CPIM Academy

CPIM

CENTER FOR PUBLIC INVESTMENT MANAGEMENT

A PROGRAM BROUGHT TO YOU BY:

JOSH MANDEL

TREASURER OF OHIO

SECURITY 110

Fraud Prevention and Cybersecurity

2015

Learning Objectives

- Fraud Prevention
  - Understand Current Fraud Trends
  - Whistleblower Programs
  - Fraud Types
  - Fraud Risk Assessments
- Cybersecurity
  - Understand Cybersecurity and Social Engineering
  - Assess Current State of Cybersecurity Threats
  - Understand notable examples of cyber crime
  - Highlight traditional cybersecurity pitfalls
  - Define cybersecurity roles
  - Build and implement a cybersecurity plan
  - Navigate barriers to success
  - How to monitor and evolve

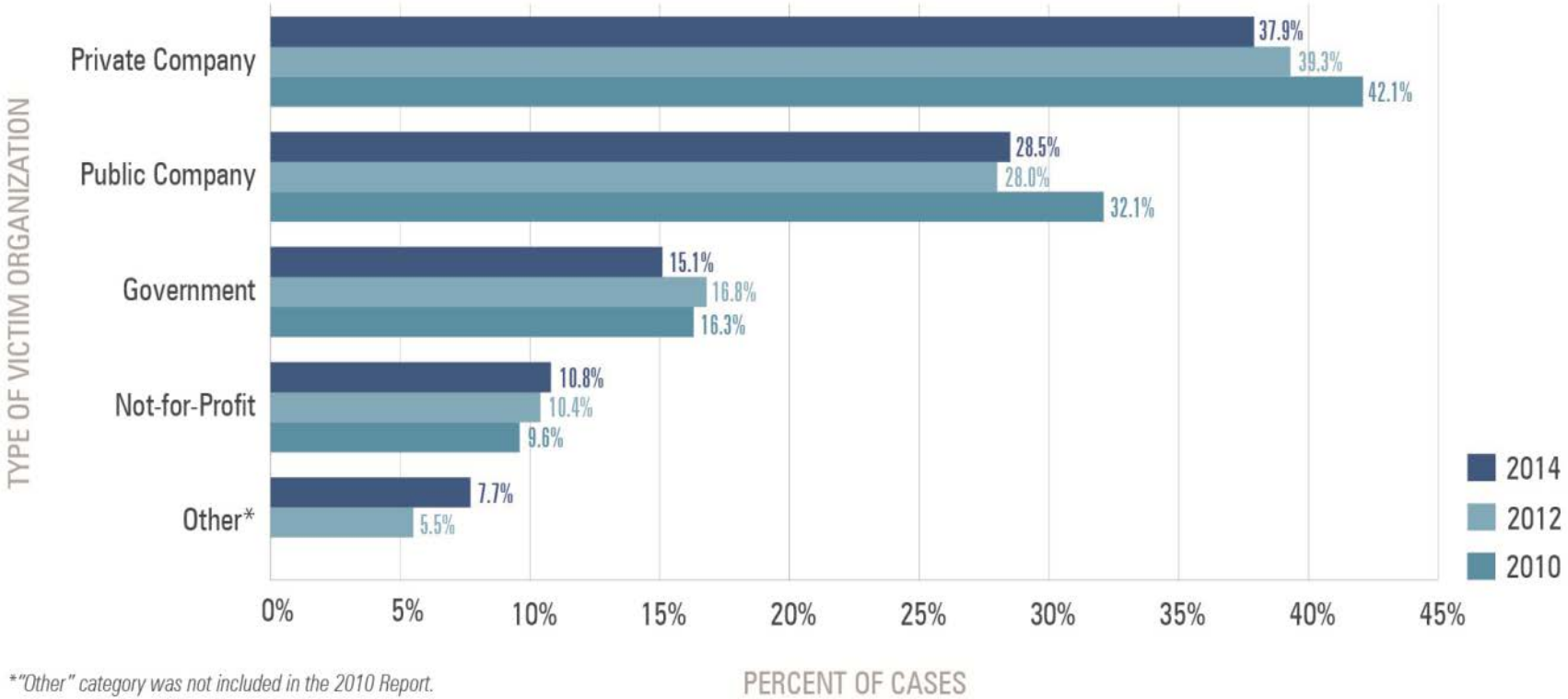
FRAUD PREVENTION

"Fraud and stupidity look an awful lot alike."

- Alan Bachman, CFE, MBA
Education Manager at ACFE

Fraud Statistics

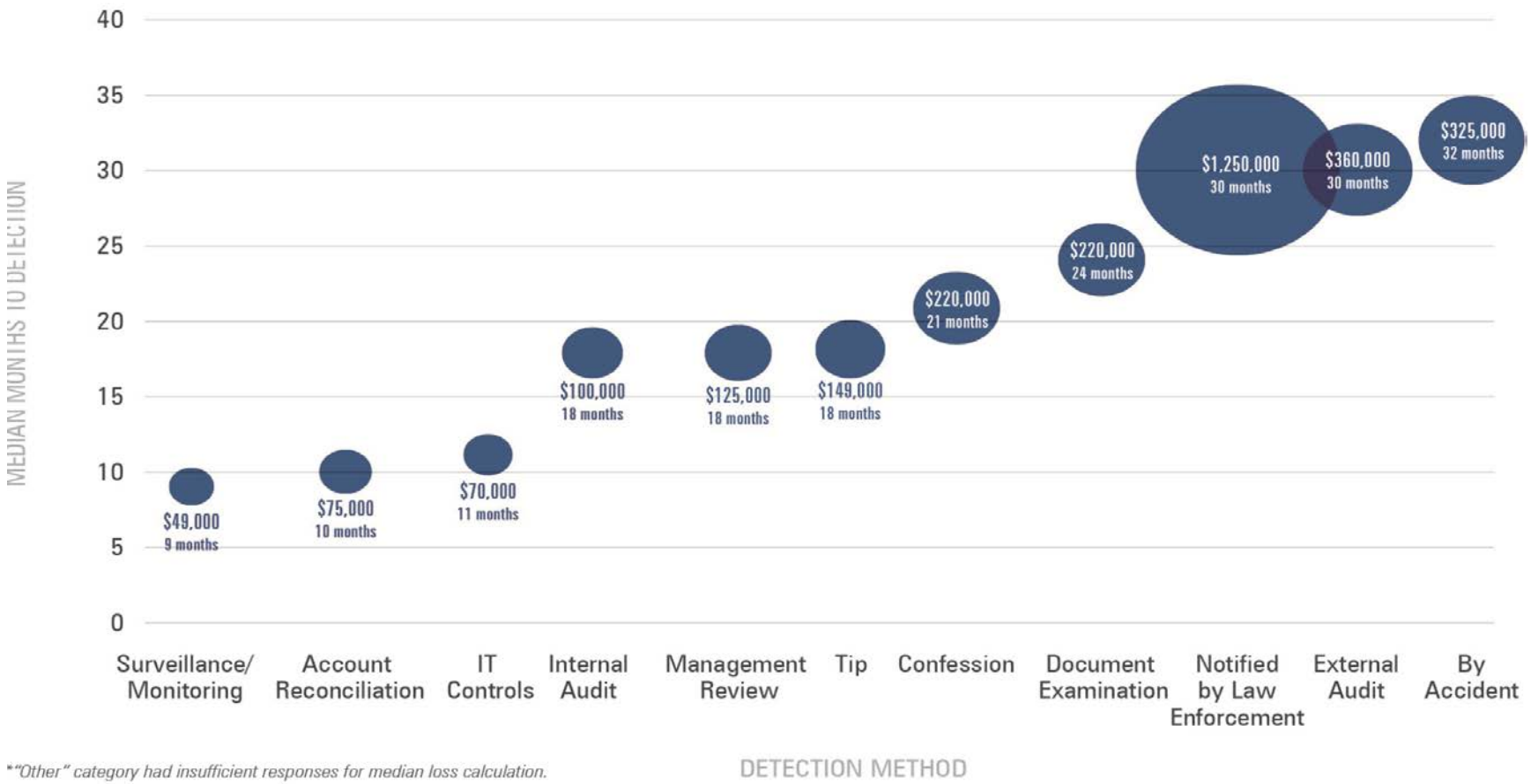
Figure 17: Type of Victim Organization — Frequency



*"Other" category was not included in the 2010 Report.

Fraud Statistics

Figure 12: Median Loss and Median Duration by Detection Method

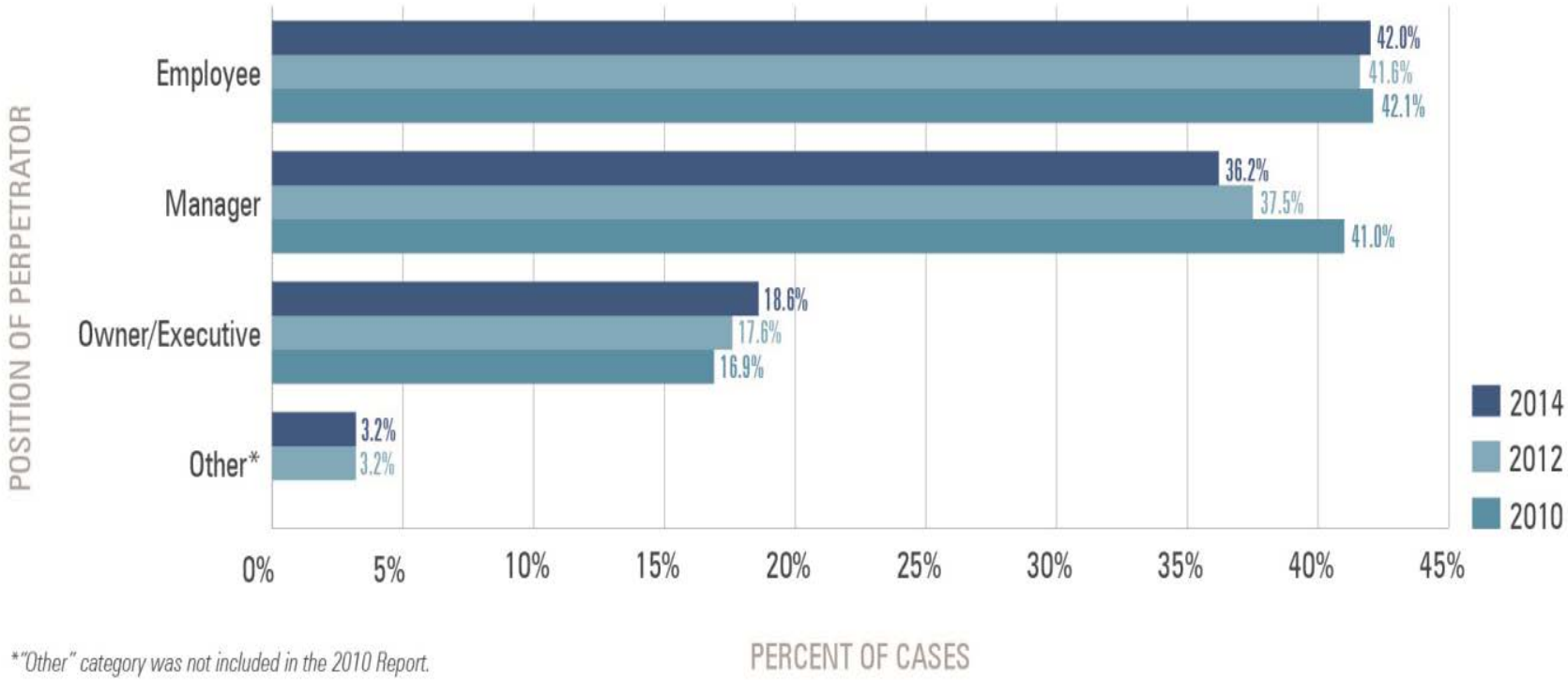


*"Other" category had insufficient responses for median loss calculation.

ACFE 2014 REPORT TO THE NATIONS

Fraud Statistics

Figure 40: Position of Perpetrator — Frequency



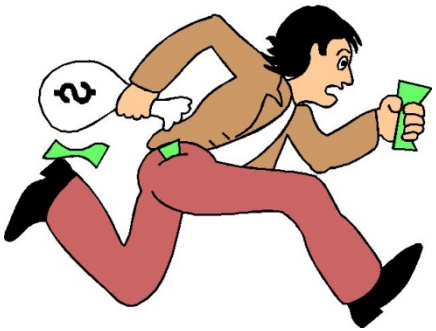
*"Other" category was not included in the 2010 Report.

Fraud Statistics

Figure 41: Position of Perpetrator — Median Loss

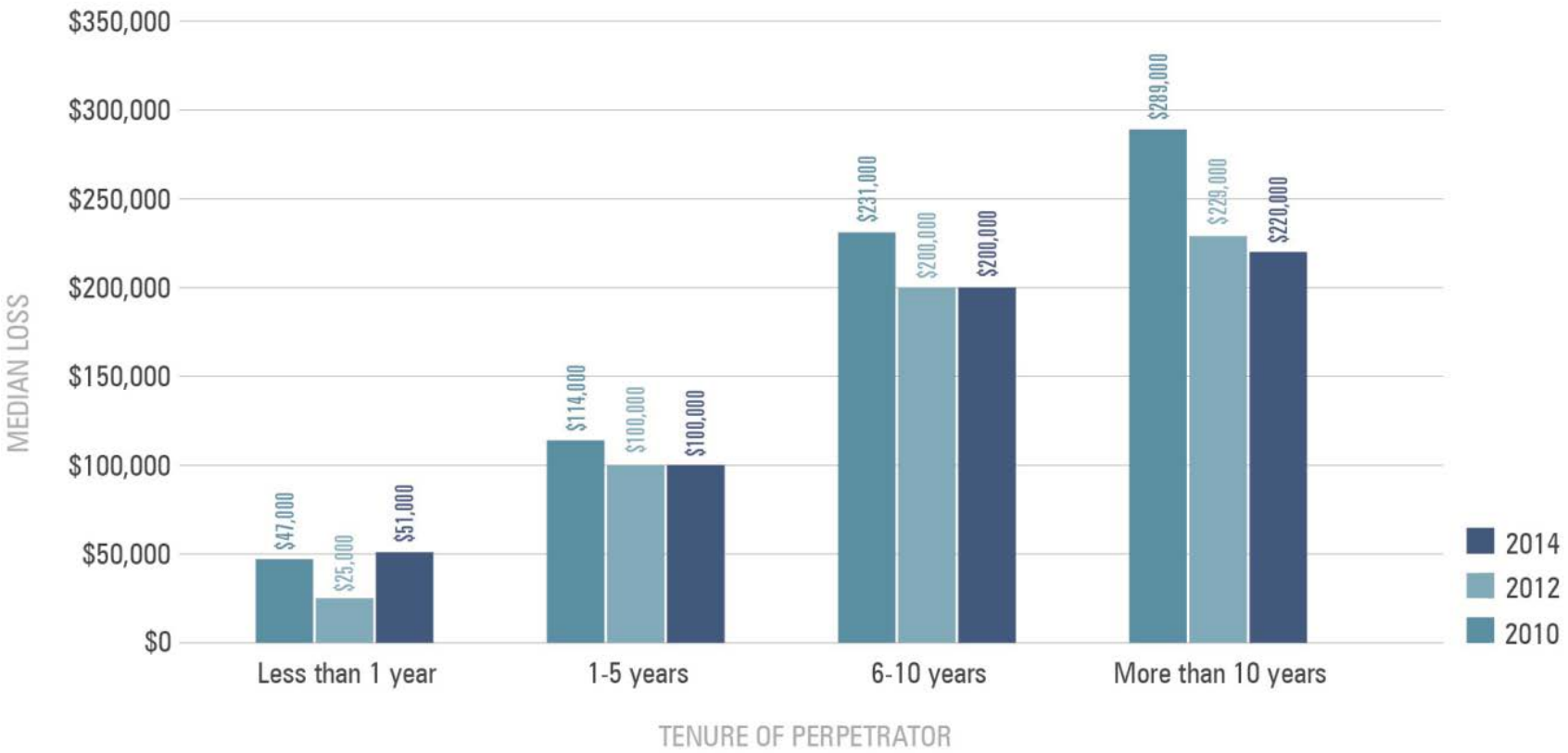
*"Other" category was not included in the 2010 Report.

Escalation Fraud Theory



More Fraud Statistics

Figure 64: Tenure of Perpetrator — Median Loss



Fraud Opportunity

When an organization's primary focus is on cost reduction and speed/convenience of conducting business, an environment conducive for fraud may arise due to the combining of sensitive responsibilities and authorities within job functions.

Employee's years of service

X

Number of key responsibilities residing with the employee

X

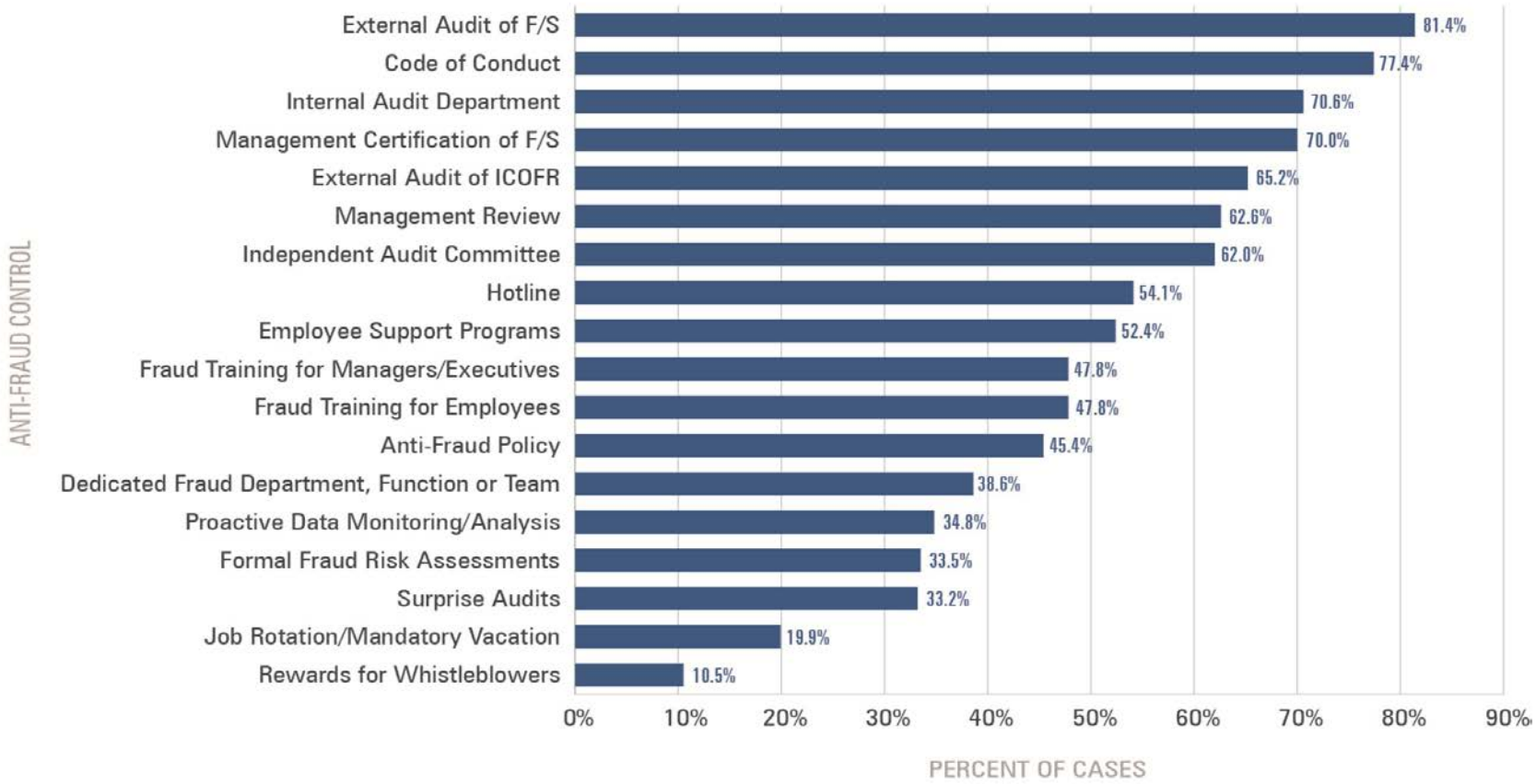
Organization's complacency level with respect to validating controls and monitoring activities

=

Potential for fraud to be committed

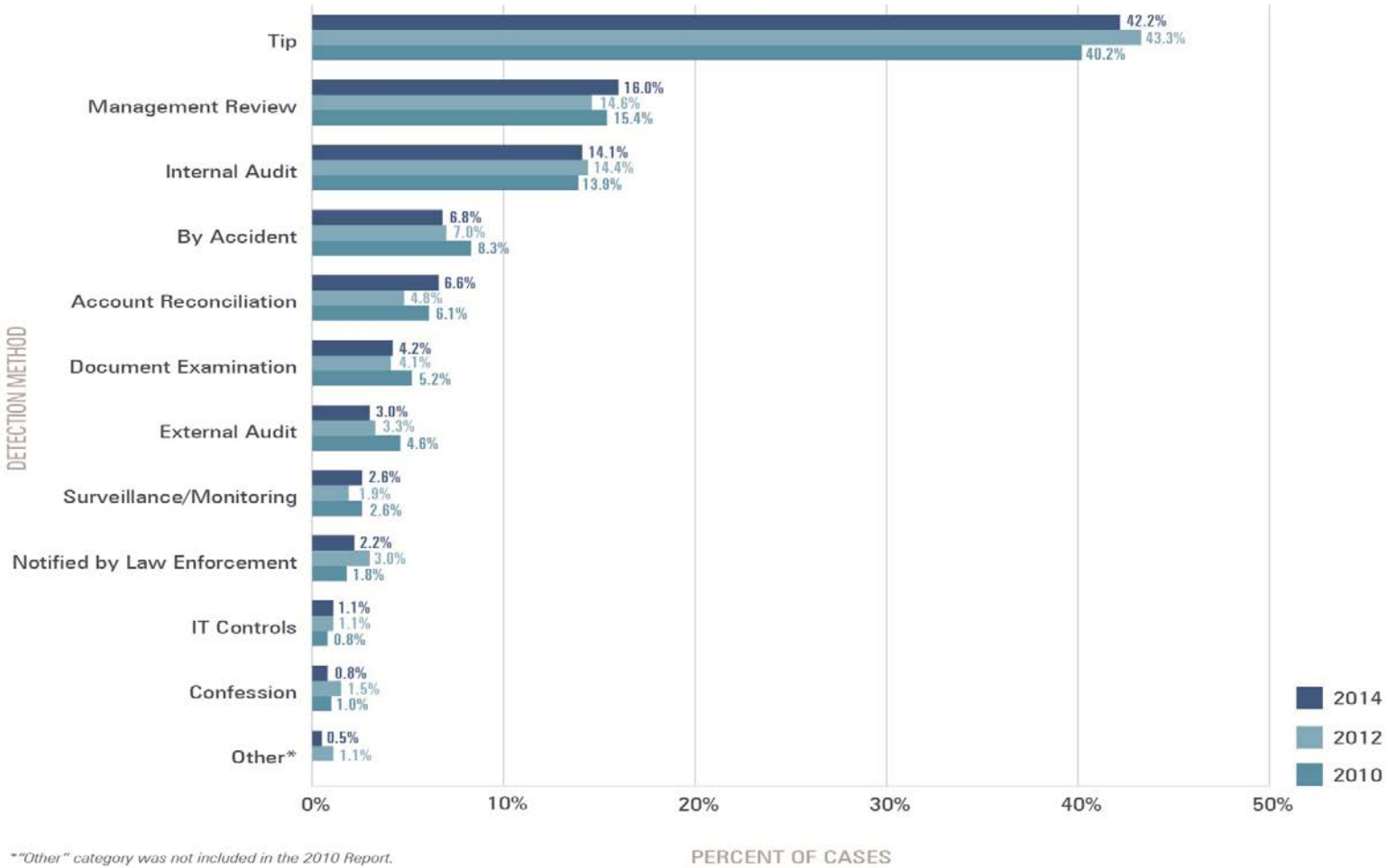
Anti-Fraud Controls

Figure 26: Frequency of Anti-Fraud Controls



Detecting Fraud

Figure 11: Initial Detection of Occupational Frauds



*"Other" category was not included in the 2010 Report.

ACFE 2014 REPORT TO THE NATIONS

SEC/IRS/DOJ Whistleblower Programs

- The Securities and Exchange Commission announced an expected award of more than **$30 million** to a whistleblower who provided key original information that led to a successful SEC enforcement action.

- The Securities and Exchange Commission announced a whistleblower award of more than $300,000 to a company **employee who performed audit and compliance functions** and reported wrongdoing to the SEC after the company failed to take action when the employee reported it internally.

- Former UBS **AG banker who went to prison** after telling the Internal Revenue Service how the bank helped thousands of Americans evade taxes, secured a whistleblower award of $104 million, the largest individual federal payout in U.S. history.

- **The Department of Justice has paid nearly $3 billion in rewards to everyday citizens for reporting fraud. The average reward is $1.5 million.**

Importance of a Whistleblower Program

It's better for a company to promote and encourage employees to report matters through an internal whistleblower hotline than to face the uncertainty associated with inquires from the SEC, IRS, DOJ or other government agency responding to anonymous complaints received through the agency's hotline.

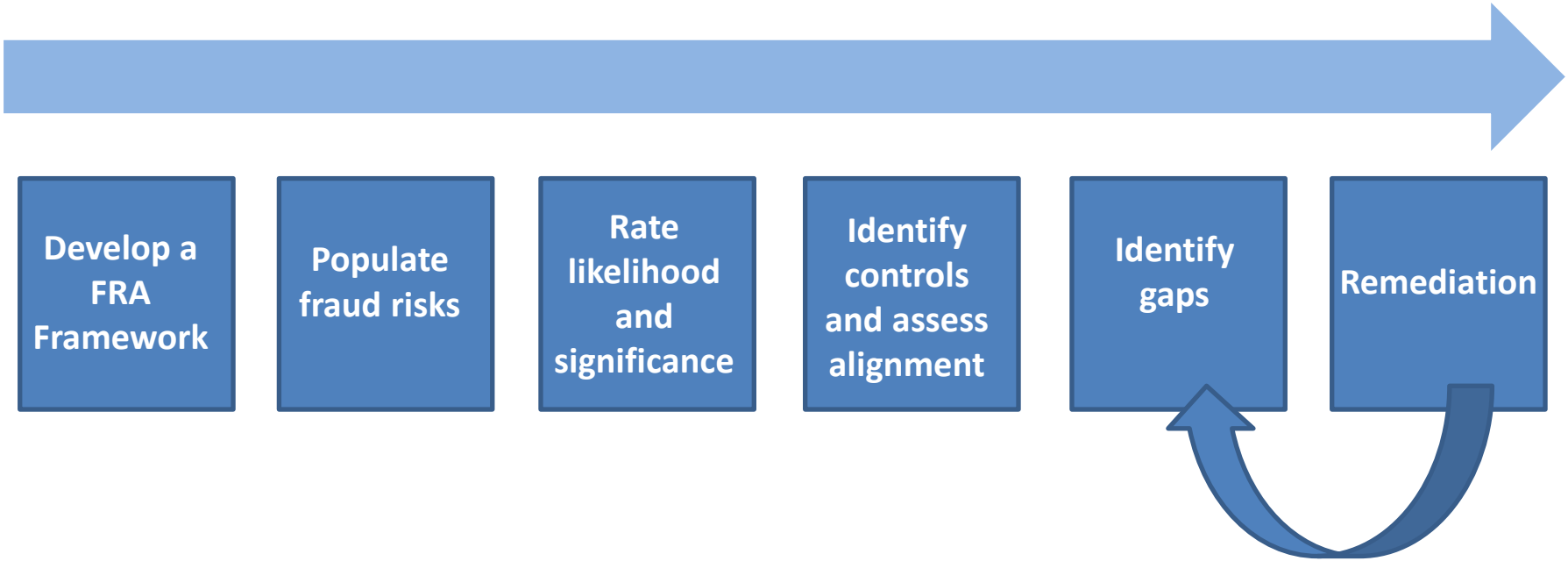
Fraud Types

Fraudulent Financial Reporting	**Misappropriation of Assets**	**Corruption**
• Revenues • Expenses • Improper valuation or misclassification	• Cash theft • Fraudulent disbursements • Payroll fraud • Expense reimbursement • Capital assets/inventory	• Bribery • Bid rigging/Kickbacks • Illegal payments • Conflicts of interest • Aiding and abetting fraud (money laundering)
Almost always material - directly impacts the financials	May or may not be material - directly impacts financials	May or may not be material - indirectly impacts the financials
Almost always involves senior management	Can involve any level of employee	Can involve any level of employee
Controls are less effective in preventing and detecting fraud	Controls can be effective, particularly with regard to those below top management	Controls can be difficult and expensive to implement. Requires close scrutiny of employee activities and cost to do business

Fraud Types (cont.)

Theft of Sensitive Data	**Defrauding Customers**	**Compliance**
• Customer and employee personal information • Proprietary information/trade secrets • Patents, copyrights, other legally protected intellectual property	• Intentionally misrepresenting products and services • Inflating invoices/ duplicate billings • Shorting orders/product	• Undocumented employees • Unrecorded wages • Unreported accidents • Manipulation of data • Unfair, deceptive acts
May or may not be material /measurable – indirectly impacts the financials	May or may not be material - directly impacts financials	May or may not be material – indirectly impacts the financials
Can involve any level of employee	Can involve any level of employee	Can involve any level of employee
Controls can be difficult and expensive to implement	Controls can be effective, particularly with regard to those below top management	Controls can be effective at all levels

Fraud Risk Assessment

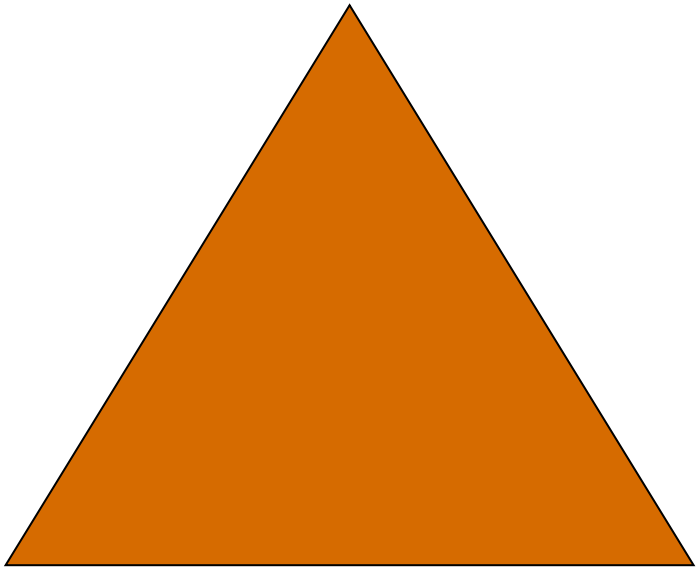


Fraud Triangle

The fraud triangle is a common pictorial of the three factors that drive fraud.

Rationalization

(Justification of Act)



Opportunity

(Process and Controls)

Need/Pressure/ Motivation

(Influences /Incentives)

Fraud Diamond

The fraud diamond consists of four factors that drive fraud.

Incentive

(Influences /Motivation)

Rationalization

(Justification of Act)

Opportunity

(Process and Controls)

Capability

(Competency to execute)

Controlling Fraud Risk

- An organization **CANNOT** control individuals'
  - Needs/pressures/motivations/incentives
  - Rationalization

- However, an organization **CAN** control:
  - Opportunities for fraud to be perpetrated
  - Having the necessary controls and monitoring activities to effectively limit and/or remove opportunities

CYBERSECURITY

- NIST definition:
  - "The process of protecting information by preventing, detecting and responding to attacks."
  - **Key: PROTECTING INFORMATION ---------->**
- Threats not limited to Internet hackers
  - Social engineering
  - Phishing
  - Disgruntled employees
  - Human error

- **Theft**
- **Misuse**
- **Manipulation**
- **Damage**
- **Loss**

Why is Cybersecurity Important?

CSO

Most read:

skyhigh — Cloud Adoption & Risk Report Reveals Top 20 Cloud Services

Home > Data Protection > Malware/Cybercrime

SALTED HASH-TOP SECURITY NEWS

By Steve Ragan | Follow

About — Fundamental security insight to help you minimize risk and protect your organization

NEWS

Ransomware attack knocks TV station off air

Data Breach TODAY

Prevention. Response. Notification.

Response | Breaches | Forensics | Governance | ID Theft | Prepare

News | Blogs | Interviews | Webinars | White Papers | Memberships | Resources | Events

Home > Blogs

The Expert's View

Insights from industry experts, consultants and practitioners

Breaches: Retailers Aren't Doing Enough

Banks Need Congressional Support for Stronger Data Security

By Dennis Koons, October 13, 2014.

NEWS | VIDEO | WEATHER | SPORTS | TV | COMMUNI

New Mexico hospital sued over patient data breach

Posted: Oct 12, 2014 1:12 PM EDT
Updated: Oct 12, 2014 1:12 PM EDT

LAS VEGAS, N.M. (AP) - A New Mexico woman is suing a hospital and its parent company, saying their negligence led to hackers obtaining personal information belonging to her and more than 4 million other patients.

DALLAS BUSINESS JOURNAL

News | People | Events | Jobs | Resources | Store

Home Depot now facing 21 class-action lawsuits over data breach

Oct 13, 2014, 3:44pm CDT

REUTERS

HOME | BUSINESS | MARKETS | WORLD | POLITICS | TECH | OPINION

Sears says Kmart stores hit by data breach

North Dakota University System Suffers Third IT Security Breach This Year

TRENDING: CSO Daily Dashboard · Social Engineering · InfoSec Careers · Mobile Security · CSO Events · Resources/White Pape

CSO

Most read:

Home > Data Protection > Data Breach

BRICK OF ENLIGHTENMENT

By Dave Lewis | Follow

About — Bringing fire to the village.

NEWS

Touchstone Medical Imaging reveals data breach

THE WALL STREET JOURNAL. | MARKETS

$12 for 12 Weeks — SUBSCRIBE NOW

TOP STORIES IN MARKETS

1 of 12 — CSX Deal Hopes Could Run Off the Rails

2 of 12 — Weichai Power Can't Keep On Truckin'

3 of 12 — Macau Gamblers Find Best Odds with SJM

Big Banks Look to Get B

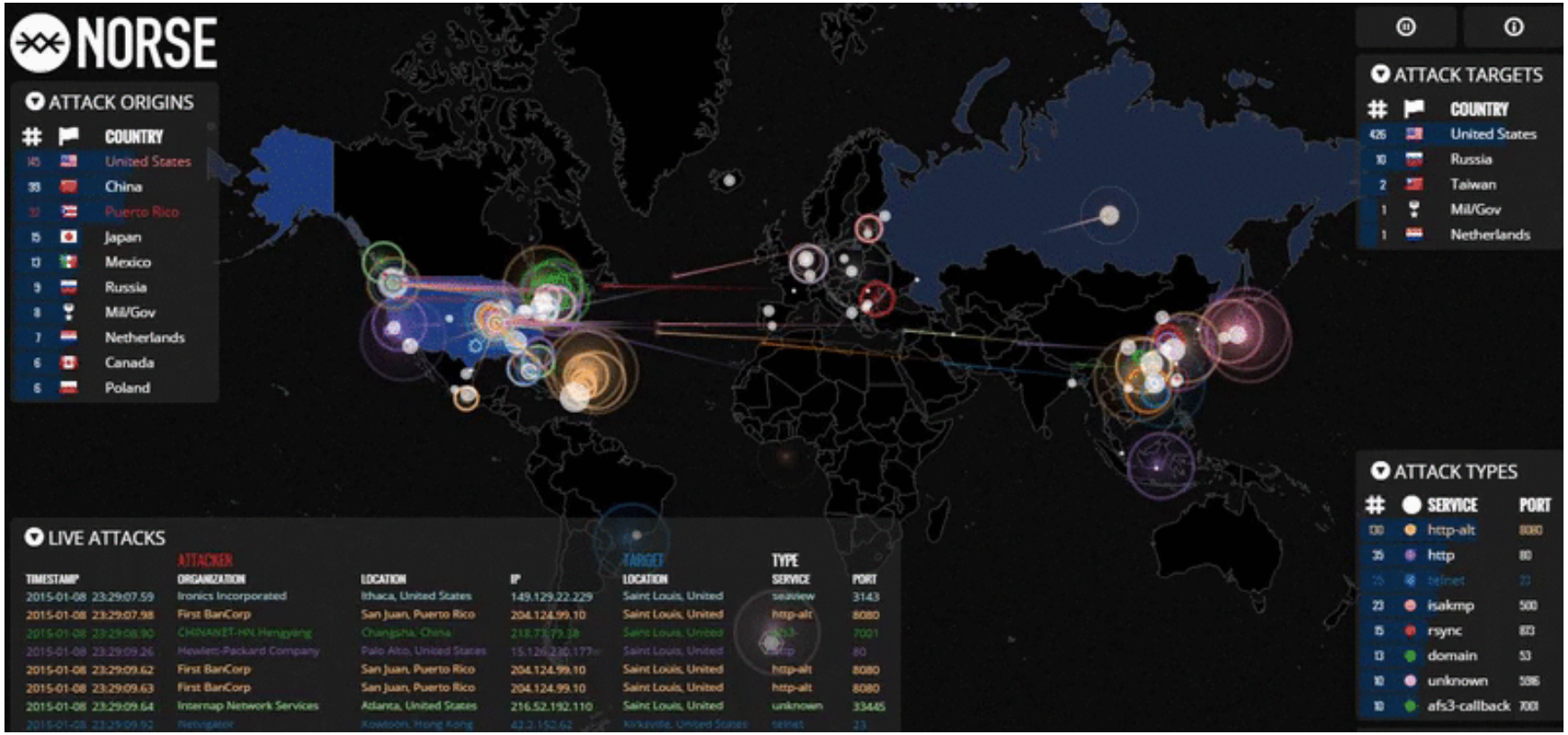
Subscriber Content Read Preview

MARKETS

J.P. Morgan Says About 76 Million Households Affected By Cyber Breach

Bank, in Update on Previously Disclosed Data Breach, Says Hackers Got Contact Information But Not Logins

Cyber Crime is Global



Source: http://map.ipviking.com

Cyber Criminal Actors and Their Motivation

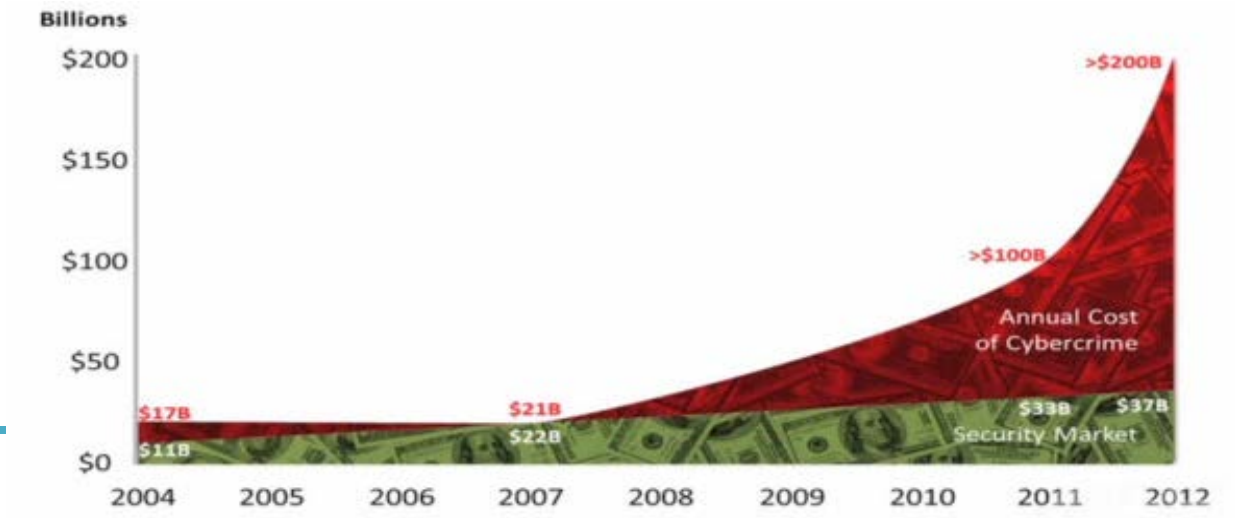
- Individuals - Test/demonstrate ability
- Activists - Promoting ideology
- Organized Crime - Financial gain
- Governments - Espionage

What Cyber Criminals Steal – And Why

- Bank Credentials (e.g., online banking, PIN numbers)
  - Theft of funds
- Personally Identifiable Information (PII)
  - Identity theft
- Debit/credit card data
  - Access to credit, sale of data, identity theft
- Email addresses
  - Sale of data, phishing operations
- Intellectual property and confidential information
  - Blackmail, sale of data, avoid paying IP royalties, sabotage, espionage

Cyber Crime Proliferation

- Cyber crime now costs the global economy $445 billion a year
  - Source: Center for Strategic and International Studies
- The cyber crime black market is now more profitable than the global drug trade
  - Source: RAND Institute
- Cyber crime costs are now drastically eclipsing cybersecurity costs
  - Source: OECD



Basic Types of Attacks

- Two basic types:
  - Targeted
  - Opportunistic
- Targeted attacks up 91% in 2013 (source: ISACA)
- Opportunistic attacks still account for 75% (source: Verizon)
  - 78% of exploits utilize vulnerabilities less than two years old (source: ISACA)
  - Zero-day attacks attempt to exploit previously unknown vulnerabilities that do not have a patch

Sophisticated Attacks Involving Organized Crime

- **Programmers:** Write/code the viruses that infect a business' computer network.
- **Carders:** Specialists distribute and sell stolen credit and debit card data.
- **Hackers:** These intruders break into a company's PC networks via their vulnerabilities.
- **Social engineers:** Concoct ingenious schemes to trick people into giving up personal information or visit websites that download viruses. These players represent the creative end of the crime ring.
- **Rogue systems providers:** Run scrupulous businesses that provide servers for cyber thieves.
- **Money mules:** These individuals purchase things at retailers using stolen credit cards. Some launder money while others ship products.
- **Bosses:** The head honchos of a crime ring, who hire the worker bees but rake in all the money.

Source: 11 Ways to Protect Your Business From Cyber Criminals, Entrepreneur Magazine, http://www.entrepreneur.com/article/238369

Five Largest Confirmed Data Breaches 2013-2014

1. JP Morgan Chase – 76 million records
2. Target – 70 million records
3. The Home Depot – 56 million records
4. Michael's – 3 million credit cards
5. Neiman Marcus – 1.1 million credit cards

Source: Credit Union Times

Other Recent Attacks

- **Sony attack ----------->**
- iCloud celebrity photo hack
- German steel plant (company undisclosed)
- White House computer network
- US Central Command Twitter Account
- Anthem

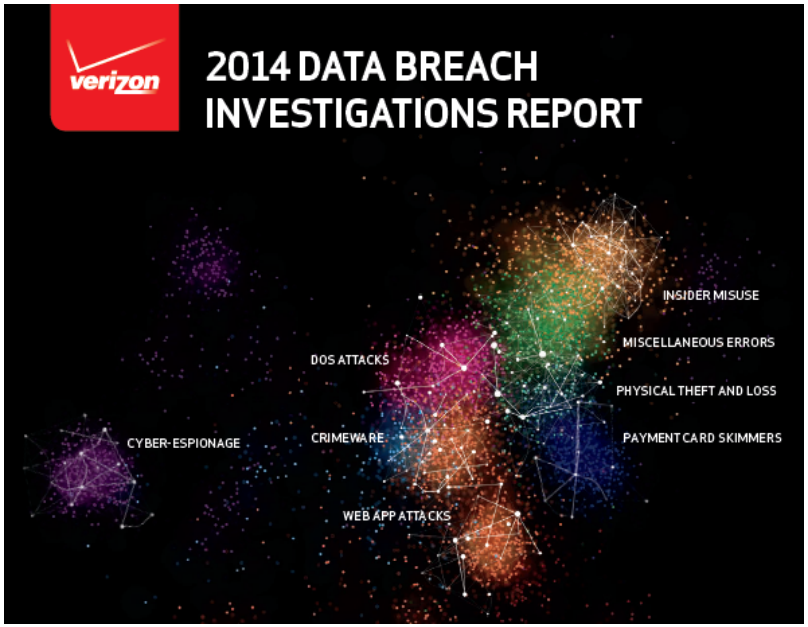
Other Notable Data Breaches in US History

- **2013** Adobe Systems – 130 million customers
- **2011** Sony – 77 million customers
- **2008** Heartland Payment Systems – 130 million customers
- **2007** TJX Companies – 94 million customers (46 million credit card)
- **1984** TRW/Sears – 90 million customers

Source: CNN Money

State of Cybersecurity - Verizon Data Breach Report

- Published Every Year Since 2008
- 50 Global Organizations
- 95 Countries Represented
- 1,367 Confirmed Breaches
- 63,437 Security Incidents

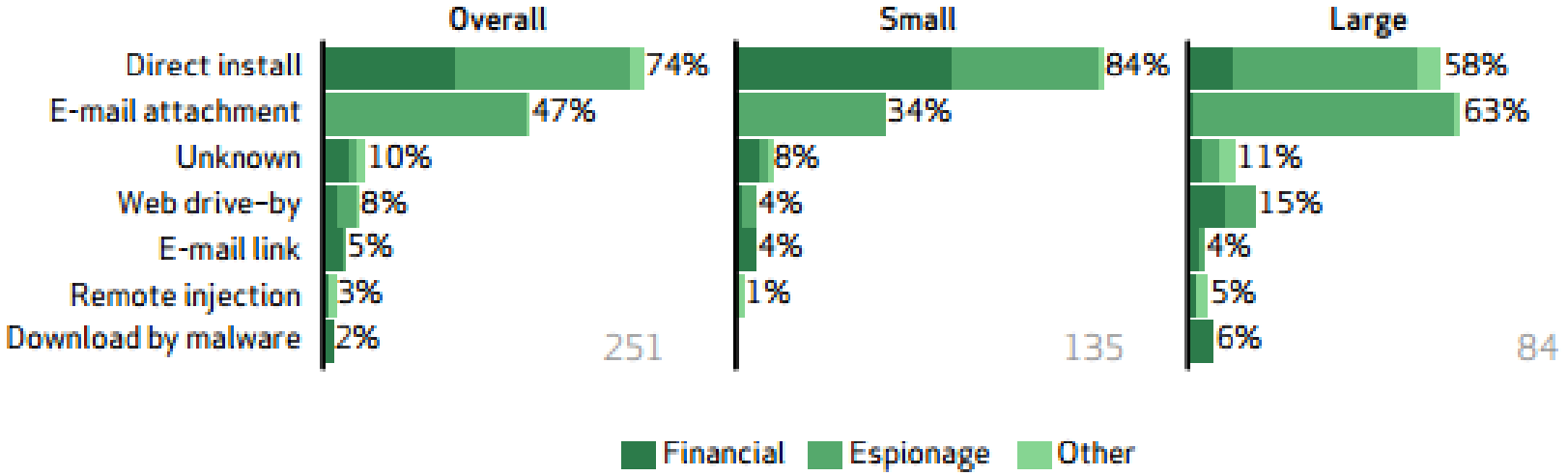


Verizon Data Breach Report – Biggest Takeaways

- Employees at core of most attacks
  - **Stolen credentials is the primary cause 80% of time**
  - 78% of intrusions are "relatively easy"
- Social engineering is the most common attack vector
- 92% of breaches came from outside the organization
  - 55% from organized crime
  - 19% affiliated with other state agencies
- 69% discovered by external parties
- 66% took months or more to discover

Verizon Data Breach Report – Malware Sources

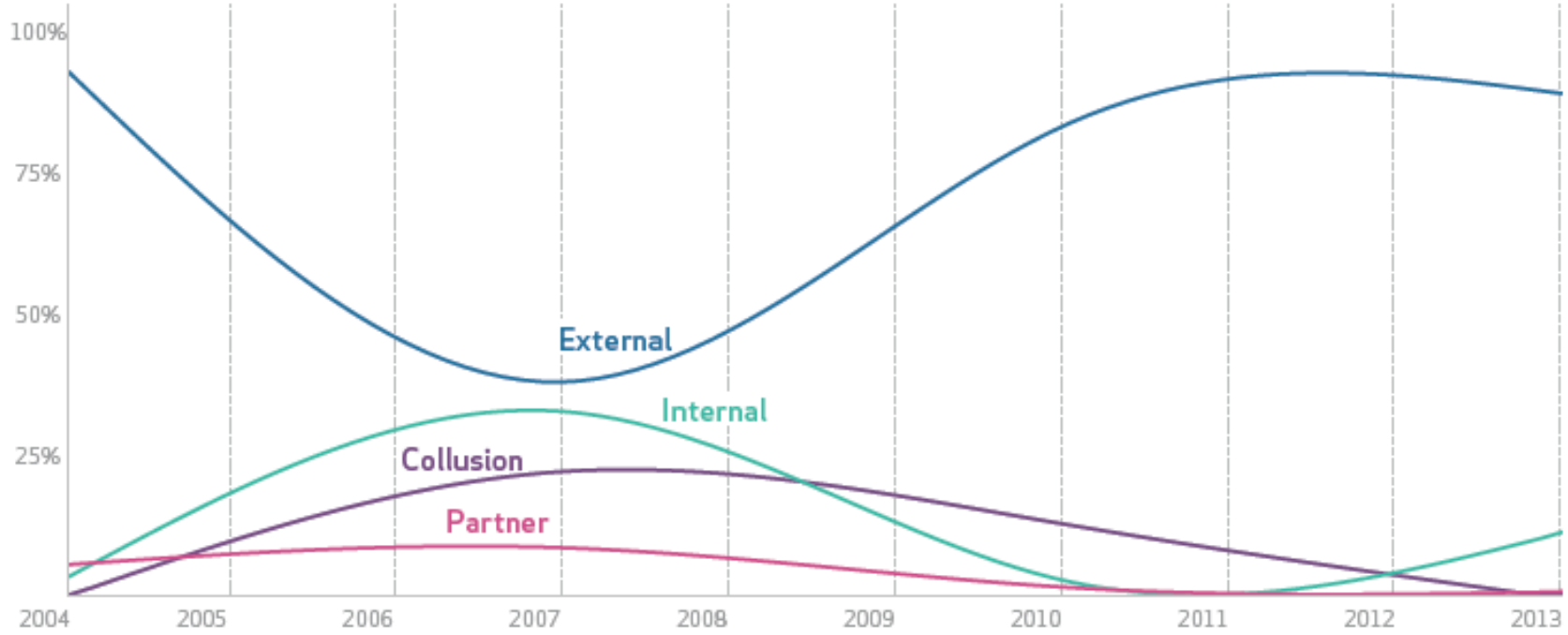
Figure 20: Vector for malware actions



Verizon Data Breach Report – Industry Dispersion

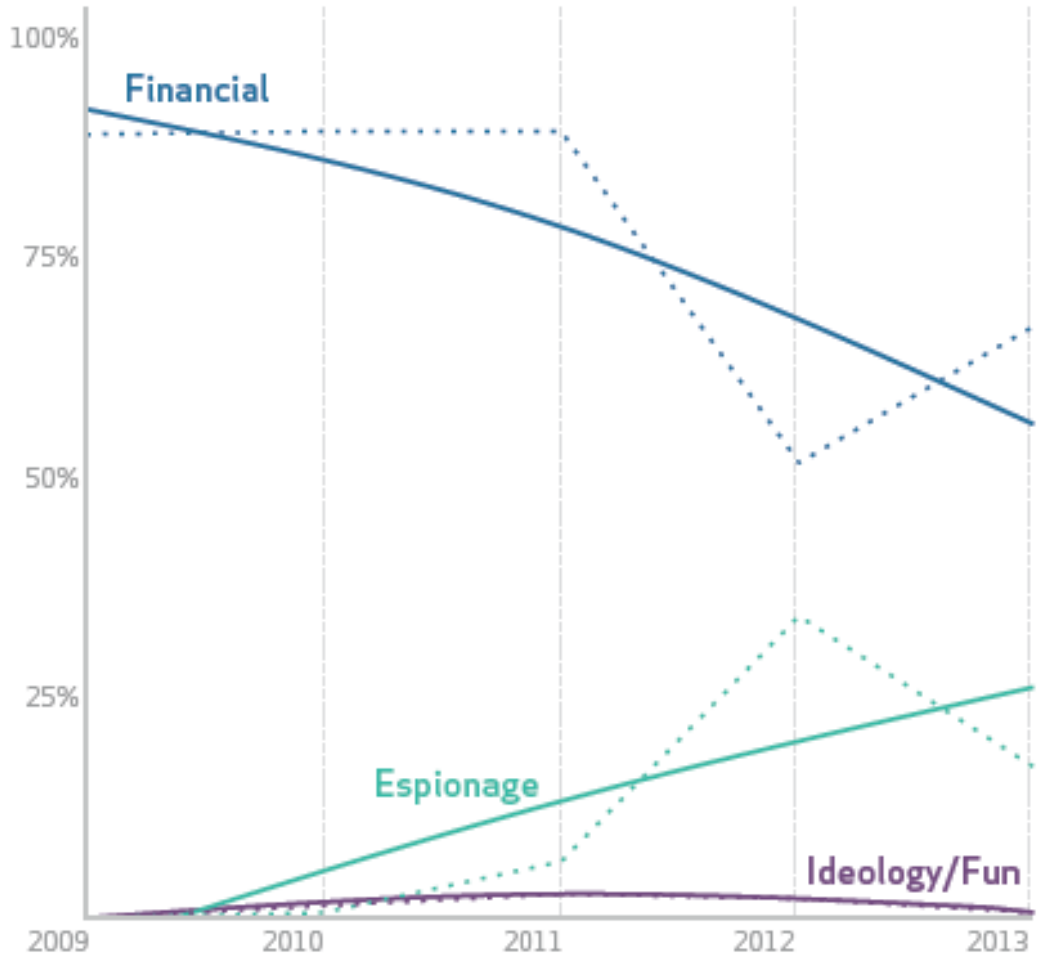
Industry	Total	Small	Large	Unknown
Accomodation	137	113	21	3
Finance	465	24	36	405
Manufacturing	59	6	12	41
Professional	75	13	5	57
Public	175	16	26	133
Retail	148	35	11	102
Utilities	80	2	-	78
Other	228	34	33	161
Total	**1,367**	**243**	**144**	**980**

Percent of Breaches by Threat Actor Over Time



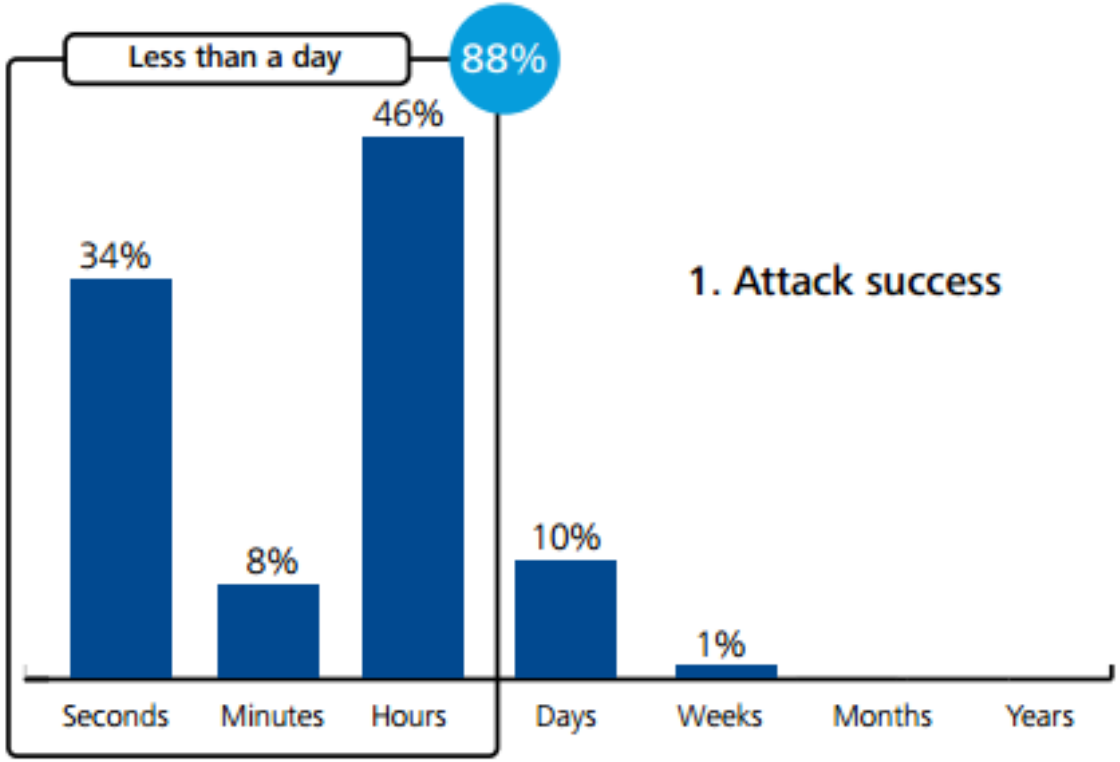
Source: Verizon Data Breach Report

Percent of Breaches By Motive Over Time



Source: Verizon Data Breach Report

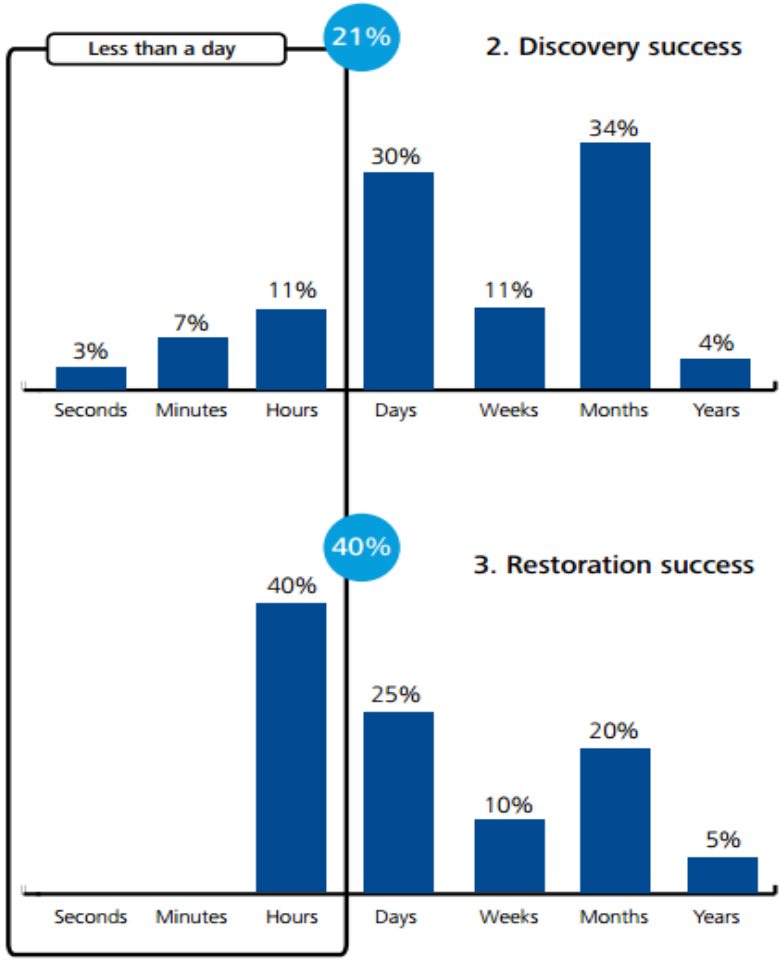
Attackers Time to Exploit Vulnerability versus…



Source: Verizon Data Breach Report

38

…Organization's Ability to Defend



Targeted attacks are the most difficult to detect: 225 days on average

Source: Verizon Data Breach Report

Target Breach

How the Hackers Broke In

1. They probably used credentials of an HVAC vendor to get into Target's network, spending weeks on reconnaissance to install a pair of malware programs.

2. The hackers sent credit card number-stealing malware to cashier stations in all domestic Target stores.

3. They also installed malicious code that sent card data to three hijacked "staging point" servers in the U.S. before the data headed to Moscow.

4. On Dec. 2, the credit card numbers started flowing out. Target's security system detected the hack, but the company failed to act.

5. Federal investigators warned Target of a massive data breach on Dec. 12.

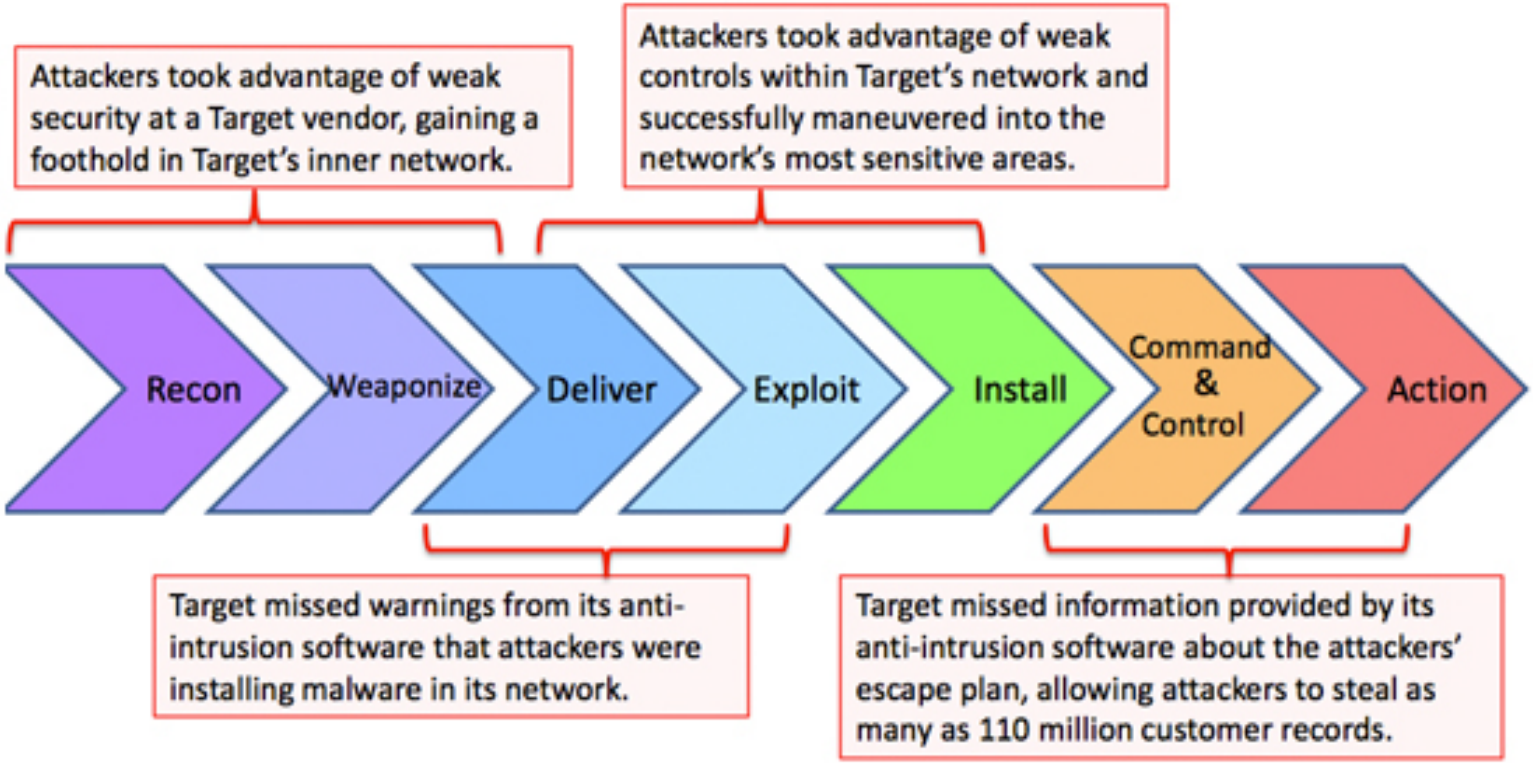
6. Target confirmed and eradicated the malware on Dec. 15, after 40 million credit card numbers had been stolen.

DATA COMPILED BY BLOOMBERG; GRAPHIC BY BLOOMBERG BUSINESSWEEK

Target Response to Hack

- Target had already deployed $1.6 million malware detection tool (FireEye)
  - Round-the-clock monitoring from security specialists in Bangalore
- **November 30, 2013:** FireEye detects loading of exfiltration software
  - Target security team in Minneapolis notified
  - No action taken
- **Mid-December:** Security experts monitoring underground markets for stolen data detect a large influx of credit card information
  - US Department of Justice notified
- **December 12:** Target was notified by the Department of Justice of a potential breach
- **December 15:** Target confirms breach
- **December 19:** Target releases public statement confirming the breach
- **March 5, 2014:** Target CIO Beth Jacob resigns

Target Control Failures



Social Engineering Risks

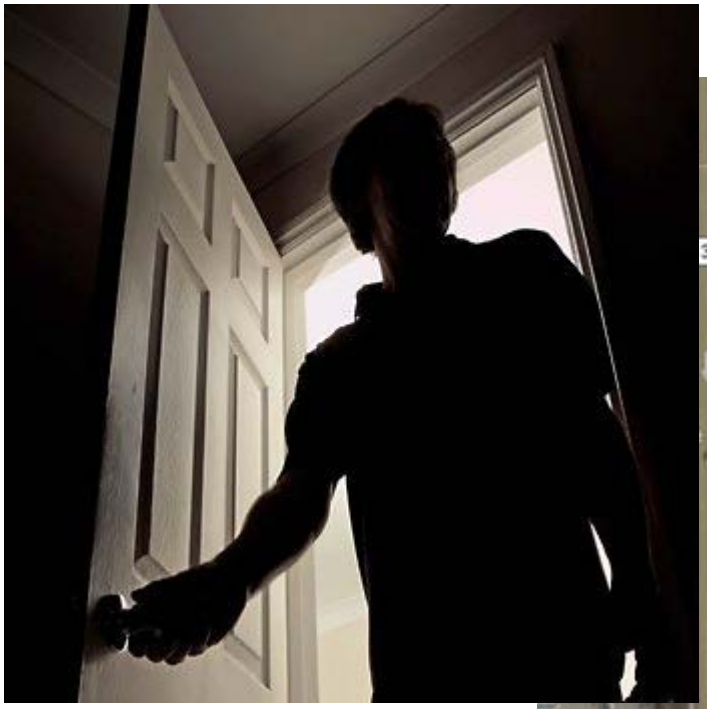
- **What is Social Engineering?**
  - **Exploiting human weaknesses** to gain unauthorized access to facilities and/or systems
- **Examples**
  - Phishing
  - Phone solicitation
  - In-person solicitation
  - Tailgating
  - Dumpster diving
  - Media Dropping

Social Engineering Example - Solicitation Attempts (“Pretexting”)

Social Engineering Example- Media Dropping

- **Media with pre-loaded malware left in conspicuous locations, such as a parking lot or waiting area**

Social Engineering Example - Tailgating

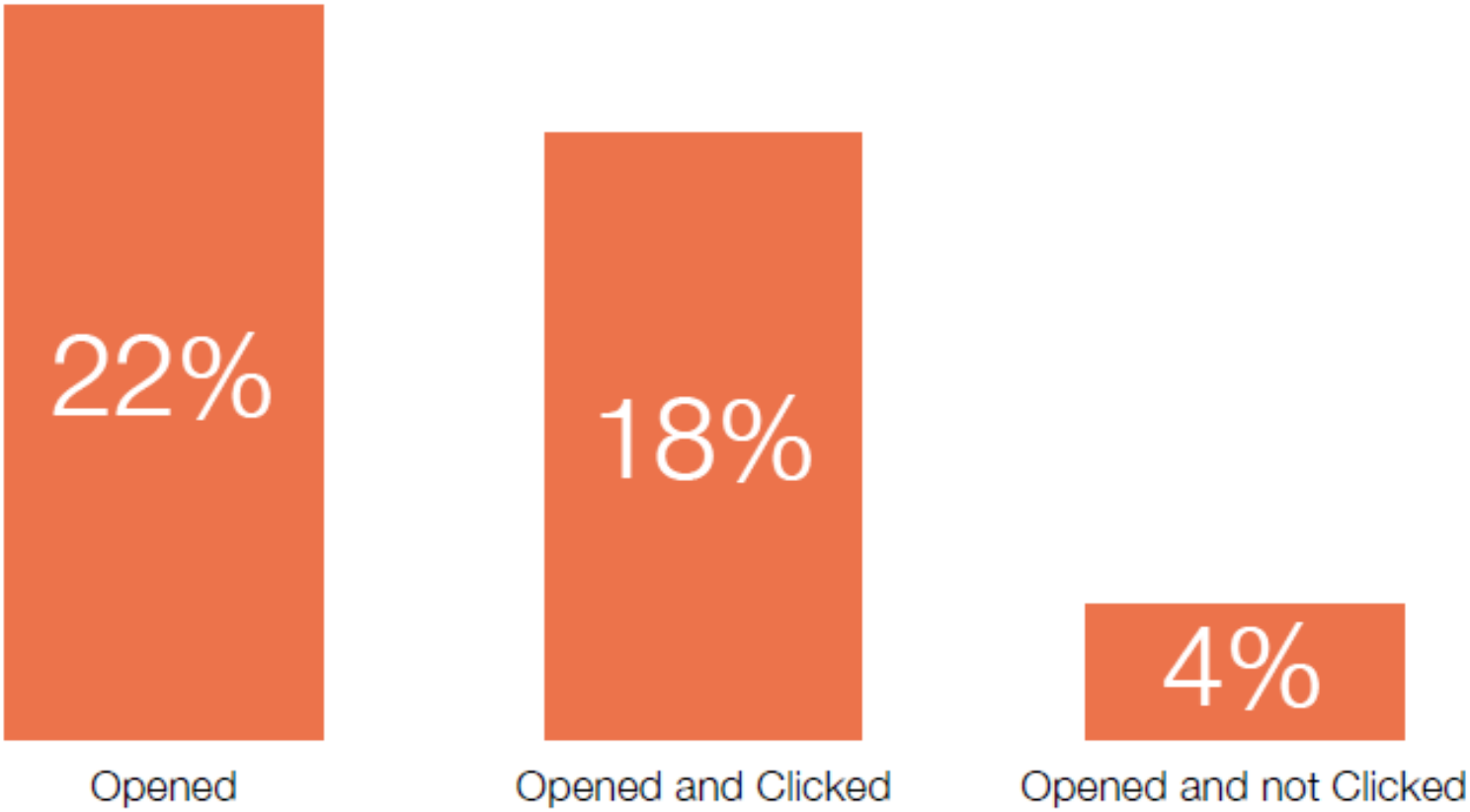


Social Engineering Example - Dumpster Diving

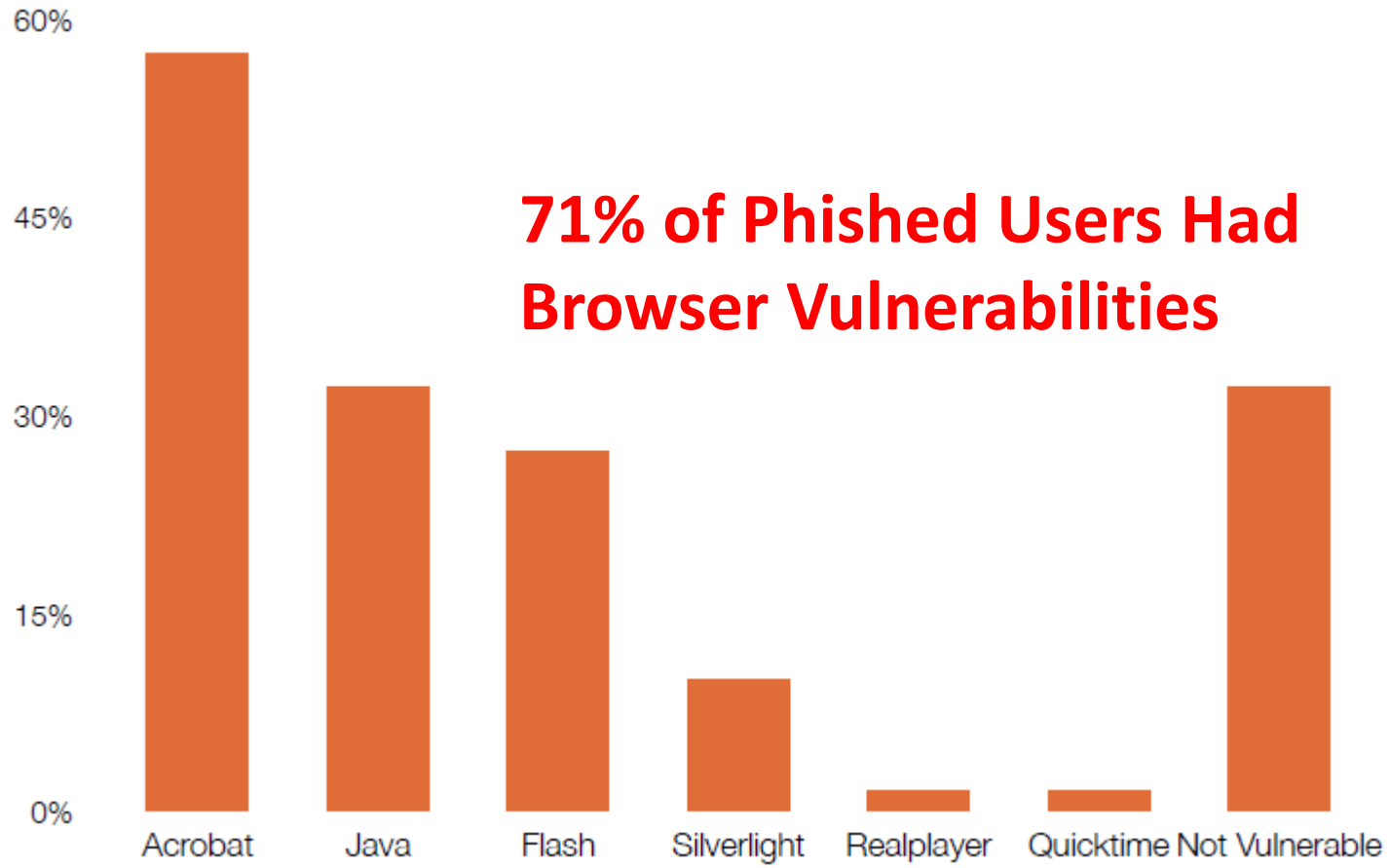
Social Engineering - Phishing Attacks

- **Phishing:** Attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- **Spear phishing:** Phishing attempts directed at specific individuals or companies, using personal information about their target to increase probability of success
- **Whaling:** Attacks directed specifically at senior executives and other high profile targets within the businesses
- **Clone Phishing:** A legitimate email with an attachment/link is used to create an almost identical email with a malicious attachment or link
- **Phone/Voice Phishing (Vishing):** Voice messages claiming to be from a bank tell users to dial a fake phone number regarding problems with their bank accounts. Users are then prompted to enter account numbers, PIN, SSN, etc.

ThreatSim – Phishing Simulation Response Rates



ThreatSim – End-User Browser Vulnerabilities



71% of Phished Users Had Browser Vulnerabilities

Schneider Downs Phishing Simulation Results

I've shared Survey Questions.docx
Click to open:
Survey Questions.docx

Online Docs makes it easy to create, store and share online documents, spreadsheets and presentations.

This email has been scanned by the Symantec Email Se
For more information please visit http://www.symantec

Your account is suspended.

Your NetworkMeet account has been suspended due to unauthorized or illegal access.

And for your security, we recommend you to connect and resolve your problem before that your WebEx account will be blocked from our NetworkMeet services.

Sign in

Sign in to re-enable your account.

Delivering the power of collaboration,
NetworkMeet Team

ACT-L-001

15% Overall Response Rate

Malware / Crimeware – Common Types

- **C2 (Command & Control):** Gets workstation to do whatever it wants (e.g., botnet)
- **Spyware / Keylogger**: Watches your every move; captures login credentials
- **Downloader:** Gives ability to download other (more evil) malware onto your PC
- **Spam:** Turns your PC into a mail forwarder, sending thousands (or millions) of spam messages without your knowledge
- **Client-side Attack:** Attacks the human first (phishing, weak passwords), then invades the client machine
- **Backdoor:** Developers leave "trap doors" open for easier development/testing; can also be used for nefarious purposes
- **DoS (Denial of Service):** Prevent use entirely (e.g., ransomware)
- **Adware:** Hijacks browser to display advertisements (e.g., pop-ups)
- **Export Data:** Grabs files and uploads to FTP server without your knowledge
- **Ransomware**: Locks computer until a fee is paid for the unlocking code

Malware Example: Keyware and Screen Captures

Malware Example: Ransomware

By the way, we got hit by a ransomware virus that encrypted 5 of our servers. The user clicked on a facebook email requesting a password change. She clicked on it 3pm Sunday and we worked all night and were 90% up by Monday 8am. Was not a good time. Several other firms in the area just recently got hit. Some twice.

What is a privacy incident going to cost me?

- **Summary of Ponemon Institute's 2012 Annual Cost of a Data Breach Report:**
  - Average cost and per record cost declined for the first time but remain significant, $5.5 million and $194, respectively.
  - Direct costs are estimated at $59 per record. (legal counsel, notification letters, credit monitoring, etc.) The primary driver is legal defense costs.

Cost by industry class	Per record
Average	$194
Education	$112
Retail	$185
Healthcare	$301
Financial Institutions	$353

Is Your Organization Prepared?

Source: IIA Tone at the Top; April 2014

Most Common Cybersecurity Mistakes

- Belief that it is only IS's responsibility
- Not understanding your IS footprint
- Belief that your organization would not be targeted
- Not planning for the inevitable
- Lack of detective monitoring
- Overreliance on third-party technology
- Belief that 100% security is attainable
- Overreliance on traditional preventive measures…

Traditional Preventive Approach to Network Security

Firewall / DMZ	Anti-Virus / Anti-Malware
Vulnerability Scan	Compliance & IT Audits

Three Primary Cybersecurity Capability Measures

1 PREVENT

2 DETECT

3 RESPOND

Steps for Securing Your Environment

1. Define roles and responsibilities
2. Adopt a framework
3. Understand your environment
4. Assess risk
5. Establish and implement controls and technology
6. Evaluate effectiveness
7. Identify, prioritize and remediate gaps
8. Monitor/refresh

Step 1: Assign Roles and Responsibilities

1. Management's Role in Combatting Threats

- Create and reinforce the perception/understanding of cybersecurity threats
  - **Set tone at the top**
  - Establish, support and communicate security policies
  - Establish awareness that controls and processes have been specifically designed to prevent attacks
    - New hire orientation
    - Ongoing awareness and communication
    - Visible to the organization

1. Information Security's Role in Combatting Threats

- **Design and implement a security plan**
- Respond to threats
- Maintain vigilance and a level of knowledge
- Identify, understand and respond to changes in the operating environment
- Provide timely, accurate and complete information to assessors

1. Audit's Role in Combatting Cyber Threats

- Assess/evaluate the functioning of the plan's components
- Communicate findings and monitor remediation activities
- **Build advisory relationship with Information Security**
- Do not impair objectivity or independence
- Go beyond processes (IT-intensive)
- Frequent collaboration and interaction with IT
- Maintain a level of diligence and knowledge about cybersecurity

1. Employee's Role in Combatting Threats

- Be diligent – Always Assume the Worst
- **Understand and Follow Policies and Procedures**
- Report Suspicious Activity
- Avoid Malicious Web Sites
- **Don't Open Suspicious E-mails**
- Ask for Identification
- Require Authorization for Access
- Safeguard Social Media Content
- Educate/Inform Customers
- **Avoid Untrusted WiFi**

Step 2: Adopt a Framework

2. Adopt a Framework

- **ISO 27000 Series**
- Department of Energy
  - Cybersecurity Capability Maturity Model (C2M2)
    - Electronic Subsector (ES-C2M2)
    - Oil and Gas Subsector (ONG-C2M2)
- **National Institute of Standards and Technology (NIST)**
  - Cybersecurity Framework
  - Roadmap for Improving Critical Infrastructure Cybersecurity
- National Initiative for Cybersecurity Education (NICE)
  - Capability Maturity Model (CMM)
- ISACA - Transforming Cybersecurity Using COBIT 5

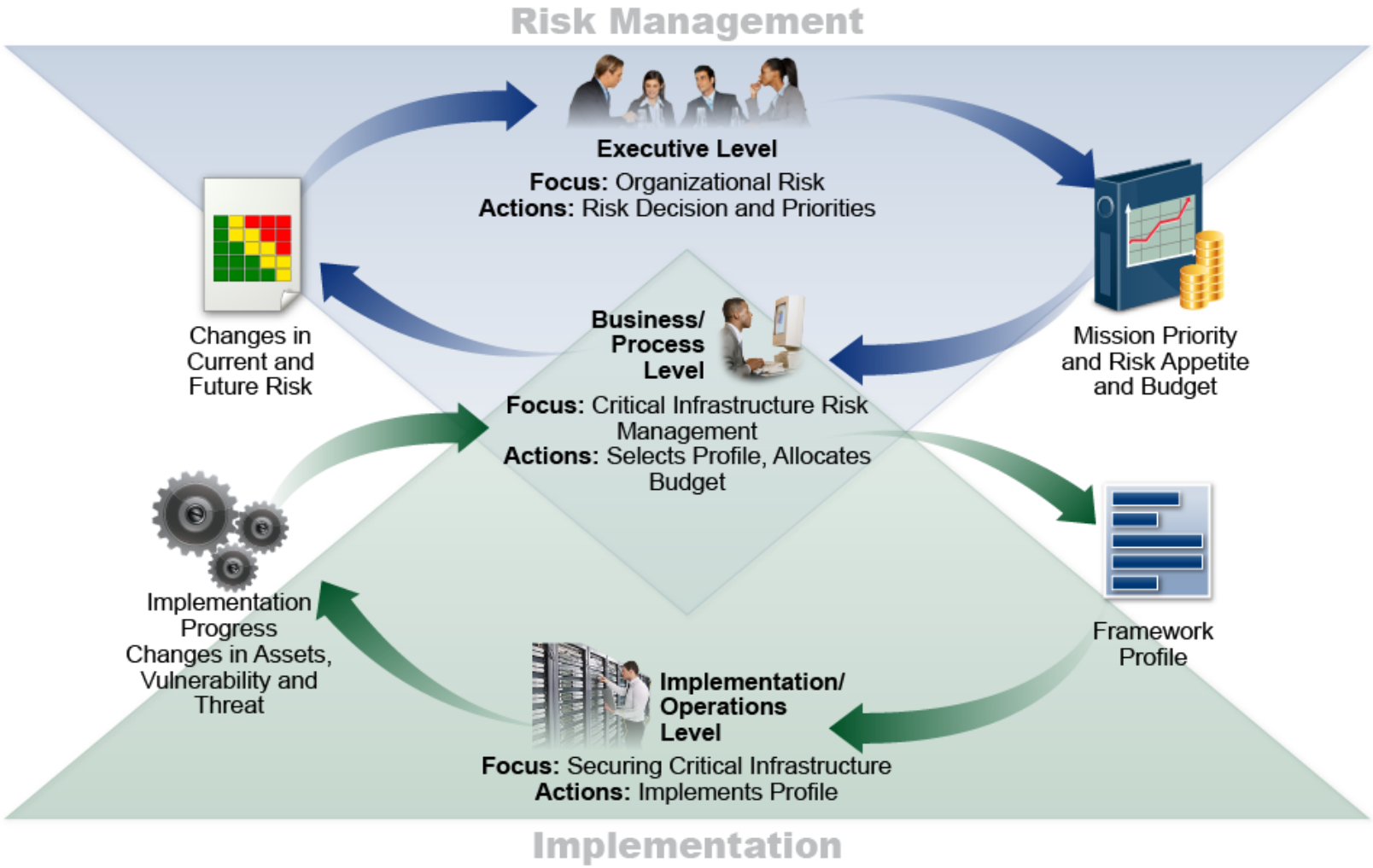
2. Framework Example – NIST Cybersecurity

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

2. NIST Cybersecurity Framework Objectives

- Describe your current cybersecurity posture;.
- Describe your target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.

2. NIST Framework Communication



2. NIST Framework Core Categories

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

Step 3: Understand the Environment

3. Understand the Environment

- **Operating environment**
- Hardware type and location
- **Applications**
- **Databases**
- File systems
- **Security**
- Network architecture
- **Third-parties**
- Middleware

3. Start with Asset Identification

- Asset Classification
  - Location
  - Owner
  - Usage
  - Type
  - Status
  - Risk level
- Identify all assets
  - Databases
  - Files
  - Servers
  - Applications
  - Hardware
  - Web sites

3. Inventory and Classify Your Data

- Restricted Data
  - Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk.
  - Examples: Credit cards numbers, social security numbers
- Private Data
  - Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk.
  - Examples: Addresses, names of employees
- Public Data
  - Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk.

Step 4: Assess Risk

4. Assess Risk

- Identify risks
- Assign risk ranking and determine **risk tolerance**
- Address areas at or above threshold
- Look at **external and internal threats**, and differentiate between them
- Identify **recent/ongoing changes** in the environment
- Leverage existing risk management processes such as:
  - ISO 31000:2009 or ISO/IEC 27005:2011
  - NIST Special Publication 800-39
  - Department of Energy Cybersecurity Risk Management Process (RMP) Guideline

4. Assessing Risk: Common Mistakes

- Not understanding the environment
- Avoiding unfamiliar technical content
- Underestimating the complexity of cybersecurity threats
- Not allocating sufficient time for a comprehensive review
- Making assumptions about IS's level of knowledge/proficiency (taking them at their word)
- Exclusion of recent changes to the environment

4. Enlisting the Help of Security Professionals

- Benefits of Utilizing External Specialists
  - Reduce costs
  - Expertise
  - Independence
  - Ability to focus
  - Benchmarking relative to other organizations
- Assessing Specialist Ability
  - Certifications
  - Experience
  - References

Step 5: Establish and Implement Controls and Technology

5. Establish Objectives and Associated Controls

- Can be high-level governance to extremely technical
- Preferred approach is **risk-based**:
  - Existing vulnerabilities
  - Actual or suspected threats
  - Incidental information
- Should address all identified risks and scenarios
- Prioritize based on data classification
- Best aligned to defined governance/management goals

5. Align Controls to Objectives

Cybersecurity Objective	Controls
Attacks and breaches are identified and treated in a timely and appropriate manner.	• Monitoring software is in place for all servers. • Notifications are sent when any suspicious activity is detected. • Notifications are logged, prioritized and responded to.

5. Utilize Existing Control Frameworks as a Guide

Council on Cybersecurity Top 20 Critical Security Controls

Area	Critical Security Control
Asset Management	1. Inventory of Authorized and Unauthorized Devices 2. Inventory of Authorized and Unauthorized Software
Monitoring and Response	3. Maintenance, Monitoring, and Analysis of Audit Logs 4. Incident Response and Management
Wireless/BYOD	5. Wireless Device Control

5. Utilize Existing Control Frameworks as a Guide

Council on Cybersecurity Top 20 Critical Security Controls

Area	Critical Security Control
Logical Access	6. Limitation and Control of Network Ports, Protocols, and Services 7. Controlled Use of Administrative Privileges 8. Controlled Access Based on the Need to Know 9. Account Monitoring and Control
Network Design	10. Boundary Defense 11. Secure Network Engineering

as a Guide (cont)
Council on Cybersecurity Top 20 Critical

Area	Critical Security Control
Server and Device Hardening	12. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers 13. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Human Resources	14. Security Skills Assessment and Appropriate Training to Fill Gaps

5. Utilize Existing Control Frameworks as a Guide

Council on Cybersecurity Top 20 Critical Security Controls

Area	Critical Security Control
Vulnerability and Pen Testing	15. Continuous Vulnerability Assessment and Remediation 16. Penetration Tests and Red Team Exercises
Application Security	17. Malware Defenses 18. Application Software Security
Data Management	19. Data Recovery Capability 20. Data Protection

5. Recommended Baseline Network Security Controls

- **Security policy**
- Network and data flow diagrams
- IT asset inventory and data classification scheme
- **Firewall and intrusion detection/prevention**
- DMZ
- **Anti-virus/malware**
- Server hardening standards
- **Vulnerability scan and penetration test** performed
- Log and monitor network activity

5. Baseline Network Security Controls - Continued

- Restrict remote access
- Enforce **strong password** and lockout policies
- Content filtering
- **Employee security training**
- User access reviews
- Device encryption
- Monitor and evaluate third-party service providers
- Restrict web access
- Properly dispose of physical assets

5. Baseline Network Security Controls - Continued

- **Patch servers and workstations regularly**
- Keep browsers and Java run-time up-to-date
- Disable Java in the browser when possible
- Apply network segmentation
- **Limit administrative access**
- Modify/remove vendor default accounts
- Configure **wireless security**
- Lock down network access points
- **Develop an incident response plan**

Step 6: Evaluate Control Environment Effectiveness

6. Test Control Environment Effectiveness

- **IT General Controls Audit**
  - Logical Access
  - Backup/Recovery
  - Monitoring
  - Server and anti-virus patching
- Firewall Audit
- Network Configuration Review
- Server Hardening Standards Review
- **Social Engineering and Phishing Assessment**
- Policies/Procedures Review
- **Vulnerability and Penetration Test**

Step 7: Identify, Prioritize and Remediate Control Gaps

7. Identify/Prioritize/Remediate Control Gaps

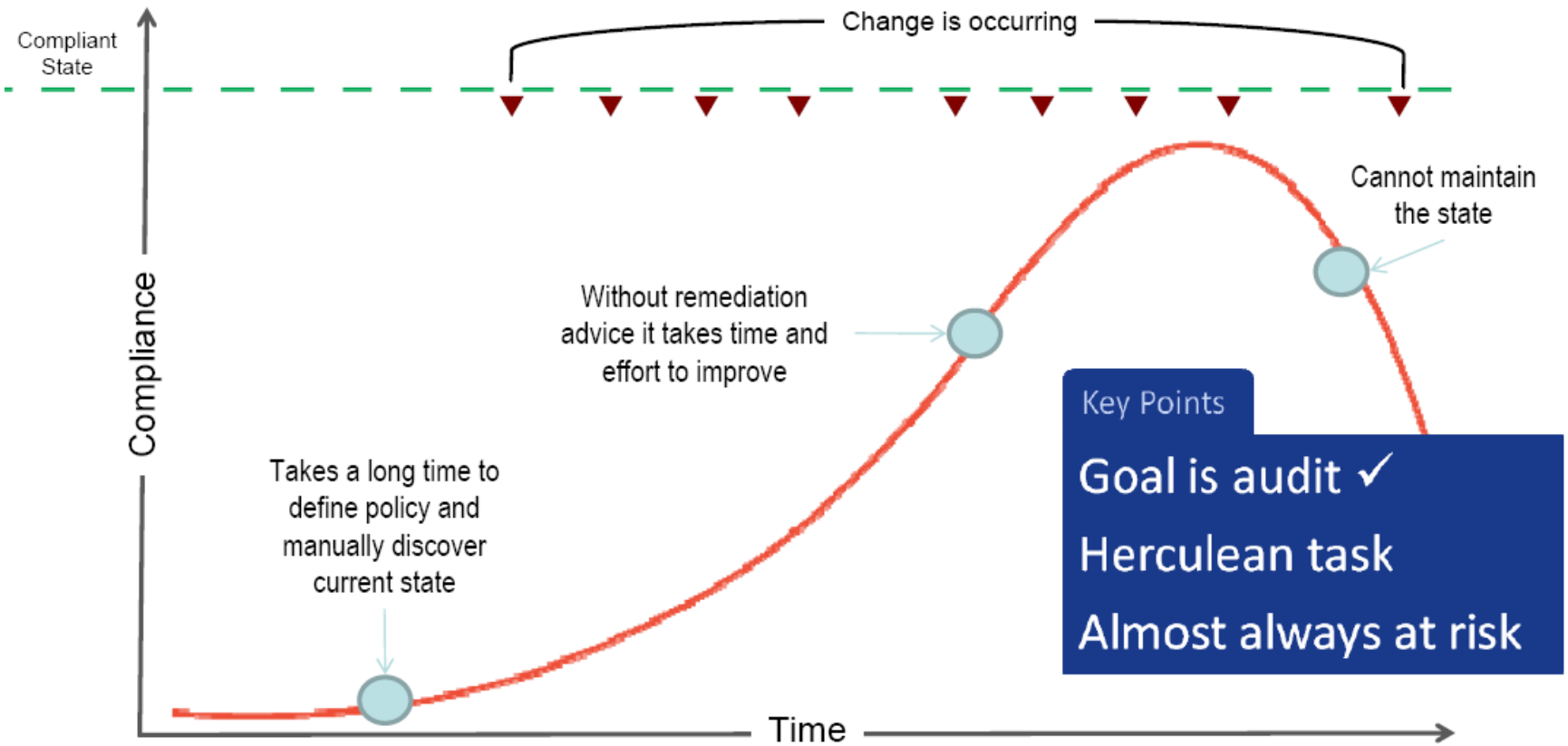
- Review with IS and validate findings
- **Assign risk rating**
- **Develop a remediation plan** with IS
  - Establish action plan
  - Assign responsibility
  - Assign timeline
- Update documentation/communication as necessary
- Review findings with management

Step 8: Monitor and Refresh

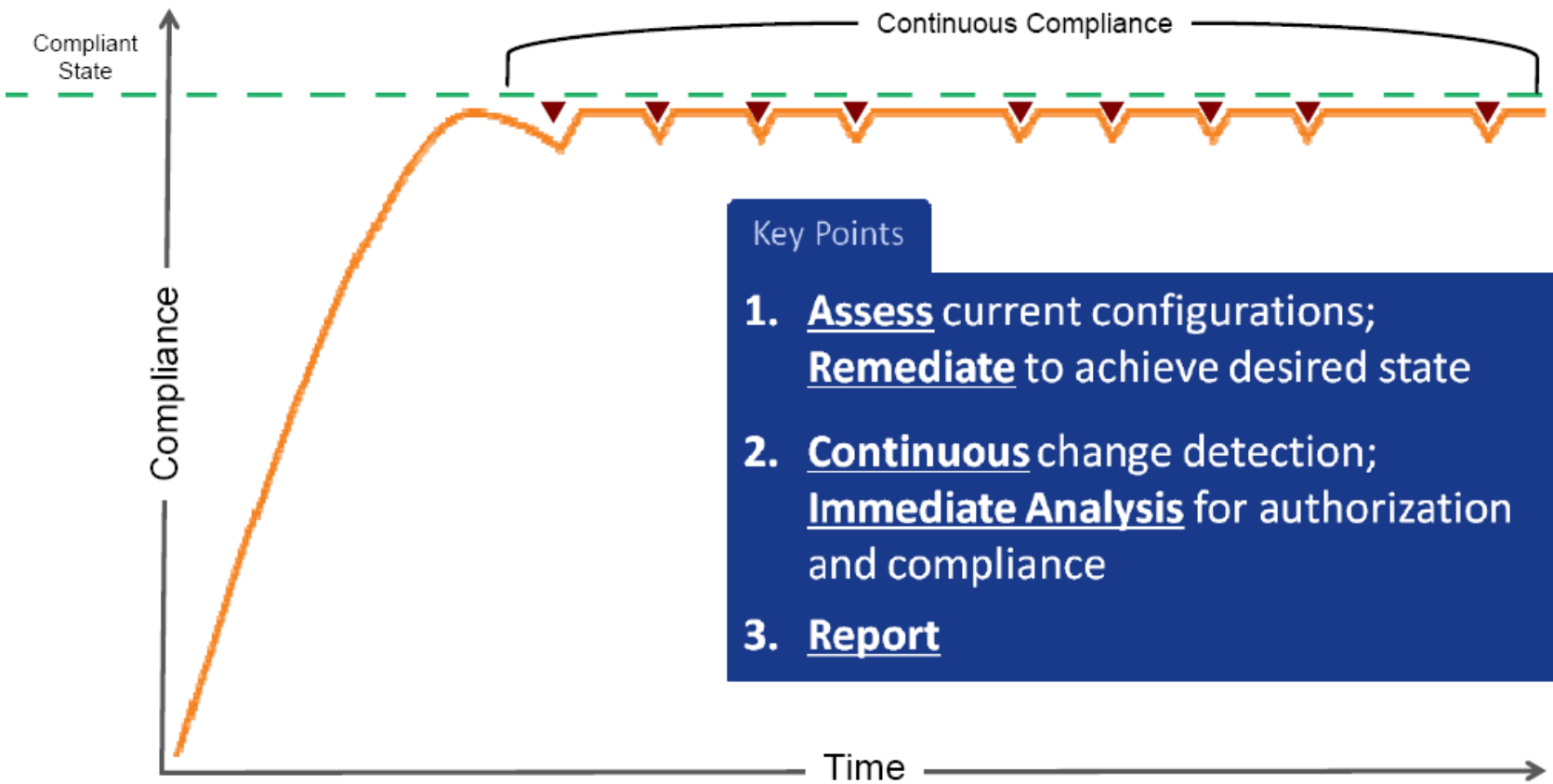
8. Monitor and Refresh

- Evaluate IS compliance with established action plans
- Communicate deviations from action plans with management
- Monitor existing IS and business activities that may impact action plans or inherent risks
- **Strive for continuous monitoring to ensure rapid communication and remediation cycles**

8. Static Compliance Model



8. Continuous Compliance



Key Points

1. **Assess** current configurations; **Remediate** to achieve desired state
2. **Continuous** change detection; **Immediate Analysis** for authorization and compliance
3. **Report**

Final Recommendations

- Educate and involve all levels within the organization
- Integrate cyber risk strategy into the organization's strategic plan
- Have a team dedicated to managing cyber threats
- Automate as much as possible
- Collaborate internally AND externally
- Dedicate just as much to detection and response as you do to prevention

Useful links

- International Association of Privacy Professionals (https://privacyassociation.org/)
- NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/)
- ISACA Cybersecurity Nexus (http://www.isaca.org/cyber)
- SANS Institute Critical Cybersecurity Controls (https://www.sans.org/critical-security-controls/)
- ISO/IEC 27002:2013 (http://www.iso.org/iso/catalogue_detail?csnumber=54533)
- Department of Homeland Security Cybersecurity (https://www.dhs.gov/topic/cybersecurity)
- Verizon Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/)
- NIST SP 800-123 Guide to General Server Security (http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf)

Questions

Chris Debo
Senior Manager, Technology Advisors
cdebo@schneiderdowns.com
614-586-7108

Steve Earley
Senior Manager, Internal Audit and Risk Advisory Services
searley@schneiderdowns.com
614-586-7115

Business Address:
Schneider Downs & Co., Inc.
41 S. High Street
Suite 2100
Columbus, OH 43215