Ransomware: Risk, Prevention, and Mitigation

Session #91, February 21, 2017

Tatiana Melnik, Melnik Legal PLLC
Brian R. Balow, Dawda Mann PLC
Speaker Introduction

Brian, Balow, JD
Member
Dawda Mann PLC
Speaker Introduction

Tatiana Melnik, JD
Attorney
Melnik Legal PLLC
Conflict of Interest

Tatiana Melnik, JD

Has no real or apparent conflicts of interest to report.

Brian Balow, JD

Has no real or apparent conflicts of interest to report.
Agenda

I. Learning Objectives
II. A Bit About Ransomware
III. Case Study
IV. Concluding Thoughts
Learning Objectives

• Recognize aspects of your environment that might invite a ransomware attack
• Identify measures that you can adopt to help prevent a ransomware attack
• Evaluate which prevention measures are appropriate for your environment in light of the risks presented
• React to a ransomware attack in a manner designed to minimize and mitigate the negative consequences of the attack
An Introduction of How Benefits Were Realized for the Value of Health IT

1. Satisfaction: Improved safeguards = sleep insurance = satisfaction

2. Treatment: Avoiding interruption of access to, and corruption of, clinical data and PHI

3. Electronic Secure Data: Preventing against an increasingly prevalent form of cyber breach

4. Patient Engagement: Preserving trust in the security of PHI

5. Savings: Avoiding breach response costs, fines, and reputational harm
Ransomware In the News...

Hollywood Presbyterian Medical Center Pays Hackers $17K Ransom

LOS ANGELES — A Los Angeles hospital paid a ransom of about $17,000 to hackers who infiltrated and disabled its computer network because it was the most efficient way to solve the problem, the medical center’s chief executive said Wednesday.

Hollywood Presbyterian Medical Center paid the demanded ransom of 40 bitcoins — currently worth $16,664 dollars — after the network infiltration that began Feb. 5, CEO Allen Stefanek said in a statement.
Ransomware In the News...

Two more hospitals struck by ransomware, in California and Indiana

Both Alvarado Hospital Medical Center and King's Daughters' Health say that quick response times appear to have minimized potential damage.

By Mike Miliard | April 04, 2016 | 10:55 AM
MedStar Health turns away patients after likely ransomware cyberattack

By John Woodrow Cox  March 29, 2016

MedStar Health patients were being turned away or treated without important computer records Tuesday as the health-care giant worked to restore online systems crippled by a virus.

By Tuesday evening, MedStar staff could read — but not update — thousands of patient records in its central database, though other systems remained dark, a spokeswoman said.

MedStar officials have refused to characterize the attack as “ransomware,” a virus used to hold systems hostage until victims pay for a key to regain access. But a number of employees reported seeing a pop-up message on their computer screens seeking payment in bitcoins, an Internet currency. One woman who works at MedStar Southern
Ransomware In the News...

MedStar Health turns away patients after likely ransomware cyberattack
By John Woodrow Cox March 29, 2016

MedStar Health patients were being turned away or treated without important computer records Tuesday as the health-care giant looked to restore online systems crippled by a virus.

By Tuesday evening, MedStar staff could read — but not print — thousands of patient records in its central database, though other systems remained dark, a spokeswoman said.

MedStar officials have refused to characterize the attack as “ransomware,” a virus used to hold systems hostage as victims pay for a key to regain access. But a number of employees reported seeing a pop-up message on their computer screens seeking payment in bitcoins, an alternative currency. One woman who works at MedStar Southern

MedStar attack found to be ransomware, hackers demand Bitcoin
By Jack McCarthy April 04, 2016 09:26 AM Share

The malware that shut down MedStar Health’s computer systems and locked up patient records now appears to be a ransomware attack.

MedStar employees encountered a pop-up message demanding payment of 45 Bitcoin, approximately $18,000 in exchange for a digital key that would unlock the data, according to several reports.

The malware has blocked MedStar employees from accessing patient data and, in some cases, having to turn patients away.
Maryland hospital: Ransomware success wasn’t IT department’s fault

MedStar denies ransom payment, denies earlier JBoss bugs played role.

SEAN GALLAGHER - 4/7/2016, 10:12 AM
Hospitals are hit with 88% of all ransomware attacks

Written by Max Green | July 27, 2016 | Print | Email

Hospitals and health systems have more to lose than organizations in other sectors when it comes to hacks. Patient data sells for more money than any other kind of information on the black market. Adding insult to injury, a new report suggests that the healthcare industry is hit significantly harder by ransomware than in any other -- 88 percent of attacks hit hospitals. 

Of the 88 percent of ransomware attacks that occurred in healthcare organizations, 94 percent were linked to a specific variant of software called Cryptowall, according to Solutionary’s Security Engineering Research Team Quarterly Threat Report for Q2 2016.

One reason hospitals may be particularly vulnerable is they use so many systems and devices that there are more entry and pivot points for cybercriminals to exploit, according the report.
Hospitals are now the top targets for ransomware attacks.

Report predicts more healthcare cyber and ransomware attacks in 2017

By Joseph Conn  |  December 2, 2016

The healthcare industry will be a target for cyber attackers in 2017 while the nefarious practice of holding patient records for ransom will be an industry scourge, according to predictions by credit reporting firm Experian.

“Personal medical information remains one of the most valuable types of data for attackers to steal,” according to the 10-page report, the company’s fourth annual data breach forecast.

Patient data is useful in both identity theft and in a more insidious variant, medical identity theft. The latter is when a person uses another’s identity to obtain medical treatment, creating a double whammy by defrauding the victim’s insurance company and muddling up the victim’s medical records.
How Many Ransomware Infections Has Your Company Suffered?
1. 0
2. 1
3. 2 – 4
4. I stopped counting…
Ransomware Defined

“Ransomware exploits human and technical weaknesses to gain access to an organization’s technical infrastructure in order to deny the organization access to its own data by encrypting that data.”

What Did the Attackers Exploit in your Company?

1. People
2. Technology
3. Both
4. Have no idea…. 
Ransomware Techniques

• Brute Force Hacking
• Phishing Emails
• Drive-by Downloading
• Vulnerable Web Servers
• Web-based Instant Messaging Applications
Example: Reveton

• Types of Ransomware
  – CryptoWall (April 2014)
  – CTB-Locker (June 2014)
  – TeslaCrypt (Feb. 2015)
  – MSIL or Samas (SAMSAM) (Early 2016)
  – Locky (Early 2016)

Why the Proliferation?

How Ransomware Became a Billion-Dollar Nightmare for Businesses

One cybersecurity firm estimates that extortion attacks now cost small and medium companies at least $75 billion in expenses and lost productivity each year.

ADAM CHANDLER  |  SEP 3, 2016  |  BUSINESS
Ransomware Risks

Interference with Patient Care
Ransomware Risks

Business Interruption/Restoration Costs
Ransomware Risks

Data Breach Laws/Regulations
Is Ransomware Reportable to OCR?

1. Yes
2. No
3. This is a trick question
Is Ransomware Reportable to OCR?

Yes

No

This is a trick question.

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
Is Ransomware Reportable to OCR?

1. Yes
2. No
3. This is a trick question

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015). Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

Ransomware Risks

- **Complex** Enforcement Environment

Federal Trade Commission
- CFPB
- Credit Unions
- Banks
- Credit Card Companies
- Insurance Regulators

HHS Office for Civil Rights

State’s Attorneys’ General
- SEC
- FCC
- OIG Audits
- FFIEC
- NYDFS

Consumers
Ransomware Risks

• Enforcement by HHS Office for Civil Rights
  – To date ~36 organizations have paid out a total $30M+ in settlements (with two fines)

  o Cignet Health ($4.3M) (fine)
  o UCLA Health System ($865,500) (employees talking)
  o Blue Cross Blue Shield of TN ($1.5) (stolen servers left at former office)
  o **Alaska Dept. of Health & Human Services** ($1.7M) (stolen USB hard drive)
  o Massachusetts Eye & Ear Infirmary ($1.5M) (lost laptop)
  o New York & Presbyterian Hospital ($3M)
  o Columbia University ($1.5M) (server configuration, records on search engine)
  o Anchorage Community Mental Health Services ($150K) (unpatched and unsupported software ➔ malware)
  o Cornell Prescription Pharmacy ($125K) (paper)
  o St. Elizabeth’s Medical Center ($218K) (document sharing software)
  o Triple-S Management Corp. ($3.5M) (settlement) (also fined by $6.8M by Puerto Rico insurance regulator)

  o Cancer Care Group ($750K) (stolen laptop)
  o Lincare, Inc. ($239K) (Feb. 3, 2016) (fine; case initiated on June 23, 2009)
  o North Memorial Health Care of Minnesota ($1.55M) (March 16) (no BAA)
  o Raleigh Orthopaedic Clinic, P.A. of North Carolina ($750K) (April 19) (no BAA)
  o Catholic Health Care Services of the Archdioceses of Philadelphia (June 29) ($650K)
  o Oregon Health & Science Univ. (July 18) ($2.7M)
  o Univ. of Miss. Medical Center (July 21) ($2.75M)
  o Advocate Health Care Network (Aug. 4) ($5.55M)
  o Care New England Health System (Sept. 23) ($400K) (old BAA)
  o Presence Health (Jan. 9, 2017) ($475K) (Failed to timely notify of breach)
Ransomware Risks

Source: Ponemon Institute, 2016 Cost of a Data Breach Study (US only data)
Ransomware Risks

Director/Officer Liability
Ransomware Risks

Director/Officer Liability

"If we rewind the tape, our security systems could have been better...Data security just wasn’t high enough in our mission statement."

Frank Blake, Home Depot’s recently retired Chief Executive Officer and Current Chairman of the Board

FINANCIAL INSTITUTION PLAINTIFFS’ CONSOLIDATED CLASS ACTION COMPLAINT

"If we rewind the tape, our security systems could have been better...Data security just wasn’t high enough in our mission statement."

Frank Blake, Home Depot’s recently retired Chief Executive Officer and Current Chairman of the Board
Prevention/Mitigation of Risk

“Cybersecurity Framework”

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover
Case Study

• Primary Care Office
• PA seeks access to patient medical record
• Clicks on record, receives a message stating that files have been encrypted, and payment is required to decrypt files
What Do You Do?

1. Restart the computer…
2. Send everyone an e-mail and let them know there was a breach
3. Contact the Security Officer
4. Call OCR to report because ransomware is a reportable breach
Case Study: Respond

**DO:**

1. Contact Security Officer – preferably by phone/in person
2. Security Officer contact internal or external resource responsible for technical security
3. Bring counsel into the loop
4. Initiate redundant systems, if available
5. Investigate existence and scope of encrypted data
6. Engage forensic resources as needed
7. Contact Law Enforcement

**What about your insurance company?**
Case Study: Respond

DO NOT:

1. Email blast “we have a problem” or “we have a breach”
2. Try and open other files
3. Try to hide the incident
4. Write a check
5. Call the NY Times
6. Otherwise discuss the matter unless authorized to do so
Case Study: Respond

When to Pay:

- Case-by-case assessment
- Consult law enforcement
- Depends on redundancy – good planning = little or no leverage for bad actor
- Depends on ability to recover (absent redundancy)
- If you pay once, you should be motivated to never have to pay again
How Much Did Your Organization Pay?

$0.00

less than $500

less than $5,000

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
Case Study: Recover

• Tactical Phase

• Strategic Phase

Source: Guide for Cybersecurity Event Recovery
Draft NIST Special Publication 800-184
Case Study: Tactical Phase

- Collaboration with Response Team
- Develop solid understanding of situation/scope
- Use care not to alert adversary
- Gain infrastructure control
- Prioritize restoration of system components (mission critical 1st)
- Execute restoration
Case Study: Strategic Phase

• Lessons Learned –
  – What did this incident teach about the organization’s Cybersecurity Framework (Identify, Detect, Respond, Recover)?

• Find the gaps/plug the gaps

• The “Playbook” concept for cybersecurity preparedness
Final Thoughts

1. The effectiveness of your response/recovery functions depends on the quality of your Playbook

2. The quality of your Playbook depends on the effort expended on your implementation of the CSF

3. A well-constructed and properly implemented Playbook, and particularly the response/recovery functions elements of that Playbook, will directly impact consideration of whether ransom must be paid
Krebs’s Immutable Truths About Data Breaches

• “If you connect it to the Internet, someone will try to hack it.”
• “If what you put on the Internet has value, someone will invest time and effort to steal it.”
• “Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.”
• “The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.”
• “Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets.”

So, where to get the most bang for your buck?

Source: Ponemon Institute, 2016 Cost of a Data Breach Study (US only data)
A Summary of How Benefits Were Realized for the Value of Health IT

Satisfaction: A quality Playbook = sleep insurance

Treatment/Clinical: A well-constructed response/recovery function will ensure continued availability of treatment

Electronic Secure Data: Adherence to the protect function will minimize risks attendant to data breaches

Patient Engagement: Knowledge of your adherence to CSF will increase patient trust/engagement

Savings: Implementation of CSF = avoidance of downtime, fines/penalties, and reputational harm
Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of ransomware risks and legal issues. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the legal topics covered in this presentation.
Questions

Tatiana Melnik
Attorney, Melnik Legal PLLC
Based in Tampa, FL
734.358.4201
tatiana@melniklegal.com

Brian Balow
Member, Dawda Mann PLC
Based in Bloomfield Hills, MI
248.642.6212
bbalow@dmms.com

Please complete the online session evaluation!