

The Auditor's Guide to Protecting Data in 2015

A Practical Guide to Managing Increasing Risk Levels

Core Competencies – C31

Jeffrey Whiteside

CISSP, ISO27001LA

Technology Risk Manager

Crowe Horwath LLP

November 11, 2015



Trust in, and value from, information systems

San Francisco Chapter

The CyberSizelT logo is set against a silhouette of a city skyline with a bridge, likely the Golden Gate Bridge. The word "CyberSizelT" is written in a large, stylized font where the letters are interconnected. "Cyber" is in a reddish-brown color, "Sizel" is in white with a reddish-brown outline, and "T" is in a solid reddish-brown color.

CyberSizelT

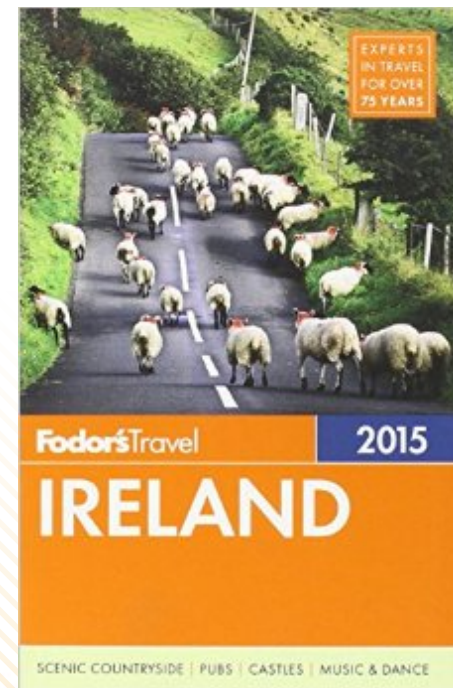
About Me

- Jeff Whiteside – CISSP
 - West Coast IT Security Manager
Crowe Horwath, LLP
 - Over seven years of industry experience
 - Wife and dog lover!
- Crowe's Risk Practice
 - Working with financial, manufacturing, healthcare and high tech
 - Security and Third Party Strategy
 - Network & Penetration Security Assessments, Social Engineering
 - Compliance Audits (PCI, GLBA, HIPAA, NERC CIP)
 - Fraud Investigations
 - Internal Audit



My goals for today's session: The Guidebook

- **History:** Recent Breaches and what we learned
- **How to get there:** Using NIST Cyber to build a roadmap
- **Where to stay:** Assessing your risk tolerance and making tough decisions
- **What to see and do:** The Auditors 2015 Data Protection highlights tour



This is not a 2010 Guidebook... ...and you are not 2010 Auditors


Resist the urge to go back to the places you've always visited! As you develop your audit plan consider:

How have we changed our audit plan since 2010?
Does that match the change in risks? Are we still stuck in a Sarbanes Oxley shaped world when it comes to Internal Audit and Data Protection? Is what we're doing actually helping the organization prevent breach?



now its time for the...

INCIDENT PARANOIA QUIZ

A close-up photograph of an HVAC repairman working on a unit. The man is wearing safety glasses and a light-colored shirt. He is focused on his work, with his hands positioned near a vertical pipe or component. The background is dark and shows various parts of the HVAC system, including pipes and insulation. The lighting is dramatic, highlighting the man's face and the metallic surfaces of the equipment.

**WHICH INCIDENT
HAS YOU LOOKING
SIDEWAYS AT
YOUR HVAC
REPAIR MAN?**

Target Breach (2013)

- According to a congressional investigation, Target:
- “Gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted Info Sec practices”
- “Failed to respond to multiple automated warnings from the company’s anti-intrusion software” first that the attackers were installing malware, and then that they were shipping data out (exfiltration)
- Failed to segment its network as “Attackers... appear to have successfully moved from less sensitive areas of Target’s network to areas storing consumer data”



http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

What's an auditor to do?

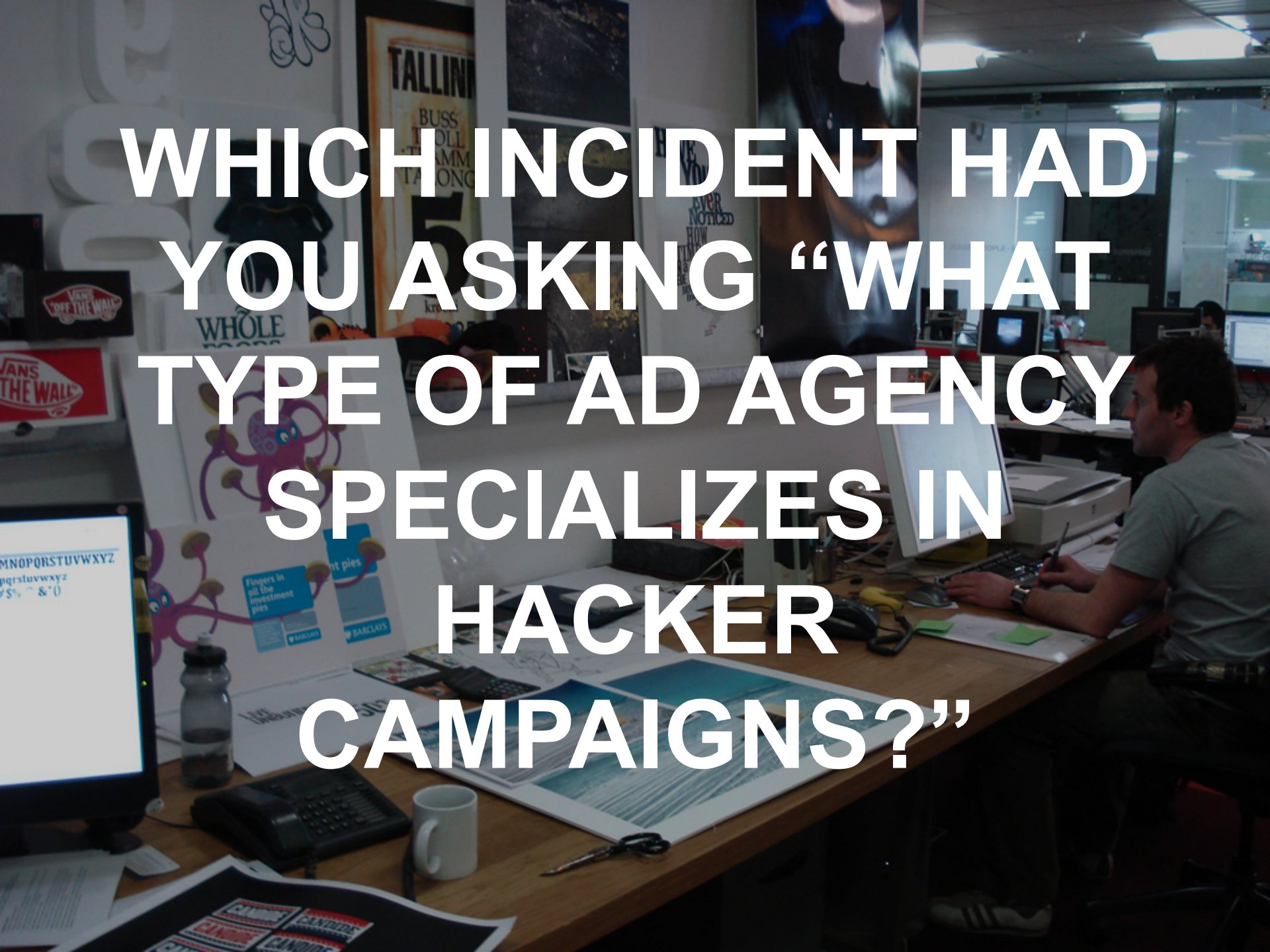
- Third Party Risk Management Audit
 - With special attention to those vendors that might have been forgotten but have access to the network
 - Consider: How do vendors get network access? Establish network connections?
- Network Architecture and Segmentation Audit
 - Ask: Do we use technical mechanisms to segment our sensitive information? Examine your organization's use of Network segmentation. Consider this a key control
 - Do we put too much emphasis on our external Firewall? Do we see the internal network as a safe happy place?



What's an auditor to do?

- Penetration Testing: Consider doing testing unannounced
 - The goal is to “Turn up the volume” and see when your systems and people detect the attack
 - This is not the typical practice of most security assessment firms, which blast the network immediately with noisy attacks
 - Plan on debrief and discussion – at what point was the attack detected? What did they do?
 - This is an optimal test for Managed Security Service Providers



A man in a light-colored t-shirt is sitting at a desk in a cluttered office, working on a computer. The desk is covered with papers, a keyboard, a mouse, a water bottle, and a white mug. In the background, there are several posters and signs, including a large 'VANS OFF THE WALL' sign, a 'TALLINN' poster, and a 'WHOLE' poster. The office has a casual, creative atmosphere.

**WHICH INCIDENT HAD
YOU ASKING “WHAT
TYPE OF AD AGENCY
SPECIALIZES IN
HACKER
CAMPAIGNS?”**

Heartbleed Vulnerability (2014)

“I really believe that the name and the logo...helped fuel the community interest in this,”

David Chartier, CEO of Codenomicon, the security testing firm which found the bug on 4/3/14

- Heartbleed is a vulnerability in OpenSSL.
 - Software that secures Internet traffic between browser and Website
 - You will see the “Lock” in your browser
 - Vulnerability allows attackers to access sensitive data
- Not the only Web or SSL Vulnerability last year – maybe not even the worst.
- The “poster child” for web-based vulnerabilities and how we will respond



What's an auditor to do?

- Web Application Penetration Assessment
 - Think beyond your network penetration assessment
 - Make sure your Pen Testers perform an authenticated, expert review of your Web Applications based on on
 - Make sure your vendors do this type of testing
- Encourage your IT/Info Sec team to respond in a calculated way to incidents like Heartbleed that may have nothing to do with you
 - Make sure your risk function isn't just reacting to the news
 - Understand the framework, and ask your Security owners to put incidents in the context of the overall program
 - The biggest news does not always equal the biggest deal



What's an auditor to do?

- Consider the “chain reaction” and be prepared to respond to Internet incidents
 - A vulnerability hits the news
 - Causing customers to ask if you're affected
 - Causing you to ask your vendors if they're affected
 - Causing your vendors to ask their vendors
 - Causing mass confusion
- Reconsider Incident Response
 - Did you send a Heartbleed letter to customers? Affiliates? Vendors?
 - How did this fit in your company's Incident Response plan?
- Discuss with your team: Can our specialization in Information Security become a differentiator to our stakeholders
 - Educating stakeholders when a new incident might impact them



A hand is pointing upwards towards a green hexagon containing a white '@' symbol. The background is dark grey with a pattern of faint, light grey hexagons. The text is centered and reads:

**WHICH INCIDENT HAS
YOU THINKING
ABOUT WHERE
EMAIL ENDED UP IN
YOUR IT RISK
ASSESSMENT?**

Sony Pictures (2014)

- 32nd largest breach last year. So why are we talking about it?

NATION-STATE SPONSORED?

“..the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment...the FBI now has enough information to conclude that the North Korean government is responsible for these actions.”

- FBI press release, 12/19/14



<http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>

<http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html>

Sony Pictures (2014)

HACKING ORGANIZATION & MALICIOUS INSIDER?

- Private sector security firms Norse and CloudFlare refute the FBI claims that the malware can be directly tied to North Korea
- Guardians of Piece claims responsibility, North Korea declines
- Malicious Insider with ties to Guardians of Piece
- Questions of whether North Korea has the right level of skill to execute the attack.
- <https://www.youtube.com/watch?v=ZVAbFzII0cU>

<https://www.youtube.com/watch?v=ZVAbFzII0cU>

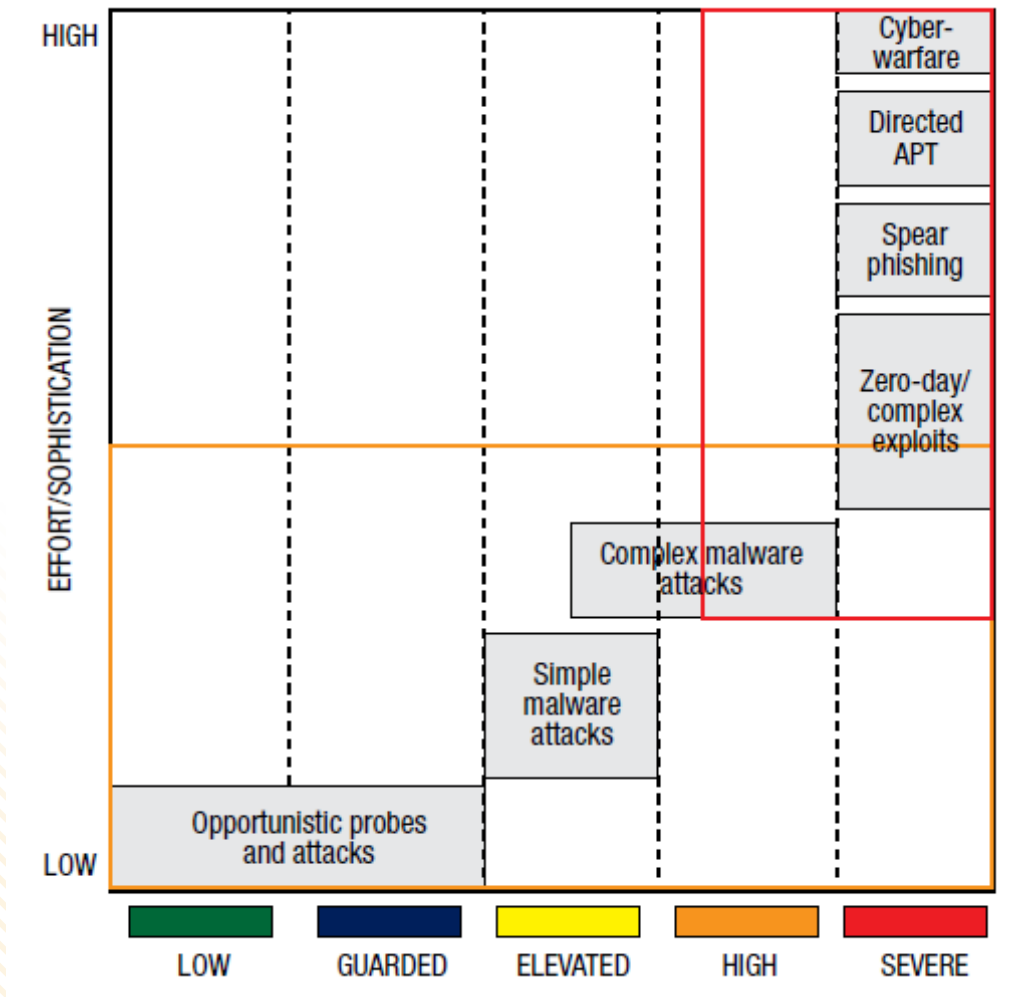
Sony Pictures (2014)

RESULT OF A ZERO-DAY VULNERABILITY?

“Sources familiar with the Sony investigation told Re/code the attackers took advantage of what's known as a "Zero-Day" vulnerability as part of a campaign to destroy the studio's corporate network...known as Zero-Day because the original programmer has zero days after learning about it to patch the code before it can be exploited in an attack...Kevin Mandia — founder and head of Mandiant, the security firm hired to investigate the breach — that the attack was one for which neither Sony "nor other companies could have been fully prepared.””

Well now that's not fair is it?

<http://www.cnbc.com/id/102351695>



<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx>

Sony Breach (2014)

“The big lessons from the Sony breach are that businesses need better planning and to shift security investment away from trying to protect the network from attacks and toward quickly detecting and dealing with breaches

While today no large enterprises have plans for dealing with aggressive cybersecurity business disruption attacks, within three years, 40% will”

- Gartner as reported by Network World, February 2015

<http://www.networkworld.com/article/2888297/security0/sony-breach-is-a-new-breed-of-attack-that-needs-new-responses.html>

Sony Breach (2014)

> 200 days: The amount of time an attacker spends in enterprise systems before someone notices

2 out of 3: Frequency with which the breach is not detected by the organization, but by an external party like the FBI

88%: Percentage of CISOs who think that the increase in attack sophistication will outpace their team's increase in sophistication

- <http://www.wsj.com/articles/how-the-sony-data-breach-signals-a-paradigm-shift-in-cybersecurity-1423540851>

Sony Breach (2014)

Wait! There's even a tie to Internal Audit! Employee class-action lawsuit presents this evidence:

“The lawsuit contends that the studio’s security practices fell below “prudent industry standards.” It cites, among other things, an audit by PricewaterhouseCoopers in September 2014 that found gaps in the company’s monitoring of its systems”

- <http://variety.com/2015/biz/news/sony-hack-scandal-lawsuit-1201445372/>

What's an auditor to do?

- Audit your containment strategy
 - They're in. Now what.
 - Again, more need for segmentation
 - Better detection, quicker, even after hours
- Challenge your Incident Response Plan
 - Are the people at the table planning the same people that would be involved if a Sony-scale breach happened?
- Consider if you are prepared for the malicious insider
 - Has SOD really been extended to employee monitoring?

**WHICH RECENT
INCIDENT MADE
YOU SAY: ENOUGH
IS ENOUGH!**

Anthem Breach (2015)

“On January 29, 2015, Anthem, Inc. (Anthem) learned of a cyberattack to our IT system. The cyberattackers tried to get private information about current and former Anthem members. We believe it happened over the course of several weeks beginning in early December 2014. The information accessed may have included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, employment information, including income data.”

- Anthem customer notification, February 2015

<https://www.anthemfacts.com/>

Anthem Breach (2015)

Attackers set up the domain we11point.com

Attackers execute a spear phishing attack on Anthem

Five sets of Administrator credentials are compromised circa Dec 2014

Administrator credentials are used to access Anthem's customer database

A Database Administrator notices unusual queries and the breach is discovered

- (<http://www.infoworld.com/article/2898658/security/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html>)
- <http://www.forbes.com/sites/frontline/2015/02/24/behavioral-analysis-could-have-prevented-the-anthem-breach/>
- <http://www.usnews.com/news/business/articles/2015/02/06/anthem-hacker-tried-to-breach-system-as-early-as-dec-10>


Anthem Breach (2015)

What Anthem did well: They were very quick to notify the public- 8 days between discovering and reporting the breach.

What Anthem did not do well: They have been slow to send out customer notices, more than an month later.

What's an auditor to do?

- Test responses to Social Engineering
- Assess time to respond
 - Are the right people involved?
 - Are we prepared to notify at the point we can confirm breach, not at the point where we have pinned down the details?
- When it comes to data access, you must be on premises or we need Multifactor authentication

A blue stethoscope is centered in the image, with its chest piece and tubing visible. The background is a solid, light grey color. The text is overlaid on the stethoscope.

**WHICH INDUSTRY
MADE THE MOST
HEADLINES THIS
YEAR FOR HACKING
INCIDENTS?**

Health Data Breaches 2015

- Anthem disclosed of the data breach affecting 78.8 million people on February 4.
- One month later, Premera Blue Cross announced that as many as 11 million personal and health data may have been compromised (March 17).
- CareFirst BlueCross BlueShield announced on May 20 of a data breach that compromised the personal information of 1.1 million customers.
- UCLA Health System announced on July 17 of a data breach occurred where the personal and medial records of as many as 4.5 million people may have been compromised.

Anthem 

PREMERA | 
BLUE CROSS


CareFirst



Encryption is Key

- Athem and UCLA Health System did not protect private and medial data with encryption.
- Premera encrypted their data but the attackers circumvented the control by gaining unauthorized system access.
- Many organization besides healthcare still do not encrypt customer data in storage.
- LastPass announced on June 15 of data breach where the hashes of their user's master password may have been compromised; however due to the use of strong hashing algorithms the master passwords were not at risk.

What's an auditor to do?

- Perform a Data Protection Assessment
 - Review the Data Protection Program
 - Assess the effectiveness of the Data Protection Solutions
 - Assess the security around data in motion and data at rest
 - Inquire about data flow and process
 - Determine who has access to the data and how it may be leaked

Book your trip...

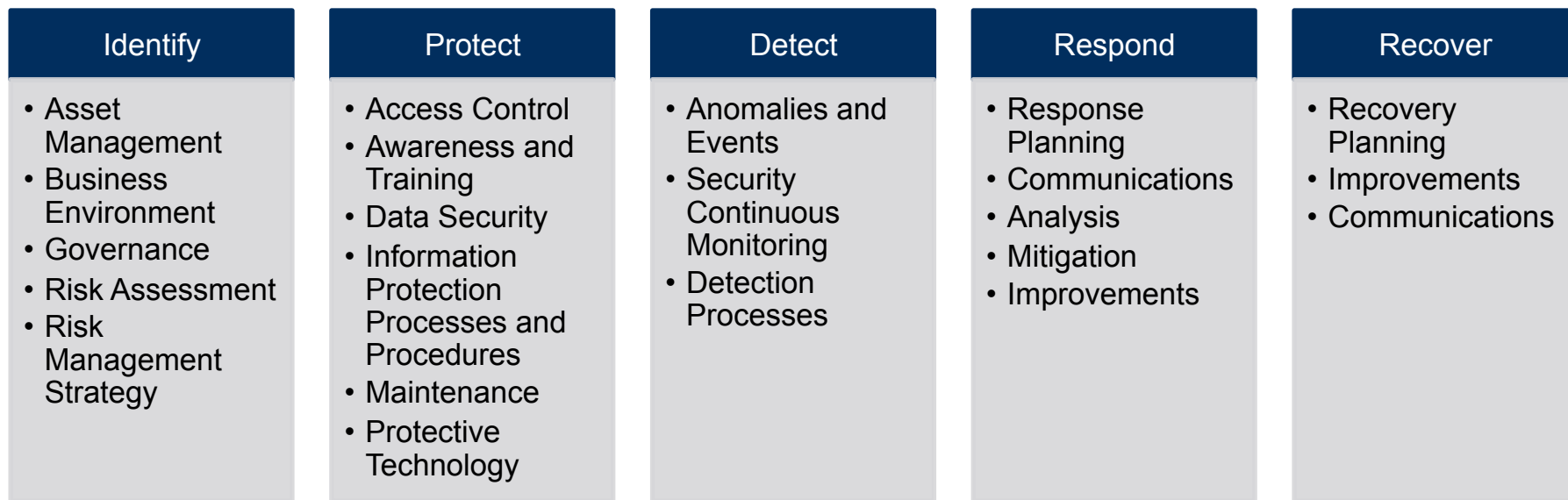
Building a roadmap with NIST Cyber



Background on NIST Cybersecurity Framework

- February 2013: President Obama issued Exec Order 13636 “Improving Critical Infrastructure Cybersecurity”.
 - It directed NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks.
 - NIST is the National Institute of Standards and Technology, an agency of the US Dept of Commerce
- First Version Released on February 12, 2014.
 - “Framework for Improving Critical Infrastructure Cybersecurity”
- NIST is seeking commentary based on this release, Version 2 anticipated
 - NIST has said that they will “continue to serve in the capacity of ‘convener and coordinator’ at least through version 2.0 of the Framework.”
- The latest update was released on July 31, 2014.
 - A formal RFI asking for further feedback will be issued.
- Additional commentary was released December 5, 2014

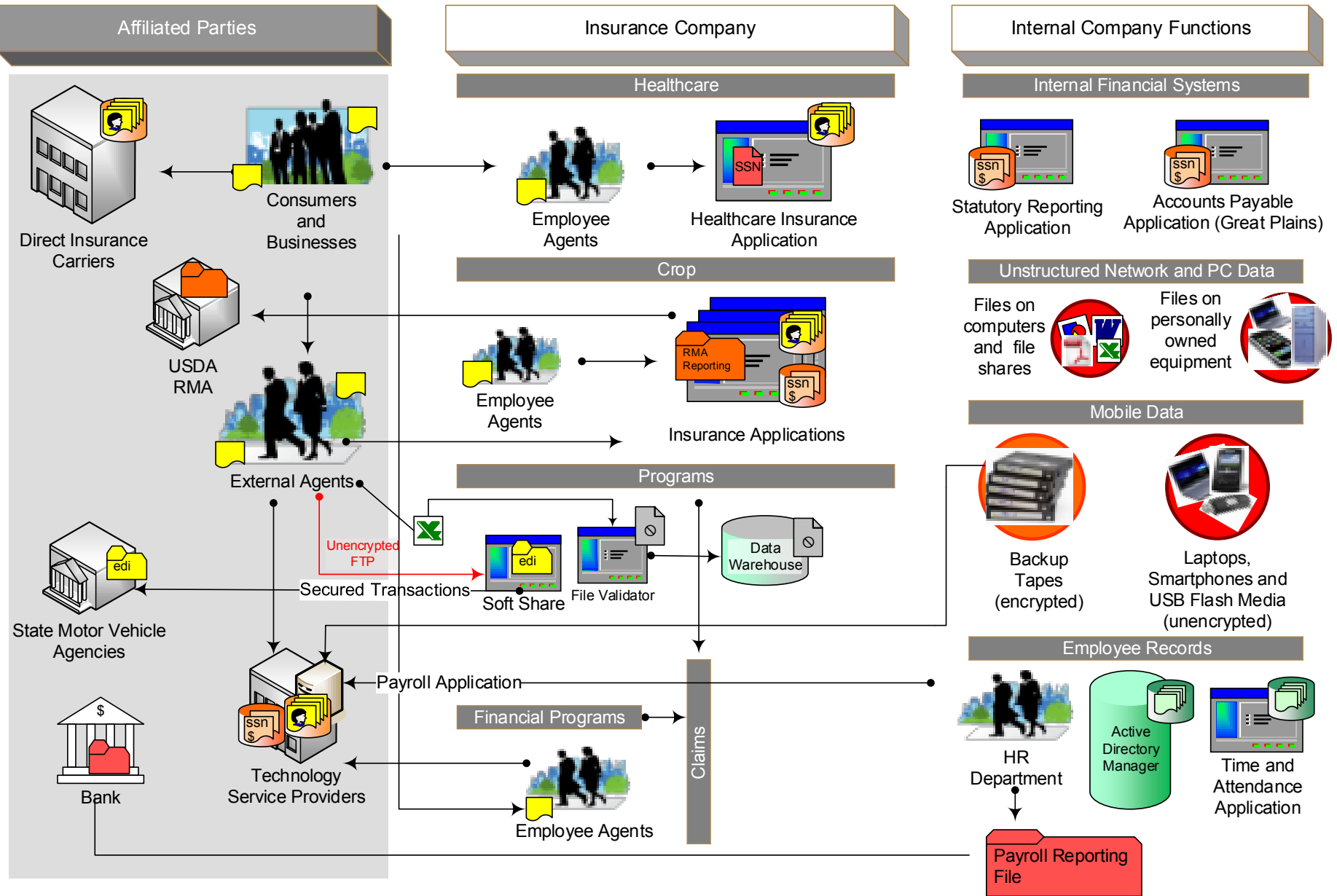
Overview of Cybersecurity Framework



Identify: Know what you have to protect

1. Get serious about asset management. Its not fun or sexy but its mandatory.
2. It is IT's job to 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. Consider your CISO's influence outside of IT.

Electronic Confidential Personal Information Universe Diagram



Protect: Bring together new and “back to basics”

Back to Basics

- Employee Awareness and prevention of social engineering
- Vendor Risk Management
- Patching and Vulnerability Management
- Monitoring
- Incident Response

New Kid on the Block

- No squishy center
- Multifactor Authentication
- Third Party Risk and TCO
- Executives and Incident Response

Protect: Back to Basics

- Security has always been based on layers
 - Onion concept dates back many years
- Technology has gotten more sophisticated
- The “Internet of Things”, Mobile, and Social Media movements confuse things a bit more
- All of this leads us to rely on cool new technology and forget the basics: its an onion
- The moral: Assume one or more controls fail, and then look at your attack vectors.
- As Auditors, we need to review news articles like those today such that we can evaluate management’s attestation of compensating controls



Protect: The New Kid(s) on the Block

- Your security department should be the experts. So what can internal audit do?
- What IA is good at: Assess the process.
 - Does your Information Security department evaluate the new fixes available to address new problems?
 - Are you bringing in talent to continue to augment your team?
 - Is your Security team taking steps to monitor the environment? Attending conferences? Speaking at conferences?
 - Once technology has been evaluated, does the team have the right reporting structure and executive support to make the right decisions?



Protect: No squishy center

- Old school networks - Security guards are placed only at the exterior doors.
- Current paradigm – Assume that someone you let in is bad, or that a bad guy can “airlift” themselves in.
- In a world of APT, there are certain doors you have to assume will be breached. Think: the pentagon. We assume someone can break down the front door. So the key secrets are buried inside.

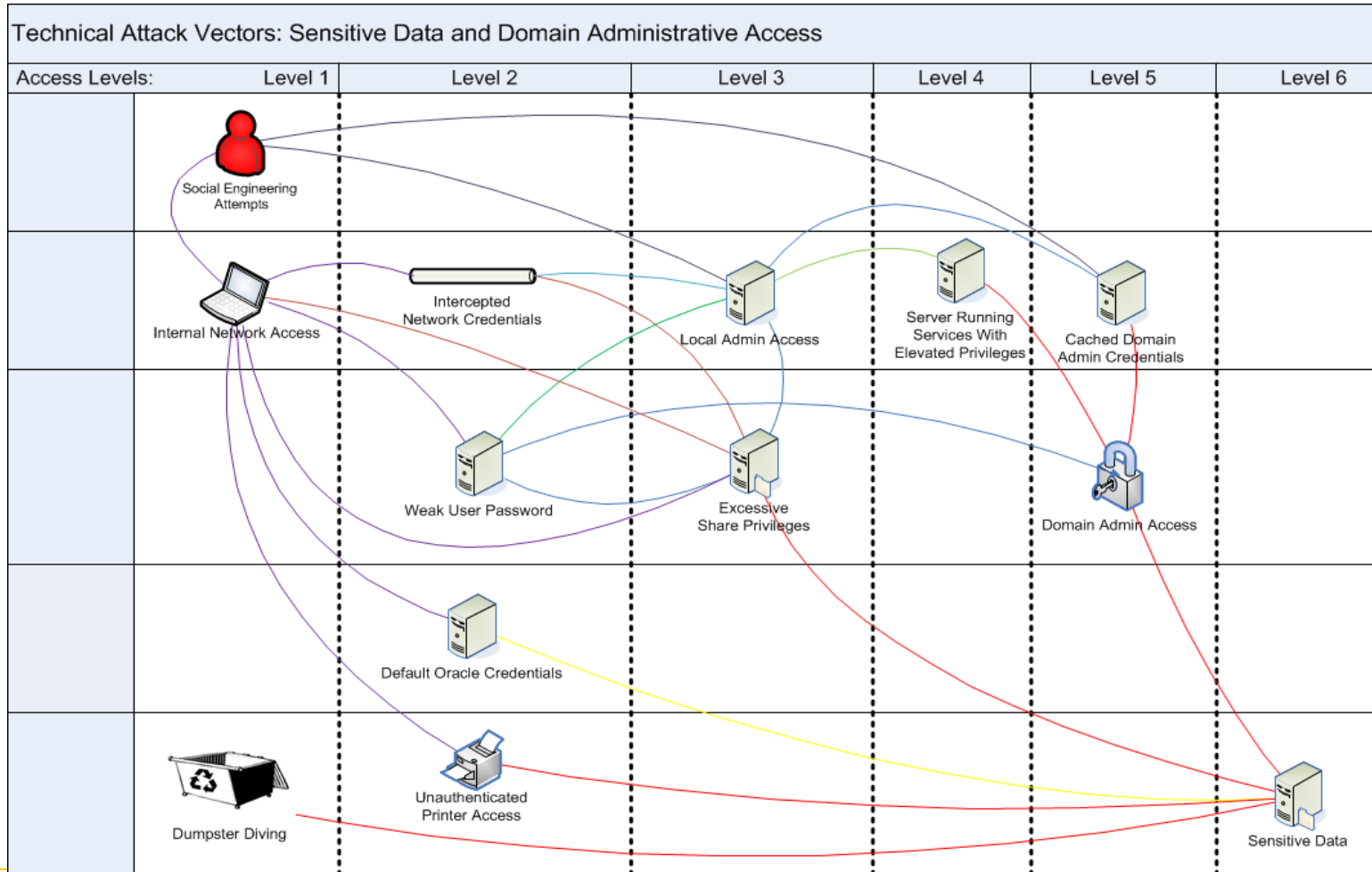


Protect: No squishy center

- Data Segregation – interior guards and locks
 - Is harder to do
 - Is critical to do
- Assume your users have been phished!
- Ask yourself: Do our audits put too much emphases on border controls?
 - External Network Pen vs. Internal Pen Testing



Protect: Sample Attack Vector Diagram



Protect: Multifactor – Not your Grandma’s token

- Multifactor or MFA is based on the premise that userIDs and passwords can and will be harvested. This is the reality of the present day.
- While we’ve had this technology for some time, problematic implementations made it hard to use.
- In 2015, MFA will become even more prevalent
 - Soft tokens
 - “Push” multifactor
- Most users whine at first but get onboard



Protect: Duo Mobile Videos

- https://www.youtube.com/watch?v=WH_KuCCf0c0#action=share

Detect: Assume you will be breached

JPMC is reported to have spent \$250MM on Security and had a breach in 2014. The moral of the story: You can run but you can't hide. So what do we do?

1. Monitor traffic and activity in a meaningful way
2. Have smart ways of filtering and alerting. Manual review is not going to cut it.
3. Find ways to get and safely share threat intelligence data
4. Have a Security Operations Center that is reviewing alerts and actioning based on the intelligence at hand.

Detect: Federal Government wants us to share

- February 12, 2015 Executive Order Promoting Private Sector Cybersecurity Information Sharing

- Encouraging Private-Sector Cybersecurity Collaboration
 - Encourage the development of Information Sharing Organizations:
 - Develop a common set of voluntary standards for information sharing organizations:
- Enabling Better Private-Public Information Sharing
 - Clarify the Department of Homeland Security's authority to enter into agreements with information sharing organizations:
 - Streamline private sector companies' ability to access classified cybersecurity threat information
- Providing Strong Privacy and Civil Liberties Protections
- Paving the Way for Future Legislation

Recover: Precise & prompt with the right players

- The Shift has occurred:
 - Old School – IT Leads Incident Response efforts. Senior Executives show up to tabletop exercises and try to look interested.
 - New Age – Corporate Executives and Boards, spawned by events like the firing of the Target CEO, are asking questions and leading discussions on this topic.
- What’s an internal auditor to do?
 - Sit in. Evaluate the result, but more importantly, the process.
 - Is the team collaborating? Are the right experts at the table?
 - Is the right information making it from smart Info Sec people’s heads to the CEO?
- Bottom line: You should see your organization get aggressive on Incident Response.

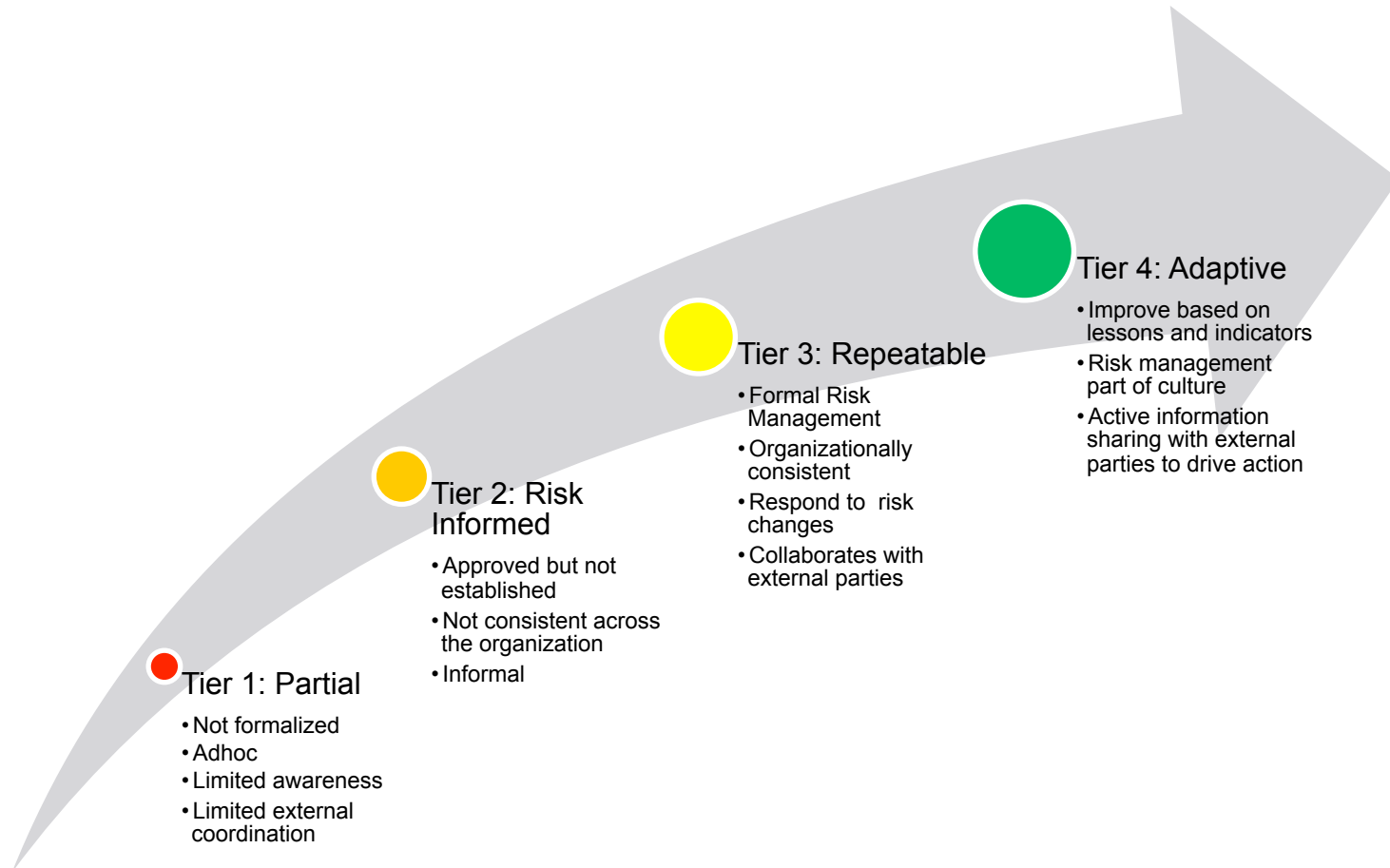
Recover: Other Trends in Incident Response

How will we escalate? What is the path from low level associate detecting something up through the CEO finding out about it? Can this happen in a matter of hours not days?

What's our operating protocol? Incident Response can be a 24x7 activity that needs to continue until the analysis is done. Is your team prepared to work “round the clock”?

Who will help us? In the event of a large scale breach, have you prepared by aligning with vendors that will help you? Legal? Forensics experts (maybe more than 1)? Public Relations? Printing vendors to send notices? Vendors to provide credit monitoring?

NIST Cybersecurity Control Maturity Scale



NIST Cybersecurity Control Maturity Scale

- What does the maturity scale mean:

In Cybersecurity, there is usually not a black and white answer. Its usually a question of current and desired maturity.

Your takeaway: Define your risk tolerance. Where do you have no tolerance, and are willing to invest? Where do you have more tolerance, and are willing to live with a less mature control set?

NIST Cyber Project Plan



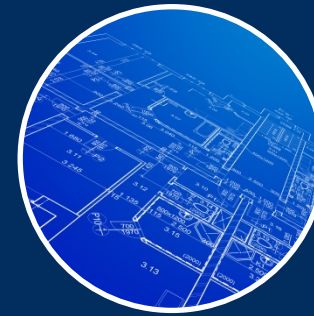
Assess your program against the NIST Cybersecurity Framework



Based on this assessment, provide a maturity scale rating for each of the five framework functions and categories described on slide 3



Provide a roadmap for increased maturity against the NIST Cybersecurity Framework



Provide strategic and tactical recommendations for improvement, while aligning with info sec overall plan



5 things Internal Audit should do in 2015 to protect data

1. Become a breach news junkie
2. Consider whether your audits are impacting Information Security in a forward-thinking way. Is it only the same old findings?
3. Ask specifically about:
 - Multifactor Authentication
 - Threat detection and monitoring on the inside
 - Network Segmentation
4. Look at Incident Response with a new lens.
5. Redefine your team's role in Data Protection.