Crowe Horwath.

The Unique Alternative to the Big Four®

Crowe Cybersecurity Services

Cybersecurity Risk Management

How You Can Respond Now

Audit | Tax | Advisory | Risk | Performance

Today's Presenters

Raj Chaudhary
CGEIT, CRISC, P.E.
Principal - Technology Risk
Cybersecurity Services Practice Leader
@chaudhary_raj54

Jared Hamilton
CISSP, CCSK, MCSE
Sr. Manager - Technology Risk
Cybersecurity and Cloud Computing Solution Leader
@ITSecurityJared

Agenda and Learning Objectives

- Acknowledge latest breaches and attack vectors
- Identify top cybersecurity trends
- Recognize foundational response steps
- Utilize a practical approach for assessing cybersecurity risks
- Prepare a cybersecurity breach prevention and response program

Constantly Changing Threat Landscape

Source: Cyber Security Consulting: Kennedy Consulting Research & Advisory

Top 2015 Breaches (So far…)

- Anthem (80 Million)
- Premera Blue Cross (11 Million)
- Office of Personnel Management (4 Million)
- CareFirst BlueCross BlueShield (1.1 Million)
- Auburn University (364,012)
- Beacon Health System (220,000)

- Government
- Healthcare Providers and Insurers
- Higher Education
- Business
  - Software Companies
  - Retail
  - Major League Baseball Team

Totals for Category:	Banking/Credit/Financial	# of Breaches: 32	# of Records:	408,377
		% of Breaches: 8.9%	%of Records:	0.4%
Totals for Category:	Business	# of Breaches: 145	# of Records:	121,307
		% of Breaches: 40.2	%of Records:	0.1%
Totals for Category:	Educational	# of Breaches: 31	# of Records:	724,318
		% of Breaches: 8.6%	%of Records:	0.7%
Totals for Category:	Government/Military	# of Breaches: 26	# of Records:	5,334,457
		% of Breaches: 7.2%	%of Records:	5.0%
Totals for Category:	Medical/Healthcare	# of Breaches: 127	# of Records:	100,792,898
		% of Breaches: 35.2	%of Records:	93.9%
Totals for All Categories:		# of Breaches: 361	# of Records:	107,381,357
		% of Breaches: 100.0	%of Records:	100.0%

2015 Breaches Identified by the ITRC as of:	6/16/2015

Total Breaches:	361
Records Exposed:	107,381,357

Source: http://www.idtheftcenter.org/

Poll Question #1

Have you had a breach within the past year?

a) Definitely not
b) Yes
c) More then one
d) The company would not know if we did
e) Unsure/don't know/would rather not say

Common Threat and Response – The Death of Passwords

- Threats:
  - Phishing and spear phishing
  - Personal verses business email
  - Reset processes
  - Unnecessary accounts
    - Test accounts
    - Temp accounts
  - Weak Passwords
    - Blank
    - “Joe” password
    - (username = password)
    - Guessable (Summer2015)
  - Password Sharing
    - Temp1
    - Intern1

- Threat Responses:
  - Multi-factor authentication
  - Personal computing restrictions
  - Network segmentation
  - Password management systems

Common Threats and Response – Unknown Data Stores

- Threats:
  - Lost or misplaced data
  - Unknown secondary and tertiary data stores
    - Third-party vendors
    - Cloud computing storage
  - Oversharing of data
  - Keep unnecessary sensitive data

- Threat Responses:
  - Data classification system
  - Data custodians
  - Digital rights management
  - E-discovery
  - Cloud access security brokers

Common Threats and Response – Lack of IT Asset Management

- Threats:
  - Vulnerable software
  - Misconfigured end points
    - Encryption
    - User configuration policies
    - Logging and monitoring
  - Bots and breach “pivot points”

- Threat Responses:
  - Asset management systems
  - Onboading / offboarding procedures
  - Procurement procedures
  - Inventory network scanning

Common Threats and Response – Ransomware

- Threats:
  - Lost data
  - Business interruption
  - Financial loss

- Threat Responses:
  - Vulnerability management
  - Content filters and malware protection
  - Security awareness training
  - System hardening
  - Data backups
  - Business continuity and disaster recovery plans
  - Cybersecurity insurance

Common Threats and Response – Lack of Available IT Security Resources

- Threats:
  - Lack of information security program
  - Missing or weak security controls
  - Untested controls
  - Security of low priority
  - Security program misaligned with the business
  - Uninformed boards

- Threat Responses:
  - Dedication and training of current staff
  - Recruitment with head hunter
  - Outsourced IT security
  - Staff augmentation
  - Managed security service providers

U.S. employers posted 50,000 jobs requesting CISSP credentials in 2013, a year in which the population of CISSP holders numbered 60,000.

Source: http://www.burning-glass.com/research/cybersecurity/

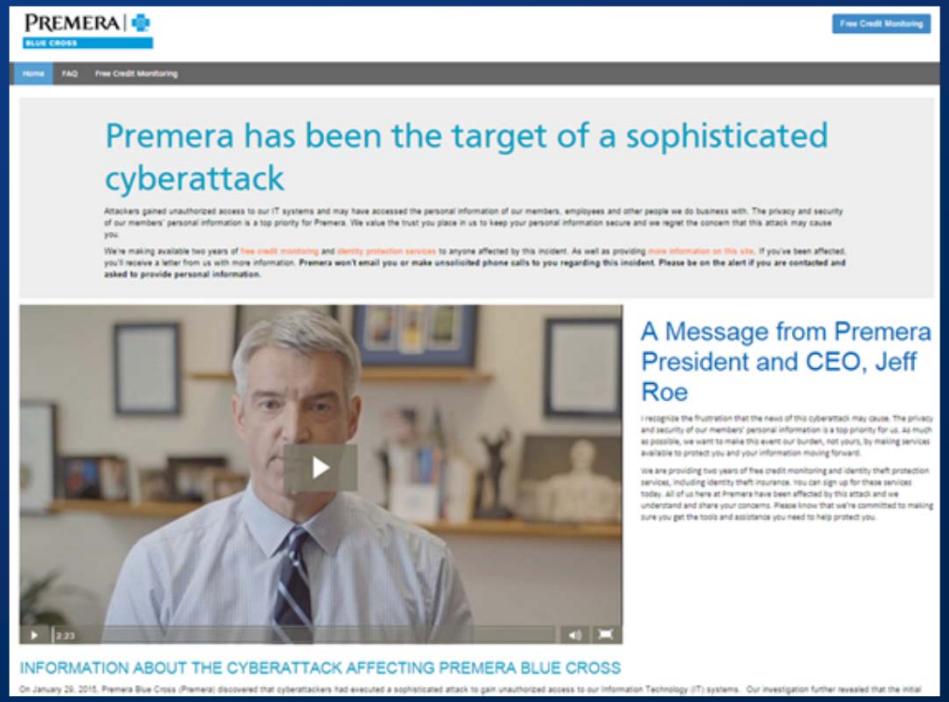
Trends in Cybersecurity – “The Internet of Things”

- Everything has an IP
  - HVAC
  - Cars
  - Garage door opener
  - Refrigerator
  - Webcams
  - Washers
  - Hot tubs
  - Light bulbs

Be Prepared – Incident Response Planning

- 34% of organizations lack a formal and documented incident response plan
- 23% have not reviewed or updated their plan since it was created or within past 5 years

- What will I do?
- What are the laws?
- What will my regulator say?
- How much will my customers ask?
- Who will I call?
- How do I stop it?



Source: http://www.securityweek.com/incident-response-plans-lacking-many-organizations-survey

Successful Organizations

- May suffer a breach…and may show up in headlines
- Operate through the breach without disruption to the business
- Don't have changing stories
- Can demonstrably prove diligence in responding to an attack
- Can articulate why they failed
- Don't take 200+ days to find an attack
- Don't wait for others to tell them about an attack
- Don't let others control the disclosure

Poll Question #2

Does your company have a cyber-incident response plan?

a) Yes
b) No
c) Unsure / don't know

Cybersecurity Assessment

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

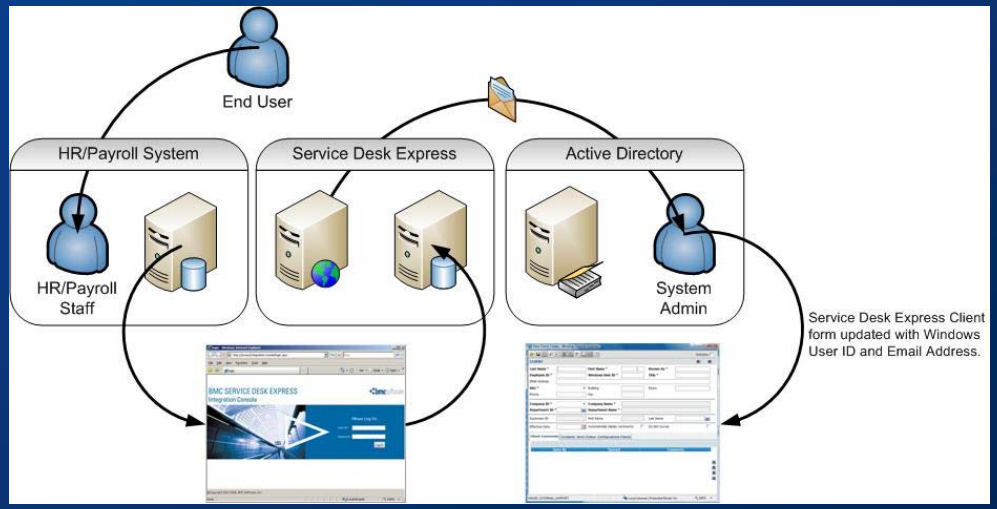
Step 1 - Identify Critical Data

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

Cybersecurity Assessment – A Practical Approach (cont'd)

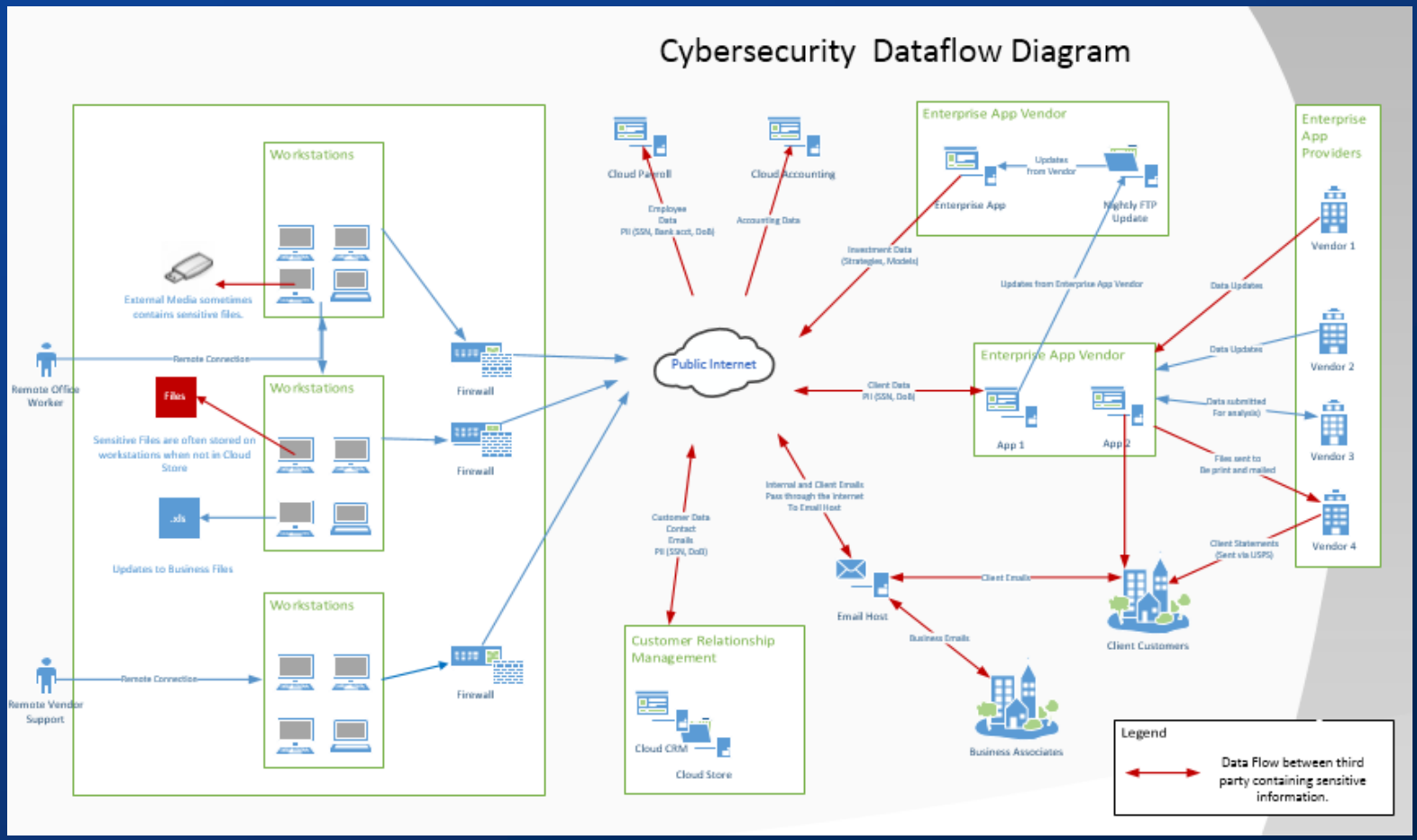
Step 2 - Map Data Stores and Flows

- 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, companies should identify risks and mitigate 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)

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

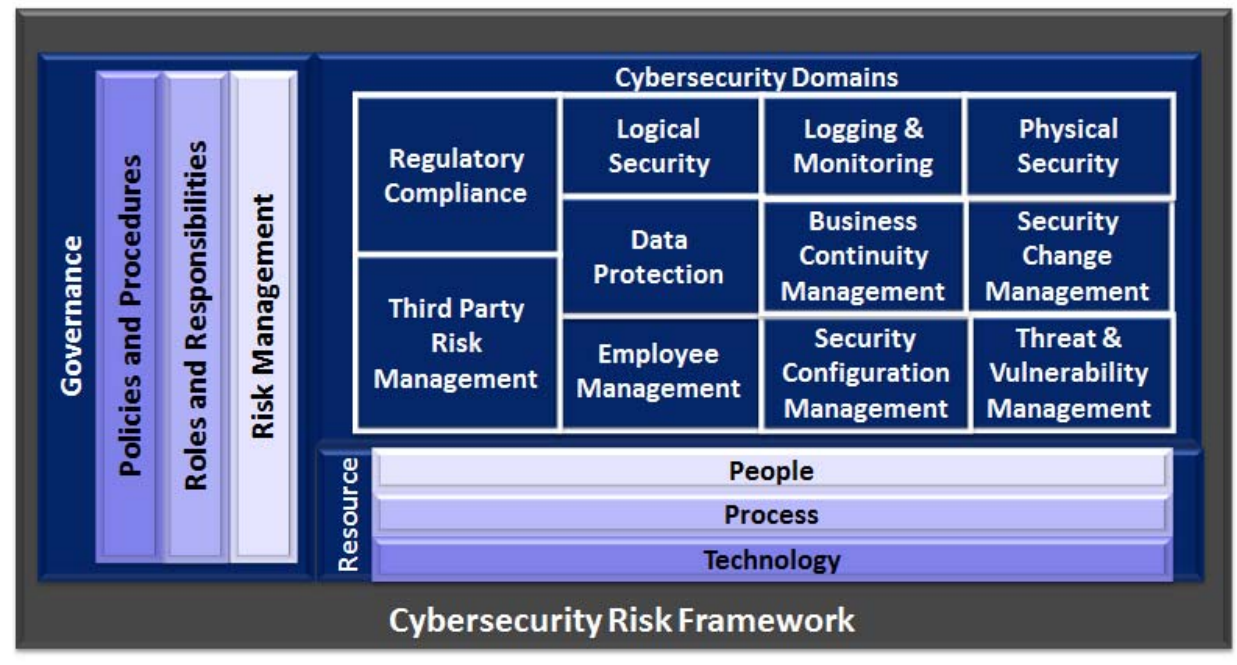
Undertake Some Basic Testing – Find your Weaknesses

- External Penetration
  - Technical services review
  - Web applications
  - Stealth penetration
  - Remote social engineering
    - Email/telephone/social media
- Internal Penetration Test
  - Onsite social engineering/physical security review/USB drop
  - Remote option with Pwnie Exress PwnPlug
- Advanced Persistent Threat (APT) prevention / Data Loss Prevention (DLP)
  - What channels can we utilize to get data out? Can it be detected?
- Wireless Testing

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.

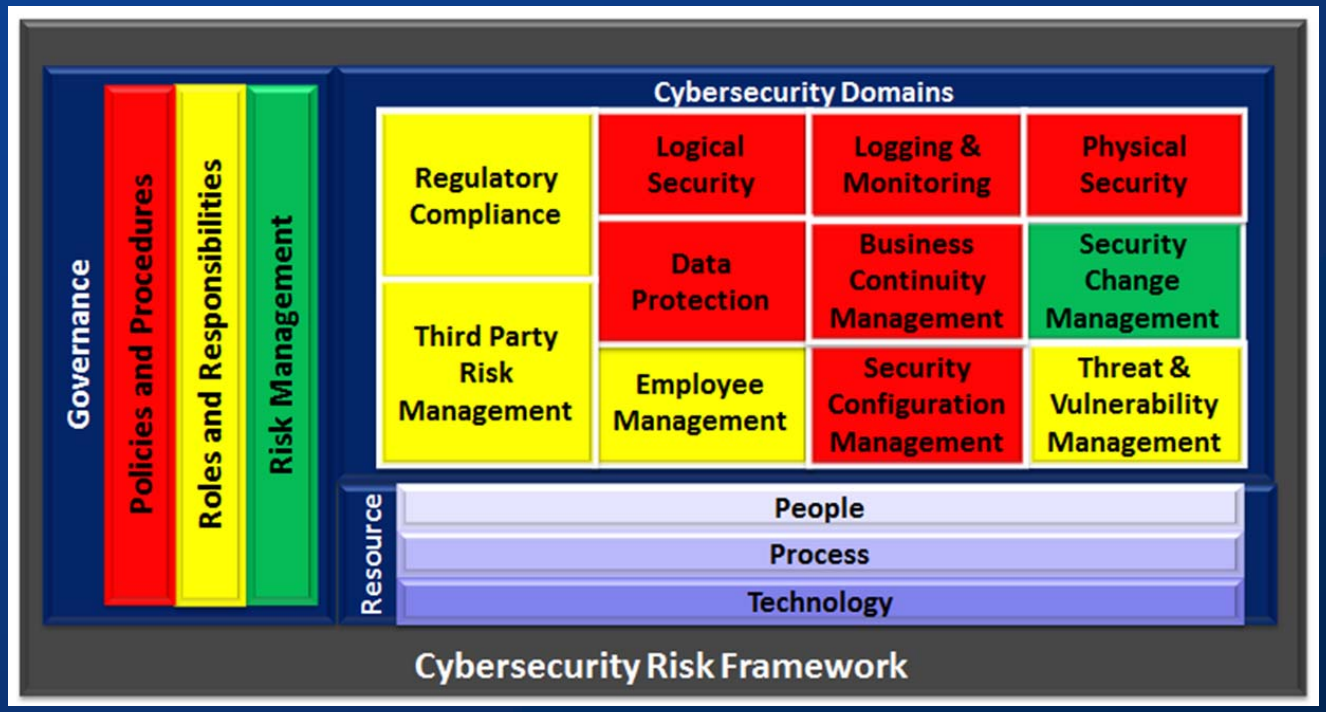


Source: Crowe Cybersecurity Risk Framework

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 4 – Rate Maturity of Security Controls

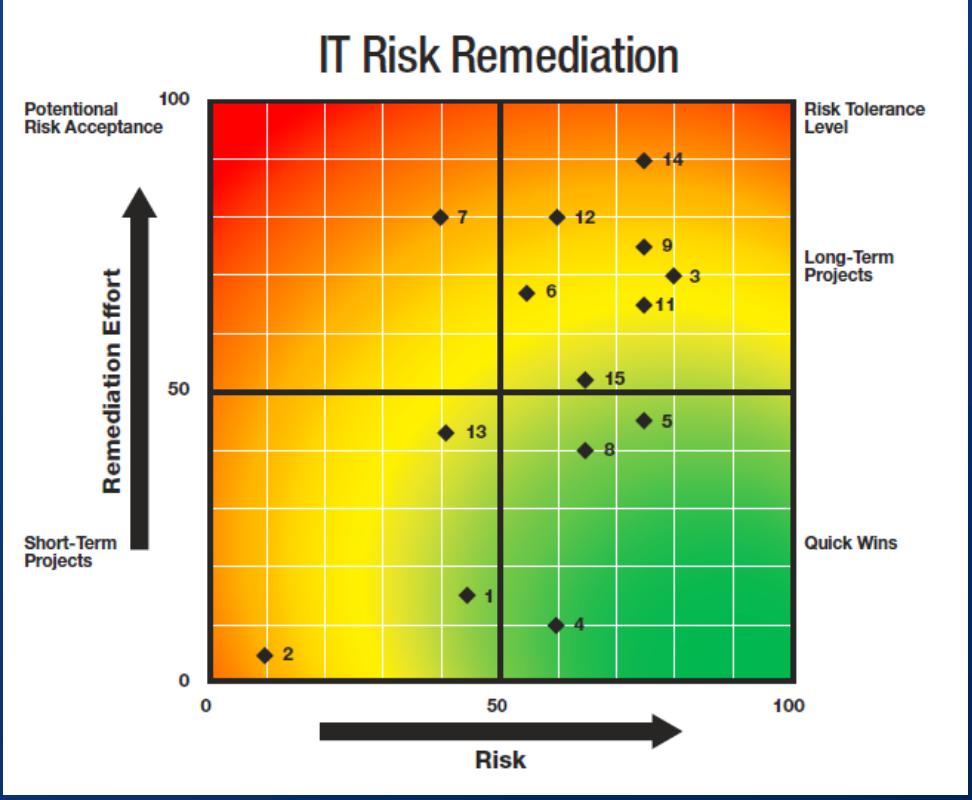
- Identify the "blind spots" in your cybersecurity program



Source: Crowe Cybersecurity Risk Framework

Cybersecurity Assessment – A Practical Approach (cont'd)

Step 5 – Build a Short and Long-Term Remediation Plan



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 #3

When have you performed a cybersecurity assessment?

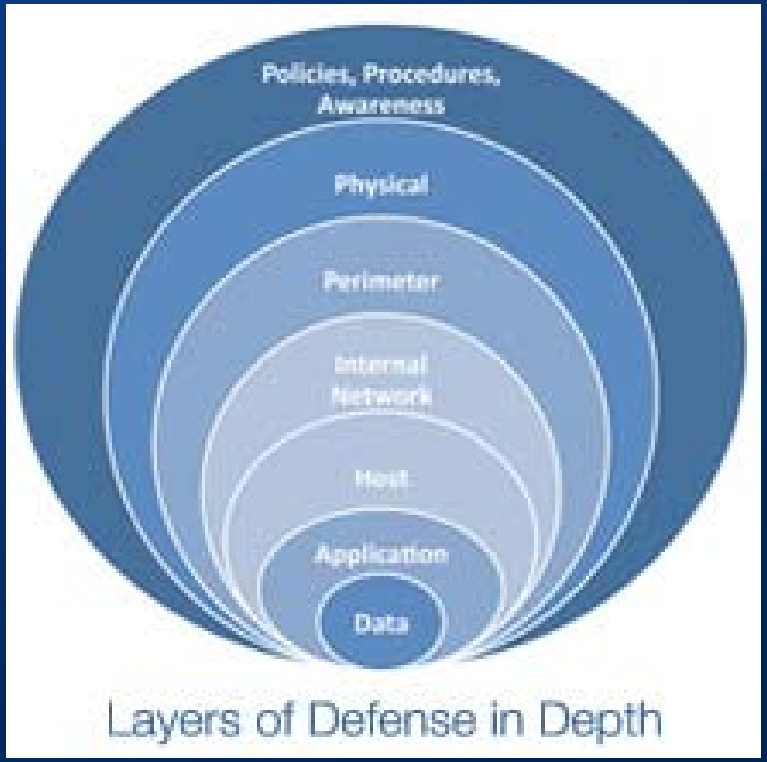
a) Performed a cybersecurity assessment or similar in the past 12 months
b) Performed a cybersecurity assessment but it has been over a year
c) We have not performed any type of cybersecurity assessment
d) We have performed security assessments, but not specific to cybersecurity
e) Unsure / don't know

There is No “Fix”

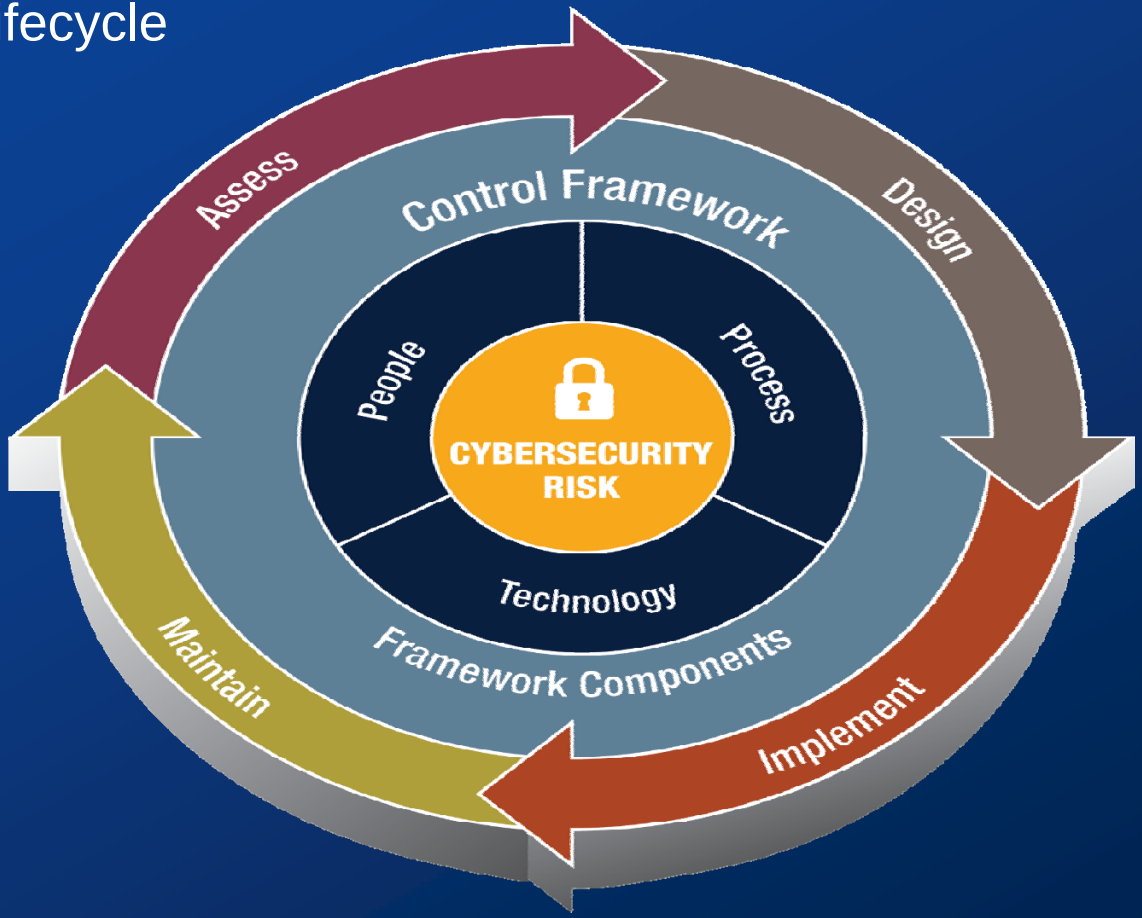
Defense-in-Depth

Layers of Security / Defense

- Sensitive Data
- Applications
- Host/Operating system
  - HIPS, anti-virus, Windows firewall
- Internal network
  - VLANs, internal firewalls
- Physical / building security
  - Access controls, cameras
- Network perimeter / edge
  - IDS/IPS, firewalls, content filtering, etc.
- Policies, procedures, and awareness



The Security Lifecycle



Poll Question #4

Has your board asked management about cybersecurity?

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

Key Takeaways

- Compliance does not equal security
- Do you have an information security program?
  - Has it been tested?
- Do you know where all of your data is stored?
  - How confident are you?
- How strong are your detective controls?
  - If you had a breach, would you know?
- Identify your current state of cybersecurity risk
  - Plan for the future and be “prepared”

For more information, contact:

Raj Chaudhary
Direct 312.899.7008
raj.chaudhary@crowehorwath.com
@chaudhary_raj54

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

Material Creation: June 22, 2015