In the Trenches: OCR Audits, Data Breaches, and Cybersecurity Threats & Mitigations

Health Care Compliance Association

June 16, 2017

PRESENTED BY

Leeann Habte

Partner, Best Best & Krieger

Darrell Contreras

Chief Compliance Officer, Millennium Health

Linh Sithihao

Information Security Consultant, Woodford Consulting Inc.

BBK BEST BEST & KRIEGER ATTORNEYS AT LAW

Enforcement

- Increasing Federal Enforcement
  - OCR Audits
  - OCR Investigations of HIPAA Complaints
  - OCR Breach Investigations
- State Enforcement Less Pronounced Recently

BBK BEST BEST & KRIEGER ATTORNEYS AT LAW

The Good News

- Audit
  - Phase II desk reviews conducted for 166 Covered Entities and 43 Business Associates
  - On-site reviews on hold for 2017
- Issues Identified in Audits
  - Poor controls over systems that maintain PHI
  - Mobile devices, including laptops, that are not properly protected

BEST BEST & KRIEGER ATTORNEYS AT LAW

The Bad News

- Aggressive Enforcement Continuing by Office for Civil Rights (OCR)
  - $14+ million in fines/civil monetary penalties in 2017
  - Heightened fines expected going forward
  - Increased focus on security safeguards to protect against digital health threats, cyber threats

BEST BEST & KRIEGER ATTORNEYS AT LAW

Trends – Types of Violations Fined

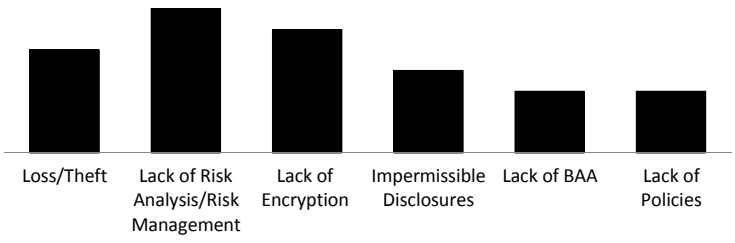
- Highest Fines in 2017

Amount of Fine	Violations Cited	Number of Persons
$2.2 Million	Impermissible disclosure to news media	1
$2.5 Million	Loss/theft + lack of risk analysis/risk management + lack of HIPAA policies	1,391
$5.5 Million	Lack of access/audit controls	115,143
$3.2 Million	Loss of blackberry and laptop + lack of risk analysis/risk management + lack of corrective action	
$2.2 Million	Loss/theft of USB drive + lack of risk management	2,209

BEST BEST & KRIEGER ATTORNEYS AT LAW

Trends - Types of Violations Cited

- Most Common Violations Cited – 12 months



BEST BEST & KRIEGER ATTORNEYS AT LAW

OCR's Wall of Shame - 2016

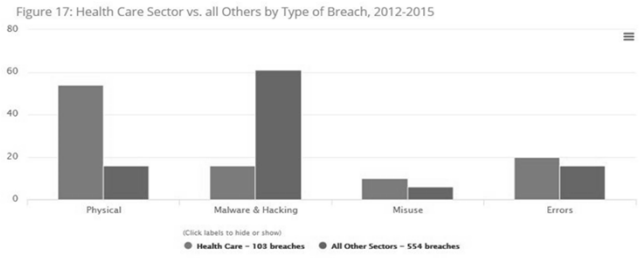
- Breach Type
  - Hacking/IT
  - Theft/Loss
  - Impermissible Disclosures
- Further Analysis Shows:
  - 30% of breaches reported involve third parties.
  - 48% of total incidents reported were Insider Breaches.
    - 52% - employee errors or accidents
    - 48% - intentional wrong-doing by employees

Source: 2016 Healthcare data breaches in review, www.databreaches.net

BEST BEST & KRIEGER ATTORNEYS AT LAW

California Office of Attorney General

- Health Care Sector Breaches
  - The health care sector accounted for 16 % of breaches (103) and 14 percent (6.8 million) of Californians' records breached from 2012 - 2015.
  - Significantly higher incidence of breaches resulting from physical theft and loss: 54 percent compared to just 16 percent in all other sectors. See Figure 17.
- Health Care Sector vs. Others - Type of Breach



(Source: *Source: California Data Breach Report, February 2016, Kamala D. Harris, Attorney General, California Department of Justice*)

BEST BEST & KRIEGER ATTORNEYS AT LAW

Future Guidance by OCR

- Text messaging
- Social media
- Security of Electronic Health Records
- The “minimum necessary” requirement

- Provide individuals harmed by HIPAA violations with a percentage of any civil monetary penalties or settlements collected by Office fo Civil Rights

BEST BEST & KRIEGER ATTORNEYS AT LAW

Mitigation Strategies for the Current Enforcement Landscape

BEST BEST & KRIEGER ATTORNEYS AT LAW

Summary of Recent Settlements

- Over $14M in 2017 so far!
- Memorial Healthcare System - $5.5M failure to terminate access rights and review system access logs (PHI stolen by employees)
- Children's Medical Center of Dallas - $3.2M for 1 lost BlackBerry and 1 stolen laptop
- CardioNet, Inc. - $2.5M for 1 laptop stolen from a car and no policies
- Memorial Hermann - $2.4M (privacy issue)
- (2016) Catholic Health Care Services of the Archdiocese of Philadelphia - $650,000 resulting from theft of mobile device with PHI and no risk management plan.

BBK
BEST BEST & KRIEGER
ATTORNEYS AT LAW

Data Breach Nuggets

2016 Report:

- The average health care breach cost: $358/record
- 48% of all breaches caused by malicious or criminal attacks

Look back approach:

- If breach, then which rule would have prevented it?

BBK
BEST BEST & KRIEGER
ATTORNEYS AT LAW

How to Mitigate the Risk

CONTENT:

- Security Assessment – Select a path for ePHI
  - How could ePHI leave the organization?
  - Where is our ePHI located?
  - How could someone gain access to the ePHI?

STRUCTURE:

- Evaluate your basic program
  - Do you have policies?
  - Is a risk assessment performed?
    - Has action been taken based on the risk assessment?
  - Is there an incident response plan?

BEST BEST & KRIEGER ATTORNEYS AT LAW

Example – ePHI on mobile devices

Steps:

1. Identify all of the types and inventory of devices that contain ePHI
   - Who has it and do they need it?
2. What safeguards are on the devices?
   - Are they password protected?
   - Are the devices otherwise encrypted?
   - What if they are lost?
     - Remote wipe capabilities
     - Use of remote wipe capabilities ("I'm sure it's not lost…")
3. Have you tried to hack the device?
   - Intrusion and penetration testing can be worth the cost
4. Are there policies in place and has training occurred?
   - Do employees know what to do if they THINK the device is lost?

BEST BEST & KRIEGER ATTORNEYS AT LAW

What happens if you have a security breach?

1. Reporting is expected – no "voluntary disclosure program."
2. Coordinate with legal counsel
3. Pull the relevant policies
   - Is it too late to create policies?
4. Pull training records
   - Is it too late to do training?
5. Review security assessments and risk assessments
   - Security assessments performed on systems
   - Risk assessments to identify potential risk areas
     - Known, unaddressed risks are more "dangerous" than unknown risks
     - If something did not get addressed, why?
6. Do not forget state-specific privacy laws, *e.g.*, California breach notification laws

BEST BEST & KRIEGER ATTORNEYS AT LAW

Cybersecurity Threats & Mitigations

BEST BEST & KRIEGER ATTORNEYS AT LAW

CyberSecurity Risk: 2017 Trends

- MOST at risk for Cyber threats: Financial (24%), Healthcare (15%), Retail (15%), and Public (12%)
- External threat agents (75%), Internal actors (25%) are responsible for the majority of the recent breaches.
- 66% of the breaches came from malicious email attachments
- Ransomware with cryptography is a lucrative attack technique for cyber criminals
- Internet of Things (IoT) growth serves as a popular attack vector for cyber criminals (ex: medical devices, refrigerators, Rx Dispensers, thermostats)

(Source: 2017 Verizon's Data Breach Incident Report)

BEST BEST & KRIEGER ATTORNEYS AT LAW

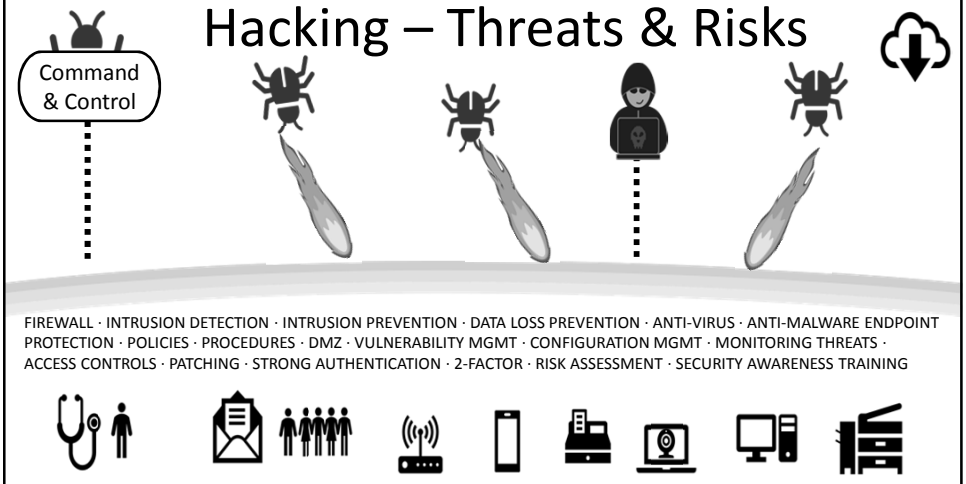
Compliance and CyberSecurity

- Cybersecurity refers to an organization's ability to protect or defend the use of cyberspace from cyberattacks.
- Compliance and security are distinct disciplines often with shared objectives.
- You can be compliant without being secure and possible to be secure (relatively speaking – as no environment is ever completely secure) without achieving compliance.
- Threat analysis and comprehensive risk management should drive security priorities, and then be tested for compliance. This should be done rather than using compliance checklists to drive security.
- Effective Cyber Security Risk Management is upper management driven, selecting a risk framework, and executing on the strategic and tactical plans

(Source: 2017 Verizon's Data Breach Incident Report)

BEST BEST & KRIEGER ATTORNEYS AT LAW

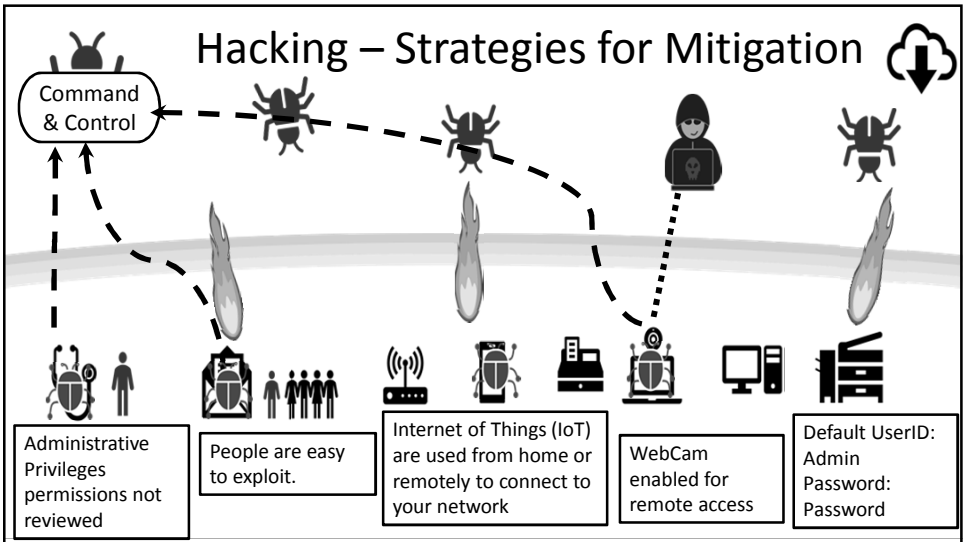
Hacking – Threats & Risks



Computer hacking is the unauthorized intrusion or infiltration into a computer or a network. Hacker's goal is to look for weaknesses to exploit, infiltrate the network, alter the software, circumvent the security measures of the computer or network, and/or obtain critical data.

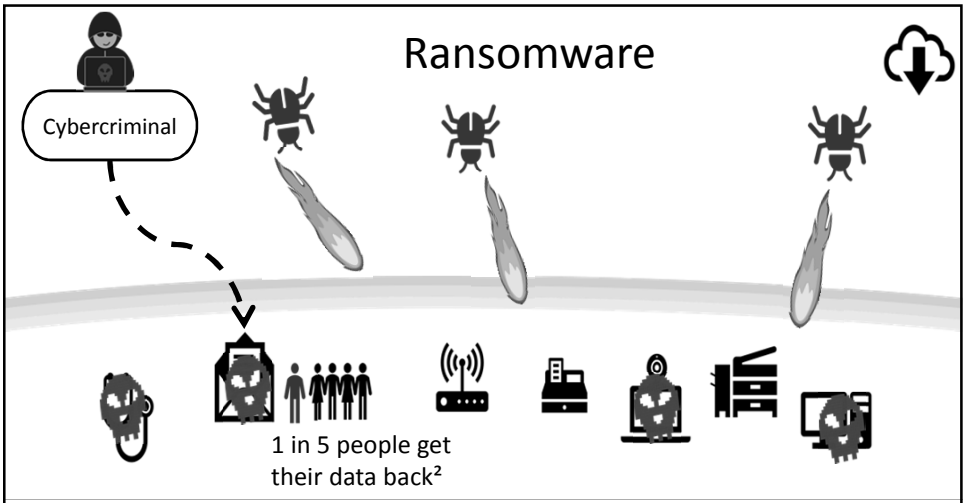
A multi-layer security defense is essential to detect and prevent infiltration, but threats can still infiltrate porous layers.

Hacking – Strategies for Mitigation



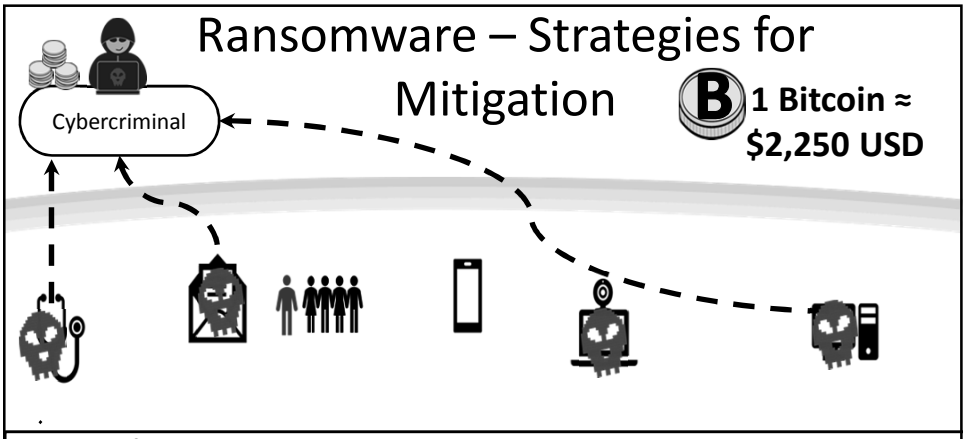
Strategies for Mitigation:

- Use good system and network hygiene (disable default password, unused ports, update patches on applications and systems, use anti-virus, limit permissions, disable remote access if not needed, no incidental web-browsing on servers)
- Perform penetration testing (third party or internal penetration tester)
- Continuous security incident monitoring and detection



Ransomware is a type of malware that prevents or limits use of a computer by locking the screen or the computer's files until a ransom is paid. You may or may not get a decrypt key. Ransomware has evolved to using cryptography to hold data hostage without infiltrating your network, does not rely on command-and-control, and has the user to contact the bad guys for help. [1]

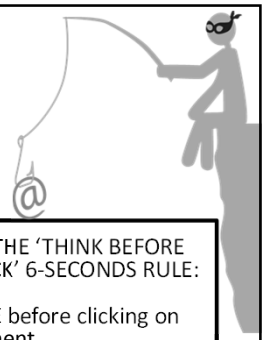
(Source: 2017 RSA – 7 Most Dangerous New Attack Techniques[1]; Kaspersky Security Bulletin 2016[2])



Strategies for Mitigation:

- Plan ahead on who will pay and how to pay (be realistic and make quick-decisions)
- Check for decryption keys to recover your data (nomoreransom.org)
- Back up your data frequently and save to an alternative location (Backup servers in the data center or offsite location)
- Up-to-date patching and antivirus enabled for automatic update, where possible, on end-user devices and servers
- Limit network shares to folders and files and be vigilant on an individual's permission rights (least privilege rule)

Phishing



- Phishing attack is an attack that cybercriminals use to fool you and collect valuable personal and financial information. Cybercriminals get you to click on a link from an email to redirect you to a suspicious website where you are prompted to enter your personal or financial information.
- Victims of phishing campaigns fall prey, repeatedly, even with additional training as a follow up.
- Is 100% training compliance is equivalent to being secure?
- 95% of phishing attacks that led to a breach were followed by some sort of software installation. (Verizon DBIR 2017)
- A breach at DocuSign led to targeted email malware campaign in May 2017.

APPLY THE 'THINK BEFORE YOU CLICK' 6-SECONDS RULE:

1-Second to PAUSE before clicking on the link or attachment.

2-Seconds to ASK who is it from and was I expecting this email?

3-Seconds to HOVER mouse over any link(s) to determine legit or malicious.

Strategies for Mitigation:

- Use 2-Factor or Multi-factor authentication to access critical websites (ex: email, EMR, financial data).
- Security Awareness & Training and applying the 'Think Before You Click Rule'
- Phishing campaign and awareness are effective when coupled with a negative consequence or a positive reinforcement.

STAYING AHEAD OF CYBER RISKS

- Identify and Prioritize your mission-critical assets and continuous maintenance
- Perform ongoing Vulnerability scanning and mitigation of prioritized vulnerabilities on mission-critical assets. The faster you identify vulnerabilities and execute a mitigation plan, you reduce the likelihood of an negative impact to the business.
- Execute Patch Management – deploy patches on systems with critical assets and reduce Patch cycles to days or as soon as possible.
- Continuous Audit logs & Security event monitoring
- Sharing information with other healthcare organizations
- Implement Incident Response plan and continuous exercise/testing

BBK BEST BEST & KRIEGER ATTORNEYS AT LAW

Thank you for attending.

Leeann Habte
Partner
Best Best & Krieger LLP
leeann.habte@gmail.com
(213) 787-2572

Darrell Contreras
Chief Compliance Officer
Millennium Health

Linh Sithihao
Information Security Consultant
Woodford Consulting, Inc.

BBK
BEST BEST & KRIEGER
ATTORNEYS AT LAW