Protecting the Castle: Avoiding, Addressing, and Mitigating Ransomware

Cathlin E. Sullivan, Esq.
William P. Conaboy Jr., Esq.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

www.bipc.com

Recent Headlines

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

www.bipc.com

KIM ZETTER SECURITY 03.30.16 01:31 PM

WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE

Cyber-Safe

Why hospitals are so vulnerable to ransomware attacks

by Selena Larson @selenalarson

May 16, 2017: 1:46 PM ET

Recommend 3

3

Home > Security

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO

FEB 14, 2016 3:43 PM PT

About

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

NEWS

Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers

Network has been offline fore more than a week, $3.6 million demanded as ransom

BUSINESS / Technology

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

4

Privacy & Security

Methodist Hospital recovering from five day ransomware attack, claims it did not pay up

Cybercriminals locked down enough of the Kentucky hospital's data that it was forced to declare an internal state of emergency. Now officials are saying they resolved the situation without giving into attackers' demands.

By **Bernie Monegain** | March 22, 2016 | 09:47 AM

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

5

Spokeswoman Ann Nickels said that its facilities, which stretch from Arlington to Baltimore, have operated safely throughout the crisis.

But two nurses said the cyberattack created a chaotic environment in at least one MedStar location, and a doctor at another facility said it had created a "patient safety issue."

At MedStar Washington Hospital Center, one nurse who worked

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

6

Hackers offering bulk discount to unlock encrypted MedStar data

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

7

What is ransomware?

- Malicious software
- Encrypts data and renders the data unreadable and unusable.
- Once complete, user is notified that the encryption has occurred, and a ransom is demanded.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

8

HOWEVER…

- Paying a ransom is not a guarantee that your data will be returned – or that it wasn't and/or won't be disclosed.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

9

How does ransomware get in?

- Hacking
- Malicious email
  - Spoofing
  - Phishing and Spear Phishing
- Outdated/default credentials
- Easy-to-guess passwords

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

10

Phishing Emails

- **156 million** phishing email messages are sent out each day
  - **16 million** get past spam and phishing filtering tools

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

11

What data is at risk?

- Anything internet-connected – and anything connected to that data.
  - Medical records
  - Operating systems
  - Medical devices
  - Devices on the Internet of Things

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

12

How to Prevent Ransomware

- You can't.
- BUT
  - You can prepare your organization and train your staff to identify, avoid, and mitigate ransomware.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

13

Breach Response

- Activate security response plan and team
  - Take systems offline
  - Bring in outside consultants (lawyers, forensic analysts)
  - Notify law enforcement
  - Evaluate scope of incident
  - Risk Assessment
  - Data review
  - Breach notifications **within 60 days**

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

14

HIPAA Considerations

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

www.bipc.com

15

HIPAA Considerations

- PHI: individually identifiable information that relates to the provision of healthcare services to an individual.
  - Information stored in an EHR is a primary example of individually identifiable PHI.
- The Security Rule sets out how a covered entity must protect the confidentiality, integrity, and availability of ePHI, and requires administrative, physical, and technical safeguards.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

16

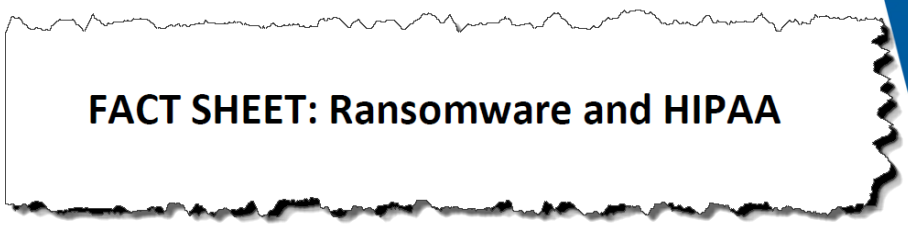
HIPAA Considerations

- Security Awareness and Training
  - Addressable
  - Can include anti-virus software, email scanning, and workforce training.
  - Also: access controls that limit access to the minimum necessary
- Risk Analysis
  - Identify risks and vulnerabilities, and create risk management plan

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

17

Is Ransomware a Breach?



https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

18

OCR Guidance

- Ransomware is a "presumed breach"

> Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the

  - A breach is the "acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of PHI."
  - Data encryption is considered "acquisition," because bad actors have taken possession and control of the data.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

19

Risk Assessment

- Must do fact-specific risk assessment
- Assess probability of compromise
  - Nature and extent of PHI
  - Unauthorized person who used PHI or to whom the disclosure was made
  - Whether PHI was actually acquired or viewed
  - Extent to which risk to PHI has been mitigated

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

20

Risk Assessment

- Four factors allow for fact-specific review of risk of compromise to the PHI.
- If result does not demonstrate low probability of compromise, incident must be treated as a breach.
  - Reminder: OCR considers ransomware to be a "presumed breach," so any finding of LoProCo must be well-supported.
- Maintain written RA and supporting documentation.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

21

What about encryption?

- With ransomware, is a factual inquiry
- Encryption must actually render the data unreadable, unusable, and indecipherable.
  - If machine encrypted only while powered down, but while using the machine a user clicks on a malware link that infiltrates the system, data is not encrypted at that point.

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

22

Breach Reporting

- Reports must be made within 60 days of incident
  - Reports are based on number of affected individuals, and separate reports may be required under state law
  - Law enforcement may request delay in reporting

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

23

Best Practices

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

www.bipc.com

24

Best Practices

- Employee awareness and training
  - Strong passwords
  - How to identify malware, including ransomware
  - Update credentials and permissions regularly
- Frequent backups, including offline backups
- Installation and management of patches
- A well-crafted, well-practiced security incident plan
- Tabletop breach exercises

Buchanan Ingersoll Rooney PC | KNOW GREATER PARTNERSHIP

25