Crowe Horwath

Demystifying Cybersecurity: What You Need to Know

Aug. 13, 2014

Agenda

- Understanding Cybersecurity
- Frameworks and Regulator Expectations
- A Practical Approach to Assessing Cybersecurity Risk
- A Boardroom Discussion

Poll Question 1

- What does cybersecurity mean to you?

a) Denial of Service Attacks (DoS)
b) Advanced Persistent Threats (APTs)
c) Cloud computing security
d) Breaches of personal, financial and healthcare data
e) Homeland Security and Nation-State Attacks
f) Unsure/don't know

Understanding Cybersecurity

- What is it?
- Who does it impact?
- How is it different than information security?
- What are the trends?

Definition of Cybersecurity

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.
- The general security objectives comprise the following
  - Availability
  - Integrity, which may include authenticity and non-repudiation
  - Confidentiality

Source: ITU-T X.1205, Overview of cybersecurity

Simplest Definition

- "Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."
- Regardless of the source of definition, objectives still continue to be:
  - The Triad of Security – CIA of "CRITICAL DATA"
    - Confidentiality
    - Integrity
    - Availability
  - Who does it impact?
    - Anyone, individual or organization, connected to the internet

Source: Merriam Dictionary

Information Security vs. Cybersecurity

- **Information security**, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)
- Cybersecurity is a sub-set of information security
  - It is related to threats (and protection of data from these threats) that come from globally connected networks like internet
- Information security is related to overall protection of data regardless of the form of data.

Trends in Cybersecurity

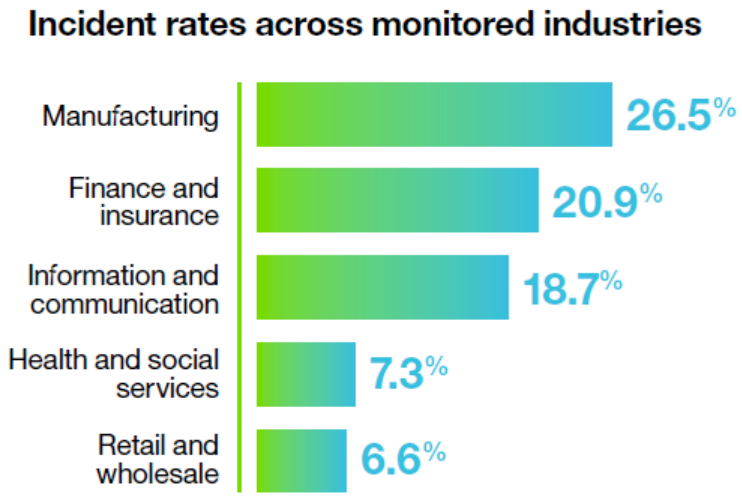
- Expect cyber attacks
  - More frequent, varied and mobile
- Center stage and becoming more public
- More corporate accountability and resulting litigation
- More regulatory pressure

As a result of the above four trends, other sub-trends are:

- Standard frameworks
- Growing workforce
- Expanded research
- Mobile coverage

IBM's Cyber Security Intelligence Index

- Analysis of cybersecurity attack and incident data
  - Security "events" to "attacks" to "incidents"
  - For an average size client of IBM here are the **annual** stats:
    - Approximately 82 million events
    - 73,400 attacks
    - 90.2 incidents



Source: IBM Security Services Cyber Security Intelligence Index Report

Poll Question 2

What framework or guide should you utilize?

a) NIST Cybersecurity Framework
b) SEC/OCIE Cybersecurity Examination Guide
c) FFIEC Cybersecurity Assessment
d) SANS Top 20
e) FCC Cybersecurity Planning Guide
f) Open Cybersecurity Framework Project (OCFP)
g) Unsure/don’t know

Cybersecurity Frameworks and Examination Guides

- Many cybersecurity frameworks exists, but all have a common goal to:
  Establish the confidentially, integrity and available of data and information networks.

Leading Frameworks:

- NIST - The most comprehensive and applicable to all organizations
- FCC Cybersecurity Planning Guide

Examination Guides:

- SEC/OCIE Cybersecurity Examination Guide
- FFIEC Cybersecurity Assessment
- HIPAA Security Rule

The Cybersecurity Framework Need

- Homeland Security Secretary Janet Napolitano warns on January 24, 2013:
  - “A cyber 9/11 could happen imminently.”
  - "Attacks are coming all the time. They are coming from different sources, they take different forms. But they are increasing in seriousness and sophistication.”
  - “There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage."

Source: http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124

The NIST Cybersecurity Framework is Born

- Cyber Security Executive Order
  - February 2013 State of the Union
  - Increasing the sharing of information (Real Time) for “Critical Infrastructure”
- Calls for risk-based set of industry standards and best practices

- Cyber Security Framework
  - NIST released the draft on October 22, 2013 and Version 1 on February 12, 2014.
  - Created through the collaboration between government and public sectors to strengthen networks and guard against hackers and cybersecurity threats.
  - It outlines ways that companies could protect their networks and act fast if and when they experience security breaches.
  - Adopting this framework would be voluntary for companies.
  - The framework was written with the involvement of roughly 3,000 industry and academic experts.

The NIST Cybersecurity Framework – Three Parts

1. Framework Core
   - Functions
     - Identify
     - Protect
     - Detect
     - Respond
     - Recover
   - Categories
   - Subcategories
   - Informative References

2. Framework Implementation Tiers
   - (1) – Partial, (2) – Risk Informed, (3) – Repeatable, (4) – Adaptive
3. Framework Profiles (Gaps) - The Current vs. Future State

The FCC Cyber Security Planning Guide

- Planning guide for security small-mid size companies to protect their business reputations and customer from cyberthreats.
- Developed with input from private and public sector, including the Department of Homeland Security and the National Cybersecurity Alliance.
- Dictates an action plan, including:

1. Conduct an inventory of data
   - What data do you have?
   - How is the data handled?
   - Who has access to the data and why?
2. Keep record of data and implement controls
3. Create a privacy policy
4. Protect data collect on Internet
5. Create layered network security: access controls, encryption, backups, etc.
6. Plan for data loss or theft

Planning Guide available at:

http://transition.fcc.gov/cyber/cyberplanner.pdf

Cybersecurity - Regulators Expectations

- SEC/OCIE Cybersecurity Examination
  - Established the Cybersecurity Exam on April 15, 2014
  - Will conduct examinations of more than 50 registered broker-dealers and investment advisors, focusing on:
    - Governance
    - Identification and assessment of cybersecurity risks
    - Protection of networks and information
    - Remote customer access and funds transfers
    - Vendors and third parties
    - Detection of unauthorized activity
    - Threat response

Public list of requests and documents listed on OCIE website:
http://www.sec.gov/ocie

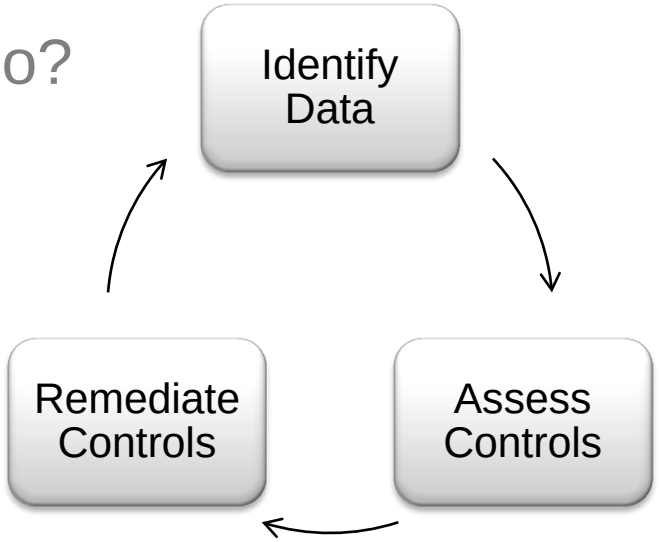
Cybersecurity - Regulators Expectations

- FFIEC
  - Established the Cybersecurity and Critical Infrastructure Working Group in June 2013
  - Created the Cybersecurity Assessment Exam designed for federal and state banking regulators to assess cybersecurity threats and mitigations.
  - Builds upon the FFIEC IT Handbook, to include:
    - Assessing complexity of the institution's IT environment and how it's IT services are managed.
    - Assessing an institution's current and overall cybersecurity preparedness, including:
      - Risk management and oversight
      - Threat intelligence and collaboration
      - Cybersecurity controls
      - External dependency management
      - Cyber incident management and resilience

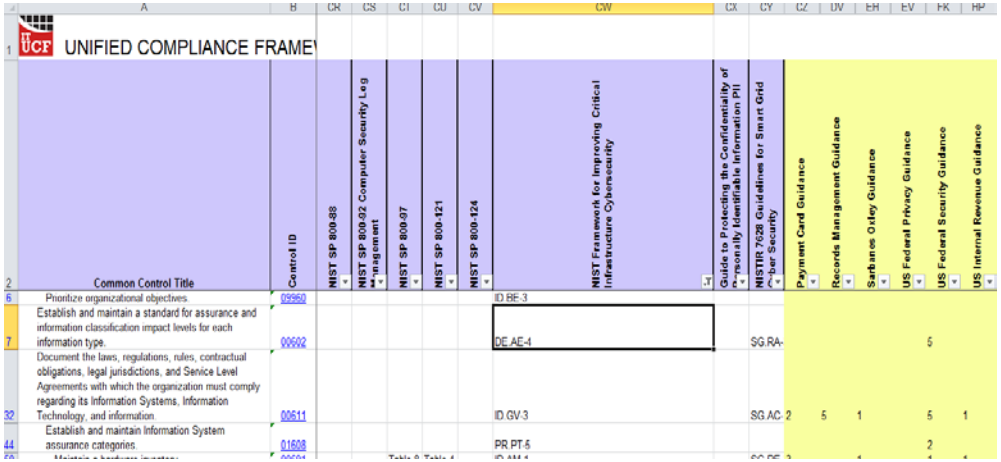
Public notification of the exam is listed on FFIEC website: https://www.ffiec.gov/pdf/cybersecurity/2014_June_FFIEC-Cybersecurity-Assessment-Overview.pdf

This is Overwhelming - What Can I Do?

- All of the frameworks say the same thing:
  1. Know your data
  2. Assess your data controls with a risk assessment
  3. Remediate by implementing security controls
  4. Repeat



- There are so many frameworks and expectations, how do I consolidate everything that applies to me?
- Answer: Unified Controls Framework https://www.unifiedcompliance.com/



Poll Question 3

- When and how did you perform a cybersecurity assessment?

a) Performed a cybersecurity assessment or similar in the past year
b) Performed a cybersecurity assessment but it's been over 1 year
c) Performed a cybersecurity assessment but it's been over 2 years
d) I have not performed any type of cybersecurity assessment
e) Unsure/don't know

Cybersecurity Assessment – A Practical Approach

- Based on input from the Cybersecurity Frameworks and Crowe's experience in helping assess and remediate information security controls, a practical approach to assessing cybersecurity has been designed, which includes the following steps:

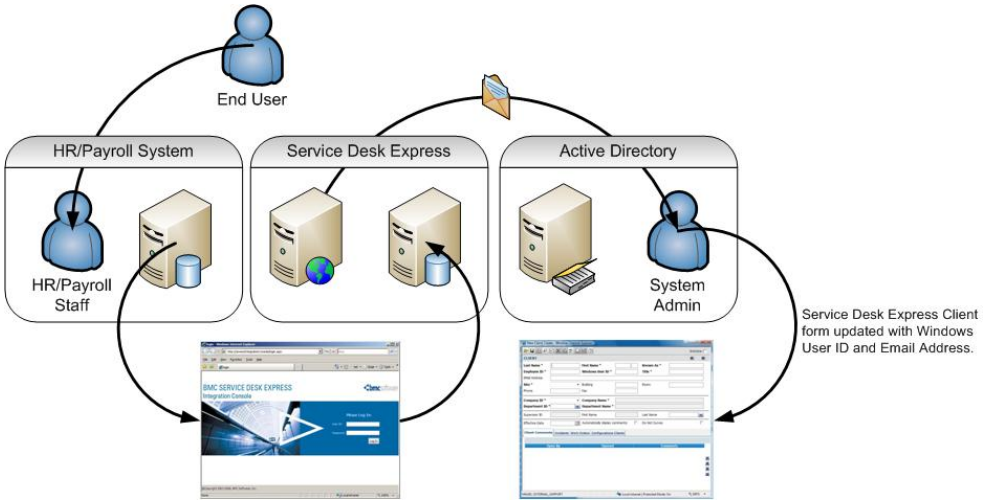
Step 1 - Identify Critical Data

- Criticality data depends on industry:
  - Aerospace and manufacturing = Intellectual Property (IP)
  - Financial services and insurance = Personal Identifiable Information (PII) and Financial Data
  - Healthcare = Protected Health Information (PHI)
  - Retail = Customer and credit card information

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 2 - Map Data Stores and Flows

- Web and application databases
- File shares
- Workstations
- Email
- Mobile devices
- The cloud
- Data replications and backups
- Vendors
- USB devices



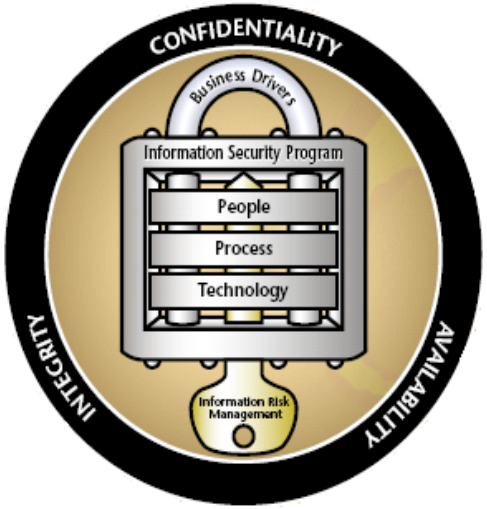
- You can't dream up where your data can end up…

Follow the Data!

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 3 – Perform a Controls Risk Analysis

- Utilizing data stores and data flow maps, identify risks and mitigating controls at the people, process and technology levels.

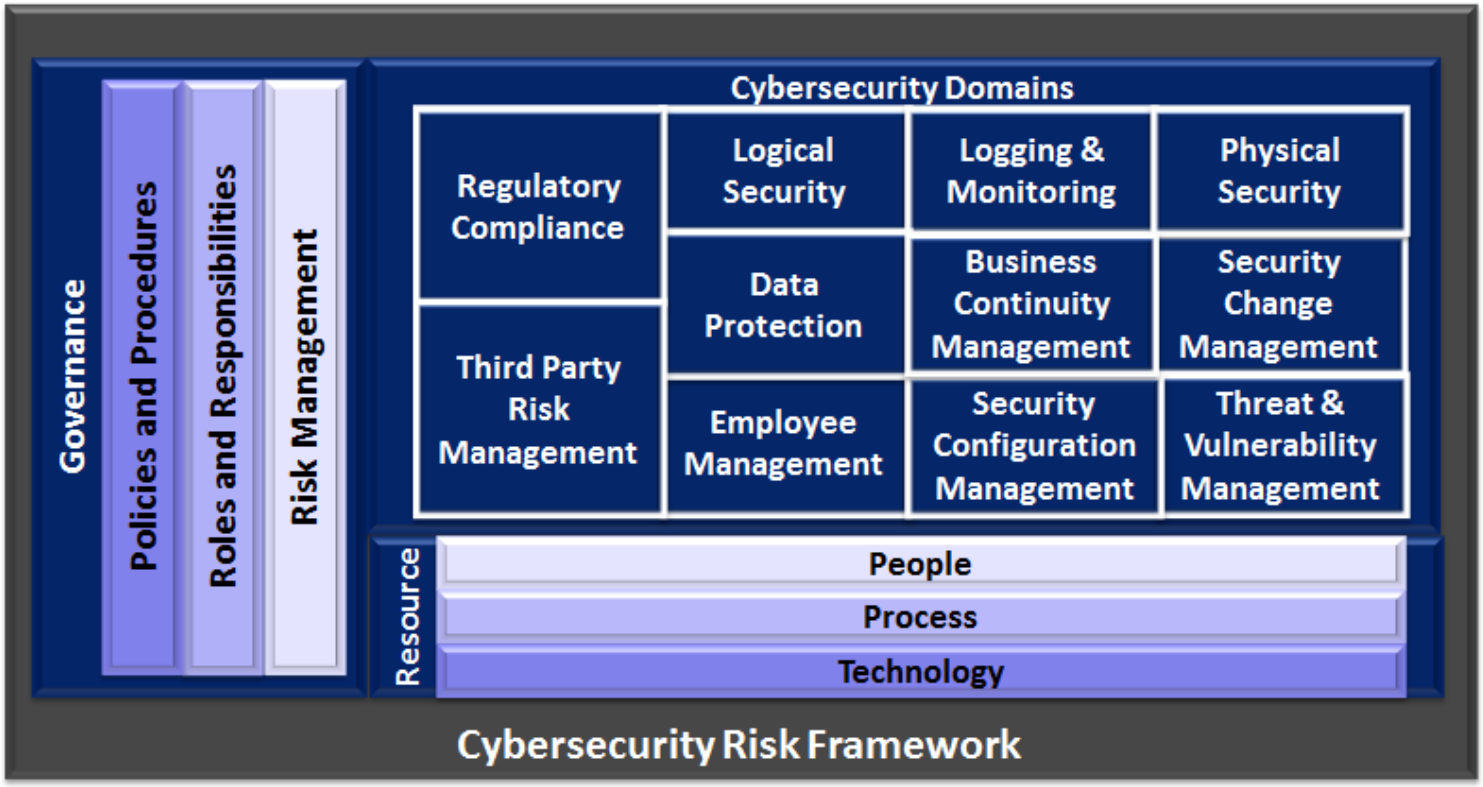


- Risk Examples:
  - **People:** Lack of security awareness by employees could allow for successful social engineering and phishing attacks, leading to the compromise of sensitive information.
  - **Process:** Breakdowns in the vendor management program could result in data being sent to an unsecured vendor that is breached.
  - **Technology:** Exploitable systems, weak passwords, or unsecured applications could allow for unauthorized access to data.

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 4 – Rate Maturity of Security Controls

- Utilize a security domain framework to rate the maturity of the security controls protecting your critical data.



Source: Crowe Cybersecurity Risk Framework

Cybersecurity Assessment – A Practical Approach (cont'd)

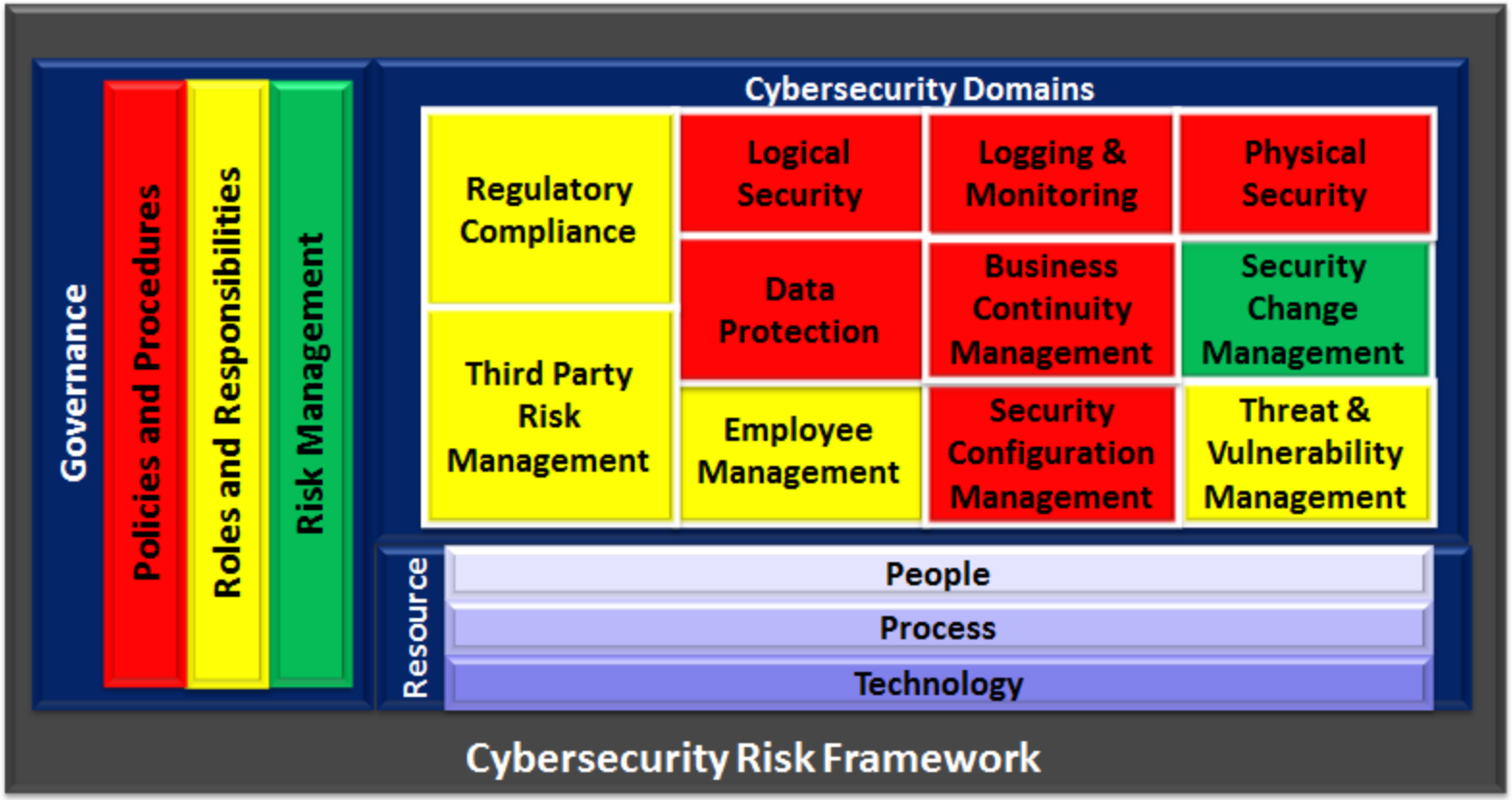
Security Domain	Domain Components
Third Party Risk Management (TPRM)	• Data Sharing Inventory • Security Review - Vendor Selection • Security Review – Ongoing
Regulatory Compliance (RC)	• HIPAA Compliance • ISO 27001 • PCI Compliance • FFIEC Compliance
Data Protection (DP)	• Data Classification • Data Inventory • Data Protection Controls Framework • Encryption • Data Destruction • Incident Response
Logical Security (LS)	• Authentication • Access Management (User Requests and Terminations) • User Access Reviews • Segregation of Duties
Employee Management (EM)	• Hiring Practices • Security Training • Employee Policies and Standards
Logging and Monitoring (LM)	• Application / Database • Server • Network / Wireless

Security Domain	Domain Components
Business Continuity Management / Disaster Recovery (BCM)	• Contingency Plans • Critical IT Systems Redundancy • Disaster Planning • Backup Processes
Security Configuration Management (SCoM)	• Server • Database • Mobile Security • Network Systems • System Certification
Physical Security (PS)	• Documentation Storage and Security • Clean Desk Policy • Data Center Physical Security
Security Change Management (SChM)	• Change Management • System Development Lifecycle • Security Integration • Application Risk Profiling • Security Testing • Secure Coding Practices
Threat & Vulnerability Management (TVM)	• Anti-virus Standards • Patch Management • Vulnerability Management Programs

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 4 – Rate Maturity of Security Controls

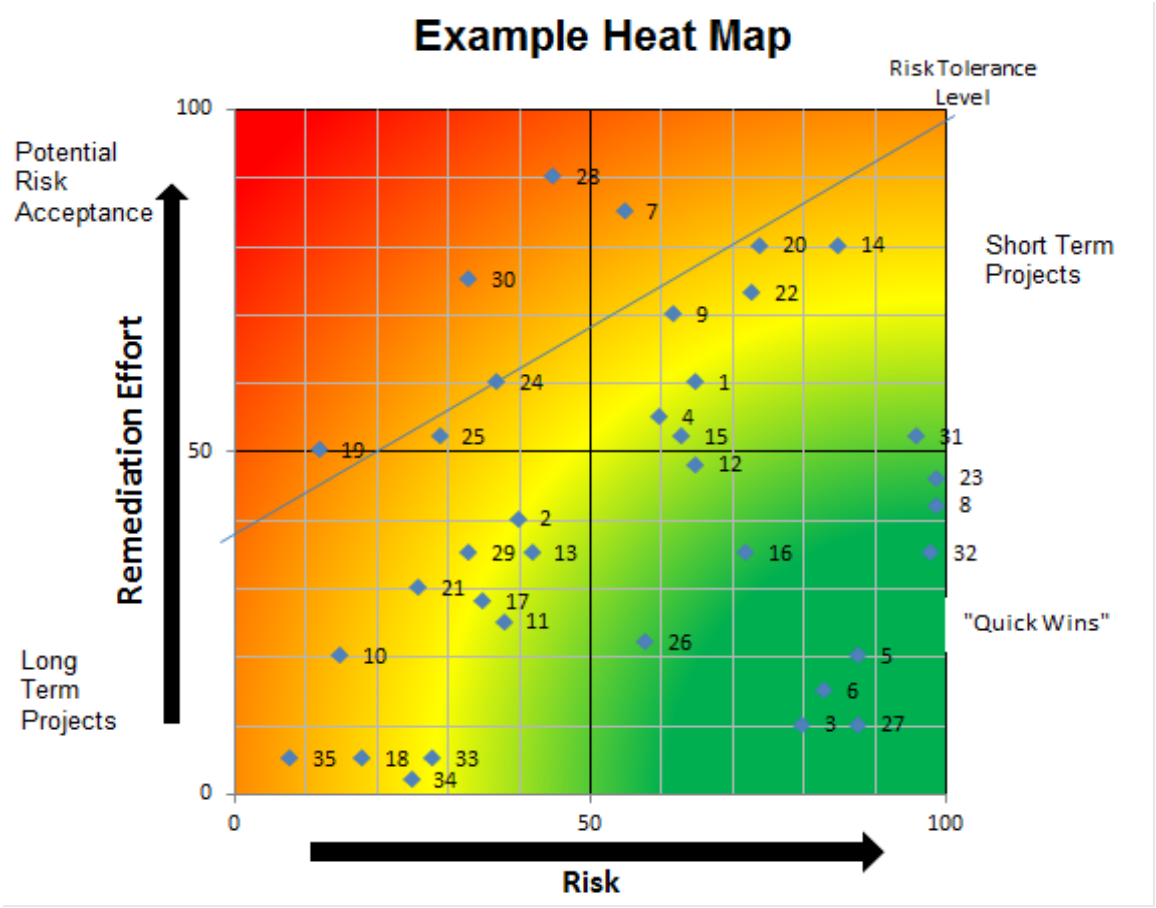
- Identify the "blind spots" in your cybersecurity program



Source: Crowe Cybersecurity Risk Framework

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 5 – Build a Short and Long Term Remediation Plan



Source: Example IT Risk Mediation Heat Map

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 5 – Build a Short and Long Term Remediation Plan (Example Roadmap)

Gap Analysis Category	Timeframe						
	Immediate	3 Months	6 Months	9 Months	12 Months	18 Months	24 Months
Legal and Compliance	Leverage legal counsel to review: ▪ Call recording practices at ABC ▪ Legal and Privacy Statements on the ABC website		Establish an audit/assessment schedule for ABC's Information Security Program				Evaluate PCI requirements; document results
Business Continuity Management			Perform a Business Impact Analysis (BIA) to drive the creation of a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP.				
Risk Management			Formalize a IT Risk Management function for ABC				
Vendor Management	Update GLBA vendor risk assessment document				Establish scheduled and periodic reviews of vendor management risk assessment		
Remote Locations			Establish a schedule to audit all remote location physical security and practices		Commence physical security and practice audit of all remote locations (to occur over time per the audit schedule)		
Training Program				Re-evaluate the current information security training	Re-establish training program for data security practices and information security policies and procedures	Evaluate policies, processes, and procedures for consistent data security practices	Re-evaluate revised training program effectiveness
Policies and Procedures				Revisit the data protection policies per the detailed observation section: Retention Policy, Data Classification Policy, and Incident Response Plan; incorporate into revised training program			
Mobile Device/Media Security					Evaluate laptop encryption solution and identify true, full disk encryption solution for use at ABC	Evaluate use of mobile devices and mobile media at ABC and identify appropriate mobile device management solution	Deploy mobile device and media security controls

Poll Question 4

- Has your board asked management about cybersecurity?

a) Several times
b) Once
c) No, but I suspect they will soon
d) No, and I doubt they ever will
e) Unsure/don't know

Cybersecurity - A Boardroom Conversation

- A recent article in Compliance Week quoted results from a survey of board members. What areas do Audit Committees feel uncomfortable asking specific questions:
  - IT Risks – especially emerging technologies
  - IT Projects – gone awry
  - **Data security**

Cybersecurity - A Boardroom Conversation

- According to a board survey conducted by IT Governance Ltd. Published in Boardroom Cyber Watch US – 2014 had the following findings to report:
  - Complacent about cyber risks
  - Breaches can go undetected
  - IT function and the board don't communicate
  - Lack of knowledge of cybersecurity at the board level
  - **Cyber resilience** is top of mind
  - Customer demand for assurance

Cybersecurity - A Boardroom Conversation

- Personal Experience
  - 50% of the boards asked about standards such as
    - NIST
    - ISO
  - Another common theme
    - How do we know we are not the next “Target”?

Questions?

For more information, contact:

Raj Chaudhary
312.899.7008
raj.chaudhary@crowehorwath.com

Jared Hamilton
317.706.2724
jared.hamilton@crowehorwath.com
@ITSecurityJared