Crowe Horwath.

Smart decisions. Lasting value.™

Healthcare’s 2017 Cybersecurity Challenge:

How You Can Respond

May 9, 2017

Jared Hamilton, CISSP
Healthcare Cybersecurity Solutions Leader
Crowe Horwath LLP

Today's Presenter

Jared Hamilton, CISSP

Senior Manager

Crowe Horwath

Healthcare Cybersecurity Solutions Leader

+1 317 706 2724

jared.hamilton@crowehorwath.com

The information provided herein is educational in nature and is based on authorities that are subject to change.

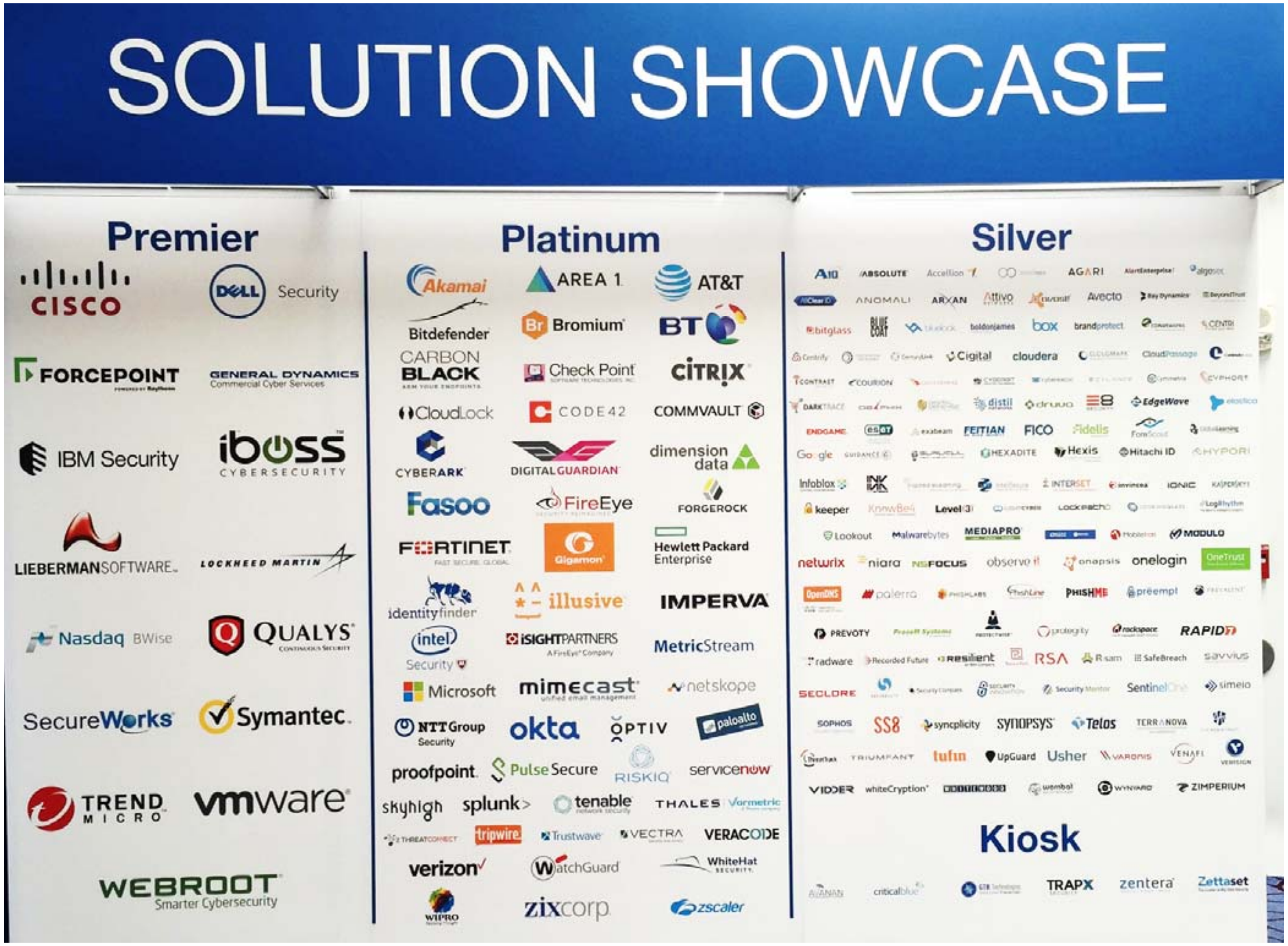
Agenda

- Cybersecurity Defined
- Top Healthcare Threats and Responses
- Compliance vs. Security
- Take Action
- Questions and Answers

The IT Security World in 1998

The IT Security World in 2017

Confusion in the Marketplace



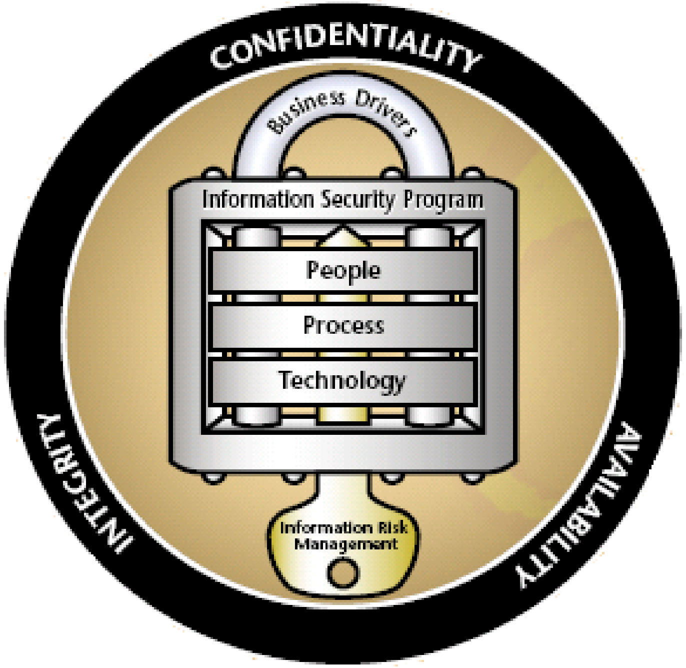
What is Cybersecurity?

- NIST – “The ability to protect or defend the use of cyberspace from cyber-attacks “

- “The Triad of Security – CIA of “CRITICAL DATA”
  - Confidentiality
  - Integrity
  - Availability

- Who does it impact?
  - Anyone, an individual or organization, connected to the Internet

- Defense requires 3 types of controls:
  - People
  - Process
  - Technology



Richard Kissel, Ed., Glossary of Key Information Security Terms, NIST, US Dep’t Com., http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Cybersecurity Trends

- Who is attacking me?

  ~ 80% of all breaches are due to external actors

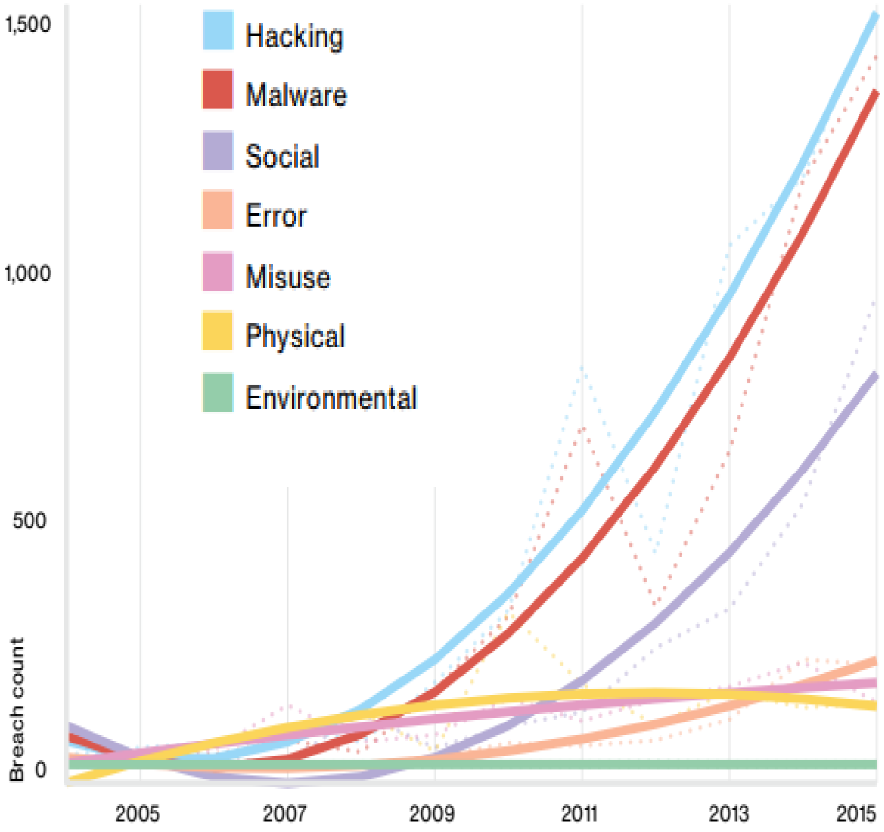
  ~ 20% from insider actors

- Why?

  ~ 80% for financial gain

  ~ 15% espionage

  ~ 5% all others – (ideological, grudge, fun)

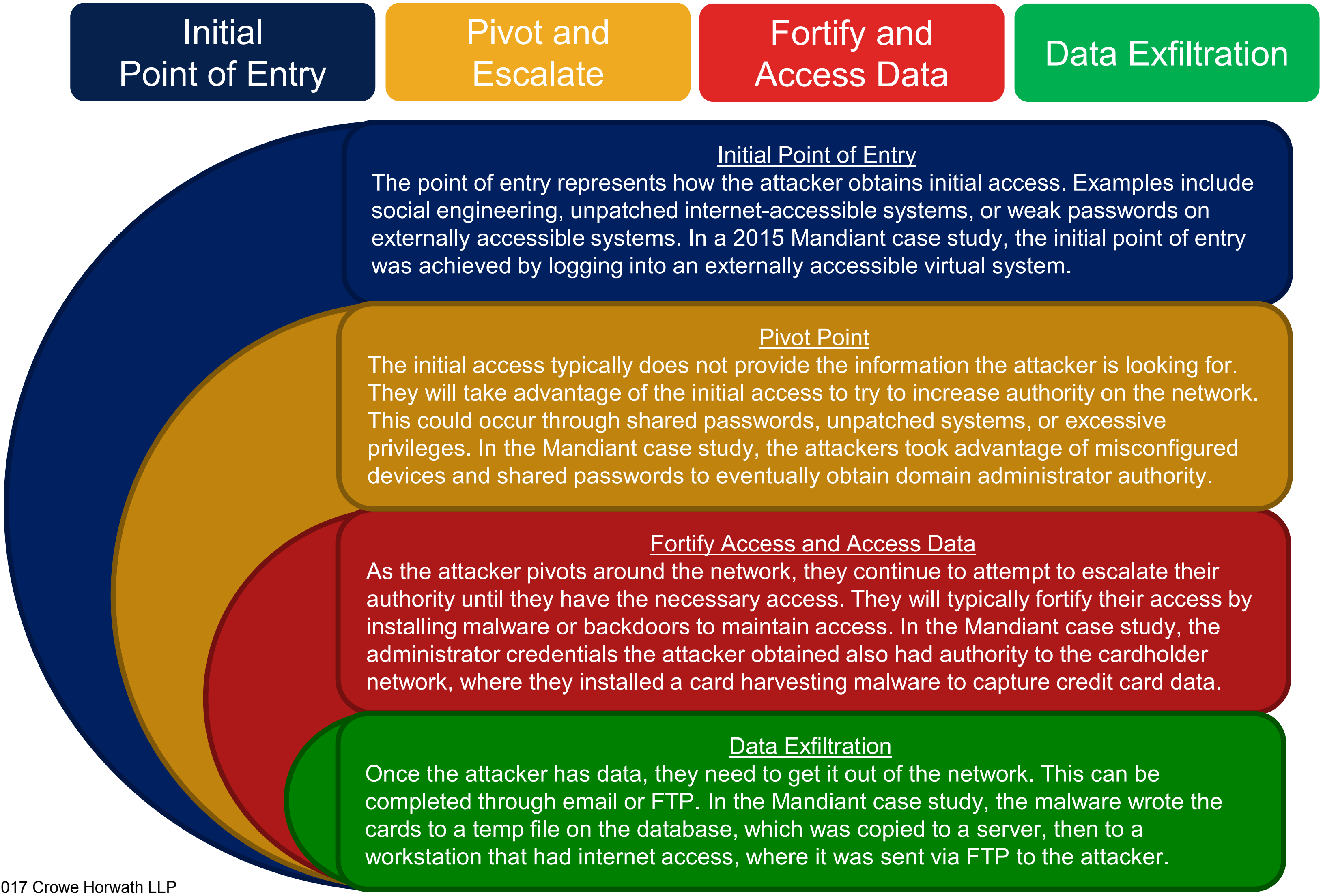


Source: Verizon 2016 Data Breach Investigations Report (DBIR), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Figure 4.

Number of breaches per threat action category over time, (n=9,009)

How Do Breaches Happen?



Initial Point of Entry

Pivot and Escalate

Fortify and Access Data

Data Exfiltration

Initial Point of Entry

The point of entry represents how the attacker obtains initial access. Examples include social engineering, unpatched internet-accessible systems, or weak passwords on externally accessible systems. In a 2015 Mandiant case study, the initial point of entry was achieved by logging into an externally accessible virtual system.

Pivot Point

The initial access typically does not provide the information the attacker is looking for. They will take advantage of the initial access to try to increase authority on the network. This could occur through shared passwords, unpatched systems, or excessive privileges. In the Mandiant case study, the attackers took advantage of misconfigured devices and shared passwords to eventually obtain domain administrator authority.

Fortify Access and Access Data

As the attacker pivots around the network, they continue to attempt to escalate their authority until they have the necessary access. They will typically fortify their access by installing malware or backdoors to maintain access. In the Mandiant case study, the administrator credentials the attacker obtained also had authority to the cardholder network, where they installed a card harvesting malware to capture credit card data.

Data Exfiltration

Once the attacker has data, they need to get it out of the network. This can be completed through email or FTP. In the Mandiant case study, the malware wrote the cards to a temp file on the database, which was copied to a server, then to a workstation that had internet access, where it was sent via FTP to the attacker.

Source: “M-Trends 2015: A View From the Front Lines,” Mandiant, 2015, https://www2.fireeye.com/WEB-2015RPTM-Trends.html

Threat Actors

HACKTIVISM
CRIME
INSIDER
ESPIONAGE
TERRORISM
WARFARE

Polling Question #1

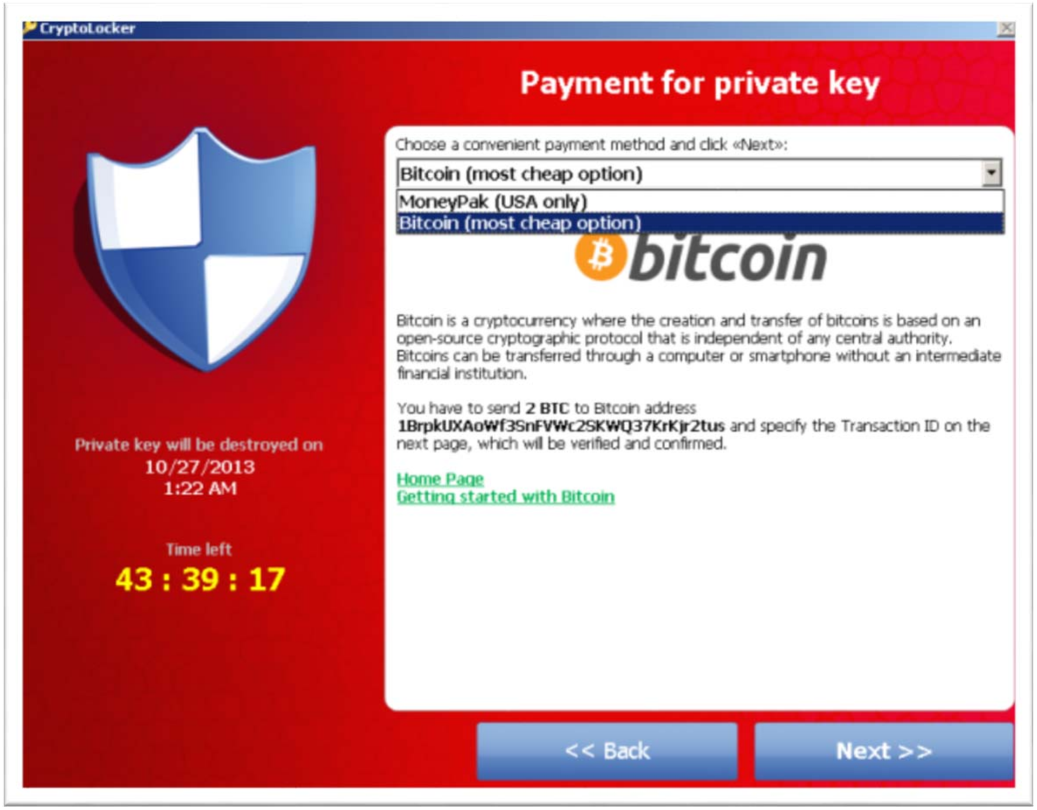
If your organization was hacked / breached, would you know it?

A. Yes, we would definitely know it
B. We would mostly likely identify it
C. If it was a non-sophisticated attack we would be able to recognize it
D. I have no idea!

#1 Top Healthcare Cyber Threat – Ransomware

- Threats:
  - Lost data
  - ePHI compromise
  - Service 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



Payment for private key

Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 39 : 17

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

MoneyPak (USA only)
Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

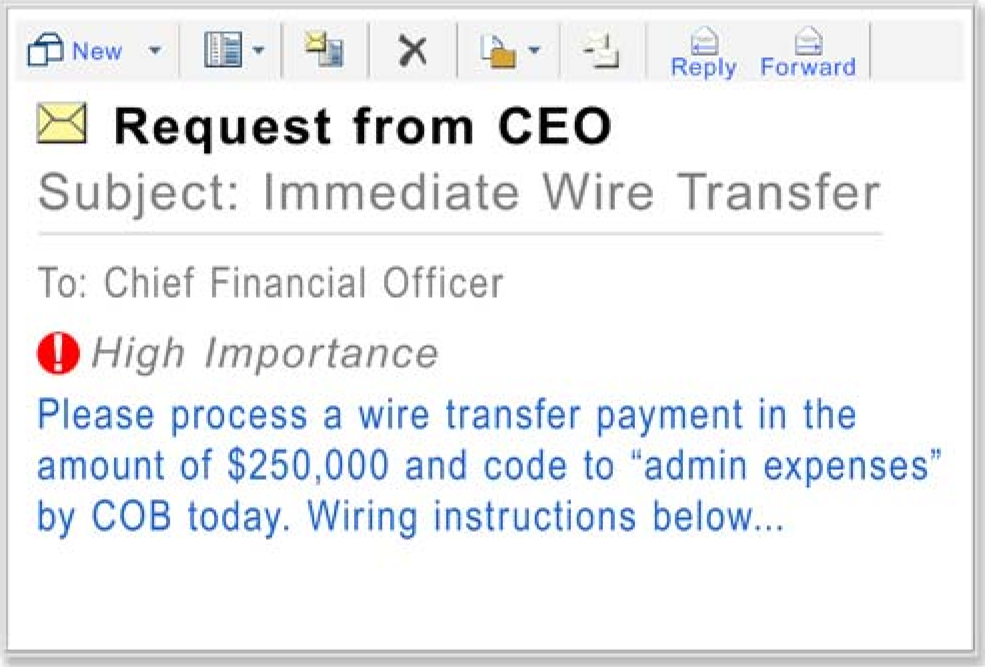
You have to send **2 BTC** to Bitcoin address **1BrpkUXAoWf3SnFVWc2SKWQ37KrKjr2tus** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

#2 Top Healthcare Cyber Threat – Phishing

- Threats:
  - Financial loss
  - PII/PHI Loss

- Threat Responses:
  - Email filtering
  - Limit social media
  - Security awareness training
  - Incident response plans
  - Cybersecurity insurance



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

The 3.1 Billion Dollar Scam
14,032 U.S. Victims

https://www.ic3.gov/media/2016/160614.aspx

#3 Top Healthcare Cyber Threat – Third Party Vendors

- Threats:
  - Lost data
  - Business interruption
  - Reputational loss
  - Compliance fines

- Threat Responses:
  - Vendor management
  - Security reviews
  - Business Associate Agreements
  - Cybersecurity insurance

#4 Top Healthcare Cyber Threat – BioMedical Devices

- Threats:
  - Lost ePHI
  - Service Interruption
  - Spread of Malware

- Threat Responses:
  - Inventorying
  - Vulnerability Analysis
  - Network Segmentation

#5 Top Healthcare Cyber Threat – Lack of Expertise

- Threats:
  - Insufficient Controls
  - Undetected Breaches
  - Compliance Gaps
  - Inability to Stay Current

- Threat Responses:
  - Internal Promotion & Training
  - Headhunter ($$$)
  - Virtual Information Security Officer

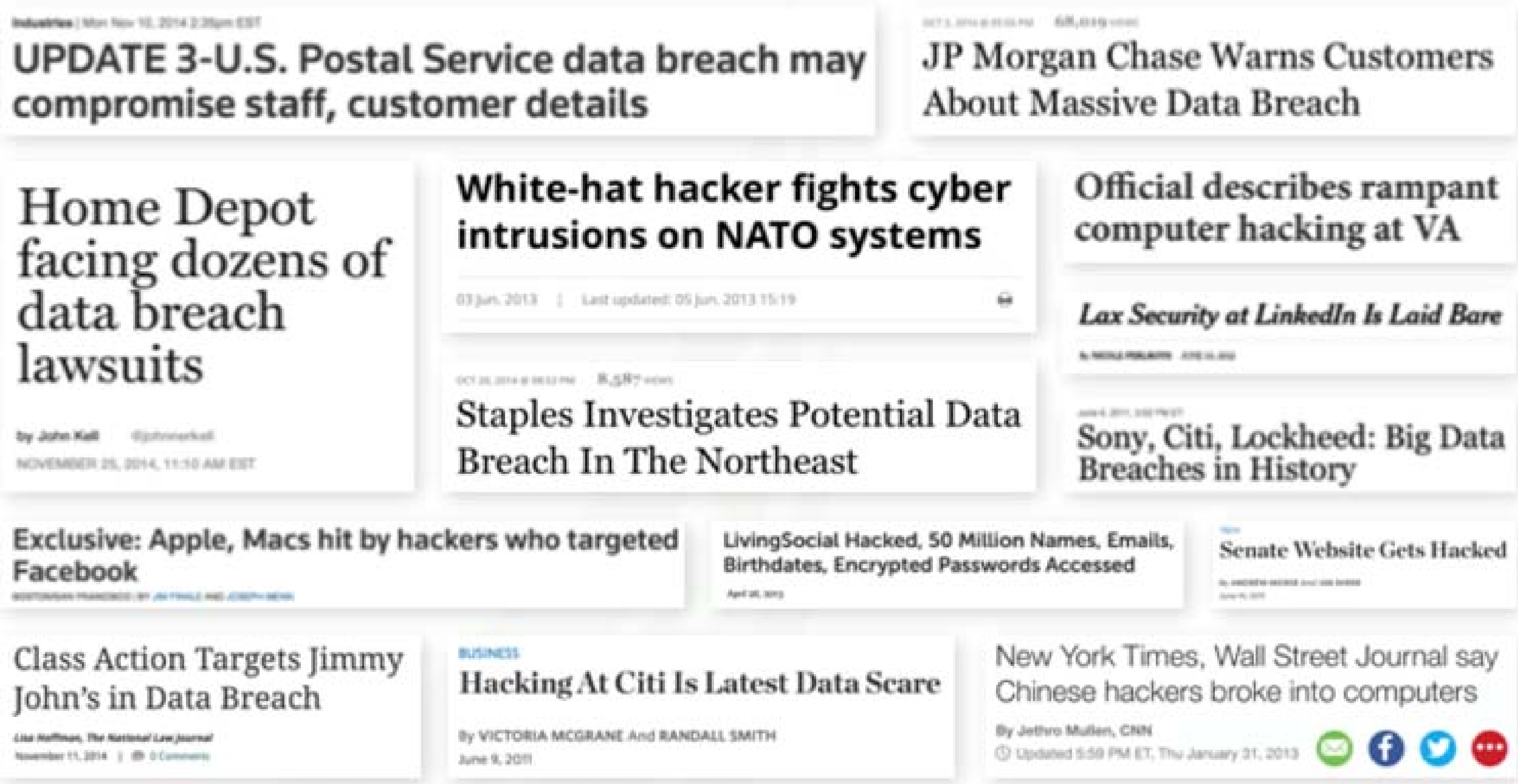
Polling Question #2

Who is in charge of your cybersecurity program?

A. We have a CISO / Security Officer and Security Team
B. It’s a shared responsibility in IT
C. We contract / outsource our security program
D. Nobody

Compliance

Compliance



Industries | Mon Nov 10, 2014 2:26pm EST

UPDATE 3-U.S. Postal Service data breach may compromise staff, customer details

[illegible] 68,019 views

JP Morgan Chase Warns Customers About Massive Data Breach

Home Depot facing dozens of data breach lawsuits

by John Kell @johnmarkell

NOVEMBER 25, 2014, 11:10 AM EST

White-hat hacker fights cyber intrusions on NATO systems

03 Jun. 2013 | Last updated: 05 Jun. 2013 15:19

[illegible] 8,587 views

Staples Investigates Potential Data Breach In The Northeast

Official describes rampant computer hacking at VA

Lax Security at LinkedIn Is Laid Bare

[illegible]

[illegible]

Sony, Citi, Lockheed: Big Data Breaches in History

Exclusive: Apple, Macs hit by hackers who targeted Facebook

[illegible]

LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed

April 26, 2013

Senate Website Gets Hacked

[illegible]

Class Action Targets Jimmy John's in Data Breach

Lisa Hoffman, The National Law Journal

November 11, 2014 | 0 Comments

BUSINESS

Hacking At Citi Is Latest Data Scare

By VICTORIA MCGRANE And RANDALL SMITH

June 9, 2011

New York Times, Wall Street Journal say Chinese hackers broke into computers

By Jethro Mullen, CNN

Updated 5:59 PM ET, Thu January 31, 2013

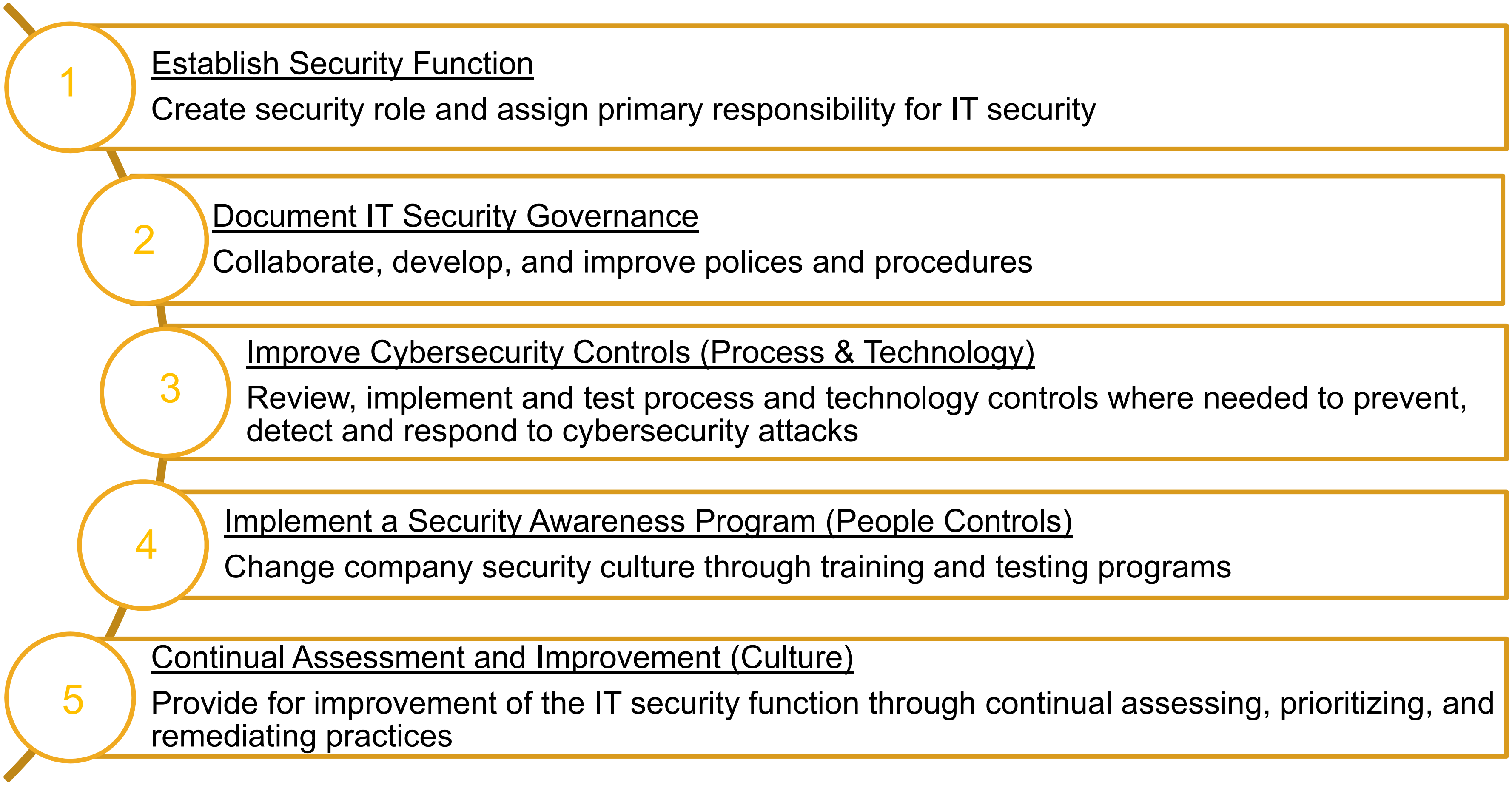
Cybersecurity Strategy

Who’s In Charge?

- Who is leading the initiative?
- Is everything on the same page?
- What is our top priority?
- Would we know if we were hacked?
- Who would respond?
- What does your board think?

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

Cybersecurity Program Implementation



1. Establish Security Function

   Create security role and assign primary responsibility for IT security

2. Document IT Security Governance

   Collaborate, develop, and improve polices and procedures

3. Improve Cybersecurity Controls (Process & Technology)

   Review, implement and test process and technology controls where needed to prevent, detect and respond to cybersecurity attacks

4. Implement a Security Awareness Program (People Controls)

   Change company security culture through training and testing programs

5. Continual Assessment and Improvement (Culture)

   Provide for improvement of the IT security function through continual assessing, prioritizing, and remediating practices

Polling Question #3

Do well do you feel you have minimized your cybersecurity risk?

A. We have a very mature cybersecurity program
B. We have the basics in place, but there is room for improvement
C. We are at more risk than I feel comfortable with
D. I don’t have the data to be able to respond

Step 1 – Understand Data Assets

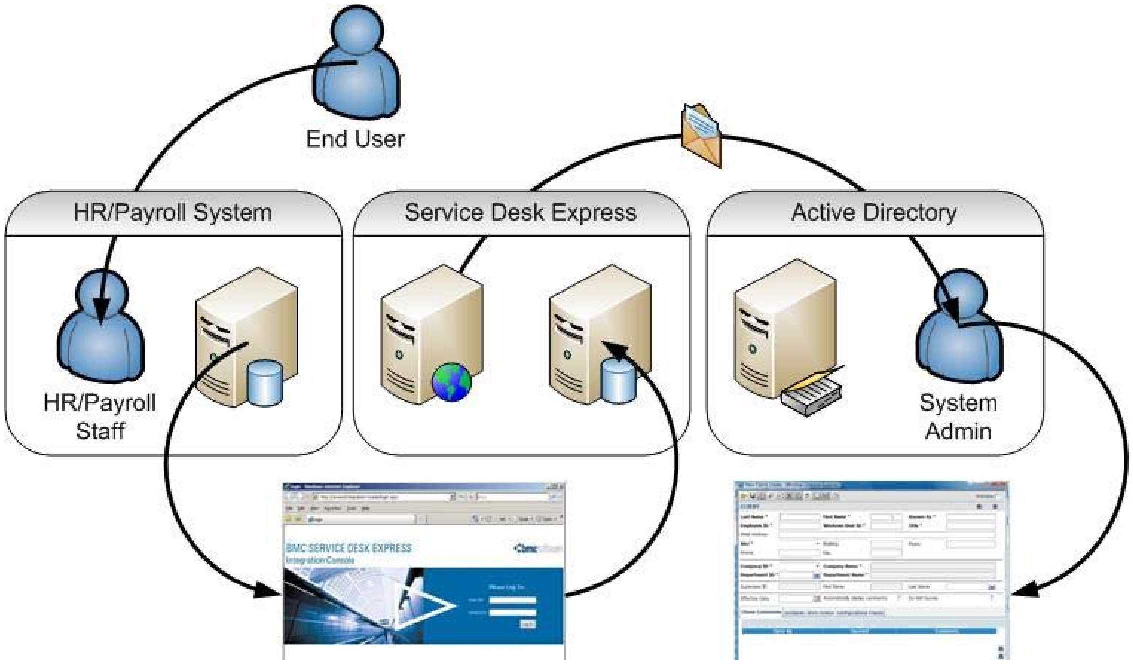
1. Get serious about data asset management; It's not fun, but it is critical.

2. Know what data is on what systems and why; Define roles well and make sure they are reasonable.

3. The proliferation of data outside of IT is a real and growing issue that needs prompt action.

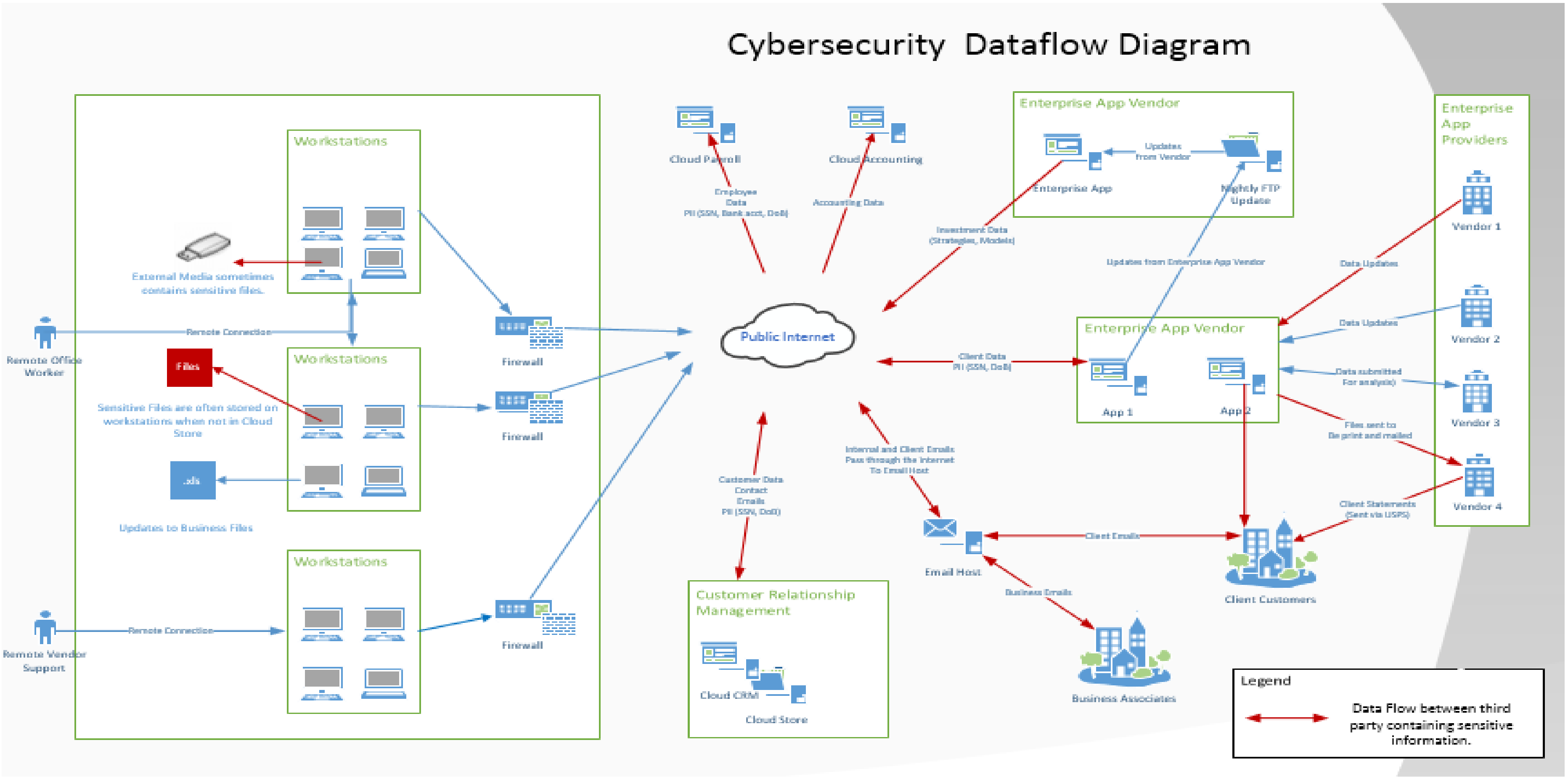
Step 2 – Map Data Stores and Flows

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

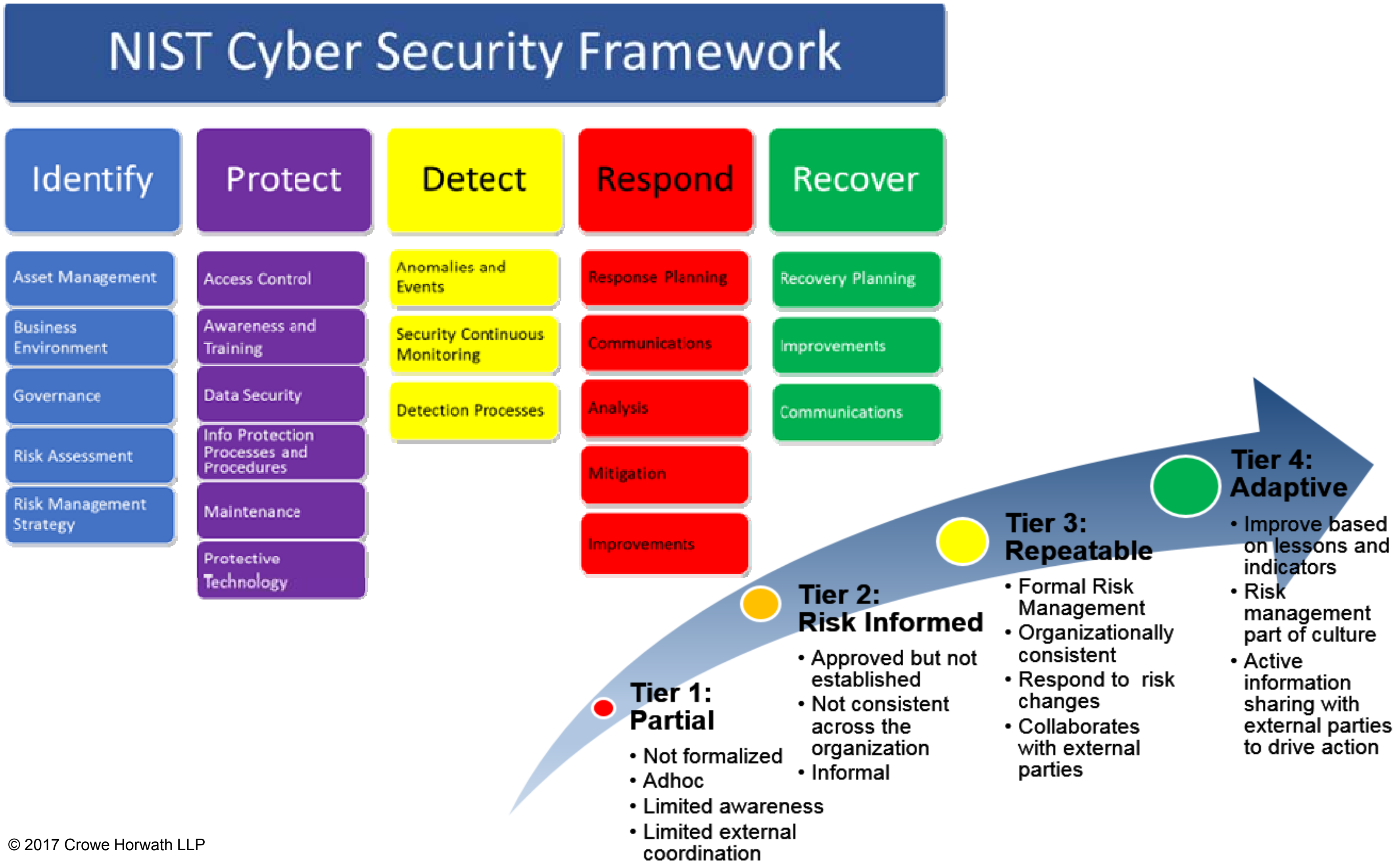


You can't dream up where your data can end up… **Follow the Data!**

Dataflow Example


Cybersecurity Dataflow Diagram
Workstations
External Media sometimes contains sensitive files.
Remote Connection
Remote Office Worker
Files
Sensitive Files are often stored on workstations when not in Cloud Store
Workstations
.xls
Updates to Business Files
Workstations
Remote Connection
Remote Vendor Support
Firewall
Firewall
Firewall
Cloud Payroll
Cloud Accounting
Employee Data PII (SSN, Bank acct, DoB)
Accounting Data
Public Internet
Customer Data Contact Emails PII (SSN, DoB)
Customer Relationship Management
Cloud CRM
Cloud Store
Internal and Client Emails Pass through the Internet To Email Host
Email Host
Business Emails
Business Associates
Client Emails
Enterprise App Vendor
Enterprise App
Updates from Vendor
Nightly FTP Update
Investment Data (Strategies, Models)
Updates from Enterprise App Vendor
Client Data PII (SSN, DoB)
Enterprise App Vendor
App 1
App 2
Client Customers
Enterprise App Providers
Vendor 1
Data Updates
Vendor 2
Data Updates
Vendor 3
Data submitted For analysis)
Files sent to Be print and mailed
Vendor 4
Client Statements (Sent via USPS)
Legend
Data Flow between third party containing sensitive information.

Step 3 – Assess Cybersecurity Controls



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Tier 1: Partial

- Not formalized
- Adhoc
- Limited awareness
- Limited external coordination

Tier 2: Risk Informed

- Approved but not established
- Not consistent across the organization
- Informal

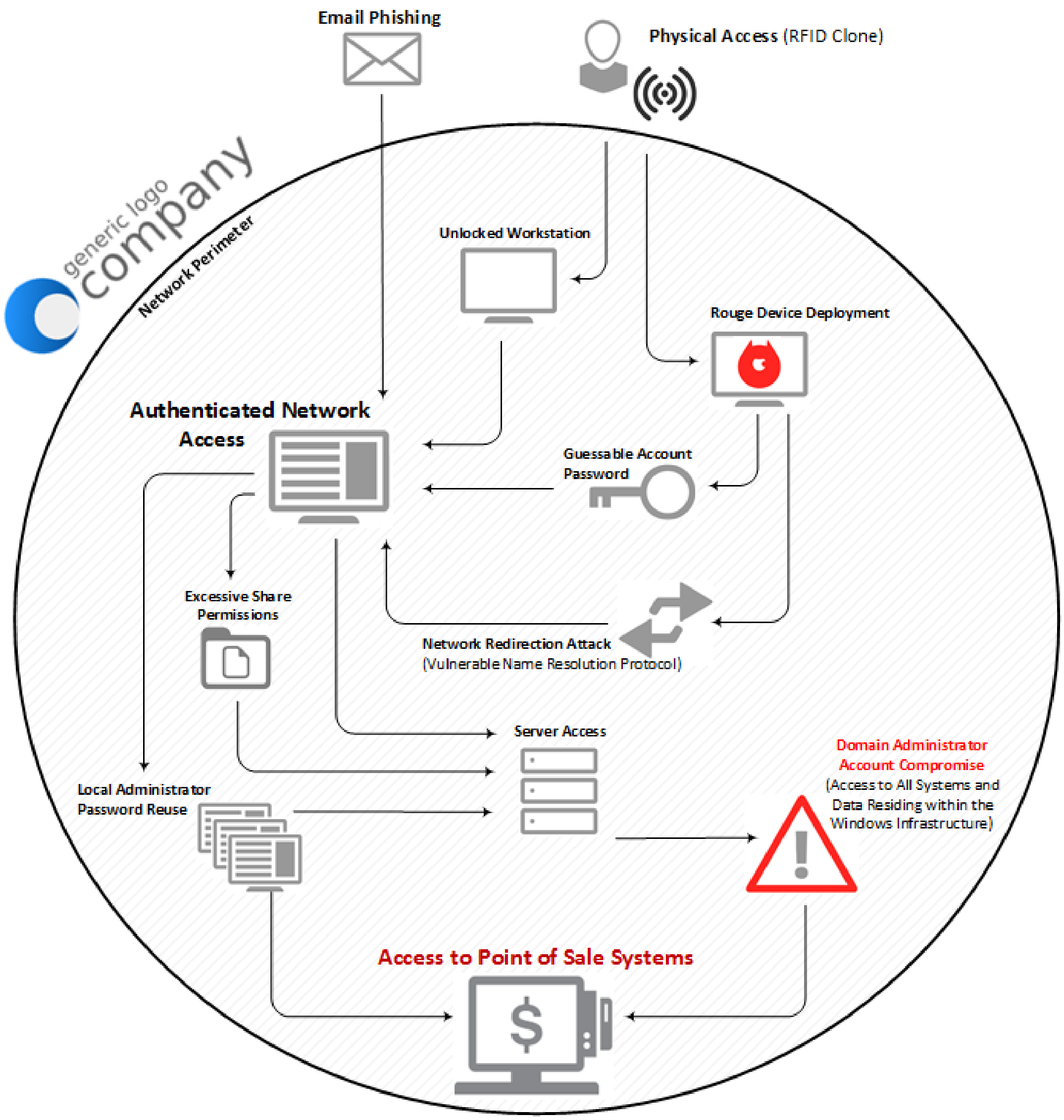
Tier 3: Repeatable

- Formal Risk Management
- Organizationally consistent
- Respond to risk changes
- Collaborates with external parties

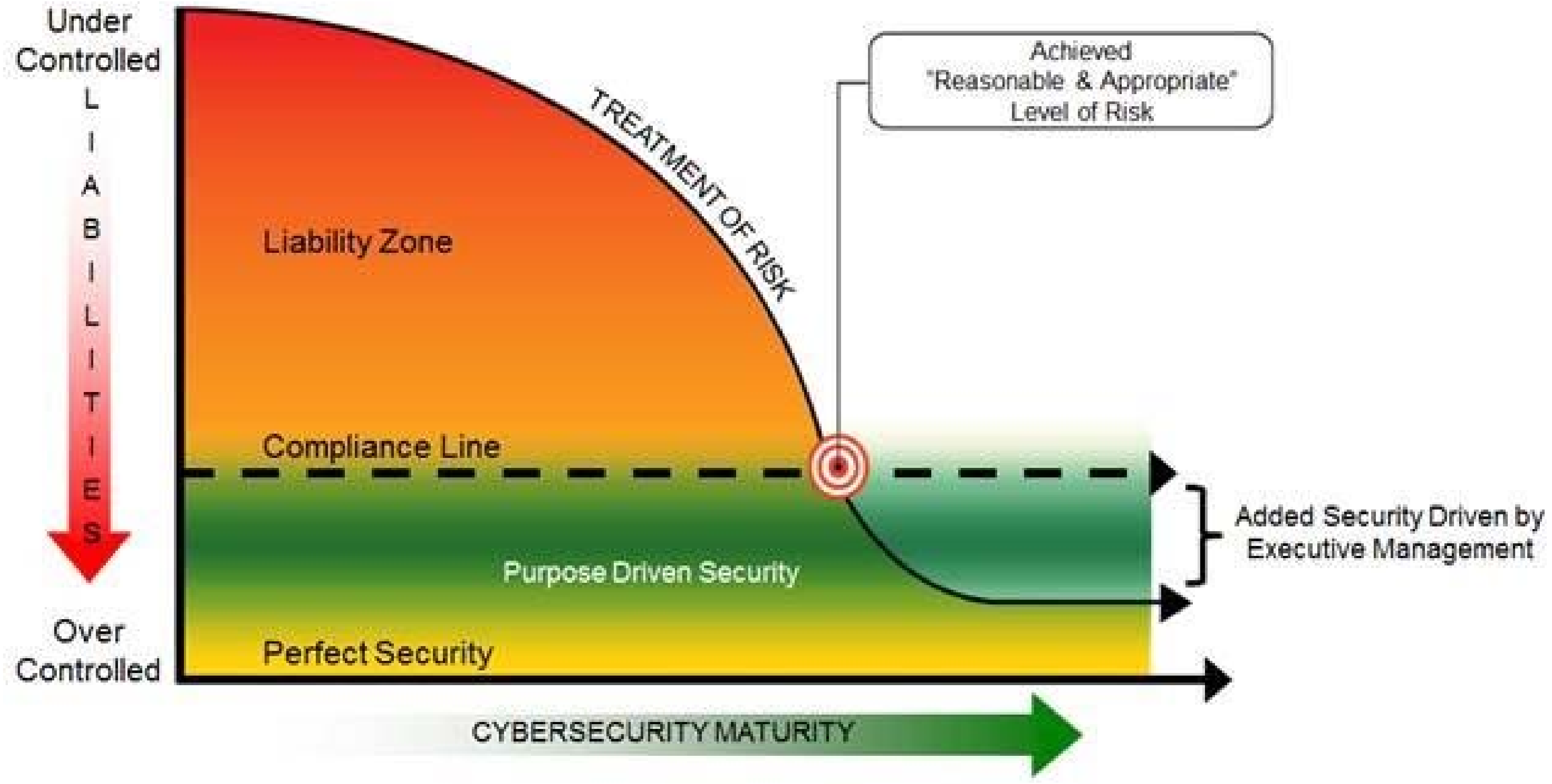
Tier 4: Adaptive

- Improve based on lessons and indicators
- Risk management part of culture
- Active information sharing with external parties to drive action

Step 4 – Test Cybersecurity Controls & Simulated a Hack


Email Phishing
Physical Access (RFID Clone)
generic logo
company
Network Perimeter
Unlocked Workstation
Rouge Device Deployment
Authenticated Network Access
Guessable Account Password
Excessive Share Permissions
Network Redirection Attack
(Vulnerable Name Resolution Protocol)
Server Access
Domain Administrator Account Compromise
(Access to All Systems and Data Residing within the Windows Infrastructure)
Local Administrator Password Reuse
Access to Point of Sale Systems

Board Communication – Know your Risk Tolerance



Polling Question #4

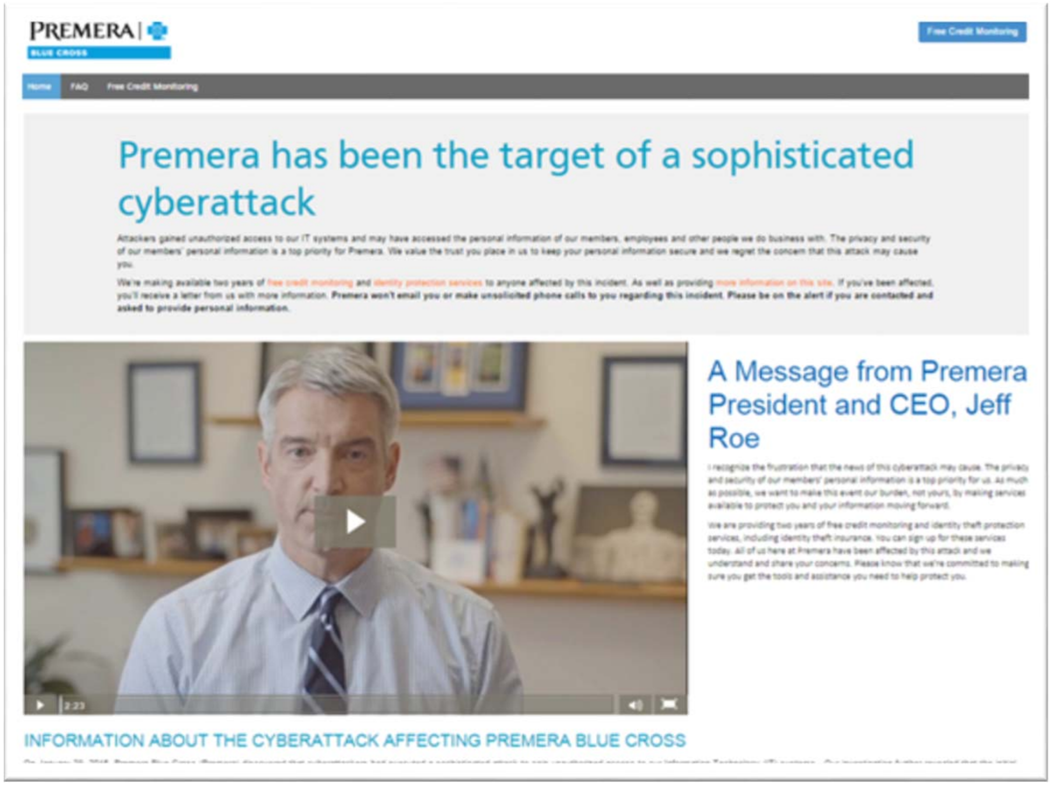
Have you had a cybersecurity incident before?

A. We have had no incidents
B. We have had 1 incident, but it was not public
C. We have had a public incident (listed on OCR Naughty List)

Be Prepared – Incident Response Planning

- 27% of organizations don’t have a breach response plan or team in place
- 37% have not reviewed or updated their plan since it was created

- 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?



Premera has been the target of a sophisticated cyberattack

Attackers gained unauthorized access to our IT systems and may have accessed the personal information of our members, employees and other people we do business with. The privacy and security of our members' personal information is a top priority for Premera. We value the trust you place in us to keep your personal information secure and we regret the concern that this attack may cause you.

We're making available two years of free credit monitoring and identity protection services to anyone affected by this incident. As well as providing more information on this site. If you've been affected, you'll receive a letter from us with more information. **Premera won't email you or make unsolicited phone calls to you regarding this incident. Please be on the alert if you are contacted and asked to provide personal information.**

A Message from Premera President and CEO, Jeff Roe

I recognize the frustration that the news of this cyberattack may cause. The privacy and security of our members' personal information is a top priority for us. As much as possible, we want to make this event our burden, not yours, by making services available to protect you and your information moving forward.

We are providing two years of free credit monitoring and identity theft protection services, including identity theft insurance. You can sign up for these services today. All of us here at Premera have been affected by this attack and we understand and share your concerns. Please know that we're committed to making sure you get the tools and assistance you need to help protect you.

INFORMATION ABOUT THE CYBERATTACK AFFECTING PREMERA BLUE CROSS

[illegible]

© 2017 Crowe Horwath LLP

Key Takeaways

1. Everybody is a target
2. Know where your data lives
3. Assess and mitigate to a reasonable level
4. Test your controls
5. Be prepared to respond to a breach
6. No silver bullet – Be a part of your culture

Questions

Jared Hamilton

317.706.2724

jared.hamilton@crowehorwath.com

@ITSecurityJared

linkedin.com/in/itsecurityjared

Cybersecurity Watch Blog

www.crowehorwath.com/cybersecurity-watch