Managing Cyber Risk—Threat Trends, Prevention & Response

Your Data Discovery and Electronic Management Experts

October 2017

Brief Company Overview

- Provider of electronic discovery, computer forensics, and cybersecurity solutions (data breach management & network forensics)
- FileQuest for Web-based review
- Founded in 2003
- Headquartered in Silicon Valley
- Operate in 26 States w/ alliances in 20 Countries

Presentation Overview

- What is Cybersecurity
- Cybersecurity within Information Governance
- Cybersecurity Threats Trends
  - Insider vs. Outsider
  - Ransomware
  - IoT Attacks
- Regulatory Enforcement Trends
- Nevada Breach Response Law & Policy
- Incident Response (good vs. bad)
- Prevention

What is Cybersecurity?

- Defined by SEC guidance:
  - "…technology, processes and practices employed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."
- Objectives:
  - Ensure the ***Confidentiality***, ***Integrity*** and ***Availability*** of information assets

The risks of improper cybersecurity and benefits of proper technology, processes and practices are many; implicating reputation, business operations and financial damages.

Cybersecurity within IG

- What is Information Governance?
  - Interdisciplinary framework of policies, procedures and processes designed to ***optimize business value*** and ***manage costs and risks*** associated with information.
- Security is one element of IG Processes that also include:
  - Retention & Deletion; E-Discovery; Privacy; Business Continuity / Disaster Recovery; Storage Management; Document Management; Enterprise Search
- The Best IG Programs (like cyber frameworks) are driven, maintained and updated by and through:
  - PEOPLE, PROCESS; and TECHNOLOGY

Threat Trends

- What's in the news?
  - Equifax, Yahoo & SEC breaches
  - Russian hacking to influence election and investigation of collusion with Trump Campaign
  - WikiLeaks disclosures of stolen information
  - Russian state ties to organized cybersecurity criminals (& Kaspersky gov't ban)
  - IP theft
  - Ransomware/cyber extortion
  - Ukrainian critical infrastructure attacks
  - Netflix Theft through Vendor

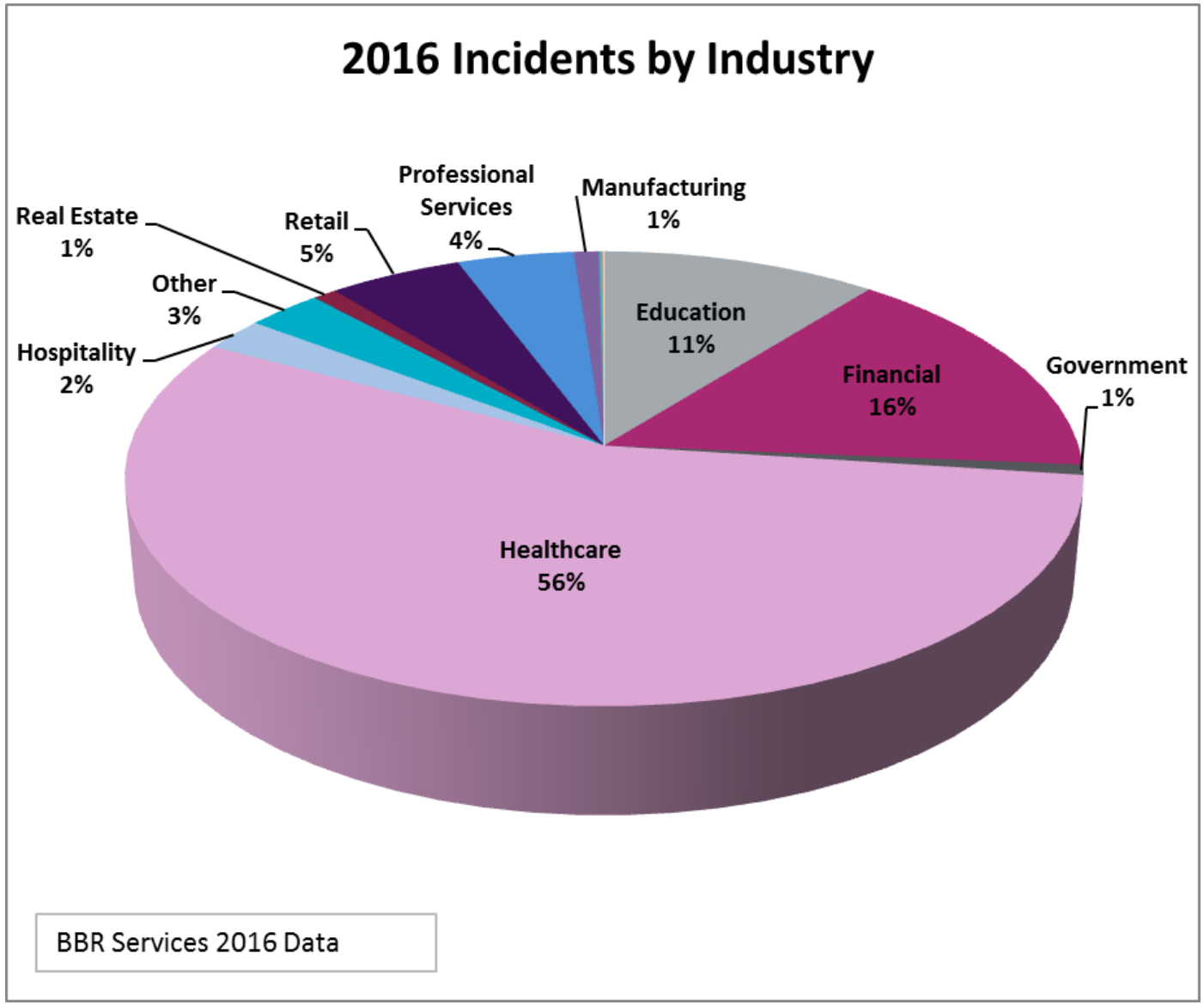
Cybersecurity Attacks

- Targeting particular persons through phishing/spear phishing
- Targeting particular systems through exploits
- Malware to exfiltrate data (PII and other) to resell on black market
- Stealing trade secrets and IP to gain competitive advantage, shortcut development
- Advanced persistent threats: attacks that play out over time (persistence) with designs to mask operations and target particular data (advanced)
- Threatening to destroy or damage systems or data unless ransom payment made
- Social engineering (coopting employees, consultants, using weaknesses in physical security to gain access to company information)

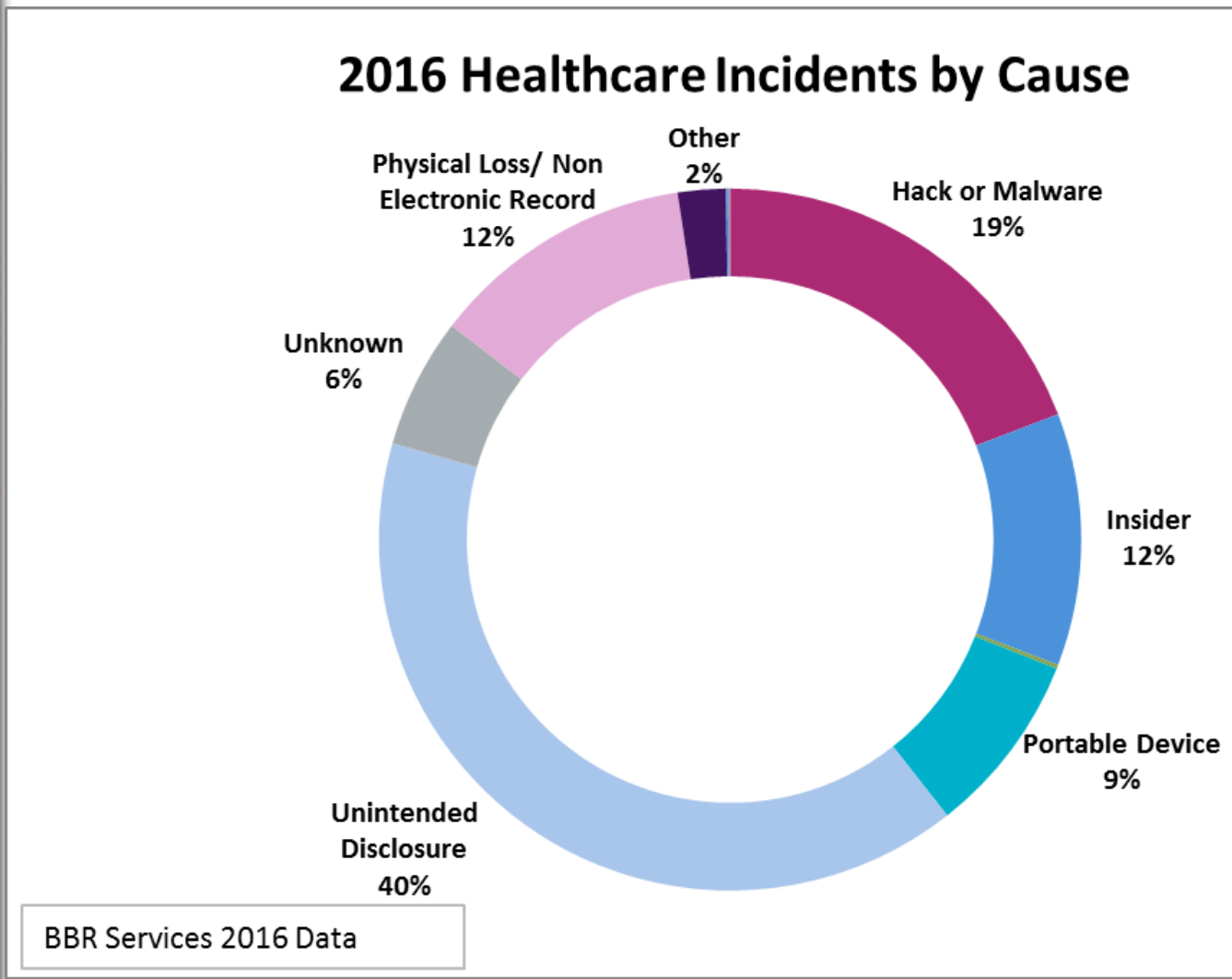
Origin of Threats

- **Insider**
  - Employee negligence
    - Security failure
    - Lost mobile device
  - Employee ignorance
    - Improper disposal of records (dumpster)
    - Lack of education and awareness
  - Malicious Employee
- **Outsider**
  - Hackers
    - Malware
    - Phishing and Spear Phishing
    - Ransomware
  - Social Engineering
  - Thieves
  - Vendors
  - State-sponsored attacks

Incidents by Industry

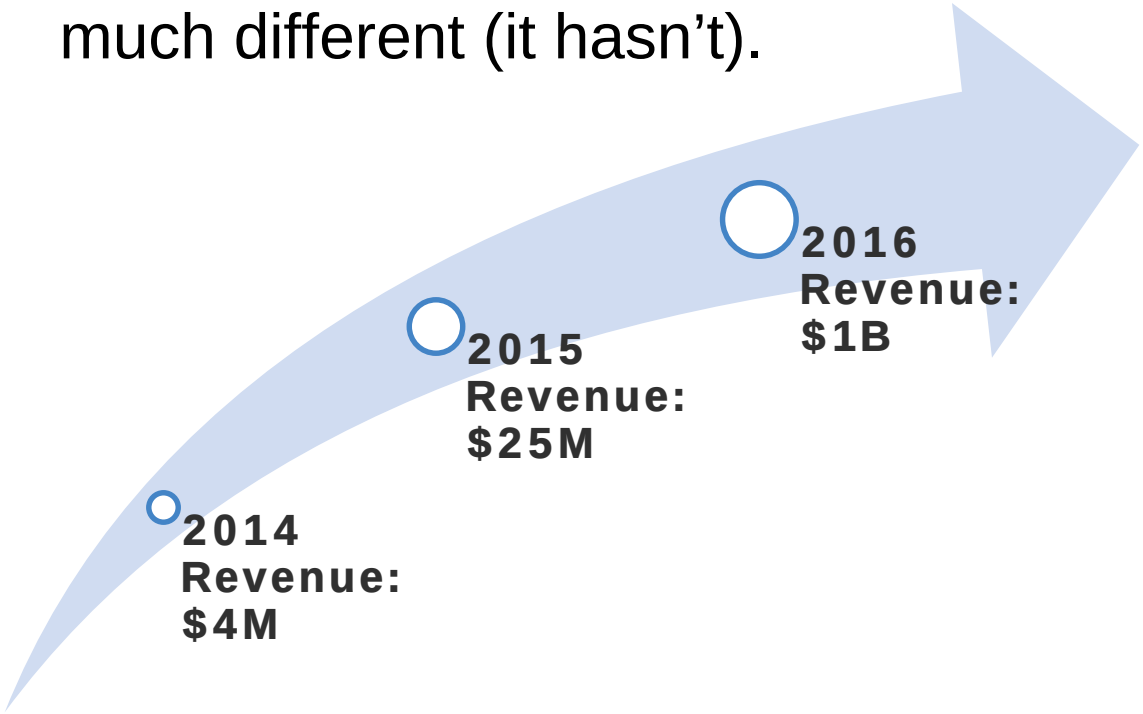


Cause of Healthcare Incidents



Ransomware on the Rise

- **2017 – The Year of Ransomware (Evolved)**
  - On April 29, 2016, the FBI issued a warning that ransomware attacks were on the rise, and there were few indications (other than awareness/prevention) that 2017 would be much different (it hasn't).



Ransomware Trends

- Historically, “patient zero” was a workstation – attackers used floppy disks and were targeting the medical industry
- Current ransomware variants are much more sophisticated and are nearly impossible to crack – if you’re a victim options are limited
- Cloud is newest attack vector, causing Malware proliferation throughout networks
- Types of cloud malware detected:
  - Javascript, Microsoft Office Macros, Ransomware (7.4%), Adware, Mobile, Backdoors
- File types targeted for encryption:
  - .exe, .pdf, .png, .psd, .wma, .doc, .ppt, .gif, .crt, .jpg, .xls, .mdb, .bmp, .pem, .jpeg, .zip, .mp3, .p12, .pfx, .rar, .mpg, .cer, .p7b

IoT DDOS Attacks

- Near the beginning of 2017, major internet sites were taken down due to DDOS attack on Dyn, a company responsible for routing internet traffic
- IoT DDOS attacks utilize multiple infected IoT devices, ranging from personal cameras to medical devices, to carry out attacks that flood a victim's server with legitimate requests thereby overloading the server's capacity and impairing functionality.
- Because open-source software, such as Mirai ("the future" in Japanese), is now widely available, IoT DDOS attacks will inevitably increase in 2018 and similar to ransomware will morph into more sophisticated and specialized variants.

Regulatory Trends

- Regulatory Hot Button Issues
  - Risk analysis and risk management plans
  - Vendor management
  - Incident report and process
  - Encryption of devices – Focus has been on mobile devices, with a recent change toward biomedical devices and desktop computers
  - Third-party access to PII/PHI
  - Inventory of PII/PHI and ePHI
  - Staff education and sanctions
  - Business associate agreements
  - Minimum necessary
  - Accounting of disclosures
  - Old data
  - Securit/Privacy rule compliance

- Memorial Healthcare System
  - February 2017 settlement for $5.5 million
  - MHS reported to the HHS Office for Civil Rights (OCR) that the protected health information of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff.
  - The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals.
  - OCR's Findings
    - MHS failed to:
  - (1) Implement **procedures to regularly review records of information system activity**, such as audit logs, access reports, and security incident tracking reports;
  - (2) implement policies and procedures that, based upon MHS's access authorization policies, establish, document, review, and **modify a user's right of access** to a workstation, transaction, program, or process.
  - Corrective Action Plan

- Advocate Health Care Network
  - August 2016 settlement for $5.55 million
  - Largest single settlement amount OCR has obtained against one entity
  - OCR began its investigation in 2013 when Advocate submitted three breach notification reports pertaining to separate and distinct incidents involving one of its subsidiaries.
  - Approximately 4 million affected individuals
  - OCR's Findings
    - Advocate failed to:
    - (1) **conduct an accurate and thorough assessment of the potential risks and vulnerabilities** to all of its ePHI;
    - (2) implement **policies and procedures and facility access controls to limit physical access** to the electronic information systems housed within a large data support center;
    - (3) obtain sa**tisfactory assurances in the form of a written business associate contract** that its business associate would appropriately safeguard all ePHI in its possession; and
    - (4) reasonably safeguard an **unencrypted laptop** when left in an unlocked vehicle overnight.
  - Corrective Action Plan

Reasonable InfoSec Program

- **Identify** types of information in custody, possession or control for which to establish security safeguards
- **Assess** anticipated threats, vulnerabilities, and risks to the security of such types of information
- **Safeguard** types of information through maintaining appropriate policies and administrative, physical, and technical controls
- **Contract** with third-parties to address the security of particular types of information
- **Respond** appropriately and proportionately to security incidents
- **Adjust** controls and policies on a periodic basis to improve over time

FTC-Recommended Security Controls: system access; physical access; encryption; transmission security; mobile device and portable media security; system change management; monitoring and detection; retention; disposal

Security Failure…now what?

- Is it a breach?
- Was ePHI or computerized data involved?
- Do you involve law enforcement?
- Do you hire a forensics company?
- Do you retain counsel?
- Do you involve regulatory agencies?
- Is crisis management necessary?
- Do you offer credit monitoring?

Nevada Breach Laws

- NRS, CHAPTER 603A - SECURITY OF PERSONAL INFORMATION
  - **NRS 603A.020 "Breach of the security of the system data" defined.**
  - **NRS 603A.030 "Data collector" defined.**
  - **NRS 603A.040 "Personal information" defined.**

Nevada Takeaways

- Personal Information is defined broader than most states (SSN; name + identifier)
  - (1) driver authorization card number or identification card number; (2) a medical identification number or a health insurance identification number; and **(3)** a user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account

Nevada Takeaways

- Applies broadly to “data collectors”
  - Any data collector that owns or licenses computerized data that includes personal information of a Nevada resident.
  - Any data collector that maintains computerized data that includes personal information that the data collector does not own.
  - “Data collector” means any governmental agency, institution of higher education, corporation, financial institute or retail operator or any other type of business entity or association that, for any purpose, whether by
  - automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

Nevada Takeaways

- Notification Triggers & Encryption
  - The statute only applies to unencrypted data.
  - Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.
  - "**Breach of the security of the system**" means unauthorized acquisition of computerized data that *materially compromises* the security, confidentiality or integrity of personal information maintained by the data collector.

Nevada Takeaways

- **Notification Letters** need not contain any specified content under NRS
- **Timing for notifications** must be given "in the most expedient time possible without unreasonable delay, consistent with needs of law enforcement [or remediation efforts]."
- **Penalty/Private Right of Action**
  - Data collectors and AG can bring actions against person/entity obtaining or benefiting from unlawfully disclosed PII

Incident Response Team

- The Incident Response Team (IRT) manages and coordinates the security event investigation, response, reporting and corrective action activities.
- The IRT should be activated upon learning of an event.
- The IRT should be authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident.

Incident Response

- Ten activities/experts that should be considered when responding to an incident:
  - Security
  - Legal
  - Forensic
  - Law Enforcement
  - Regulators
  - Insurance
  - PR
  - Stakeholders
  - Notifications
  - Employee/Personnel Management
- For all activities/experts involved there should be a central point person or small group with ONE unified message.

Forensic Investigation

- Maintaining Privilege
- Scope of investigative activities
- Attack vectors
- Malware and how it operates
- Employee or consultant responsibility
- Third parties involved?
- Law enforcement
- Conclusions may impact insurance coverage

Breach Post-mortem

- Compliance going forward – culture of security
- Lessons learned and next steps
- Back to starting point: where should the entity be, before the next one occurs?

Security Best Practices

- Organizations implement the following:
  - Backups
  - Risk Analysis
  - Penetration Testing
  - Vulnerability Patching (Equifax)
  - Application Whitelisting
  - Incident Response Plan
  - Business Continuity Plan
  - Staff Training

IoT Security Ref. Materials

- The following NIST guidelines are recommended for further review, especially for those entities that seek to utilize emerging technologies, such as sensors and IoT devices:
- Systems Security Engineering Guide (Special Publication 800-160)
  - NIST publication should be used in conjunction and as a supplement to International Standard ISO/IEC/IEEE 15288
  - Most recent and thorough guidance that can be used for a cybersecurity baseline.
  - Although this publication is targeted at engineers, it provides a framework for organizations to demonstrate **"adequate security,"** and notes that .
- **Network of 'Things' Guide** (Special Publication 800-183)
  - NIST provides an effective description of how "distributed IoT ecosystems behave," enabling attorneys and organizations to more accurately spot legal and technical issues.

Thank You & Questions

Cordero Delgadillo

- Cordero@DigitalMountain.com
- Work Mobile: 408-603-1978