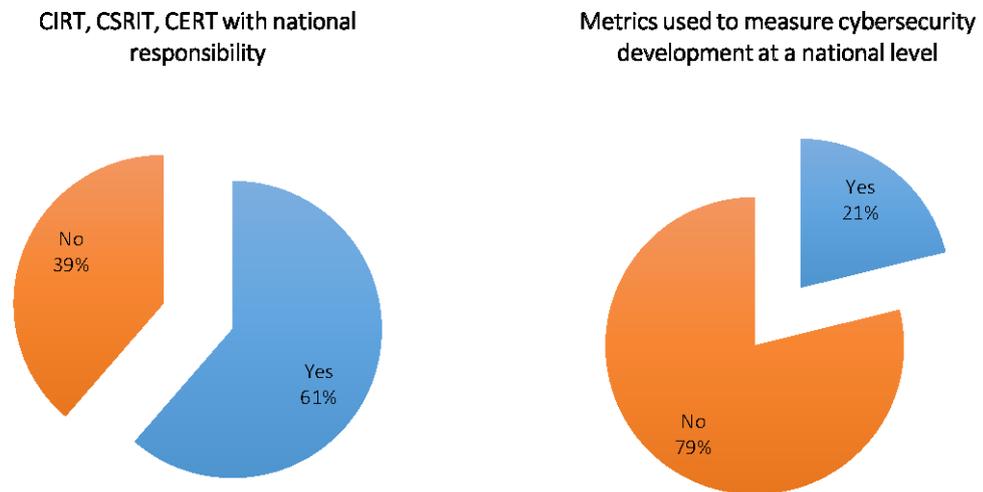
More effort is needed in this critical area, particularly since it conveys that the government considers digital risks high priority. In the area of training, efforts need to be enhanced particularly for those who are most likely going to legally handle cybersecurity crimes given that less than half the Member States (43%) have capacity-building programmes for law enforcement and the judicial system (Figure 5.1.1, right).

Figure 5.1.1: Cybersecurity strategy and training commitments



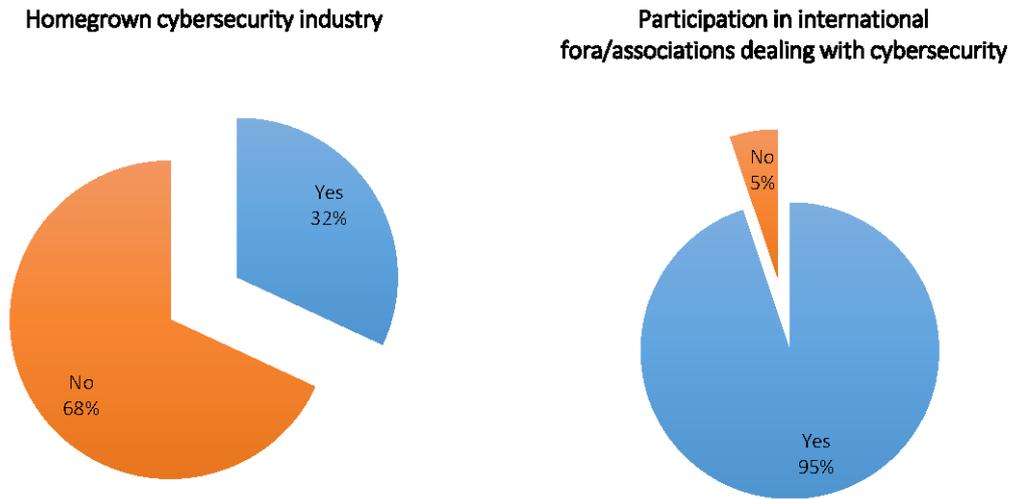
Despite half of the Member States not having a cybersecurity strategy, 61% do have an emergency response team (i.e., CIRT, CSRIT, and CERT) with national responsibility (Figure 5.1.2, left). However, just over a fifth (21%) publish metrics on cybersecurity incidents (Figure 5.1.2, right). This makes it difficult in most countries to objectively assess incidents based on the evidence and determine if protection measures are working.

Figure 5.1.2: Computer emergency response teams and metrics



Just less than a third of countries (32%) replied affirmatively to the existence of a homegrown cybersecurity industry (Figure 5.1.3, left). More efforts need to be devoted to this area as a local industry will have knowledge of national circumstances and make the security ecosystem more sustainable. The potential for global cooperation is heightened by participation in international cybersecurity events. This is almost universal with 95% of countries replying affirmatively (Figure 5.1.3, right).

Figure 5.1.3: Home-grown industry and international participation



5.2 Comparing GCI with other indices

A qualitative comparison has been performed to raise awareness on the importance of investing on cybersecurity, as an integral component of any national ICT for development strategy.

This paragraph is not intended to provide thorough, exhaustive statistical analysis, but rather an indication on how cybersecurity can relate to existing national processes, in order to emphasize the importance of investing and being committed.

Comparing GCI scores to notable ICT for Development Indices does not reveal an especially close relationship as experience shows that countries which score high in term of ICT for Development do not necessarily invest in cybersecurity with the same level of commitment, and vice versa.

For example, comparing the GCI with the ITU ICT for Development Index (IDI), shows that some countries are performing much better in the GCI than their level of ICT development would suggest.

The following figures show the relation between the GCI and IDI with each graph identifying the top three countries for each region.

Figure 5.2.1: Global comparison GCI and IDI

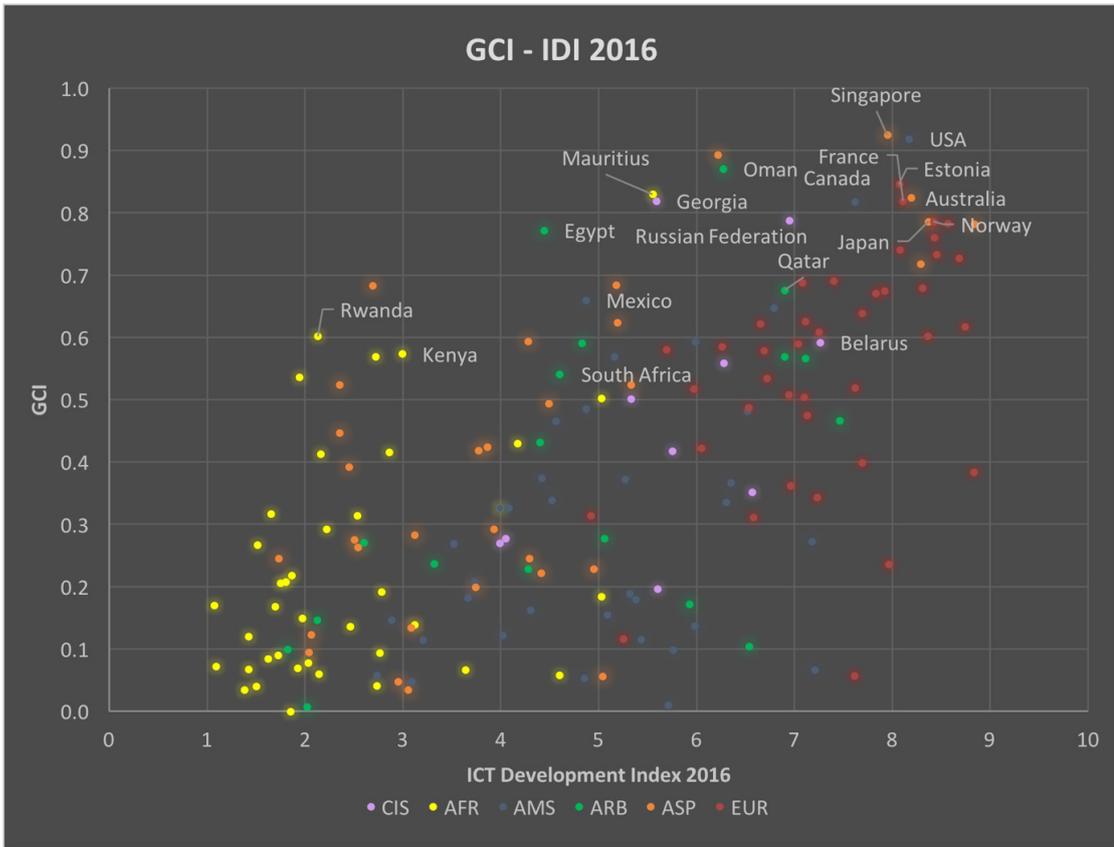


Figure 5.2.2: Comparison GCI and IDI in the Africa region

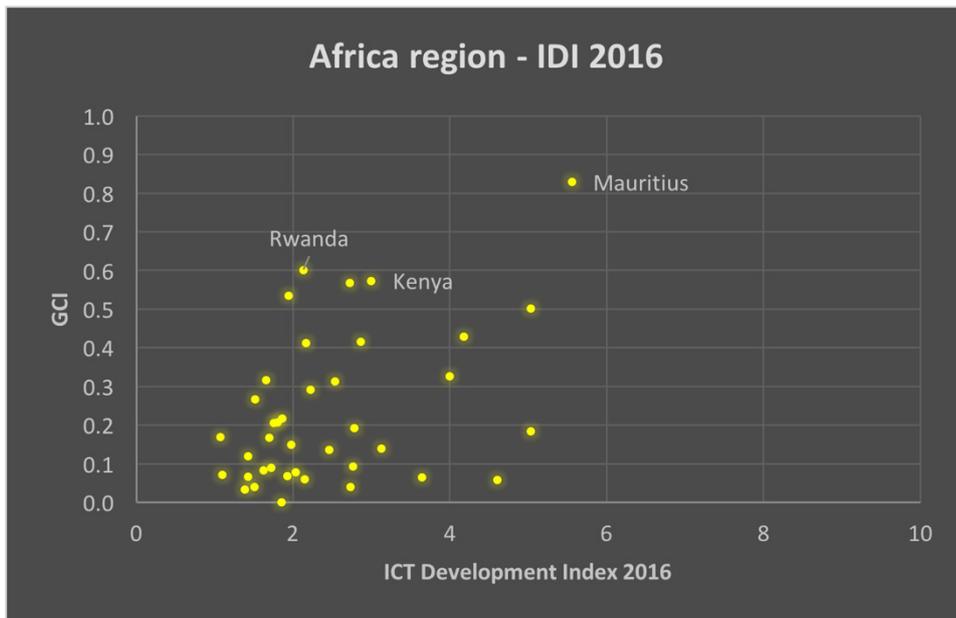


Figure 5.2.3: Comparison GCI and IDI in the Americas region

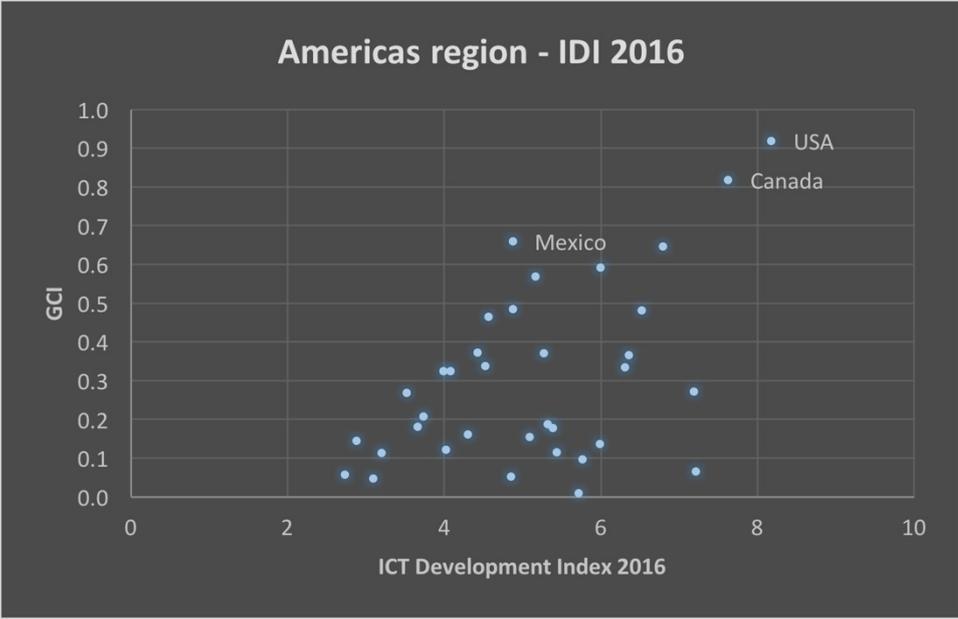


Figure 5.2.4: Comparison GCI and IDI in the Arab States

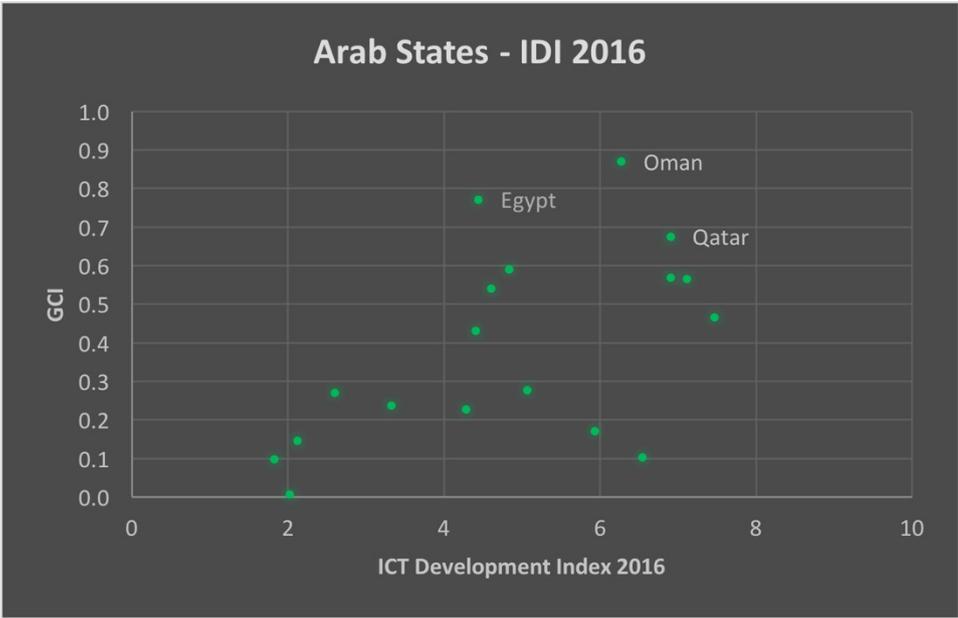


Figure 5.2.5: Comparison GCI and IDI in the Asia and the Pacific region

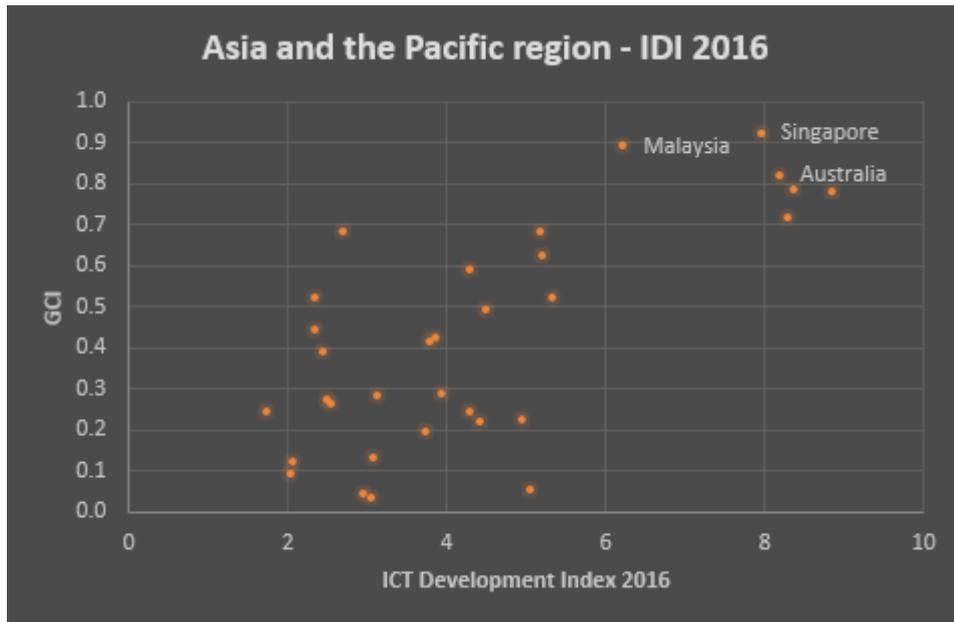


Figure 5.2.6: Comparison GCI and IDI in the Commonwealth of Independent States

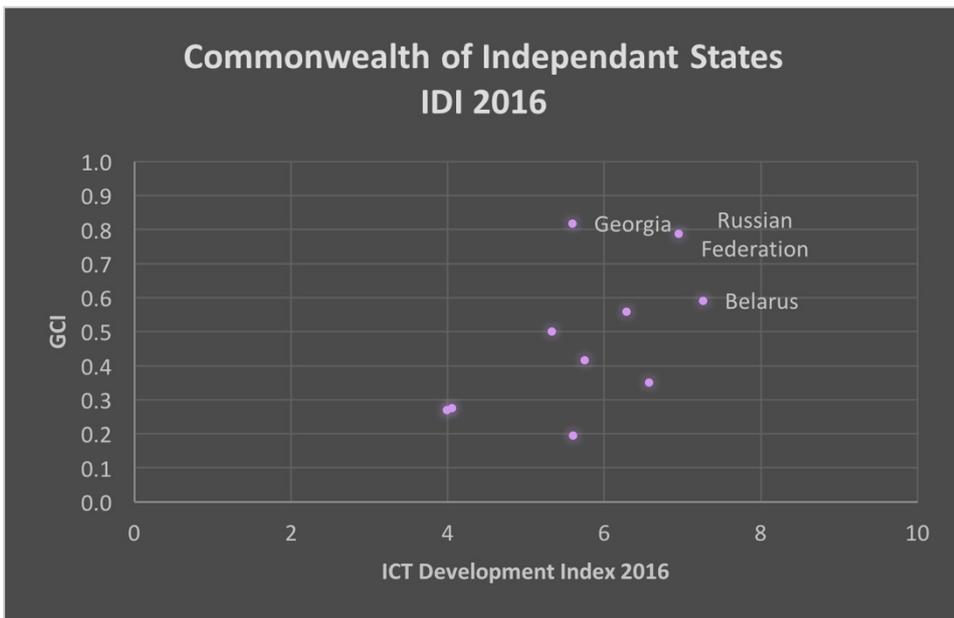
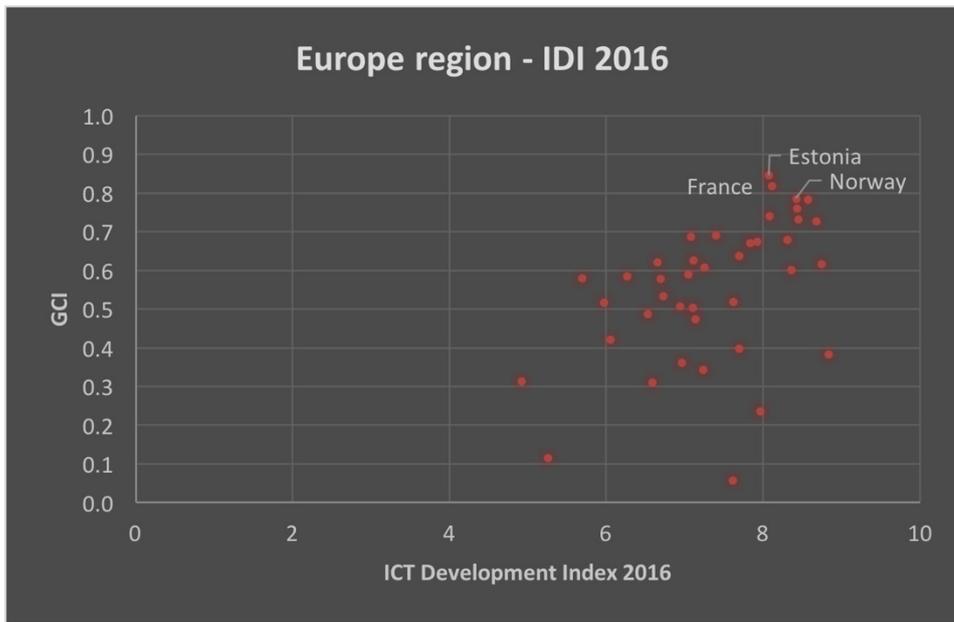


Figure 5.2.7: Comparison GCI and IDI in the Europe region



6 Regional Outlook

During the active data collection phase of the GCI 2017 exercise, there was a varied response from countries in the ITU regions:

- Out of the 44 Member States in the Africa region, 29 responded to the survey.
- Out of 35 Member States in the Americas region, 23 responded to the survey
- Out of 21 Member States in the Arab States region, 17 including the State of Palestine responded to the survey.
- Out of 38 Member States in the Asia and the Pacific region, 25 responded to the survey
- Out of the 12 Member States in the Commonwealth of Independent States region, 7 responded to the survey
- Out of 43 Member States in the Europe region, 34 responded to the survey.

Figure 6.1 illustrates the average GCI score for all countries in a particular region for the respective pillar. Scores that fall below the 33rd percentile have a red background, scores that are between the 33rd to 65th percentiles have a yellow background and scores that lie above the 65th percentile have a green background. There is scope for improvement since most regions have an average score for the different pillars (i.e., lying between 33rd and 65th percentiles).

The exception is Europe, where average scores are high across all pillars. The Africa region averages low scores for the organizational pillar while the Commonwealth of Independent States region averages a high score for the legal pillar.

The following sub-sections show the findings for each individual ITU region, highlighting the results and findings for the three top-scoring countries in each region. As well, a “regional scorecard” summarizes the countries’ level of commitment to every pillar and sub-pillars (green for high, yellow for medium, and red for low).

Figure 6.1: Average pillar scores by region

Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.61	0.60	0.45	0.49	0.46

6.1 Africa

Table 6.1.1: Top three ranked countries in Africa

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Mauritius	0.83	0.85	0.96	0.74	0.91	0.7
Rwanda	0.6	0.6	0.71	0.79	0.66	0.28
Kenya	0.57	0.75	0.73	0.36	0.41	0.6

Mauritius is the top ranked country in the Africa region. It scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to curtail threats on different networks within the country. Capacity building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2 000 civil servants in 32 government ministries and departments.



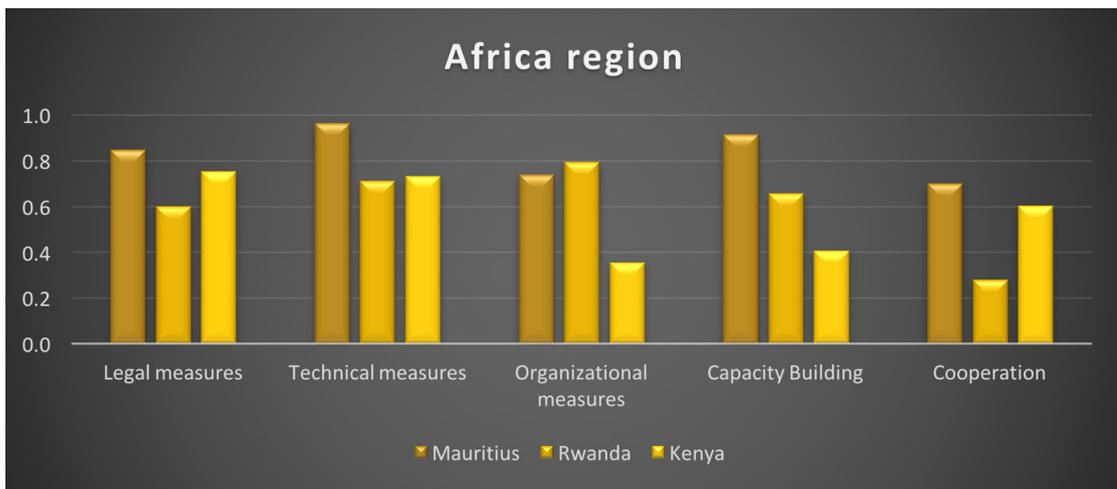
Rwanda, ranked second in Africa, scores high in the organizational pillar and has a standalone cybersecurity policy addressing both the public and private sector¹. It is also committed to develop a stronger cybersecurity industry to ensure a resilient cyber space.



Kenya, ranked third in the region, provides a good example of cooperation through its National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC)². The CIRT coordinates at national, regional and global levels with a range of actors. Nationally this includes ISPs and the financial and educational sectors; regionally it works with other CIRTs through the East African Communications Organization; and internationally it liaises with ITU, FIRST, and bi-laterally with the United States and Japan CIRTs among others.



Figure 6.1.1: Top three ranked countries in Africa and global ranked of all countries in Africa



¹ http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf

² <http://www.ke-cirt.go.ke/index.php/members/>

Figure 6.1.2: Africa region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	IGCI
Angola	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Benin	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Botswana	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Burkina Faso	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Burundi	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cameroon	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cape Verde	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Central African Republic	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Chad	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Congo	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cote d'Ivoire	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Democratic Republic of the Congo	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Equatorial Guinea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Eritrea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ethiopia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Gabon	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Gambia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ghana	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Guinea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Guinea-Bissau	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Kenya	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Lesotho	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Liberia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Madagascar	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Malawi	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mali	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mauritius	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mozambique	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Namibia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Niger	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Nigeria	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Rwanda	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sao Tome and Principe	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Senegal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Seychelles	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sierra Leone	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
South Africa	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
South Sudan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Swaziland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tanzania	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Togo	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Uganda	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Zambia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Zimbabwe	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

6.2 Americas

Table 6.2.1: Top three ranked countries in the Americas

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
Mexico	0.66	0.91	0.89	0.48	0.68	0.34

The top three ranked countries in the Americas region are the members of the North American Free Trade Association (NAFTA).

The United States of America has the highest scores for the legal and capacity building pillars. One notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines³.



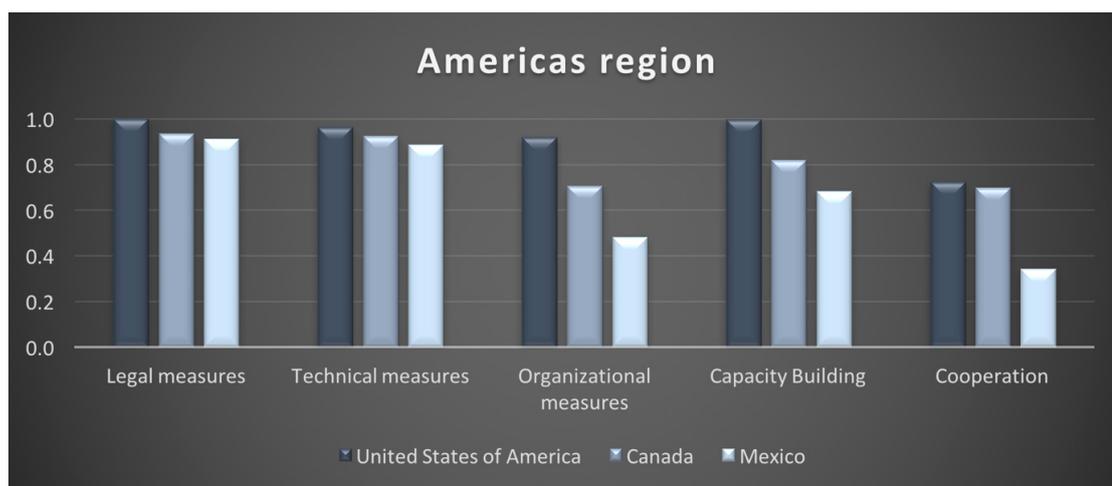
Canada ranks second in the region with its highest score in the legal pillar. The country's Personal Information Protection and Electronic Documents Act (PIPEDA) features several sections relating to cybersecurity⁴. It requires organizations to notify privacy authorities in the event of privacy breaches that could cause significant damage with penalties for those who fail to report them.



Mexico is third and some 16 points behind Canada, illustrating the cybersecurity divide in the region. Like the other top ranked countries in the region, it scores best in the legal pillar with a full suite of cyber legislation covering criminality, data protection, data privacy and electronic transactions.



Figure 6.2.1: Top three ranked countries and an average score of all the Americas



³ <https://www.nga.org/cms/statecyber>

⁴ <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/>

Figure 6.2.2: Americas region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GC
Antigua and Barbuda	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Argentina	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Bahamas	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Barbados	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Belize	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Bolivia	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Brazil	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Canada	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Chile	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Colombia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Costa Rica	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Cuba	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Dominica	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Dominican Republic	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Ecuador	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
El Salvador	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Grenada	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Guatemala	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Guyana	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Haiti	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Honduras	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Jamaica	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Mexico	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Nicaragua	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Panama	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Paraguay	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Peru	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Saint Kitts and Nevis	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Saint Lucia	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Saint Vincent and the Grenadines	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Suriname	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Trinidad and Tobago	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
United States of America	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	
Uruguay	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	
Venezuela	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	

6.3 Arab States

Table 6.3.1: Top three ranked countries in the Arab States

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Egypt	0.77	0.92	0.92	0.4	0.92	0.7
Qatar	0.67	0.83	0.82	0.65	0.78	0.33

Sultanate of Oman is the top ranked in the Arab States with the highest scores in the legal and capacity building pillars. Oman has a robust organizational structure, including a high-level cybersecurity strategy and master plan and comprehensive roadmap.



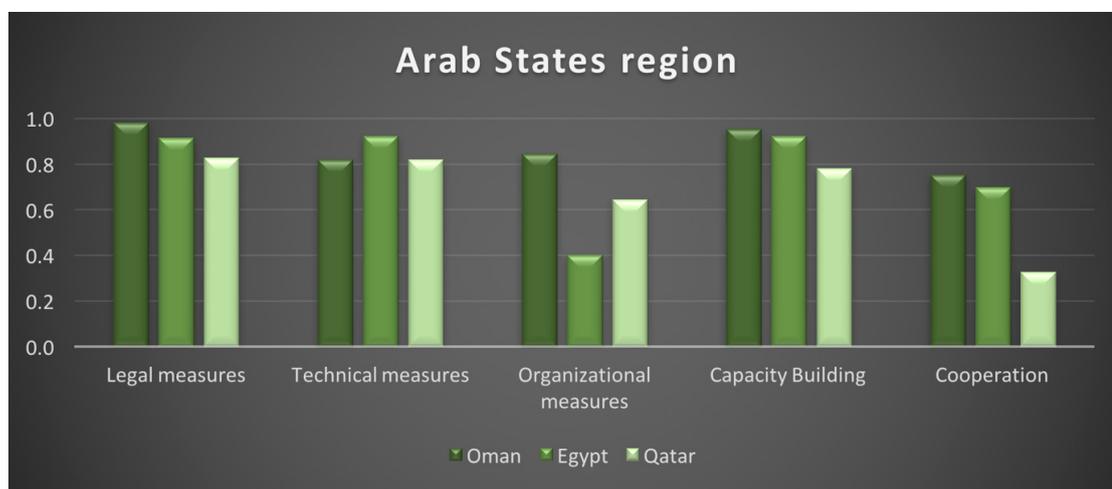
Egypt ranks second with a full range of cooperation initiatives. It is a member of the UN Government Group of Experts (GGE) on cybersecurity⁵, has chaired the ITU Working Group for Child Online Protection⁶, was a founding member of AfricaCERT⁷, and has a number of bi-lateral and multilateral agreements on cybersecurity cooperation.



Qatar ranks third and has been building a cybersecurity culture through campaigns such as Safer Internet Day and has spread warnings about online threats, such as fraud and Internet scams, via print and social media. The Qatar Cyber Crimes Investigation Center and Information Security Center support efforts to safeguard the public and crack down on those who use technology to carry out criminal activities.



Figure 6.3.1: Top three ranked countries and an average score of the Arab States



⁵ <https://www.un.org/disarmament/topics/informationsecurity/>

⁶ <http://www.itu.int/en/council/cwg-cop/Pages/default.aspx>

⁷ <https://www.africert.org/home/>

Figure 6.3.2: Arab States scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Inter-agency partnerships	COOPERATION	GCI
Algeria	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Bahrain	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Comoros	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Djibouti	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Egypt	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Iraq	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Jordan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Kuwait	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Lebanon	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Libya	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mauritania	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Morocco	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Oman	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Qatar	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Saudi Arabia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Somalia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
State of Palestine	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sudan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Syrian Arab Republic	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tunisia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
United Arab Emirates	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Yemen	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

6.4 Asia and the Pacific

Table 6.4.1: Top three ranked countries in Asia and the Pacific

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Australia	0.82	0.94	0.96	0.86	0.94	0.44

Singapore is the top ranked country in the region. The island state has a long history of cybersecurity initiatives. It launched its first cybersecurity master plan back in 2005. The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity and the country issued a comprehensive strategy in 2016⁸.



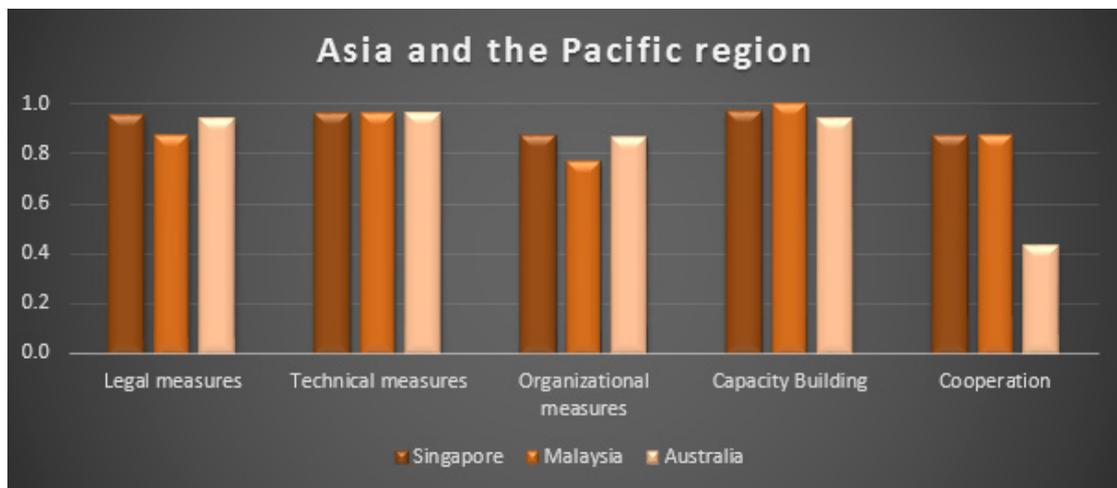
Malaysia is ranked second in the Asia and the Pacific region and scores a perfect 100 on capacity building due to a range of initiatives in that pillar. Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training via higher education institutions in Malaysia. It maintains the *Cyberguru* website, dedicated to professional security training⁹.



Australia¹⁰ is third ranked in the region and home to AusCERT, one of oldest CERTs in the region formed in 1993¹¹. The highest scoring pillar is technical where there is a certification programme for information security skills provided by the Council of Registered Ethical Security Testers (CREST)¹². Modelled after CREST, the council offers assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities in both Australia and New Zealand.



Figure 6.4.1: Top three ranked countries and an average score of all Asia and the Pacific



⁸ <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>

⁹ <http://www.cyberguru.my>

¹⁰ <http://thecommonwealth.org/member-countries>

¹¹ <https://www.auscert.org.au>

¹² <https://www.crestaaustralia.org>

Figure 6.4.2: Asia and the Pacific Region Scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURE:	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURE:	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURE:	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GCI
Afghanistan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Australia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Bangladesh	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Bhutan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Brunei Darussalam	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cambodia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
China	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Democratic People	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Fiji	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
India	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Indonesia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Iran	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Japan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Kiribati	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Lao	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Malaysia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Maldives	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Marshall Islands	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Micronesia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mongolia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Myanmar	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Nauru	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Nepal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
New Zealand	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Pakistan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Palau	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Papua New Guinea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Philippines	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Republic of Korea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Samoa	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Singapore	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Solomon Islands	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sri Lanka	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Thailand	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Timor-Leste	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tonga	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tuvalu	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Vanuatu	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Viet Nam	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

6.5 Commonwealth of Independent States

Table 6.5.1: Top three ranked countries in Commonwealth of Independent States

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Georgia	0.81	0.91	0.77	0.82	0.9	0.7
Russian Federation	0.78	0.82	0.67	0.85	0.91	0.7
Belarus	0.59	0.85	0.63	0.33	0.68	0.47

Georgia is top ranked in the CIS. After large-scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems¹³. The Information Security Law¹⁴ established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.



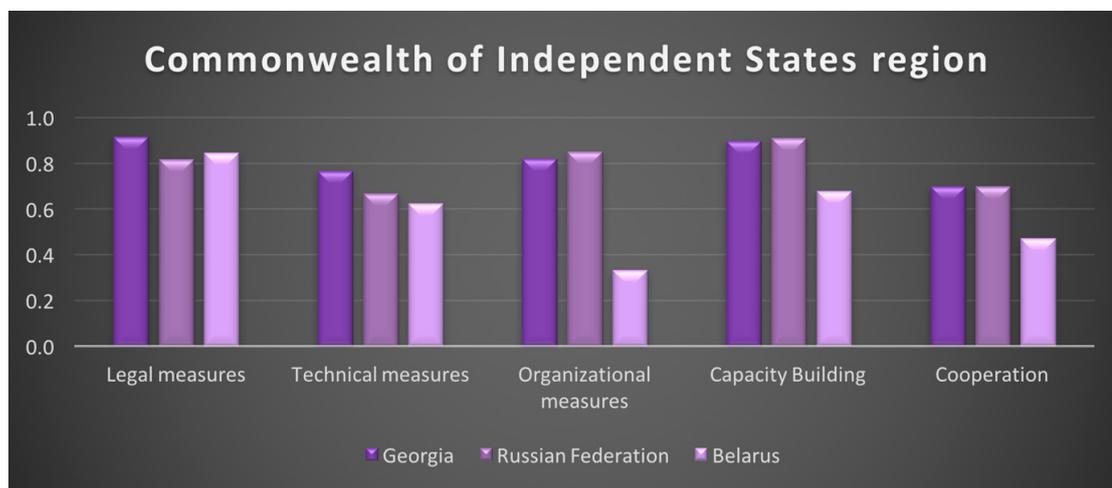
The Russian Federation, ranked second in the region, scores best in capacity building. Its commitments range from developing cybersecurity standards to R&D and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, founded in 1997 and whose software protects over 400 million users and some 270 000 organizations¹⁵.



Belarus is the third ranked country, where child protection initiatives include public and private partnerships. Mobile operator MTS has implemented a project with the Ministry of Education to teach children about safe Internet practices that has so far reached some 6 000 children¹⁶.



Figure 6.5.1: Top three ranked countries and an average score of all CIS



¹³ <http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US>

¹⁴ <https://matsne.gov.ge/en/document/view/1679424>

¹⁵ <https://usa.kaspersky.com/about>

¹⁶ <http://www.mts.by/news/97338/>

Figure 6.5.2: CIS region scorecard

	Cybercriminals	Cybersecurity law	Cybersecurity	LEGAL MEA	National CERT/CI	Government CERT/CI	Sectoral CERT/CI	Standards for orga	Standards for prof	Child online prt	TECHNICAL ME	Strate	Responsible	Cybersecurity	ORGANIZATIONAL I	Standardization	Cybersecurity good	R&D progra	Public awareness, c	Professional trainin	Education progr	Incentive meca	Home-grown li	CAPACITY BU	Bilateral agrea	Multilateral agrea	International part	Public-private part	Interagency part	COOPERA	GC
Armenia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Azerbaijan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Belarus	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Georgia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Kazakhstan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Moldova	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Russian Federation	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tajikistan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Turkmenistan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ukraine	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Uzbekistan	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

6.6 Europe

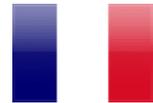
Table 6.6.1: Top three ranked countries in Europe

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
France	0.81	0.94	0.96	0.6	1	0.61
Norway	0.78	0.96	0.89	0.64	80.8	0.57

Estonia is the highest-ranking nation in the Europe region. Like Georgia, Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet¹⁷. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence¹⁸.



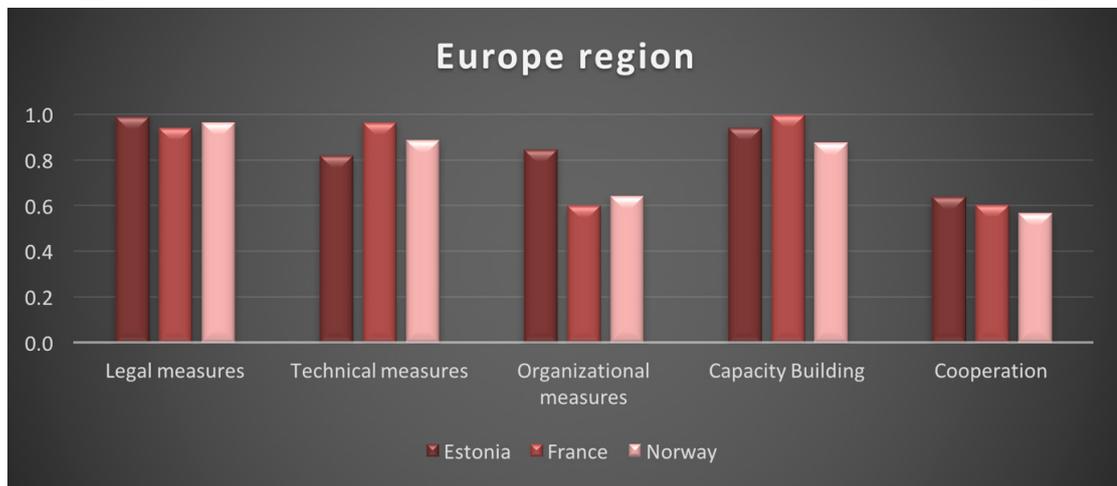
France is the second highest ranked in the Europe region, scoring a perfect 100 in capacity building. There is widespread cybersecurity training available in the country, and the National Agency for Information System Security (ANSSI in French) publishes a list of dozens of universities that provide accredited cybersecurity degrees recognized¹⁹.



Norway is ranked third in Europe with its highest score in the legal pillar. Apart from laws dealing with cybersecurity, Norway has also conducted research on its cybersecurity culture including surveying citizens about the degree to which they will accept monitoring of their online activities.²⁰



Figure 6.6.1: Top three ranked countries and an average score of all Europe



¹⁷ <http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/>

¹⁸ <https://ccdcoe.org>

¹⁹ <https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/>

²⁰ <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>

Figure 6.6.2: Europe region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	COOPERATION	GCI
Albania	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Andorra	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Austria	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Belgium	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Bosnia and Herzegovina	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Bulgaria	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Croatia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cyprus	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Czech Republic	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Denmark	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Finland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
France	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Germany	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Greece	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Hungary	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Iceland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ireland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Israel	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Italy	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Latvia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Liechtenstein	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Lithuania	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Luxembourg	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Malta	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Monaco	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Montenegro	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Netherlands	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Norway	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Poland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Portugal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Romania	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
San Marino	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Serbia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Slovakia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Slovenia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Spain	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sweden	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Switzerland	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
The former Yugoslav Republic of Macedonia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Turkey	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
United Kingdom	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

7 Illustrative practices by pillar

This chapter identifies noteworthy and thought-provoking practices in cybersecurity across the various GCI pillars. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken in their focus areas.

7.1 Legal

Examples for this pillar illustrate practices in national cybercrime legislation regarding unauthorized access, data and system interference or interception, and misuse of computer systems.

7.1.1 Cybercrime legislation

Colombia became one of the first countries in the world when, in 2009, it enacted a law specifically targeting cyberspace. Law 1273 (entitled "By means of which the Penal Code is amended, a new legal right is created- called 'protection of information and data'- and systems that use information and communication technologies are fully preserved, among other provisions"¹) calls for a prison sentence or large fines for anyone convicted of information systems or telecommunication network crimes. The law covers areas such as illegally accessing personal information, intercepting data, destroying data or using malicious software.



Georgia established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing.²



7.1.2 Cybersecurity regulation

Sultanate of Oman established the eGovernance Framework, a set of standards / best practices and process management systems to enhance the delivery of government services in alignment with the mission of e.oman (Sultanate of Oman Digital Oman Strategy and eGovernment). The framework spells out the rules and procedures that ensure that government IT projects and systems are sustainable and in compliance with the Information Technology Authority (ITA) strategies and objectives. It provides assurance about the value of IT projects and framework for the management of IT-related risks. It helps in putting controls to minimize risks and better delivery of IT initiatives³.



7.1.3 Cybersecurity training

Mauritius makes available training for law enforcement and judiciary which has been conducted under the GLACY Project since 2013 and is still ongoing. CERT-MU also carried out cybersecurity trainings on digital forensic investigator professional and network forensic (packet analysis) for law enforcement officers. Training on



¹ Government of Colombia. Law 1273 of 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.* <http://www.mintic.gov.co/portal/604/w3-article-3705.html>

² <https://personaldata.ge/en/legislation/national-legislation> ; <https://matsne.gov.ge/ka/document/view/16426?impose=translateEn>

³ http://www.ita.gov.om/ITAPortal/Government/Government_Projects.aspx?NID=76

information security standards and best practices is given to the technical officers of the IT Security Unit (ITSU) of the Ministry of Technology, Communication and Innovation⁴.

The **New Zealand** (NZ) Police is introducing a 3-tiered training program for specialist cyber staff, investigators and then frontline staff. This is outlined in NZ Police's Prevention First National Cybercrime Strategy 2014-2017⁵. NZ Police also provides training to the judiciary and prosecutors.



7.2 Technical

Examples for this pillar illustrate practices in areas such as existence of technical institutions, child online protection and industry standards and certification.

7.2.1 National CERT/CIRT/CSIRT

Egypt provides computer emergency response team (EG-CERT) support to several entities in the ICT sector, the financial sector as well as the government sector, in order to help them tackle cybersecurity related threats. EG-CERT is expanding and is currently upgrading its laboratories in the four key operational departments. Additional laboratories are being planned for mobile cybersecurity and industrial control systems cybersecurity⁶.



Brazil has three computer emergency response teams with different functions, namely: the national CERT, a government CSIRT and a sector specific SCIRT. The Brazil Federal Police participates in the I-24/7 global police communications system developed by Interpol to connect law enforcement officers, including cybercrimes. There is also a complementary Standard No. 17/IN01/DSIC/GSIPR that establishes guidelines for the certification and accreditation for information and communication security professionals of the direct and indirect Federal Public Administration.



7.2.2 Government CERT/CIRT/CSIRT

Luxembourg created a computer emergency response team (GOVCERT.LU) in 2011 to help protect government computer systems and data as well as specific infrastructures and is engaged at both national and international level under the name of NCERT.LU⁷. GOVCERT.LU is also a critical player in the event of a large cyber-attack affecting country's ICT assets.



7.2.3 Sectoral CERT/CIRT/CSIRT

Sri Lanka created the Financial Sector Computer Security Incident Response Team (FINCSIRT) in 2014 with responsibility for receiving, reviewing, processing and responding to computer security alerts and incidents affecting banks and other licensed financial institutions in the country⁸. FINCSIRT is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka computer emergency response team and is steered and funded by the banking sector. Related to FINCSIRT is LankaClear, the country's certification authority owned by the Central Bank and commercial banks⁹.



⁴ http://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/glacy-support-to-mauritius-judicial-training-courses-on-cybercrime-delivered

⁵ <http://www.dpnc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf> (page 10)

⁶ <http://www.egcert.org>

⁷ <https://www.govcert.lu/en/ncert.html>

⁸ <http://www.fincsirt.lk>

⁹ <http://www.lankaclear.com/about/index.php>

7.2.4 Cybersecurity standards implementation framework for organizations

Malaysia created the Information Security Certification Body (ISCB), a department of Cybersecurity Malaysia, which manages information security certification¹⁰. The certification services are consistent with international standards and guidelines and include among others the Malaysian Common Criteria Evaluation and Certification (MyCC), which certifies security functions of ICT products based on the ISO/IEC 15408 international standard¹¹.



Hungary national regulation lays out the framework for information security training for state and local government officials¹². The National University for Public Service (NKE) is charged with training and establishing a certification system¹³. Certificates issued include information security risk assessment and testing of electronic information systems.



7.2.5 Child online protection

Singapore's Internet Content Providers (ICPs) and Internet Access Service Providers (IASPs) are licensable under the Broadcasting Act and they are required to comply with the Internet Code of Practice to protect children online. Since 2012, all service providers have been legally obligated to offer filtering services with Internet subscriptions and to make this known to consumers when they subscribe or renew. The Info-communications Media Development Authority also symbolically blocks 100 pornographic, extremist or hate websites.



7.3 Organizational

Examples for this pillar illustrate practices where governments are organized by having a cybersecurity strategy, a coordinating agency and compilation of indicators for tracking cybercrime.

7.3.1 Strategy

United Kingdom issued in 2016 its second five years *National Cyber Security Strategy*¹⁴. The strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.



Russian Federation officially adopted its National Security Strategy in 2000 and National Security Concept of the Russian Federation as well as Concept of the Foreign Policy of the Russian Federation in 2013. It established an Information Security Doctrine of the Russian Federation in 2000 and each government entity in the Russian Federation performs an annual audit of its own networks and systems in line with the doctrine and the areas identified in the various strategies adopted.



¹⁰ http://www.cybersecurity.my/en/our_services/iscb/main/detail/2327/index.html

¹¹ http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

¹² http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717

¹³ <http://en.uni-nke.hu>

¹⁴ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

7.3.2 Public consultation

Canada conducted a three-month public consultation on updating its cybersecurity strategy, asking security professionals and citizens for inputs and views. The consultation was done to help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cybersecurity and capitalize on the advantages of new technology and the digital economy¹⁵.



7.3.3 Responsible agency

Iceland created the Cyber Security Council, appointed by the Minister of the Interior that is responsible for overseeing the implementation of the National Cyber Security Strategy. In addition, a cyber security forum has been created as a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities.



7.3.4 Cybersecurity metrics

Netherlands uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report¹⁶. The National Cyber Security Centre (NCSC) compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and acted on.



7.4 Capacity building

Examples of practices for capacity building include the aspects of developing the technical and human resources for fighting cybercrime. This includes raising awareness about cybersecurity among the public, the existence of cybersecurity standards and standards bodies, best practices guides, education initiatives and research and development.

7.4.1 Standardization bodies

Romania created the National Standardization Organization¹⁷ to produce relevant national standards on processes, tools and technologies for software products and systems in the area of security in information technology. It also tests the standardization integrity of encryption algorithms, authentication services and algorithms for confidential services in compliance with accepted international standards¹⁸.



7.4.2 Good practice

Canada created the Investment Industry Regulatory Organization (IIROC) that is the national self-regulatory organization overseeing investment dealers and their trading activity in the country's debt and equity markets. IIROC published a cybersecurity best practices guide for its members¹⁹.



¹⁵ <http://www.itworldcanada.com/article/breaking-news-ottawa-announces-public-consultation-on-cyber-security-strategy/385740#ixzz4dm1QjsTu>

¹⁶ <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html>

¹⁷ <http://www.asro.ro/>

¹⁸ <http://www.asro.ro/CTmementoSite.html#BM208>

¹⁹ http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

7.4.3 Cybersecurity research and development programmes

Germany signed an agreement in 2009 on cooperation in IT security research between the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior (BMI). The IT Security Research programme covers research and development in new information security technologies. The BMBF has been supporting three research centres since 2011 that bring together leading university and non-university establishments in cybersecurity²⁰.



Kenya Education Network, (KENET), is the National Research and Education Network (NREN) of Kenya. KENET is the computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA) as a not-for-profit operator serving the education and research institutions. They most notably provide affordable, cost-effective and low-congestion Internet bandwidth services to member institution campuses in Kenya.



7.4.4 Public awareness campaigns

Latvia has published a series of articles on its national CERT portal about free-of-charge security solutions including anti-viruses, firewalls, NoScript, etc.²¹ Twice a year, the national CERT organizes a campaign where people can bring their computers for a check-up to see if they are infected, and it also distributes commercial anti-virus installations during the campaigns that are made available free-of-charge for one year.



7.4.5 Cybersecurity professional training courses

Bulgaria established the International Cyber Investigation Training Academy in 2009, which is a non-governmental organization²². The academy aims to improve the qualification of specialists working in the field of cybersecurity. It has trained over 1 300 people from both the public and private sectors.



7.4.6 National education programmes and academic curricula

Germany has several universities and institutes providing degrees and certificates in information security²³. The Federal Ministry of Education and Research funds the KASTEL competence centre that offers training leading to a certificate equivalent to a specialized master degree in IT security²⁴. The Technical University of Darmstadt has been offering a Master of Science Degree in IT security since 2010²⁵.



7.4.7 Incentive mechanisms

Korea Internet Security Agency (KISA) is committed to establishing a network foundation for Internet users and Internet companies by improving competitiveness of Internet services and reliability of Internet information and knowledge. KISA supports start-ups to commercialize their business models and enhance competitive edge in the field of security technology through programmes that aim to nurture start-ups in the Internet-of-things, security, and Fintech industry. They also established the one-stop



²⁰ <https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html>

²¹ <https://www.esidross.lv/category/bezmaksas-risinajumi/page/2/>

²² <http://e-crimeacademy.com/>

²³ <https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html>

²⁴ <http://www.kastel.kit.edu>

²⁵ <https://www.tu-darmstadt.de/studieren/abschluesse/master/it-sicherheit-msc.en.jsp>

service to support start-ups to gain ground not only in the domestic market but also the global market to expand their business models.

7.4.8 Home-grown cybersecurity industry

Ireland has the largest proportion of the Information and Communication sector of its economy compared to all other countries in Europe and is leveraging that advantage to grow its cybersecurity industry. The country is drawing on existing incentives and attractions with the aim of being a cybersecurity capital²⁶. These incentives include a favourable business environment and low taxes, a talented pool of highly skilled and multilingual workers and a good base for access to European markets²⁷.



7.5 Cooperation

This pillar considers collaborative efforts across national and international domains and between the public and private sector.

7.5.1 Bilateral agreements

Finland is an active member of many organizations, such as the Council of Europe (CoE), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN). Finland has also joined the NATO Partnership for Peace and is engaged in cooperation with the organization in, for example, crisis management. There is also local partnership with Finnish company Codenomicon, which later was acquired by Synopsys, to develop the national IDS system and automatic incident reporting service with FICORA²⁸.



7.5.2 Multilateral agreements

Denmark, Finland, Iceland, Norway and Sweden collaborate through the Nordic National CERT Collaboration. This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region²⁹.



7.5.3 Participation in international fora

Participation in international cybersecurity events, workshops and training is the one indicator where virtually all countries score high on the GCI. Therefore, it is more revealing to describe one of the most significant initiatives in this regard. The Forum of Incident Response and Security Teams (FIRST)³⁰ was founded in 1990. Its members are security and incident response teams from the public, private and academic sectors. It organizes an annual conference, technical colloquia and training workshops.

²⁶ <https://www.siliconrepublic.com/companies/cybersecurity-hub-ireland>

²⁷ http://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security/IDA_CYBER_SECURITY.pdf

²⁸ <http://forin.finland.fi/public/default.aspx?nodeid=49303&contentlan=2&culture=fi-FI> <https://www.synopsys.com/services.html>

²⁹ <https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/>

³⁰ www.FIRST.org

7.5.4 Public-private partnerships

The **United Kingdom** is working with local company Netcraft on cyber security initiatives.³¹ This includes combatting phishing and malware hosted in the United Kingdom as well as phishing targeting the government³². The partnership helped stop 34,550 potential attacks on government departments in the last six months of 2016, or 200 incidents a day.



7.5.5 Interagency partnerships

The **United States of America** started its first cross-government security information sharing agreement in 2015. The Multilateral Information Sharing Agreement (MISA) binds government agencies from defence, health, justice, intelligence community and energy to work collaboratively to enhance cybersecurity information sharing, with an emphasis on information exchanges at machine speed³³.



South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society³⁴.



³¹ <https://news.netcraft.com/archives/2016/11/01/the-chancellor-of-the-exchequer-sets-out-plans-for-the-uk-government-to-work-with-netcraft.html>

³² <https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk>

³³ <https://www.ise.gov/blog/kshemendra-paul/coordinating-cybersecurity-programs>

³⁴ <https://www.cybersecurityhub.gov.za/>

8 Conclusion

Cybersecurity is an increasingly important part of our life today, and the degree of interconnectivity of networks implies that anything and everything can be exposed, and everything from national critical infrastructure to our basic human rights can be compromised. Governments are therefore urged to consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cybersecurity strategy.

The GCI 2017 edition measured the commitment of the ITU Member States to cybersecurity and highlighted a number of illustrative practices from around the world. As a logical continuation of the first iteration of the GCI issued in 2014, this version has motivated countries to improve their work related to cybersecurity, raised awareness in countries for the need to start bilateral, multilateral and international cooperation, and increased the visibility of what countries are doing to improve cybersecurity.

However, the research also revealed that while increased Internet access and more mature technological development is correlated with improvement in cybersecurity at the global level, this is not necessarily true for countries with developing economies and lower levels of technological development. The data collection shows that developing countries lack well-trained cybersecurity experts as well as a thorough appreciation and the necessary education on cybersecurity issues for law enforcement, and continued challenges in the judiciary and legislative branches. There is a need for the developed world to help train local experts in cybersecurity, and more cooperation should be initiated between developed and developing countries to assist them in cybersecurity development.

For the Global Cybersecurity Index to have an impact on raising awareness on this crucial emerging concern over time, continuity of the GCI effort is essential. ITU therefore welcomes all Member States and industry stakeholders to actively participate in future efforts to enhance the current reference model. As well, the success of future iterations of the GCI largely depends on the engagement of Member States and the quality of their responses to the questionnaire, and ITU calls on all Member States to take part in the next GCI survey.

ITU would like to thank all Member States for their valuable support for the conduct of the GCI survey and the publication of this report as well as future ones.

Abbreviations

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructure Protection
CIS	Commonwealth of Independent States
CREST	Council of Registered Ethical Security Testers
CSIRT	Computer Security Incident Response Team
COP	Child Online Protection
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCS	National Cybersecurity Strategy
UN	United Nations
R&D	Research and Development
NATO	North Atlantic Treaty Organization
NAFTA	North American Free Trade Association
PIPEDA	Personal Information Protection and Electronic Documents Act
ANSSI	National Agency for Information System Security
ISCB	Information Security Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification
MTPS	Malaysia Trustmark for Private Sector
NCSC	The National Cyber Security Centre
BMBF	Federal Ministry of Education and Research
ISACA	Information Systems Audit and Control Association
ICP	Internet Content Provider
IASPs	Internet Access Service Provider
NCSC	Nation Cyber Security Centre
MSIP	Ministry of Science, ICT and Future Planning

IDI	ICT Development Index
GDP	Gross Domestic Product
FINCSIRT	Financial Sector Computer Security Incident Response Team
KISA	Korea Internet and Security Agency
IIROC	The Investment Industry Regulatory Organization of Canada
CERT-MU	Computer Emergency Response Team of Mauritius
National KE-CIRT/CC	National Kenya Computer Incident Response Team Coordination Centre
AfricaCERT	Computer Emergency Response Team of Africa
AusCERT	Computer Emergency Response Team of Australia
GOVCERT.LU	Government Computer Emergency Response Team of Luxembourg
NCERT.LU	National Computer Emergency Response Team of Luxembourg
OCERT	Oman Computer Emergency Response Team
APCERT	Asia and the Pacific Computer Emergency Response Team

Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region

AFRICA Region	Score	Global Rank
Mauritius	0.830	6
Rwanda	0.602	36
Kenya	0.574	45
Nigeria	0.569	46
Uganda	0.536	50
South Africa	0.502	58
Botswana	0.430	69
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Ghana	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Zambia	0.292	91
Ethiopia	0.267	99
Togo	0.218	107
Burkina Faso	0.208	108
Mozambique	0.206	109
Zimbabwe	0.192	113
Seychelles	0.184	115
Niger	0.170	120
Madagascar	0.168	121
Liberia	0.149	124
Sierra Leone	0.145	126
Gabon	0.139	128
Gambia	0.136	130
Burundi	0.120	135
Lesotho	0.094	143
Guinea	0.090	144

AFRICA Region	Score	Global Rank
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Sao Tome and Principe	0.040	161
Guinea-Bissau	0.034	162
Central African Republic	0.007	164
Equatorial Guinea	0.000	165

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81

AMERICAS Region	Score	Global Rank
Jamaica	0.339	85
Costa Rica	0.336	86
Paraguay	0.326	87
Barbados	0.273	95
Guyana	0.269	98
El Salvador	0.208	108
Saint Vincent and the Grenadines	0.189	114
Belize	0.182	116
Antigua and Barbuda	0.179	117
Dominican Republic	0.162	122
Suriname	0.155	132
Nicaragua	0.146	125
Bahamas	0.137	129
Bolivia	0.122	134
Grenada	0.115	137
Guatemala	0.114	138
Trinidad and Tobago	0.098	141
Saint Kitts and Nevis	0.066	151
Cuba	0.058	153
Saint Lucia	0.053	156
Honduras	0.048	157
Haiti	0.040	161
Dominica	0.010	163

ARAB STATES Region	Score	Global Rank
Oman	0.871	4
Egypt	0.772	14
Qatar	0.676	25
Tunisia	0.591	40
Saudi Arabia	0.569	46

ARAB STATES Region	Score	Global Rank
United Arab Emirates	0.566	47
Morocco	0.541	49
Bahrain	0.467	65
Algeria	0.432	68
Jordan	0.277	93
Sudan	0.271	96
Syrian Arab Republic	0.237	102
State of Palestine	0.228	104
Libya	0.224	105
Lebanon	0.172	119
Mauritania	0.146	125
Kuwait	0.104	139
Djibouti	0.099	140
Iraq	0.043	159
Comoros	0.040	161
Somalia	0.034	162
Yemen	0.007	164

COMMONWEALTH OF INDEPENDANT STATES CIS Region	Score	Global Rank
Georgia	0.819	8
Russian Federation	0.788	10
Belarus	0.592	39
Azerbaijan	0.559	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kyrgyzstan	0.270	97
Armenia	0.196	111
Turkmenistan	0.133	132

ASIA AND THE PACIFIC Region	Score	Global Rank
Singapore	0.925	1
Malaysia	0.893	3
Australia	0.824	7
Japan	0.786	11
Republic of Korea	0.782	13
New Zealand	0.718	19
Thailand	0.684	20
India	0.683	23
China	0.624	32
Philippines	0.594	37
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Iran	0.494	60
Pakistan	0.447	67
Indonesia	0.424	70
Sri Lanka	0.419	72
Lao	0.392	77
Tonga	0.292	91
Cambodia	0.283	92
Nepal	0.275	94
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Mongolia	0.228	104
Fiji	0.222	106
Bhutan	0.199	110
Nauru	0.140	127
Vanuatu	0.134	131
Kiribati	0.123	133
Solomon Islands	0.095	142

ASIA AND THE PACIFIC Region	Score	Global Rank
Papua New Guinea	0.067	150
Maldives	0.056	155
Palau	0.053	156
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Timor-Leste	0.034	162
Tuvalu	0.034	162

EUROPE Region	Score	Global Rank
Estonia	0.846	5
France	0.819	8
Norway	0.786	11
United Kingdom of Great Britain and Northern Ireland	0.783	12
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
Israel	0.691	20
Latvia	0.688	21
Germany	0.679	24
Ireland	0.675	26
Belgium	0.671	27
Austria	0.639	30
Italy	0.626	31
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Luxembourg	0.602	36
Croatia	0.590	41

EUROPE Region	Score	Global Rank
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Hungary	0.534	51
Spain	0.519	54
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
Cyprus	0.487	61
Greece	0.475	64
Montenegro	0.422	71
Malta	0.399	76
Iceland	0.384	78
Slovakia	0.362	82
Slovenia	0.343	84
Albania	0.314	89
Serbia	0.311	90
Monaco	0.236	103
Liechtenstein	0.194	112
San Marino	0.174	118
Bosnia and Herzegovina	0.116	136
Andorra	0.057	154
Vatican	0.040	161

Annex 2 – GCI 2017 Score

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
New Zealand	0.718	19
Israel	0.691	20
Latvia	0.688	21
Thailand	0.684	20
India	0.683	23
Germany	0.679	24
Qatar	0.676	25
Ireland	0.675	26
Belgium	0.671	27

Member State	Score	Global Rank
Mexico	0.660	28
Uruguay	0.647	29
Austria	0.639	30
Italy	0.626	31
China	0.624	32
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Rwanda	0.602	36
Luxembourg	0.602	36
Philippines	0.594	37
Brazil	0.593	38
Belarus	0.592	39
Tunisia	0.591	40
Croatia	0.590	41
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Kenya	0.574	45
Colombia	0.569	46
Saudi Arabia	0.569	46
Nigeria	0.569	46
United Arab Emirates	0.566	47
Azerbaijan	0.559	48
Morocco	0.541	49
Uganda	0.536	50
Hungary	0.534	51
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Spain	0.519	54

Member State	Score	Global Rank
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
South Africa	0.502	58
Ukraine	0.501	59
Iran	0.494	60
Cyprus	0.487	61
Panama	0.485	62
Argentina	0.482	63
Greece	0.475	64
Bahrain	0.467	65
Ecuador	0.466	66
Pakistan	0.447	67
Algeria	0.432	68
Botswana	0.430	69
Indonesia	0.424	70
Montenegro	0.422	71
Sri Lanka	0.419	72
Moldova	0.418	73
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Malta	0.399	76
Lao	0.392	77
Iceland	0.384	78
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81
Slovakia	0.362	82
Kazakhstan	0.352	83
Slovenia	0.343	84
Jamaica	0.339	85

Member State	Score	Global Rank
Costa Rica	0.336	86
Ghana	0.326	87
Paraguay	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Albania	0.314	89
Serbia	0.311	90
Zambia	0.292	91
Tajikistan	0.292	91
Tonga	0.292	91
Cambodia	0.283	92
Uzbekistan	0.277	93
Jordan	0.277	93
Nepal	0.275	94
Barbados	0.273	95
Sudan	0.271	96
Kyrgyzstan	0.270	97
Guyana	0.269	98
Ethiopia	0.267	99
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Syrian Arab Republic	0.237	102
Monaco	0.236	103
Mongolia	0.228	104
State of Palestine	0.228	104
Libya	0.224	105
Fiji	0.222	106
Togo	0.218	107
Burkina Faso	0.208	108
El Salvador	0.208	108

Member State	Score	Global Rank
Mozambique	0.206	109
Bhutan	0.199	110
Armenia	0.196	111
Liechtenstein	0.194	112
Zimbabwe	0.192	113
Saint Vincent and the Grenadines	0.189	114
Seychelles	0.184	115
Belize	0.182	116
Antigua and Barbuda	0.179	117
San Marino	0.174	118
Lebanon	0.172	119
Niger	0.170	120
Madagascar	0.168	121
Dominican Republic	0.162	122
Suriname	0.155	132
Liberia	0.149	124
Mauritania	0.146	125
Nicaragua	0.146	125
Sierra Leone	0.145	126
Nauru	0.140	127
Gabon	0.139	128
Bahamas	0.137	129
Gambia	0.136	130
Vanuatu	0.134	131
Turkmenistan	0.133	132
Kiribati	0.123	133
Bolivia	0.122	134
Burundi	0.120	135
Bosnia and Herzegovina	0.116	136
Grenada	0.115	137
Guatemala	0.114	138

Member State	Score	Global Rank
Kuwait	0.104	139
Djibouti	0.099	140
Trinidad and Tobago	0.098	141
Solomon Islands	0.095	142
Lesotho	0.094	143
Guinea	0.090	144
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Papua New Guinea	0.067	150
Saint Kitts and Nevis	0.066	151
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Cuba	0.058	153
Andorra	0.057	154
Maldives	0.056	155
Saint Lucia	0.053	156
Palau	0.053	156
Honduras	0.048	157
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Iraq	0.043	159
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Haiti	0.040	161

Member State	Score	Global Rank
Sao Tome and Principe	0.040	161
Vatican	0.040	161
Comoros	0.040	161
Guinea-Bissau	0.034	162
Somalia	0.034	162
Timor-Leste	0.034	162
Tuvalu	0.034	162
Dominica	0.010	163
Central African Republic	0.007	164
Yemen	0.007	164
Equatorial Guinea	0.000	165

**International
Telecommunication
Union**

Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN: 978-92-61-25071-3



Printed in Switzerland
Geneva, 2017

Photo credits: Shutterstock

Pew Research Center
What Americans Know About Cybersecurity

March 2017



Pew Research Center

Internet & Technology

MENU

RESEARCH AREAS

SEARCH

MARCH 22, 2017

What the Public Knows About Cybersecurity

A majority of internet users can answer fewer than half the questions correctly on a difficult knowledge quiz about cybersecurity issues and concepts

BY KENNETH OLMSTEAD ([HTTP://WWW.PEWINTERNET.ORG/AUTHOR/KOLMSTEAD/](http://www.pewinternet.org/author/kolmstead/)) AND AARON SMITH ([HTTP://WWW.PEWRESEARCH.ORG/STAFF/AARON-SMITH/](http://www.pewresearch.org/staff/aaron-smith/))

Before you read the report, test your cybersecurity knowledge by taking the interactive quiz (<http://www.pewinternet.org/quiz/cybersecurity-knowledge/>). The short quiz tests your knowledge of questions recently asked in a national poll. After completing the quiz, you can compare your score with the general public and learn more about the terms and topics in each question.

Take the Quiz (<http://www.pewinternet.org/quiz/cybersecurity-knowledge/>)

In an increasingly digital world, an individual's personal data can be as valuable – and as vulnerable – to potential wrongdoers as any other possession. Despite the risk-reducing impact of good cybersecurity habits and the prevalence of cyberattacks on institutions and individuals alike, a Pew Research Center survey finds that many Americans are unclear about some key cybersecurity topics, terms and concepts. A majority of online adults can identify a strong password when they see one and recognize the dangers of using public Wi-Fi. However, many struggle with more technical cybersecurity concepts, such as how to identify true two-factor authentication or determine if a webpage they are using is encrypted.

This survey consisted of 13 questions designed to test Americans' knowledge of a number of cybersecurity issues and terms. Cybersecurity is a complicated and diverse subject, but these questions cover many of the general concepts and basic building blocks that cybersecurity experts stress are important for users to protect themselves online. However, the typical (median) respondent answered only five of these 13 knowledge questions correctly (with a mean of 5.5 correct answers). One-in-five (20%) answered more than eight questions accurately, and just 1% received a "perfect score" by correctly answering all 13 questions.

These are the key findings from an online survey of 1,055 adult internet users living in the United States conducted June 17-27, 2016.

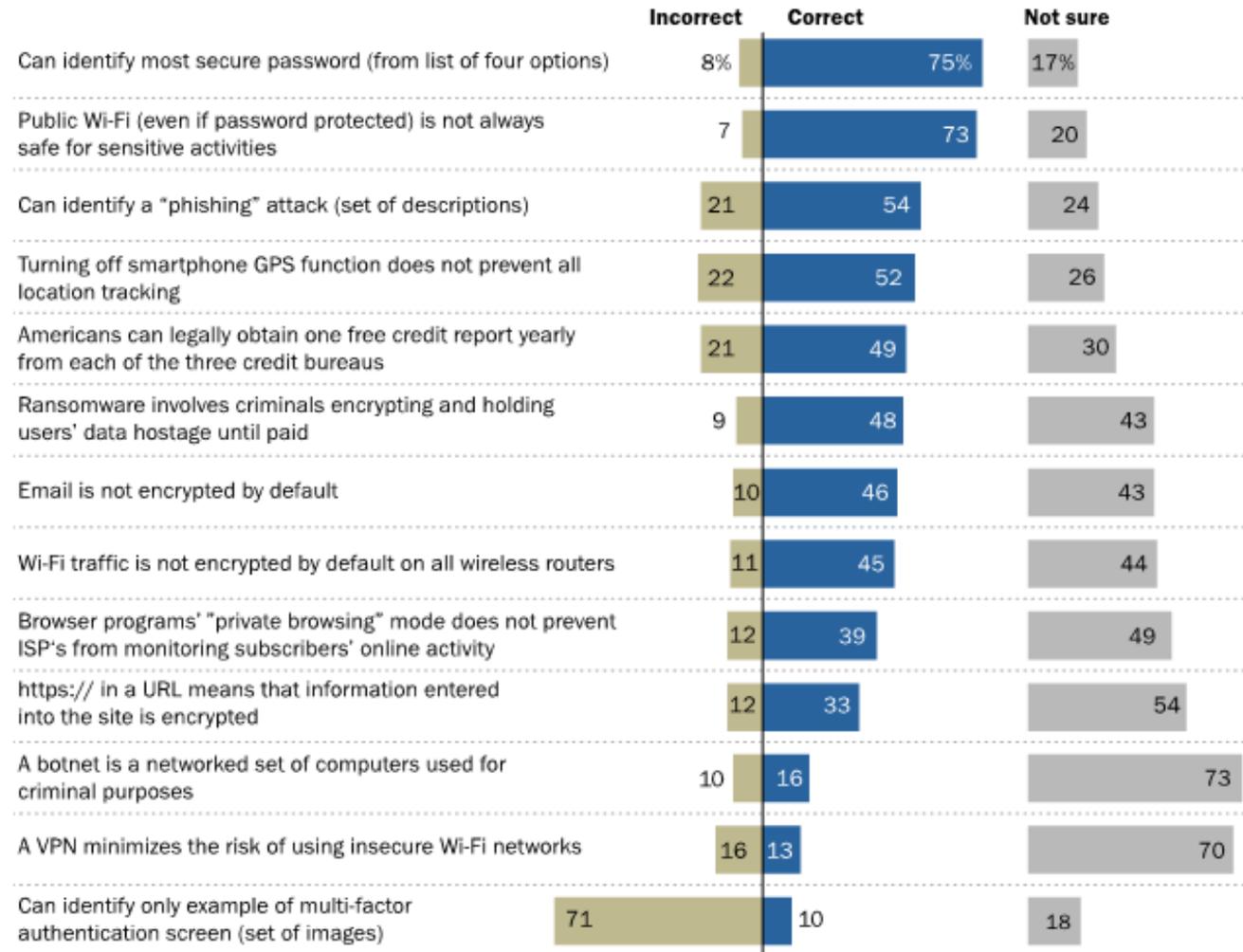
Cybersecurity knowledge varies widely by topic and level of technical detail

Of the 13 questions in the survey, a substantial majority of online adults were able to correctly answer just two of them. First, 75% of online adults can correctly identify the strongest password from a list of four options. The correct password in this case is the password that does not contain words in the dictionary; does contain letters, numbers and symbols; and has a combination of both upper and lower case letters. A similar share (73%) is aware that if a public Wi-Fi network is password protected, it *does not* necessarily mean that it is safe to perform sensitive tasks, such as online banking, using that network.

Meanwhile, around half of internet users are able to correctly answer several other questions in the survey. Some 54% of internet users are able to identify examples of phishing attacks. Similarly, 52% correctly say that turning off the GPS function of a smartphone *does not* prevent all tracking of that device (mobile phones can also be tracked via the cellular towers or Wi-Fi networks to which they are connected).

Many Americans are unsure on a range of cybersecurity topics

% of internet users answering each question ...



Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity"

Additionally, 49% of internet users know that Americans are legally entitled to get one free copy of their credit report annually from each of the three major credit bureaus. This issue is not specifically related to any technical aspects of cybersecurity, but cybersecurity experts recommend that anyone who uses the internet for financial or other sensitive transactions regularly check their credit reports to discover evidence of identity theft or other kinds of fraud. A similar share (48%) can correctly define the term “ransomware.” This refers to criminals accessing someone’s computer, encrypting their personal files and data, and holding that data hostage unless they are paid to decrypt the files.

Americans’ practical understanding of email and Wi-Fi encryption is also relatively mixed: 46% of internet users are able to correctly identify that the statement “all email is encrypted by default” is false. Some email services do encrypt users’ messages, but this is not a standard feature of all email services. At the same time, 45% correctly identify the statement “all Wi-Fi traffic is encrypted by default on all wireless routers” is also false.

Public knowledge of cybersecurity is lower on some relatively technical issues

Internet users’ understanding of the remaining cybersecurity issues measured in the survey is lower – in some cases dramatically so. For instance, 39% of internet users are aware that internet service providers (ISPs) are able to see the sites their customers are visiting while utilizing the “private browsing” mode on their internet browsers. Private browsing mode only prevents the browser itself, and in some cases the user’s computer or smartphone, from saving this information – it is still visible to the ISP. And one-third (33%) are aware that the letter “s” in a URL beginning with “https://” indicates that the traffic on that site is encrypted.

Meanwhile, just 16% of online adults are aware that a group of computers that is networked together and used by hackers to steal data is referred to as a “botnet.” A similar share (13%) is aware that the risks of using insecure Wi-Fi networks can be minimized by using a virtual private network, or VPN.

Lastly, cybersecurity experts commonly recommend that internet users employ “two-factor” or “multi-factor” authentication on any account where it is available. Two-factor authentication generally requires users to log in to a site using something the user *knows* (such as a traditional password) along with something the user *possesses* (such as a mobile phone or security token), thus providing an additional layer of security in the event that someone’s password is hacked or stolen. But when presented with four images of different types of online login screens, just 10% of online adults are able to correctly identify the one – and only one – example in the list of a true multi-factor authentication process. In this case, the correct answer was a picture of a login screen featuring a temporary code sent to a user’s phone that will only help them login for a limited period of time. Several of the other answer options illustrated situations in which users were required to perform a secondary action before accessing a page – such as entering a captcha, or answering a security question. However, none of these other options are examples of two-factor authentication.

A significant share of online adults are simply not sure of the correct answer on a number of cybersecurity knowledge questions

Although the share of online adults who can correctly answer questions about cybersecurity issues varies from topic to topic, in most cases the share providing an actual incorrect answer is relatively small. Rather, many users indicate that they simply are not sure of the correct answer to a large number of the questions in this survey.

At the low end, around one-in-five online adults indicate they are not sure how to identify the most secure password from a list (17%), how to identify multi-factor identification (18%) or whether public Wi-Fi is safe for sensitive activities (20%). At the high end, a substantial majority of internet users are not sure what purpose a VPN serves (70%) or what a botnet does (73%). There are also a number of other questions in this survey where “not sure” responses are markedly more common than incorrect answers. These include the definition of ransomware, whether or not email and Wi-Fi traffic are encrypted by default, whether private browsing mode prevents ISPs from monitoring customer activity and how to identify whether or not a webpage is encrypted. In fact, there is only one question on the survey – how to identify a multi-factor authentication screen – for which a larger share of respondents answer incorrectly than indicate they are not able to answer the question at all.

Those with higher levels of education and younger internet users are more likely to answer cybersecurity questions correctly

Broad differences in cybersecurity knowledge by educational attainment

% of internet users answering each question correctly

	HS or less	Some college	College+	College+ - HS or less diff
Wi-Fi traffic is not encrypted by default on all wireless routers.	30%	46%	64%	+34
https:// in a URL means that information entered into the site is encrypted	22	29	54	+32
Email is not encrypted by default	33	44	65	+32
Ransomware involves criminals encrypting and holding users' data hostage until paid	35	47	66	+31
Turning off smartphone GPS function does not prevent all location tracking	38	58	65	+27
Can identify most secure password (from list of four options)	63	77	88	+25
Americans can legally obtain one free credit report yearly from each of the three credit bureaus	38	52	61	+23
Can identify a "phishing" attack (set of descriptions)	45	54	65	+20
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	32	37	51	+19
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	65	75	83	+18
A botnet is a networked set of computers used for criminal purposes	11	14	25	+14
Can identify only example of multi-factor authentication screen (set of images)	5	9	19	+14
A VPN minimizes the risk of using insecure Wi-Fi networks	10	11	21	+11
AVERAGE NUMBER CORRECT OVERALL	4.0	5.5	7.0	+3.0

Note: Some college includes those who attended but did not graduate with four-year degrees as well as those with two-year degrees.

Source: Survey conducted June 17-27, 2016.

"What the Public Knows About Cybersecurity"

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/pi_2017-03-22_cybersecurity-quiz_0-02/) Internet users' knowledge of cybersecurity varies by several demographic factors. The most consistent differences are related to educational attainment.

Those with college degrees or higher answered an average of 7.0 of the 13 questions in the survey correctly, compared with an average of 5.5 among those who have attended but not graduated from college and an average of just 4.0 for those with high school diplomas or less.

Roughly one-quarter (27%) of those with college degrees answered 10 or more questions correctly, compared with 9% of those who have attended but not graduated from college and just 4% of those with high school diplomas or less.

On all 13 questions in the survey, there is at least an 11 percentage point difference in correct answers between the highest- and lowest-educated groups. And there are four questions with a difference of 30 percentage points or more between the highest- and lowest- educated groups. These include whether or not Wi-Fi traffic is encrypted by default on all wireless routers (a difference of 34 points); what “https://” in a URL refers to (32 points); whether or not all email is encrypted by default (32 points); and the definition of ransomware (31 points).

Modest differences in cybersecurity knowledge by age

% of internet users answering each question correctly

	18-29	30-49	50-64	65+	Youngest – oldest diff
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	52%	46%	31%	25%	+27
Turning off smartphone GPS function does not prevent all location tracking	63	54	49	40	+23
Can identify only example of multi-factor authentication screen (set of images)	17	14	6	3	+14
A botnet is a networked set of computers used for criminal purposes	24	19	11	10	+14
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	78	72	75	68	+10
https:// in a URL means that information entered into the site is encrypted	33	43	28	26	+7
Wi-Fi traffic is not encrypted by default on all wireless routers.	45	50	44	39	+6
Can identify most secure password (from list of four options)	78	78	69	73	+5
Email is not encrypted by default	46	49	45	42	+4
Ransomware involves criminals encrypting and holding users' data hostage until paid	49	51	46	46	+3
A VPN minimizes the risk of using insecure Wi-Fi networks	13	18	11	10	+3
Americans can legally obtain one free credit report year from each of the three credit bureaus	48	55	45	46	+2
Can identify a "phishing" attack (set of descriptions)	52	55	54	54	-2
AVERAGE NUMBER CORRECT OVERALL	6.0	6.0	5.0	5.0	+1.0

Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity"

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/pi_2017-03-22_cybersecurity-quiz_0-03/) Cybersecurity knowledge also varies by respondent age, although these differences are much less dramatic than the differences pertaining to educational attainment. Indeed, on a number of these questions internet users age 65 and older are just as knowledgeable as those ages 18 to 29. For instance, older and younger users are equally likely to be able to identify a phishing attack, identify the most secure password from a list and know how many free credit reports Americans are entitled to by law. However, younger users score higher on certain questions – such as whether “private browsing” mode prevents ISPs from tracking users’ online activities (a 27 point difference) or whether turning off the GPS feature on a smartphone disables all tracking of that device (a 23 point difference).

Overall, 18- to 29-year-olds correctly answered a mean of 6.0 out of 13 questions, compared with a mean of 5.0 among those 65 and older.