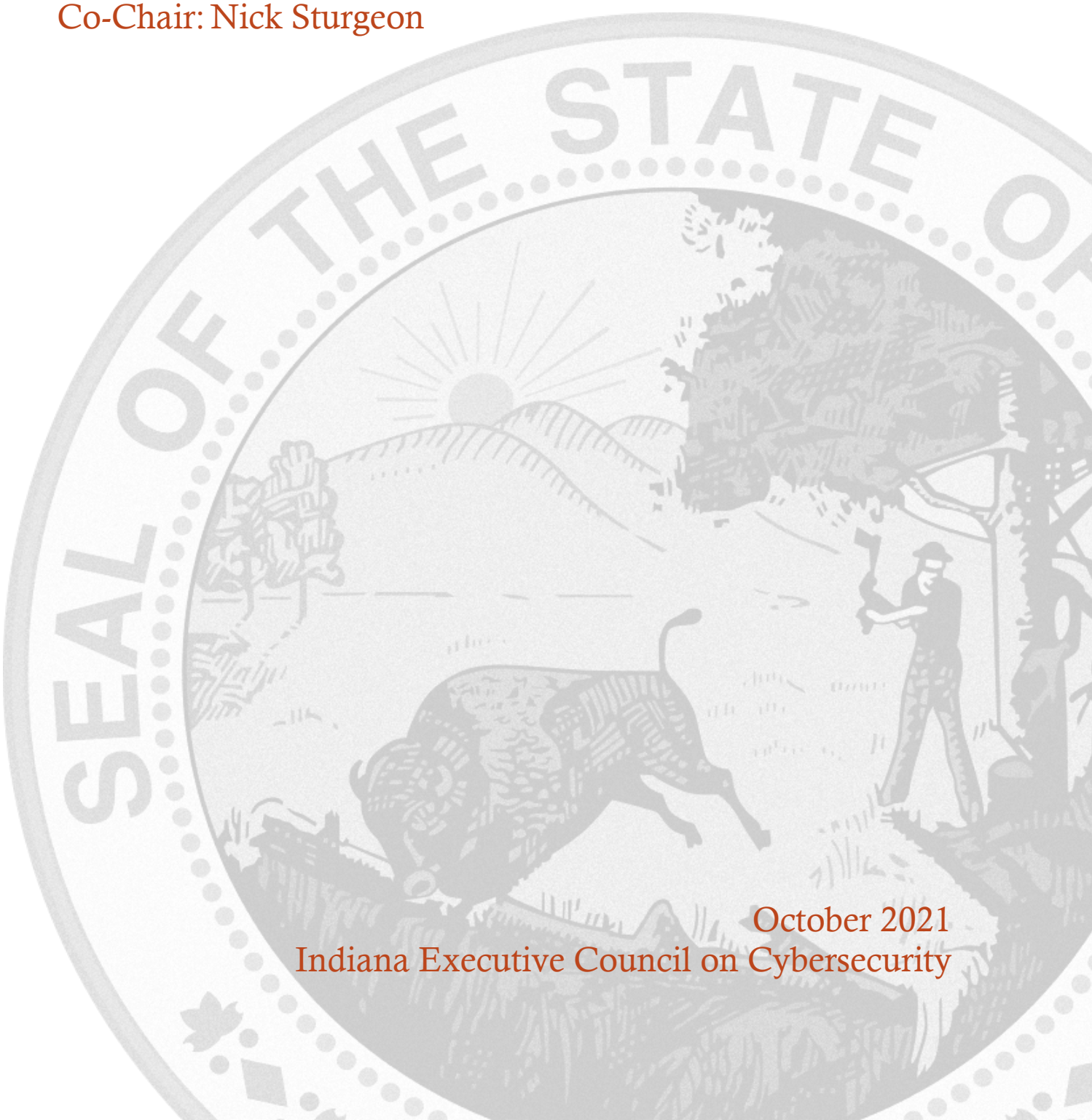
CYBER AWARENESS AND SHARING WORKING GROUP STRATEGIC PLAN

Chair: Tracy Barnes
Co-Chair: Nick Sturgeon



October 2021
Indiana Executive Council on Cybersecurity

Cyber Awareness and Sharing Working Group Strategic Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Adenike O.	Adetola	360 Security United	SOC	As Needed
Akgul	Arif	Indiana State University	Assistant Professor School of Criminology & Security Studies	As Needed
Ayers	David	Indiana Office of Technology	Program Communications Manager	Chair Proxy
Barnes	Tracy	Indiana Office of Technology	Chief Information Officer	Chair
Braidich	Richard	RCR Technology	Chief Information Security & Privacy Officer	As Needed
Bush	Ron	Ron Bush Consulting, Inc.	President	As Needed
Cerny	Kirk	Haystax, A Fishtech Group Company	Senior Director	As Needed
Davis	Philip	Community Health Network	Director, IT Risk and Compliance	As Needed
Ferrante	Anthony	FTI Consulting	Global Head of Cybersecurity, Senior Managing Director	As Needed
Giles	Clark	City of Indianapolis	Chief Technical Officer	Full Time
Harmon	Tim	Journalist	Journalist	Full Time
Hosick	David	Indiana Department of Homeland Security	Communications Director	Full Time
Jackson	Craig	IU Center for Applied Cybersecurity Research	Program Director	As Needed

Jirik	Jiri	Ivy Tech Community College	Assistant Professor - Evansville	As Needed
Johns	Jason	Sondhi Solutions	President	As Needed
Johnston	Kathleen	Michael I. Arnolt Center for Investigative Journalism, Indiana University	Founding Director	As Needed
Keller	John (Dr.)	Indiana Department of Education	Chief Information Officer, IT	As Needed
Lodin	Steve	Sallie Mae Bank	Senior Director, Cybersecurity Operations	As Needed
Lohrentz	John	Munster Police Department	Intelligence Analyst / Digital Forensic Analyst	Full Time
Lubsen	Graig	Indiana Office of Technology	Director of Communications	Full Time
McGraw	Michael	McGraw Consulting Group LLC	Senior Consultant	As Needed
Meadors	Joe	Gaylor Electric Inc	Vice President of Information Services	As Needed
Merkner	Karl	United Federal Credit Union	Security Engineer	As Needed
Ndow	Emmanuel	Marion General Hospital	Chief Information Officer	As Needed
O'Hara	Brian	BTO Associates, LLC	President/CEO	Full Time
Pirau	Ron	Archdiocese of Indianapolis	Chief Information Officer	As Needed
Potchanant	Joe	Indiana University - REN-ISAC	Director of Member Services and Support	Full Time
Rogers	Marcus	Purdue Polytechnic	Professor/Executive Director Cybersecurity Programs/Chief Scientist HTCU	As Needed
Ross	Michael	Indiana Criminal Justice Institute	Behavioral Health Division Director	Full Time

Scarbro Kennedy	Valinda	IBM	IBM Global University Specialty Programs Manager-Medical, Legal, and HBCUs	Full Time
Schmelz	Pam	Ivy Tech Community College	Chair, School of Information Technology	Full Time
Schroers	Steven	Winston and Strawn, LLP	Technical Support Supervisor	As Needed
Stahl	Tad	IN-ISAC / Indiana Intelligence Fusion Center	Director / Deputy Director for Cyber Intelligence	Full Time
Sturgeon	Nick	IU Health	Director, Information Security	Co-Chair
Vuppalanchi	Deepika	Syra Health	CEO	As Needed

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

Executive Summary

Executive Summary

- **Research Conducted**
  - State cybersecurity plans
  - Magazine articles on state cyber sharing and cyber education
  - Team member familiarity with resources and professional techniques
  - Applied experience by team members for their own operations, experience, and networks with other organizations

- **Research Findings**
  - An inventory of cyber sharing resources and cyber education/awareness from various sources
  - Articles depicting the various strategies used by state governments
  - Best practices from other industries in education and training
  - Communication types produced by the Multi-State Information Sharing and Analysis Center (MS-ISAC) (a similar model for states that Indiana might learn from for counties)

- **Additional Notes**
  - No Response

- **References**
  - State cybersecurity plans (multiple)
  - $(ISC)^2$ Cyber Edge Group 2021 Cyberthreat Defense Report
    Pew article - http://pellcener.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf
  - $(ISC)^2$ survey on cybersecurity from a Federal Executive perspective - https://www.isc2.org/-/media/ISC2/Documents/ISC2-Federal-Cyber-Survey-Report.ashx?la=en&hash=7AFB8F6E0A67C2D417D7031E17DF9E481DB21E20

- **2021 Working Group Deliverables**
  - Public Relations Campaign Plan
  - Inventory of Cyber Sharing Resources
  - MS-ISAC Member Recruitment
  - Best Practices
  - Cyber Sharing Maturity Model
  - Sharing Community Slack Channel

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. There has been limited 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.
    b. Over the last few years, the efforts of the IECC have included managing a website called the Indiana Cyber Hub (www.in.gov/cybersecurity) using the resources and subject matter expertise of the more than 200 members of the Council.
    c. In addition to the website, the IECC team along with many Council members are regular contributors to the Indiana Cyber Blog that the public can subscribe to if they would like to receive interests.
    d. Along with the website, the Indiana Cyber Hub and its cyber awareness and education efforts has included social media presence on Twitter and Facebook.
    e. Over the last several years, there continues to be an emerging number of excellent cyber sharing resources. The process of finding information can be initially difficult and sometimes the need and/or value of information is not recognized. If the need and/or desire for cyber information exists, the vast majority of it is available by searching websites and news articles.
    f. Different sources of information take various approaches to distribute material to their audiences. These approaches include:

        - Corporate sources as a primary product
        - Technical sources as an enhanced support
        - Information Sharing and Analysis Centers (ISAC) serving particular sectors against common threats
        - Fusion Centers sharing information to Federal sources and local law enforcement

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 cyberattacks.
    b. It can also be challenging to filter valuable information from the mountain of content available. The amount of information can be overwhelming and much of it is of no value to an organization. Identifying sources that provide pertinent information to a business function in an efficient manner is more difficult.
    c. Many agencies and organizations have not reached a maturity level with cybersecurity, or are not staffed to needed levels, to recognize and define the cyber information needed.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Public knowledge gap
    b. To identify needs to be facilitated by the Council and filled to scale.
    c. An understanding of where various entities in Indiana, public and private, are underserved and why they are underserved.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. A number of state entities fall under federal regulations (Internal Revenue Service (IRS), Health Insurance Portability and Accountability Act (HIPAA), Social Security Administration (SSA)). State law also directs Indiana citizens on appropriate behavior and incident response requirements.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. While Indiana led the way in developing a statewide communication plan, other states have developed and fully implemented a cybersecurity education plan since 2018. Virginia was used as an initial model. Michigan provides local governments and organizations information and has a phone app with cybersecurity awareness and education. Colorado National Cybersecurity Center has partnered with Google to implement a national campaign with state officials and legislators on cyber education.
    b. Most states find themselves in a similar position as Indiana when it comes to cyber sharing. Fusion Centers may be the most common form of information distribution at a criminal level, but are limited in audience and specific in content. ISACs, Information Sharing & Analysis Organizations (ISAO), and state-sponsored cyber sharing organizations are growing as vehicles to share to broader audiences.

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. $(ISC)^2$ Cyber Edge Group 2021 Cyberthreat Defense Report
    b. State of Cybersecurity Report 2020 I Accenture
    c. https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html
    d. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdfx

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Governors' Association and selected (few) states. Individual Indiana state agencies with limited perspectives and individually focused activities.
    b. Many states have looked to their state, local, tribal and territorial (SLTT) relationships. ISACs and Fusion Centers work to develop economies of scales. For the most part, cybersecurity training and preparedness is left to individual organizations.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Over the next 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.
    b. Identify the information available and matching it with the information needed, adding any needed value that exists, and facilitating the exchange of information between all organizations. This could be in the form of digital information, presentations, training, etc. Digital information would be the general content, threat information, advisories, vulnerabilities, etc. that entities should be aware of.
    c. Success will also be finding ways of advancing cybersecurity maturity for individual SLTT units. Often one at a time or in small groups sharing similar challenges. The difficulty is having current and useful resources/services that will be able to help with these challenges in a timely manner.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. While the State of Indiana has most certainly increased its number of resources in cyber security education within the state agencies as well as public, there could be opportunities for general cyber information to broad audiences/communications or specific information/communications for narrower audiences.
    b. There are other opportunities to make current communications, resources, and forums known to more audiences that could benefit from the information that already exists.

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. No Response

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A vibrant and energetic cyber community, complete with sharing and cyber education opportunities and effective communications, would be an attractive and prominent bullet point in attracting new opportunities.

12. **What are your communication protocols in a cyber emergency?**
    a. Over the last several years, through its development of the Indiana Cyber Annex with the Indiana Department of Homeland Security, there have been good discussion and processes put in place to best communication and assist those in need during a cyber emergency. Additionally, like other hazards, we would lean on the current procedures for Indiana Joint Operations Center and Joint Information Center for public awareness of a cyber emergency.
    b. Additional organizational communication protocols may vary with each organization, especially with sharing cyber security information. However, the State of Indiana communicates issues of concern with the MS-ISAC and other parties as needed. The Indiana Intelligence Fusion Center (IIFC) communicates with federal and local

sources. The Indiana Information Sharing and Analysis Center (IN-ISAC) works with organizations, to include elections, state agencies, K-12, on an ad hoc basis as well as publishing a weekly security brief for the Executive Branch and a monthly newsletter for the general public.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. There is a number of good information gathering organizations that effectively communicate with their constituencies. Some organizations are underserved, which provides an opportunity to deliver solutions of real value.

Deliverable: Public Relations Campaign Plan

Deliverable: Public Relations Campaign Plan - Update

General information

1. **What is the deliverable?**
    a. Update to the 2018 Public Relations Campaign Plan that will include more of a phased approach to further increase the public awareness, knowledge, and application of positive cybersecurity behaviors by all Hoosiers. The plan is also intended to promote cybersecurity as a career field and inform and educate the public about the activities of the Indiana Executive Council on Cybersecurity (IECC).

2. **What is the status of this deliverable?**
☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. As of August 2021, the initial activation of the plan is in place, with the execution of an ongoing communications program; participating in the "Days of Our Cyber Lives" podcast series; completion of significant updates to the Indiana Cyber Hub website, established presence on social media (on Twitter and Facebook – Sept. 2020) formal launch of the Indiana Cyber Blog (Dec. 2020) as a foundation for achieving the deliverable.

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?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All Hoosiers

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. While there are state departments promoting good cybersecurity habits, research suggest a continuing need to increase statewide coordination and a holistic approach to the problem.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The state of Indiana will be working with all other committees and working groups for assistance, as needed, for targeting behaviors of employees and businesses, industry, and trade groups, as well as those involving education (Pre-K-16+).

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 – partnering with CISA, USDHS as a resource for best practices
    b. State agencies: IOT, Department of Homeland Security (DHS) along with the Governor's office
    c. Associations: Selected industry and trade associations, through partnerships that exist statewide, including those whose work involving the IECC and its members

12. **Who should be main lead of this deliverable?**
    a. Program Communications Manager with IOT, at the direction of the Cybersecurity Program Director for the State of Indiana.

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

a. Implementation of some aspects of the plan will require funding and/or additional resources.

Implementation Plan

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

☐ One-time deliverable

☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Initial PR Plan Developed	IECC Working Group	100%	May 2018	
Review of PR Plan and reworked for current resources and budget constraints	IECC Communication Program Manager	100%	March 2020	
Review of PR Plan	IECC Communication Program Manager and IECC Working Group	75%	November 2021	
Approval of Update to PR Plan	IECC Program Director and IECC Working Group	0%	December 2021	
Activation of Plan	IECC Partners with the IECC Communication Program Manager leading and tracking the efforts	25%	January 2022	Be sure to share final plan with working group
Review measurable successes of outputs and outcomes of PR Plan	IECC Program Director and IECC Communication Program Manager	0%	December 2022	Present to working group
Repeat above steps every year to keep the plan refreshed and considerate of time and resources	IECC Partners with IECC Communication Program Manager leading and IECC Program Director tracking the efforts	0%	2022-2024	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
At least one	At least one	Program Communications Manager	Appropriated	None	The Program Communications Manager is a very experienced public relations professional working at the direction of the Cybersecurity Program Director and whose overall responsibility is defined as plan execution, public representation, and coordination among key agencies. Will also oversee activities and budget for additional resources, up/to including the participation of an advertising agency, purchase of external resources/services related to analytics, media monitoring, as defined/needed to provide measurement of the outcomes, as defined in the deliverable.

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	TBD	TBD	State	Private Sector and/or grant from federal government	
Purchase of advertising space	Support of campaign; broad reach; message consistency	Incl.	Incl.	TBD	TBD	

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, 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.
b. In the absence of available funding, there is a potential cost to individuals and businesses related to a cyberattack or a data breach, the average cost of which, according to a recent report from IBM, is $4.62 million and $4.24 million, respectively.

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. Additionally, educational opportunities could be lost, in the absence of encouraging people, especially middle school, high school and college students, from pursuing a career in cybersecurity. A loss in momentum and capitalizing on the progress achieved through the establishment of and the ongoing work of the IECC as a model for cybersecurity governance and its position at the forefront nationally among other state governments.

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

a. An acceptable return on investment (ROI) for a marketing campaign is, typically, a ratio of 5-to-1 in the way favorable media coverage and/or exposure with the intended audience(s) compared to the budget. An exceptional ROI is considered to be in the range of 10-to-1. There are 10 methods that can be used to help define the metrics to use as a baseline.

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

☒No ☐ Yes

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?

☐No ☒ Yes

a. Every state. But, not recommended.
b. We can examine using Ohio or Illinois or Kentucky. The challenge will be conducting sufficient research to measure their lack of activity and results.
c. In this case, it is more important to measure against a national standard (i.e., Pew Study, updated additional resources/methods) 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 (i.e., Advertising Agency and state staff support)

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

☒No ☐ Yes

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. Working with the Program Communications Manager and Cybersecurity Program Director.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Statewide with all Hoosiers, as well as by the public and private sectors (all businesses/industries, organizations, non-profits, education).

Communications

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

a. IECC
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)?

☒No ☒ Yes

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

a. No Response

Evaluation Methodology

Objective 1: The IECC Communications Program Manager will use the 2018 Statewide PR Cybersecurity Campaign Plan and develop a phased approach to the tactics as resources allow by December 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Communications Program Manager will leverage the assets of Indiana's cybersecurity program to create an increasingly larger presence on social media channels including Twitter, Facebook, and LinkedIn increasing its subscription by 30% each fiscal year.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 3: The IECC Communications Program Manager will update a weekly blog as a tool for measurably increasing public awareness by further positioning Indiana as a leader in cybersecurity and increasing its subscription by 25% each fiscal year.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Inventory of Cyber Sharing Resources

Deliverable: Inventory of Cyber Sharing Resources - Update

General Information

1. **What is the deliverable?**
    a. An update to the 2018 inventory of resources assembled by the IECC

2. **What is the status of this deliverable?**
    ☒ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% Not Started

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. The inventory serves as a resource for those needing trusted and vetted cyber information.

6. **What metric or measurement will be used to define success?**
    a. We envision this being static content on an IECC web page. One metric is the number of hits, though this will not likely drive huge web traffic. It could be of exceptional value to those needing information, especially those just ramping up their security programs.

7. **What year will the deliverable be completed?**
    a. 2021

8. **Who or what entities will benefit from the deliverable?**
    a. Business, government, and possibly citizens.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There is likely some overlap, but the accumulation of the inventory was straightforward. Keeping the list current will require little maintenance and any overlap would be inconsequential.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

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. Not applicable

12. **Who should be main lead of this deliverable?**
    a. Cyber Awareness and Sharing Working Group with the lead being IN-ISAC

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively and having the ability to share the value of the products.

Implementation Plan

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

☐ One-time deliverable
☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
List developed	IN-ISAC Manager	100%	July 2021	Ongoing only in those additional resources can be added

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

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
No Response						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. It is part of a library of resources that could be used by those needing cybersecurity guidance.

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

a. The deliverable provides information resources that will assist those needing cyber information.

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

a. No risk, but a resource that could be very valuable.

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

a. The list could be very valuable to those that visit the library of resources. It will be hard to measure the value of coming to a trusted source and viewing the information. One could measure web hits on the document, but the value from any visit will be hard to measure.

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

☐No ☒ Yes

a. A number of states have lists of resources. Michigan is one example, but there are other examples as well. The types of resources in their libraries vary.

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. There are many states that do not have a list of resources such as this. Cybersecurity and outreach from states to citizens, businesses, etc. are widely varied in both content and delivery mechanisms.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable**?
    a. None.

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. No Response

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. IN-ISAC, Indiana Office of Technology (IOT)

27. **Can this deliverable be used by other sectors?**
    a. Yes, all sectors.

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. Sector partners, local government, state agencies, businesses, and their associations, as well as the general public

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

30. **What are other public relations and/or marketing considerations to be noted?**
    a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Awareness and Sharing Working Group will complete an inventory of cyber sharing resources by August 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey – Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: MS-ISAC Member Recruitment

Deliverable: MS-ISAC Member Recruitment

General Information

1. **What is the deliverable?**
    a. MS-ISAC is a resource delivering a broad range of information to the State of Indiana. This includes vulnerability notifications, threat notifications, and other information including a monthly conference call. The Cyber Sharing group, through the efforts of the IN-ISAC, plans to push enrollment in the MS-ISAC. Education and Local government working groups may be able to assist with this deliverable.

2. **What is the status of this deliverable?**
    ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. Better cybersecurity information to a broad range of schools and local governments that are underserved.

6. **What metric or measurement will be used to define success**?
    a. Number of Indiana SLTT and K-12 schools signed up for the MS-ISAC.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. SLTT and K-12 organizations signing up for the information.

9. **Which state or federal resources or programs overlap with this deliverable**?
   a. MS-ISAC produces quality information in a variety of formats. This information is valuable and vetted.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Getting the word out to SLTT and K-12 would be very helpful.

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. Those that can help with the drive to get SLTT and K-12 organizations to join MS-ISAC.

12. **Who should be main lead of this deliverable?**
    a. Tad Stahl, IN-ISAC manager

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively and having the ability to share the value of the products.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review Outreach plan	IN-ISAC Manager	100%	February 2021	
Implement plan and tactics	IN-ISAC Manager	50%	December 2021	
Update outreach plan and implement	IN-ISAC Manager	0%	2022-2024	To be done annually

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1.0	N/A	IN-ISAC manager	State Indiana Office of Technology	N/A	

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
No Response						

Benefits and Risks

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

a. Getting good, current, and vetted cyber threat, advisory, and awareness materials to those subscribed on a regular basis.

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

a. Through better information to those involved in the daily security operations of an organization.

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

a. There are many state institutions that could benefit from the federally funded service. This service is also free to SLTT and schools. Any costs for MS-ISAC would go unrealized.

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

a. Difficult to gauge the value from participants. It can be measured in the increased numbers using MS-ISAC.

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

☐No ☒ Yes

a. All states subscribed to the MS-ISAC newsletter.

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. No

Other Implementation Factors

---

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

a. None as of now.

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

☒No ☐ Yes

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

a. No Response

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

a. IN-ISAC

27. Can this deliverable be used by other sectors?

☒No ☐ Yes

a. Local governments and schools

Communications

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

a. SLTT and schools.

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

☐No ☒ Yes

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

a. None as of now.

Evaluation Methodology

Objective 1: Indiana-ISAC will work to increase MS-ISAC membership by 25 percent each calendar year.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Sharing Best Practices

Deliverable: Cyber Sharing Best Practices - Update

General Information

1. **What is the deliverable?**
    a. Provide an updated list of cyber sharing best practices

2. **What is the status of this deliverable?**
    ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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. Provide a recommendation of best practices for information sharing in the state. This will also provide a common set of terms that will make it easier to communicate effectively.

6. **What metric or measurement will be used to define success?**
    a. The adoption of the standards and best practices throughout the State of Indiana.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The Public and Private Sectors

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. USDHS CISA practices and guides with additional resources that may overlap with this deliverable

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Not applicable

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. Not applicable

12. **Who should be main lead of this deliverable?**
    a. Cyber Awareness and Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. None

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review List developed in 2018	Nick Sturgeon	75%	March 2022	
Review with the Working Group	Cyber Sharing Working Group	0%	May 2022	
Present update on the deliverable	IECC	0%	June 2022	
Post on Cyber Hub website	IECC Communications Manager	0%	July 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0					

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
N/A						

Benefits and Risks

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

a. It will help businesses and citizens by creating and centralizing a list of best cybersecurity practices.

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

a. This will help increase knowledge of cybersecurity best practices to Indiana businesses and citizens. No real cost associated with this deliverable. With the adoption of these best practices, businesses and citizens will reduce the overall cybersecurity risk profile of the entire state.

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

a. While updating this deliverable will only cost time to make the updates to the Indiana Cybersecurity website, an organization could lose time and money if they are unaware of a best practice and undergo a cyberattack as a result. Many look to the state for key education on protecting themselves and businesses. So, developing this and people using it may create a needed efficiency and prevent an organization from a cyberattack.

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

a. Initial metrics will be based around unique website visits and total site visits. Additional metrics will be around capturing data to see if these best practices are being implemented.

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

☐No ☒ Yes

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?

☐No ☒ Yes

Other Implementation Factors

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

a. None as of now

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

☒No ☐ Yes

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

a. No Response

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

a. The only people contacted to this point are those within the Cyber Awareness and Sharing Working Group.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All Sectors

Communications

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

a. Sector partners, local government, state agencies, businesses and their associations, the general public

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

☐No ☒ Yes

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

a. None as of now

Evaluation Methodology

Objective 1: IECC Cyber Awareness and Sharing Working Group will update a list of best practices by July 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Sharing Maturity Model

Deliverable: Cyber Sharing Maturity Model

General Information

1. **What is the deliverable?**
    a. Cyber Sharing Maturity Model

2. **What is the status of this deliverable?**
    ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. Creation of a maturity model that businesses and governments can self-assess and use links/info provided to increase their cyber maturity.

6. **What metric or measurement will be used to define success?**
    a. Completion of product, sample feedback from a variety of stakeholders, and a number of downloads of the model from the cyber hub.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Businesses and government

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. No Response

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resources Working Group and the voting members of the IECC.

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. No Response

12. **Who should be main lead of this deliverable?**
    a. Cyber Awareness and Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Quantifying success of the model and keeping it simple enough for all to use.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Rework 2019 Draft of model	Cybersecurity Program Director	100%	March 2020	
Review and develop model	Cyber Awareness and Sharing Working Group, Strategic Resources Working Group	50%	February 2022	
Present model for feedback from Council	IECC	0%	April 2022	
Make edits and design	Cybersecurity Program Director and Cyber Sharing Working Group	0%	May 2022	
Finalize Model	Cyber Sharing Working Group	0%	June 2022	
Incorporate model into IECC PR and Communications Plan	Public Awareness and Training Working Group	0%	July 2022	
Distribute to stakeholders	IECC and partners	0%	August 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

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
No Response						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The Cyber Sharing Maturity Model will provide all those who use it, especially local government, K-12 schools, and small businesses, with a starting point to begin understanding the many resources around cyber threat sharing and education.

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

a. By further educating those who would like to increase their cybersecurity levels, it will help reduce their cybersecurity risks and impact because they may be better prepared for a cyber event.

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

a. As of now, many are confused by the many choices with cyber sharing and threat resources. Due to the confusion, many do not move their cybersecurity level.

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

a. The completion of the model will be one output measure of success. This model is to be used by local governments, businesses, and educators in Indiana. The users finding value in it will be another measure of success.

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

☒No ☐ Yes

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?

☐No ☒ Yes

a. While there are many states that have cyber sharing resource pages, we were not able to find a similar maturing model

Other Implementation Factors

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

a. None as of now

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

☒No ☐ Yes

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

a. No Response

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

a. Indiana University who provided the idea of a cyber sharing maturity model and are partners of this deliverable.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All Sectors

Communications

---

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

a. Sector partners, local government, state agencies, businesses and their associations, general public

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

☐No ☒ Yes

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

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Awareness and Sharing Working Group will edit and post the Indiana's updated cyber sharing maturity model by July 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Awareness and Sharing Working Group will distribute Indiana's updated cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by August 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Sharing Community Slack Channel

Deliverable: Cyber Sharing Community Slack Channel

General Information

1. **What is the deliverable?**
   a. Launch a Cyber Sharing Community Slack Channel

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices
   ☒ 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. To facility a grass roots level sharing of cybersecurity information (i.e. Indicators of Compromise (IOCs), cyber observables, threats, intelligence, tactics, techniques, and procedures) among the IECC members at a tactical/technical level.

6. **What metric or measurement will be used to define success?**
   - Number of IECC members in the IECC Cyber Sharing Community Slack
   - Channel Number of IECC members engaged in the Slack Channel.
   - Total messages in the Slack Channel.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All IECC Members and their organizations

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. DHS HSIN

Additional Questions

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

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. We will need representation from as many IECC Working Groups and members to get the most out of the effort.

12. **Who should be main lead of this deliverable?**
    a. Nick Sturgeon, Co-chair of IECC Cyber Awareness and Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Getting the IECC Members to actively participate in the Slack Channel.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Set up the Channel	Nick Sturgeon	100	May 31, 2021	
Beta Test	Nick Sturgeon	50%	November 30, 2021	
Go Live	Nick Sturgeon	0%	January 31, 2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

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
Slack Channel	This application is the medium in which the sharing will take place.	Free	$8/person	No Response	No Response	To get additional capabilities and features from the slack channel we would need to move up to the Pro plan.

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The IECC Cyber Sharing Community Slack Channel will provide a medium in which the technical cyber security staff of our members can sharing cyber information in real time.

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

a. This Slack Channel will provide the means in which our member organizations and their cyber security/IT staff share cyber information in real time. This allows them to connect with their peers in other organizations at a level they determine is sufficient. This also removes a choke point in sharing information by eliminating the need to rely on one person to distribute information. Additionally, individuals can determine what information to share and what information to consume. The biggest cost reduction is time.

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

a. That critical cyber information will not get shared as broadly as needed.

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

a. The definition of success will be the total participation and engagement of the IECC members.

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

☒No ☐ Yes

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?

☒No ☐ Yes

Other Implementation Factors

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

a. No Response

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

☒No ☐ Yes

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

a. We will need engagement from the IECC member organizations to keep this going.

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

a. IECC Healthcare Committee

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

Communications

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

a. The IECC members

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

☒No ☐ Yes

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

a. Communication to IECC members via the IECC leadership.

Evaluation Methodology

Objective 1: IECC Cyber Awareness and Sharing Working Group will create the Slack Channel by May 2021.

☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Awareness and Sharing Working Group and IECC Healthcare Committee will conduct a beta test of the Slack Channel by December 2021.

☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: Complete the Live Production Launch of the Slack Channel by January 2022.

☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

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

a. 2018 Public Relations Plan
b. Cyber Sharing Resources Inventory 2021
c. Cyber Maturity Model Draft

2018 Public Relations Plan

Indiana Executive Council on Cybersecurity

Public Awareness and Training Plan

2018-2020

Public Awareness and Training Working Group

June 2018

TABLE OF CONTENTS

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

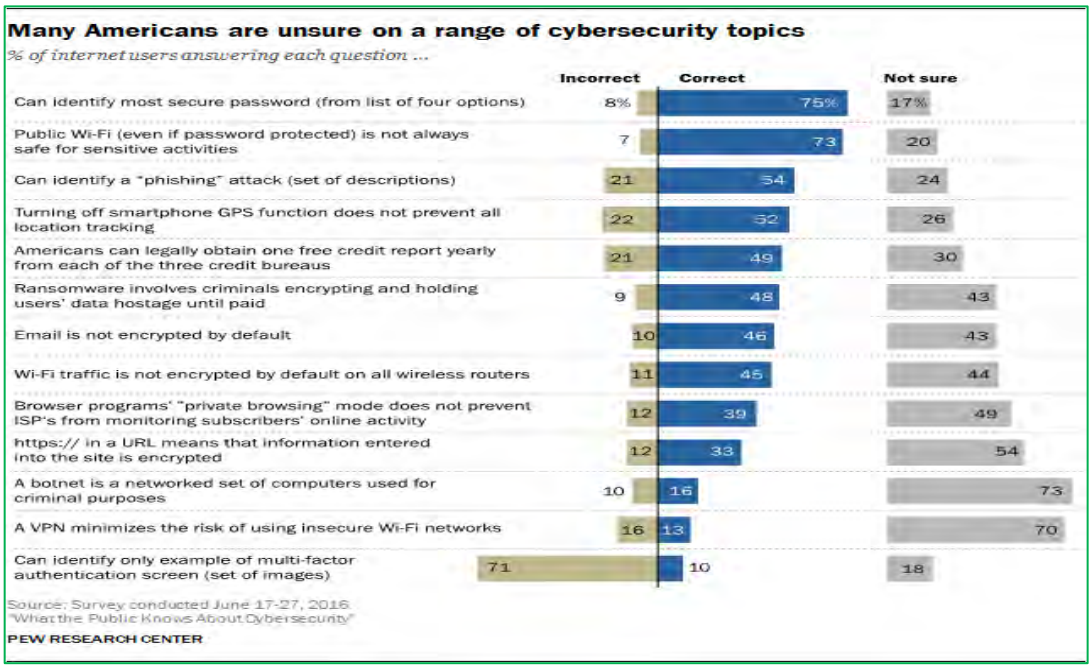
Summary

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.auscert.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

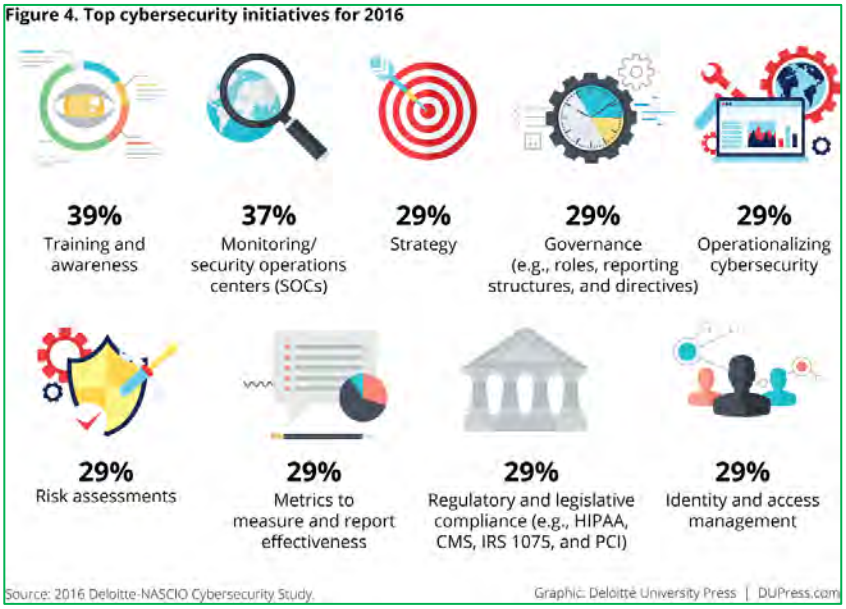
    b. Some key facts from the report:
        - The world economic forum's global risks 2015 report highlighted cyberattacks and threats as one of the most likely high-impact risks. In the United States, for example, cybercrime already costs an estimated $100 billion a year.
        - IOT Sensors and devices 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. Deliotte NASCIO Cybersecurity Study, Doug Robinson and Srini 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.

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

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

- 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.

- 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

- 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:// 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 $1,500 $10,000 <u>Total</u>: $143,000	Initial campaign development Monthly creative Monthly ad buy
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 qualitied volunteers for speakers.	$0 $42,000 $12,000	Development and maintenance. 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. 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.

Cyber Sharing Resources Inventory 2021

Inventory of Information Resources

Type of Information	Source	Interval	Audience	Notes	URL
On-line webinars	MS-ISAC	Frequent, regular	All members		https://www.cisecurity.org/ms-isac/
Monthly newsletter	MS-ISAC	Monthly	All members		https://www.cisecurity.org/ms-isac/
Advisories -UFOUO	MS-ISAC	Frequent, regular	All members	Distributes from multiple sources (DHS, FBI)	https://www.cisecurity.org/ms-isac/
SOC advisories	MS-ISAC	Frequent, regular	State of IN	We are a customer, data could be scrubbed and shared	https://www.cisecurity.org/ms-isac/
Election Communications	MS-ISAC	Frequent, regular	Sec of State	Multiple comms type, election specific	https://www.cisecurity.org/ms-isac/
News	SANS	Weekly	Subscribers	Informational	https://www.sans.org/
Advisories -UFOUO	DHS	Frequent, regular	All states		https://www.dhs.gov/
Advisories	DHS	Infrequent	All states		https://www.dhs.gov/
Advisories	FBI (IC-3)	Infrequent	All states		https://www.fbi.gov/
Advisories	McAfee	Frequent, regular	Customers	Tend to focus on McAfee products, occasional acute threats	https://www.mcafee.com/en-us/index.html
	Shadowserver.org				https://www.shadowserver.org/wiki/
	FS-ISAC				https://www.fsisac.com/
	REN-ISAC				https://www.ren-isac.net/public-resources/AlertsAdvisories.html
	Open DNS				https://www.opendns.com/
	H-ISAC				https://h-isac.org/threat-intelligence/
Advisories	FinCEN (Financial Crimes Enforement Network)				https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories
	FBI InfraGard		Members	Similar to FS-ISAC Alerts	https://www.infragard.org/
	US-CERT		Subscribers	General - Across all sectors / industries	https://www.us-cert.gov/
	Secret Service		Subscribers	General - Across all sectors / industries	https://www.secretservice.gov/
	Consumer Financial Protection Bureau		Subscribers	Bank / Non-Bank focused	https://www.consumerfinance.gov/
	Office of Comptroller of Currency		Subscribers	Bank / Non-Bank focused	https://www.occ.treas.gov/
	Federal Reserve Bank		Subscribers	Bank focused	https://www.federalreserve.gov/
	Federal Deposit Insurance Corporation		Subscribers	Bank focused	https://www.fdic.gov/
	National Credit Union Administration		Subscribers	Credit Union focused	https://www.ncua.gov/Pages/default.aspx
	Federal Financial Institutions Examination Counci		Subscribers	Bank / Credit Union focused	https://www.ffiec.gov/
	Krebs-on-Security (Blog)		Subscribers	General - Across all sectors / industries	https://krebsonsecurity.com/
	National Association of Federally-Insured Credit Unions		Subscribers	Credit Union focused	https://www.nafcu.org/
	Indiana Credit Union League		Subscribers	Credit Union focused	https://www.icul.org/Pages/default.aspx
	Credit Union National Association		Subscribers	Credit Union focused	https://www.cuna.org/

Cyber Maturity Model Draft

Cyber Sharing Maturity Model
DRAFT

Level	Maturity	Score	Resources for Model – INSERT MATURITY RESOURCE LINKS TO IMPROVE SCORE & LEVEL
5	Intake information shared by cyber sharing networks	3 – Optimizing: 2 – Progressing: 1 – Limited: 0 – Not Started	• ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Section 3.2 Applying Shared Information • ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Figure 3. Applying Information to Cybersecurity Risks • DHS Cyber Information Sharing and Collaboration Program (CISCP) • Multi-State Information Sharing & Analysis Center • Infrastructure Protection Gateway (IP Gateway):Vuln assessments & Data Analytics • **The Office of Cyber and Infrastructure Analysis (OCIA)** provides infrastructure consequence analysis and prioritization capabilities.
4	Join cyber sharing networks	3 – Optimizing: 2 – Progressing: 1 – Limited: 0 – Not Started	• ISAO Standards Org - Information Sharing Groups (57 as of Apr 2018) • DHS Cyber Information Sharing and Collaboration Program (CISCP) • Multi-State Information Sharing & Analysis Center • Infragard

			• Infrastructure Protection Gateway (IP Gateway):Vuln assessments & Data Analytics
3	Internal policies of cyber threat sharing, aware of cyber sharing networks	3 – Optimizing: 2 – Progressing: 1 – Limited: 0 – Not Started	• National Preparedness Course Catalog o AWR-177-W Information Risk Management o AWR-353-W Using the Community Cyber Security Maturity Model (CCSMM) to Develop a Cyber Security Program • Information Sharing and Analysis Organization Standards Organization • Multi-State Information Sharing & Analysis Center • DHS Cyber Information Sharing and Collaboration Program (CISCP)
2	Cyber threat detection and recognition	3 – Optimizing: 2 – Progressing: 1 – Limited: 0 – Not Started	• IBM: Raise the Red Flag: Guidelines for Consuming and Verifying Indicators of Compromise - https://securityintelligence.com/raise-the-red-flag-guidelines-for-consuming-and-verifying-indicators-of-compromise/ • National Preparedness Course Catalog o AWR-169-W Cyber Incident Analysis and Response o AWR-177-W Information Risk Management • US-CERT Alerts • DHS Cyber Information Sharing and Collaboration Program (CISCP) • DHS Enhanced Cybersecurity Services (ECS) • Multi-State Information Sharing & Analysis Center

			• Federal Virtual Training Environment (FedVTE)
1	Cyber threat awareness (prevention, protection, preparedness)	3 – Optimizing: 2 – Progressing: 1 – Limited: 0 – Not Started	• US-CERT Nat'l Cybersecurity Awareness System Tips: https://www.us-cert.gov/ncas/tips • DHS Cyber Information Sharing and Collaboration Program (CISCP) • DHS Enhanced Cybersecurity Services (ECS) • **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** • Multi-State Information Sharing & Analysis Center (MS-ISAC) • National Cybersecurity Awareness Month (NCSAM) • Federal Virtual Training Environment (FedVTE)

Definition of Maturity sublevels:

Limited – Most basic level. For example, the organization may have limited processes, but does not have a clear policy and plan.

Progressing – Planning has begun and is in process.

Optimizing – Highest level of maturity indicating that cyber sharing capabilities are fully developed and integrated into business processes. This includes automation tools.