

CPIM

CENTER FOR PUBLIC INVESTMENT MANAGEMENT



A PROGRAM BROUGHT TO YOU BY:

JOSH MANDEL

TREASURER OF OHIO

SECURITY 115

Mitigating Cybersecurity Risk: Audit Perspective

About Us



Big Thinking. Personal Focus.

- **Schneider Downs:** www.schneiderdowns.com
 - One of the largest certified public accounting and business advisory firms in the region
 - Significant work with Federal/State/Local government clients: Bureau of Workers' Compensation, Auditor of State, Treasurer of State, OSHP Retirement System
- **Steve Earley** CISA, CISSP, CRISC, CFSA, ITILv3, MCP – (614) 586-7115 or searley@schneiderdowns.com
 - Senior Manager, IT Audit, Internal Audit and Risk Advisory Services
 - 23 years IT experience, 11 years audit/risk/security
 - PCI, SOC 1 & 2, compliance (e.g., SOX, HIPAA), business continuity, IT controls assessments
 - Former Chief Information Security Officer (CISO) for Ohio Department of Public Safety
 - Retired U.S. Navy Commander; specialized in information assurance and cyberintelligence
- **Chris Debo** CISA – (614) 586-7108 or cdebo@schneiderdowns.com
 - Senior Manager, Technology Advisory Services
 - 14 years IT experience, 6 years audit/risk/security
 - Cybersecurity, enterprise risk assessments, network vulnerability assessments, data warehousing and business intelligence, ERP solution selection and implementation
 - Significant expertise in the education, government, and not-for-profit sectors

What is Cybersecurity?

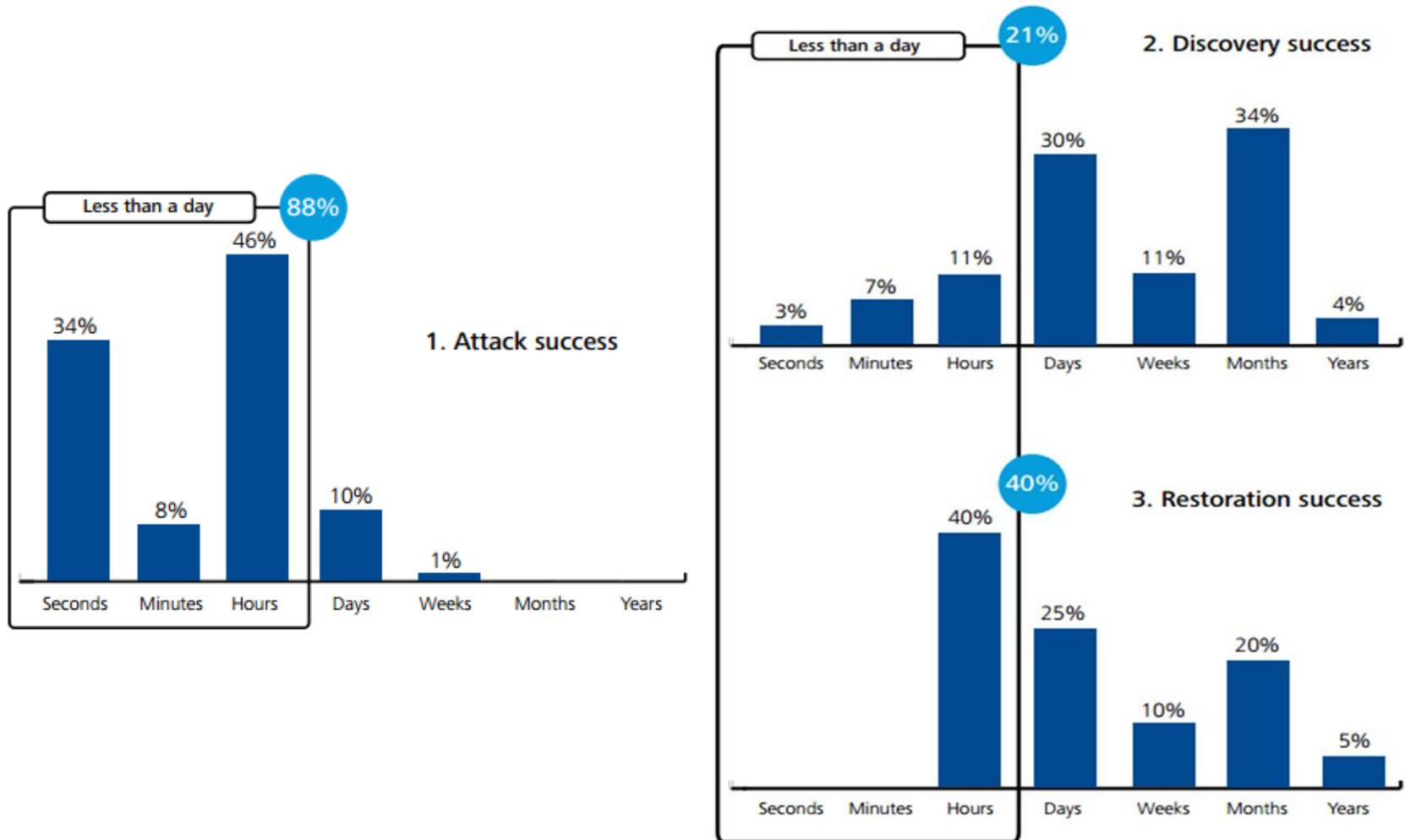
- NIST definition:
 - “The process of protecting information by preventing, detecting, and responding to attacks.”
 - Key: **PROTECTING INFORMATION** against
- Threats not limited to Internet hackers
 - Social engineering
 - Phishing
 - Disgruntled employees
 - Human error

- Theft
- Misuse
- Manipulation
- Damage
- Loss

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
- Employees at core of most attacks
 - Stolen credentials primary cause: 80% of time

Time to Attack versus Organization's Ability to Defend



Source: 2014 Verizon Data Breach Report

Common Cybersecurity Attacks

- Social Engineering: Exploiting human weaknesses
 - Phishing (email) / Vishing (phone) / In-person solicitation
 - Tailgating
 - Dumpster diving
 - Media dropping
- Attacks against unpatched systems
- Viruses/worms
- Advanced Persistent Threats (APT)
- Website attacks: Cross-site scripting, SQL injection
- Brute force attacks (e.g., password guessing)
- Keystroke loggers / packet sniffers

Steps for Securing Your Environment

1. Define roles and responsibilities

- Set tone at the top
- Design and implement security plan
- Build advisory relationship with Information Security
- Understand and follow Policies and Procedures
- Don't open suspicious e-mails!
- Avoid untrusted WiFi

2. Adopt a framework: ISO 27000, NIST, COBIT

3. Understand your environment

- Servers, Workstations, Applications, Databases
- Firewalls / Security / Infrastructure
- Encryption
- Third Parties (Vendors)

Steps for Securing Your Environment (cont)

4. Assess risk:

- Risk tolerance
- Internal/external threats
- Recent/ongoing changes to the environment

5. Establish and implement controls and technology

- Risk-based and cost-effective

6. Evaluate effectiveness: **Test!**

7. Identify, prioritize and remediate gaps

8. Monitor/refresh

Recommended Baseline Network Security Controls

PREVENT (P) → DETECT (D) → RESPOND (R)

- Security policy (P)
- Firewall and intrusion detection/prevention (P/D)
- Anti-virus / anti-malware (P/D)
- Patch servers and workstations regularly (P)
- Routine vulnerability scan and penetration tests (P/D)
- Strong password and lockout policies (P)
- Employee security training (P/D/R)
- Configure wireless security (P)
- Develop an incident response plan (R)

Key Takeaways

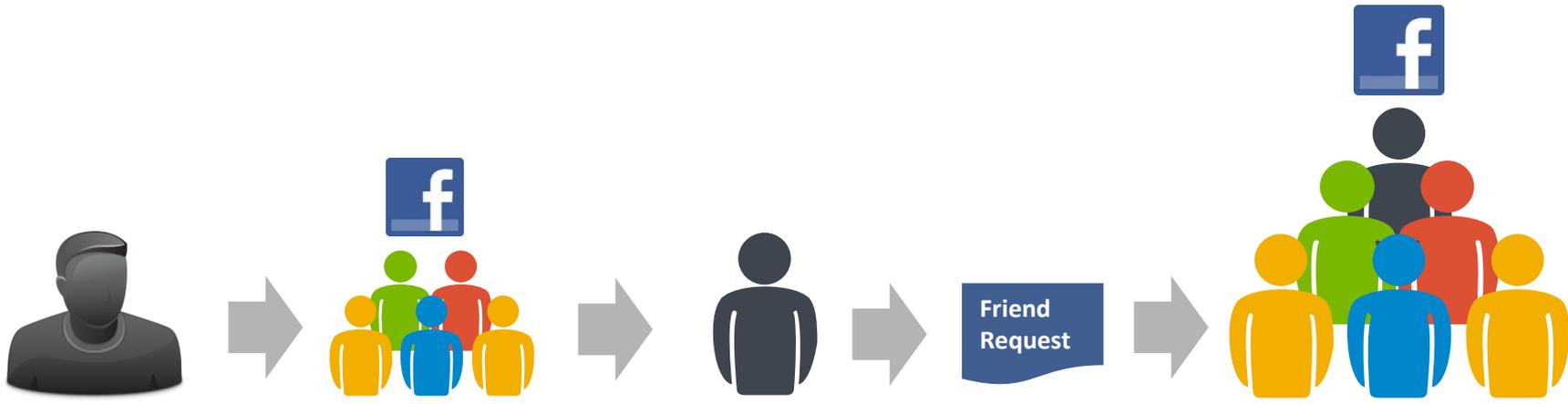
- Cybersecurity must be part of your organization's strategic plan. Not just an IT issue!
- Every organization will experience a breach at some point.
- Have an effective Incident Response Plan, and practice it regularly.
- Manage/monitor your vendors. Their cybersecurity risk equals ***your*** cybersecurity risk.
- Educate your people. Phishing is the most common means for gaining entry; employee training and endpoint protection mitigates this risk.
- Preventive controls are no longer sufficient. Monitoring and detection software must be in place to identify and isolate potential breaches.
- 100% security is a pipe dream. Manage risks, and conduct regular audits.

Breaking The Cyber Kill Chain

Tom Beith and Scott Chennells
Dell SecureWorks

SecureWorks





Threat actor researched target company. Determined social engineering vector to exploit.

Established identify of Executive Assistant to CEO on social media sites

Created online social profile

"Friended" target

Executive assistant accepted request

Threat actor crafted spear-phishing email based on information gleaned from target profile.



Sent to target's work email address

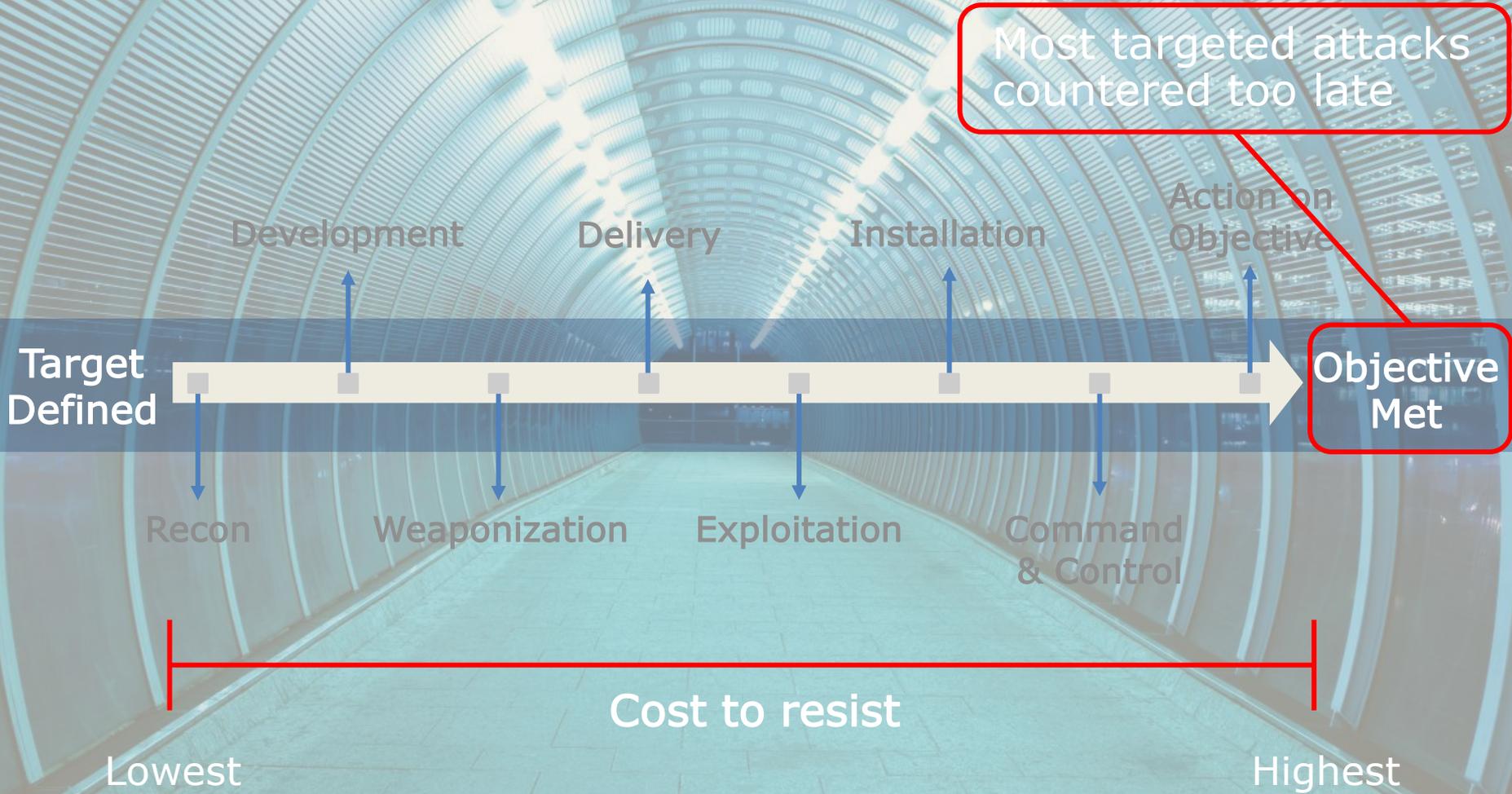


Executive Assistant opened the email and attachments.

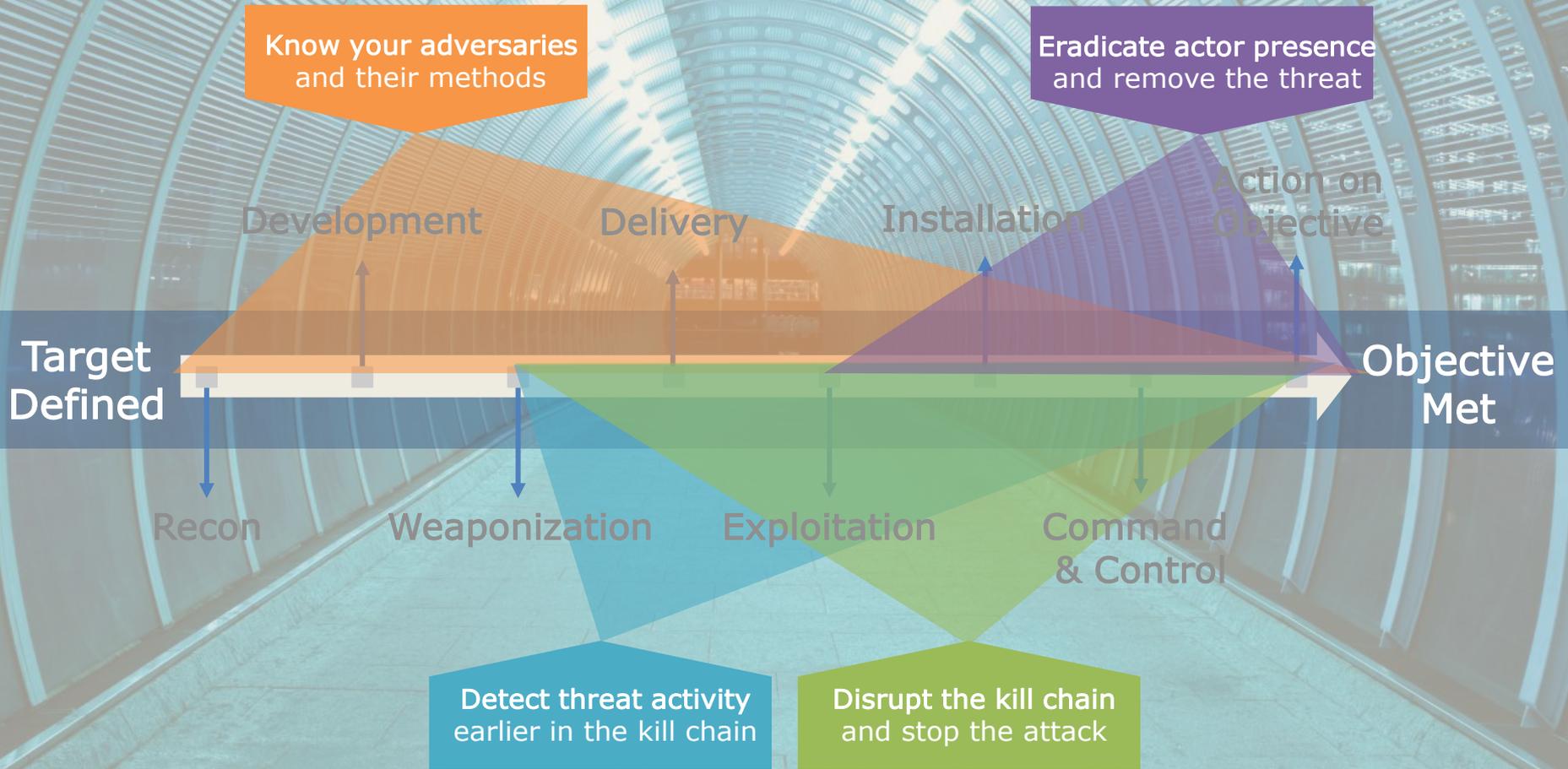
Trojan delivered. Threat actor gets foothold onto the network.

Stole intellectual property at will as a trusted insider

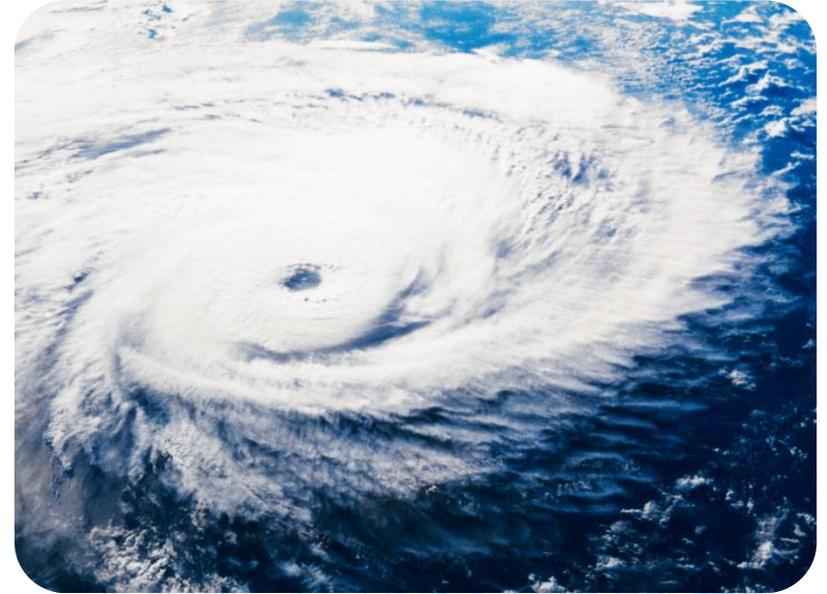
The kill chain



Breaking the kill chain



Organizations and IT need robust Incident Response capabilities to respond to major security incidents.

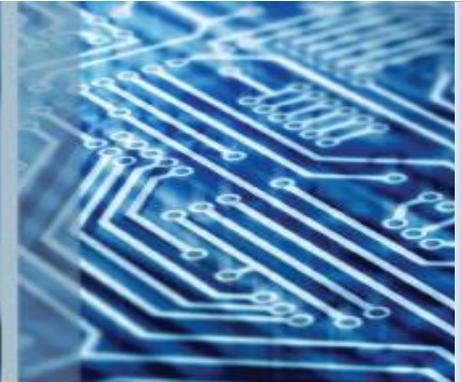


Environmental Realities

- Growing sophistication and persistence of threats is outstripping IT staff capabilities to adequately and rapidly respond to incidents
- Disruptions and costs from a major security incidents are high
- IT lacks the expertise to conduct malware analysis and forensic investigations to determine the extent of the problems

Public Entity Cybersecurity Risks

...Yes it applies to you!



James Giszczak | Sara Jodka | Dominic Paluzzi

McDonald Hopkins

Overview & Goals

- Background and the cost of security incidents
- Help you understand the legal landscape
- Local Government trends and breach examples
- Help you understand and implement an Incident Response Plan (IRP)
- Identification of resources to help you manage a security or privacy incident
- Discuss the steps you should take to investigate and respond to an incident
 - To determine the facts and scope;
 - Identify affected individuals;
 - Mitigate risk of harm to individuals; and
 - Determine your reporting obligations.

Defining PII

- **Personally Identifiable Information (PII)**
 - Social Security number
 - Drivers license number
 - Credit/debit card numbers
 - Passport number
 - Banking records
 - Date of Birth
 - Medical Information
 - Mother's maiden name
 - E-mail/username in combination with password/security question & answer



Primary Types of Privacy Incidents

- **Physical loss**: Stolen or lost laptop, PDA, thumb drive, or other portable media containing PII or other sensitive data
 - Accounts for about 25% of breaches
 - Mitigation
 - Encrypt
 - Prohibit / minimize / block saving PII on portable media
 - Records management



Primary Types of Privacy Incidents

- **Hardcopies**: Mis-mail, Misplaced, Stolen, or “Disposal Fail”
 - Accounts for about 10% of breaches
 - Mitigation
 - Handling policy and training
 - Disposal policy and training
 - Diligence/contracts with records management/disposal vendors



Primary Types of Privacy Incidents

■ Misdirected Email / Fax or “Computer Glitch”

- Accounts for about 8% of breaches
- Mitigation
 - Regular systems and/or vulnerability testing
 - Encrypt or password-protect files
 - Outlook delay



Primary Types of Privacy Incidents

- **Vendors**: Negligence, physical loss, database/server breach or stolen data at a vendor's location or server
 - Accounts for about 25% of breaches
 - Increases response costs about 20%
 - Mitigation
 - Vendor contract provisions
 - Appropriate review of vendors to confirm safeguards are in place



Primary Types of Privacy Incidents

- **Database/server breach**: Unauthorized person accesses or hacks into a data server that stores personal or other sensitive data
 - Malware; Hackers; Phishing; Ransomware
 - Accounts for about 20% of breaches
 - Mitigation
 - Penetration testing, firewalls, intrusion detection, etc.
 - Systems activity review – logging and periodic monitoring
 - Training of employees



Primary Types of Privacy Incidents

- **Stolen Data by Otherwise Authorized Users:** Rogue Employee or other malicious insider with access downloads or sends personal or sensitive data to another unauthorized location for an improper purpose
 - Accounts for about 12% of breaches
 - Mitigation
 - Systems activity review – logging and periodic monitoring
 - Access reviews



Data Breaches by the Numbers

- 932,729,111 records reported have been compromised since 2005 (Privacy Rights Clearinghouse)
- The average cost of a data breach is \$5.9 million and \$201 per compromised record (2014 Ponemon Study)
 - More important to look at trends year over year
 - Public Relations damage incalculable
- 75% of attacks are not considered difficult and 90% are avoidable through simple or intermediate controls (Verizon 2013 Data Breach Investigations Report)

Regulatory Compliance

- At least 35 Federal Laws with Data Protection or Privacy Protections
- 47 states, the District of Columbia, Puerto Rico, the Virgin Islands and numerous countries have enacted legislation requiring notification of security breaches involving PII
 - Residence of affected individuals determines applicable notice law (regardless of whether entity has a business located or transacts business within such state or country)
 - Federal Breach Notification Bill recently proposed by The President

What is a Data Breach?

- Definition varies from state to state, but typically includes:
 - Unauthorized acquisition / access / use
 - of Personally Identifiable Information (PII)
 - Unencrypted
 - Compromising the security, confidentiality or integrity of PII
 - Does not include good faith acquisition of PII

PCI DSS

(Payment Card Industry Data Security Standard)

- Established in 2004 by major credit card companies
- Requires merchants accepting credit, debit & other payment cards to safeguard cardholder data
 - Primary Account Number (PAN)
 - Cardholder Name
 - Expiration Date
 - Service Code (3 or 4 digit code)
- All merchants (anyone accepting credit card payments) are required, under merchant banking agreements, to comply with PCI standards.



PCI DSS

- Self-regulated
- The enforcement arm is the card brands via the acquiring banks/processors
- Penalties = fines and increased interchange rates imposed by acquirers/processors
- Data Security Standard (DSS) is well defined (288 requirements) but still open for interpretation
- PCI Compliant merchants are still breached (Target)
- Compliance \neq Security

Trends in Local Government

- Common Misconceptions
- Use of unsecured wireless connections to internal network
- Lack of encryption (laptops, desktops, smartphones, USB storage = > 40% data breaches)
- Ineffective password policies (complexity, length, age)
- Weak Physical Security
- Inadequate Network Security
- Lack of Vendor controls



Local Government Breach Examples

- **Wisconsin Dept. of Revenue (July 2012)**
 - An annual sales report contained the Social Security and tax identification numbers of people and businesses who sold property in Wisconsin in 2011.
 - The report was available online between April 5, 2012 and July 23, 2012 and meant for real estate professionals.
 - The report was accessed a total of 138 times before being taken down.
 - A total of 110,795 sales were made in Wisconsin in 2011, but not everyone who made a sale provided their Social Security or tax identification number for the paperwork.

Local Government Breach Examples

- **New Hampshire Dept. of Corrections (Sept. 2012)**
 - A staff member found that a cable line hooked to the computers used by inmates had been connected to a line connecting to the entire Concord prison computer system.
 - Allowed one or more prisoners to view, steal, or change sensitive records, including staff member information and sentencing and parole dates.
 - Information from the offender management database system "Corrections Offender Records and Information System" may have been compromised as well.

Local Government Breach Examples

- **Baltimore County, MD (Nov. 2013)**
 - A contractor who worked for Baltimore County between December of 2011 and July of 2012 was found to have saved the personal information of 12,000 county employees to computers for reasons unrelated to work.
 - Employees who had their paychecks direct deposited were affected and the bank account information of 6,633 employees was exposed.
 - Baltimore county employees are no longer allowed to download personal information to county computers and more than 5,000 county hard drives will be cleared of related data.

Other Real World Examples

- Third Party Vendor
- Low-tech Theft of Tax Returns
- Stolen Laptop / Unnecessary Media Notification
- Thumb Drive Bowl
- Encryption Company Gets Hacked
- Thumb Drive with Valet
- Ransomware & Phishing Attacks



Phishing - Indicators

- “Verify your account”
 - Businesses should not ask you to send passwords, login names, Social Security numbers or other personal information through e-mail
- “If you don’t respond within 48 hours, your account will be closed”
 - These messages convey a sense of urgency so you will respond immediately, without thinking
- “Dear Valued Customer”
 - Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name
- “Click the link below to gain access to your account”
 - HTML-formatted messages can contain links or forms you can fill out just as you would fill out a form on a website



PII Destruction/Disposal Laws

- Require physical destruction or permanently erase or otherwise render unreadable computer disks, CD, DVD, hard drives, databases, or other electronic storage tools that contain sensitive personal information
 - What do we do with old/retired hard drives, computers & copiers?
 - Can we prove it was done correctly?
- Paper copies should be shredded, cross-shredded, burned, or pulverized
- If you hire a disposal company, you must articulate requirements and monitor compliance
- Violations:
 - Knowing violations subject to criminal fines
 - Potential for civil suits



Proactive Measures



- Written Information Security Program (WISP)
 - Required by Massachusetts law, GLBA and FTC Red Flags Rule
- Incident Response Plan
 - Required by PCI DSS, GLBA and HIPAA
- Carefully drafted Confidentiality Agreements for employees, vendors and visitors
- Proper and ongoing training of employees on company's data security programs
- Data Privacy & Cybersecurity Review

What You Should Be Doing Now

- Assemble Incident Response Team
- Draft Incident Response Plan
- Draft WISP
- Engage vendors while all is calm (attorneys, forensics, mail house, credit monitoring, crisis communication, etc.)
- Complete Data Privacy Review
 - Identify access to PII
 - Security policies and procedures
 - Vendor contracts
 - Employment Agreements



James J. Giszczak

248.220.1354

jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi

248.220.1356

dpaluzzi@mcdonaldhopkins.com

Sara Jodka

614.474-0716

sjodka@mcdonaldhopkins.com

McDonald Hopkins

A business advisory and advocacy law firm®



We live data privacy law 24/7.

HOTLINE: 855-MH-DATA1
855-643-2821

www.mybreachcoach.com

