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

MED**IT**OLOGY
S E R V I C E S

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?

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org/DF709D1E553E78EF
    2. http://6dtxgqam4crv6rr6.onion.to/DF709D1E553E78EF
    3. http://6dtxgqam4crv6rr6.onion.cab/DF709D1E553E78EF
    4. http://6dtxgqam4crv6rr6.onion.link/DF709D1E553E78EF

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/DF709D1E553E78EF
    4. Follow the instructions on the site.

!!! Your personal identification ID:

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
  - o Consider hiring outside forensic analyst
- Do you have insurance that may cover the data breach?
  - o Review scope of coverage and provide proper notice
- Was the breach caused by the act of a third-party vendor?
  - o 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!
  - o 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