How to Navigate and Survive a Mega Breach

Regina Verde | Compliance and Privacy Officer, University of Virginia Health System (Moderator)
Nadia Fahim-Koster | Director, IT Risk Management, Meditology Services
Erin Dunlap | Shareholder, Polsinelli, PC
Abby Bonjean | Associate, Polsinelli, PC

MEDITOLOGY SERVICES

POLSINELLI

Ransomware Attack – Hollywood Presbyterian Medical Center, CA (2016)

- Ransomware virus called Locky
  - Usually spread via email
- An employee must have clicked on the link, activating the virus
- Access to network and data was locked
- Paid 40 Bitcoin (approximately $17,000) to regain access
- How can we respond to and survive such incidents?

The Locky screen of death

2

Reference: Sienko, Chris. "Ransomware Case Studies: Hollywood Presbyterian and The Ottawa Hospital." InfoSec Resources. http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref

Discovery, Investigation, Data Evaluation and Remediation

- What plans does your organization have in place to handle an incident?
- Do you have a Security Incident Response Team (SIRT)?
- Correcting and/or containing the cause of the breach
- Identifying the scope of the breach
  - Consider hiring outside forensic analyst
- Do you have insurance that may cover the data breach?
  - Review scope of coverage and provide proper notice
- Was the breach caused by the act of a third-party vendor?
  - Review applicable contracts
- Should you engage law enforcement?

3

Notification Process and Mitigation Strategies

- When do you move from an "IT centric" incident response to notify compliance, legal, public relations...etc.?
- Who to notify and when?
- What to consider when hiring outside vendors?
- What services should you provide affected individuals?
- Sanction workforce member(s) involved
- Retrain all workforce members (or specific department) to reduce likelihood of incident reoccurring
- Review any relevant policies and procedures and revise if necessary
- Cooperate with the various enforcement agencies

4

Lessons Learned and Recommendations for Prevention

- Have a post-breach meeting and revise incident response plan, if necessary
- Conduct tabletop exercises
- Establish relationships with vendors (e.g., forensic analysts and notification vendors)
- Obtain cyber liability insurance
- Know where your ePHI is and safeguard it appropriately
- Educate, educate, educate!
  - Remind employees of cybersecurity risks
- Document, document, document!

5

Questions?

Regina Verde (Moderator)
Compliance and Privacy Officer
University of Virginia Health System
RV5H@hscmail.mcc.virginia.edu

Nadia Fahim-Koster
Director, IT Risk Management
Meditology Services
Nadia.Fahim-Koster@meditologyservices.com

Erin Dunlap
Shareholder
Polsinelli, PC
edunlap@polsinelli.com

Abby Bonjean
Associate
Polsinelli, PC
abonjean@polsinelli.com

6