Crowe Horwath

Smart decisions. Lasting value.™

Demystifying Cybersecurity

Legal and Ethics Conference
December 1, 2016

Cybersecurity Watch Blog
www.crowehorwath.com/cybersecurity-watch

© 2016 Crowe Horwath LLP

Crowe Team

Scott Nickerson, CPA, CGMA
Partner – Government Audit

Blake Gardner
Sr. Staff - Technology Risk

© 2016 Crowe Horwath LLP

Agenda

1. Educate
2. Examples of Cybersecurity risks
3. How can we help government entities?

© 2016 Crowe Horwath LLP

What is Cybersecurity?

DoD Definition:

"A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current , threats and enable timely response and recovery.“

Three main areas of Cybersecurity:

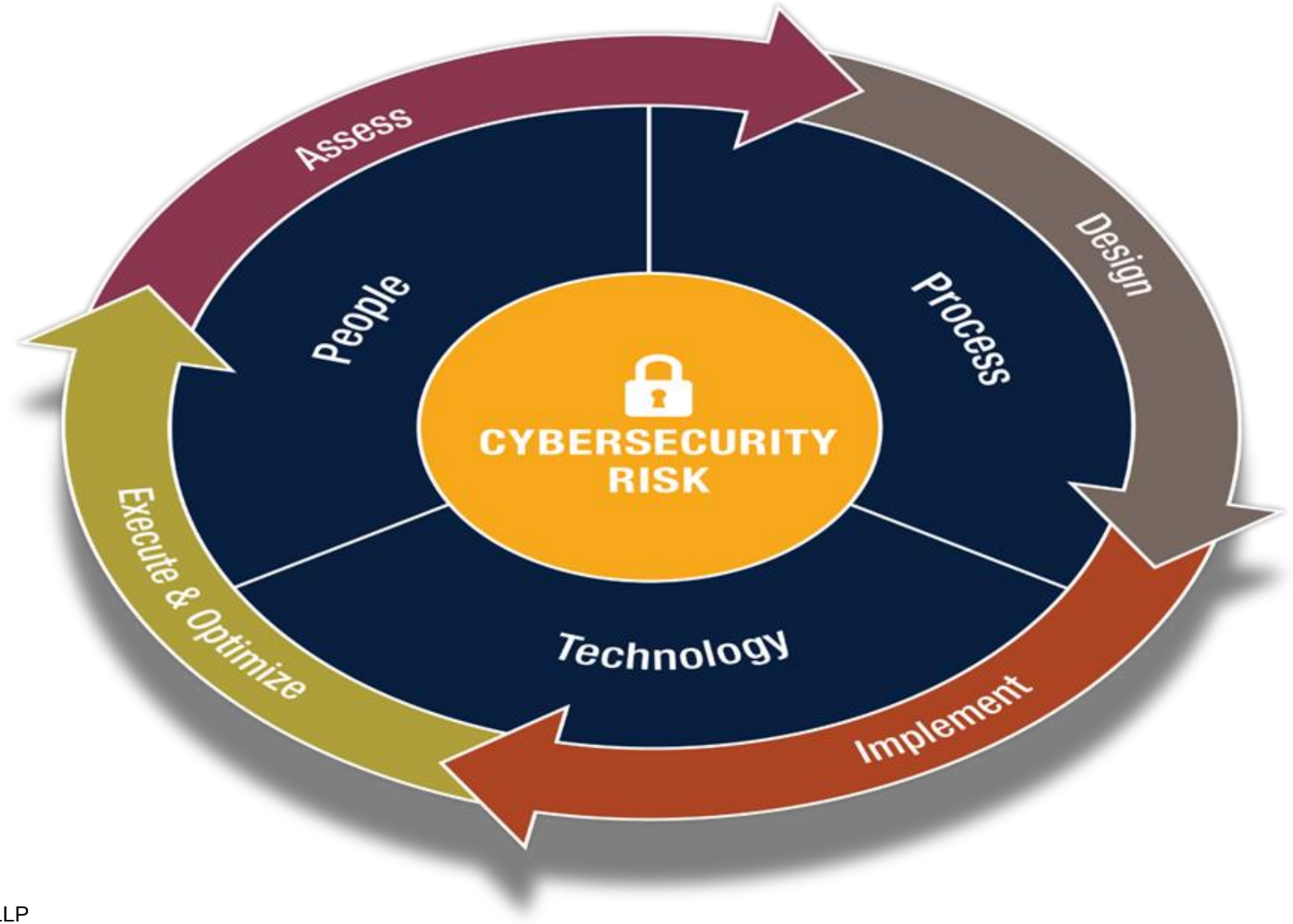
- People
- Processes
- Technology

Who does it impact?

- Anyone, individual or organization, connected to the internet

© 2016 Crowe Horwath LLP

Cybersecurity Approach



© 2016 Crowe Horwath LLP

Top Cybersecurity Threats and Vulnerabilities

1. Technology

- Lack of Encryption
- Weak Mobile Devices Controls
- Remote Access

2. People

- Lack of Security Awareness
- Weak Passwords and Password Controls
- Lack of collaboration between IT and business

3. Processes

- Third Party Management
- Lack of IT leadership, policy and procedure
- Lack Disaster Recovery Plan and Backup procedures

© 2016 Crowe Horwath LLP

The Bad Guys are Winning

- Number of breaches doubles each year
  - Malware
  - Social media
  - Hacking

- Of the incidents that lead to Breaches…

>80% from external parties

46.2% targeted technology not being monitored

>66% with the “Cyber-Espionage Pattern” have featured phishing

Source: Verizon 2016 DIBR

© 2016 Crowe Horwath LLP

What is Ransomware?

- Malware designed to hold systems and data hostage while the attacker demands that victims pay a ransom
  - Encryption of the system / data base
  - Denial of Service attacks
- Goal is to force the victims to pay a ransom to regain control of their data
  - According to the FBI, from April 2014 to June 2015, a single strain of ransomware was responsible for more than **$18 million** in losses in almost 1,000 instances.
- How does the infection occur?
  - Phishing attacks
  - Advertisements on websites
  - Malicious software downloaded by an employee
- Options besides paying
  - Early variants may have vulnerabilities allowing the victim to break the encryption
  - Strong data backup procedures
  - **Prevention is the key**

© 2016 Crowe Horwath LLP

Madison County, Indiana Ransomware Attack

November of 2016 – *Attackers were able to lock government employees out of court records and police reports through an encryption of the database where they are stored. The Sheriff's office was unable to access the jail processing system and thus were unable to book newly arrested individuals. Government workers were forced to use laptops and create word documents to record and collect information. The county was in the process of adding a backup system and full backups had not been completed. The attackers gave the county 7 days to pay the ransom, and the ransom was paid.*

"The IT department took all the security measures they could have, but hackers found a way in." – Lisa Cannon, Madison County IT Director

Motivations

- Money
- Shutting down / slowing the criminal justice process
- Revenge on local government

Common Methods of Attack

- Phishing
- Malware

http://arstechnica.com/security/2016/11/indiana-county-government-shut-down-by-ransomware-to-pay-up/

http://www.networkworld.com/article/3139975/security/ransomware-hammers-madison-county-indiana.html

© 2016 Crowe Horwath LLP

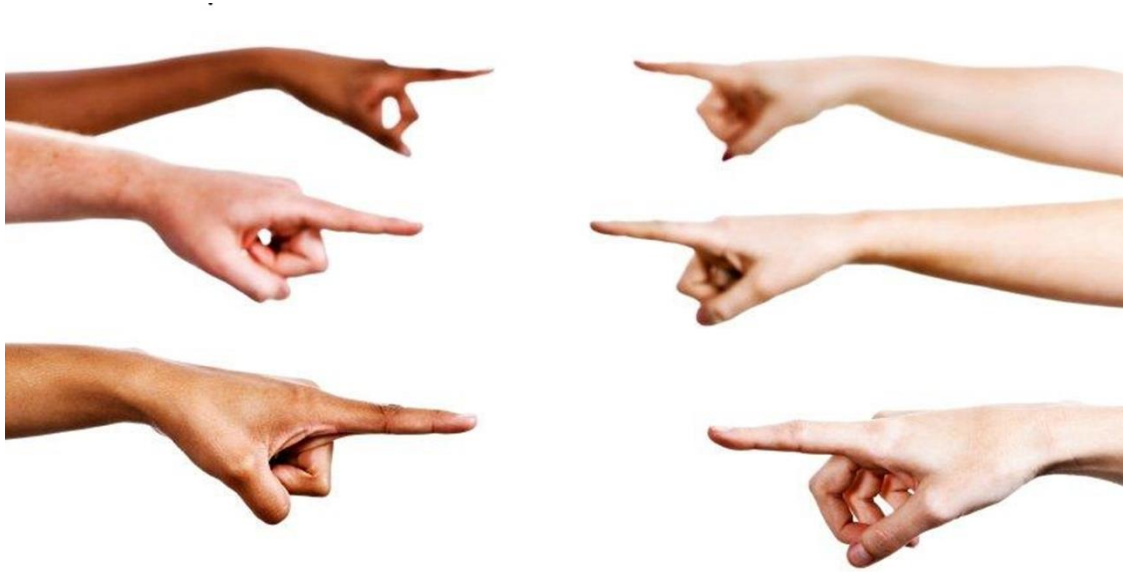
How to Prepare for and Prevent Ransomware

Disaster Recovery / Backup processes	• Documented Disaster recovery plan that includes what to do in the event of a ransomware attack • Implementation of regular backups
Awareness	• Phishing attacks • Social Engineering • Training
Monitoring	• Email Filtering • Approval process for downloaded software • Network monitoring

© 2016 Crowe Horwath LLP

Cybersecurity Strategy (How Can I Help Our Local Governments?)

- Who is leading the initiative?
- Is everything on the same page?
- What's our top priority?
- Would you know if you were hacked?
- Who would respond?
- What does your board think?
- Are you covered by insurance?



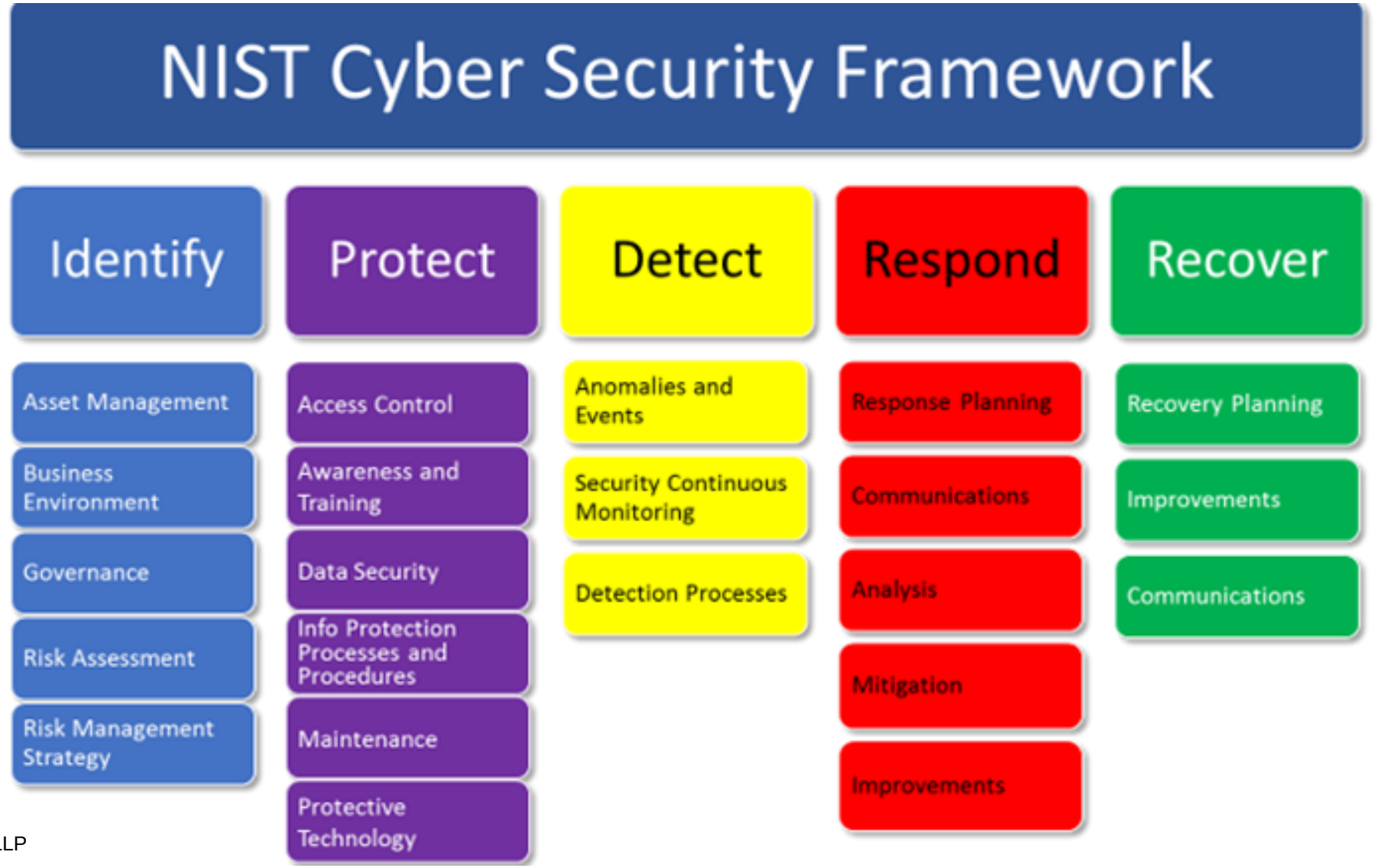
Management still regards cybersecurity predominantly a technology issue rather than a business issue.

Key Steps

1. IT Directors and CIOs should maintain focus on business impacts and outcomes from cyber risks.
2. Provide reports that help the board focus on your organization's specific cyber risk situation, instead of distracting media headlines.
3. Consider new technology and skilled personnel to organize, execute and maintain the cybersecurity initiative.

© 2016 Crowe Horwath LLP

Assess Cybersecurity Risk - NIST Framework



© 2016 Crowe Horwath LLP

Key Takeaways

- What is included in your information security program?
  - Penetration testing, security assessments, compliance reviews, etc.
  - Has it been tested?
- What are your compliance needs?
  - Consider individual state privacy laws, HIPAA, PCI, etc.
- Where is your data stored, how is it transferred and who has access to it?
  - How confident are you? Have you considered mobile devices, employees residences/vehicles, email?
- Have your cyber risk controls been reviewed?
  - If you had a breach, would you know?
- How are you communicating with your Board of Directors?
  - Do they know the risks, needs and plan for risk reduction?
  - Are they accepting the current level or risk?
- Do a high-level independent assessment.

© 2016 Crowe Horwath LLP

Cybersecurity Approach

© 2016 Crowe Horwath LLP

Cybersecurity Watch Blog
www.crowehorwath.com/cybersecurity-watch

Thank you.

Blake Gardner
Direct 317.706.2763
Blake.Gardner@crowehorwath.com

Scott Nickerson, CPA, CGMA
Direct 317.706.2693
Scott.Nickerson@crowehorwath.com

In accordance with applicable professional standards, some firm services may not be available to attest clients.

This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.
© 2016 Crowe Horwath LLP, an independent member of Crowe Horwath International crowehorwath.com/disclosure