Cyber Attacks and Breaches: How Prepared are You?

Angela Rose, MHA, RHIA, CHPS, FAHIMA
Director, HIM Practice Excellence

AHIMA
American Health Information Management Association®

© 2016

Agenda

- Environmental Scan
- Statistics
- Proactive/Reactive Privacy Aspects of Cybersecurity
- Impacts of Cybersecurity
- Incident Response and Investigation
- Guidance Solutions
- Questions/Discussion

© 2016

Environmental Scan

TARGET	ANTHEM	PREMERA	EXCELLUS BCBS
DATE	2/4/2015	1/2015 (Hacked) 3/2015 (Discovered)	2/9/2015
# RECORDS ACCESSED	78.8 million	11.2 million	10 million
INFORMATION TYPE	Social Security numbers, member ID numbers, other personal data	Social Security numbers, member ID numbers, bank account information, other data	Social Security numbers, member ID numbers, financial account information, other data

© 2016

Environmental Scan

- **Carefirst BlueCross BlueShield**
  - Hacked in May 2015
  - 1.1 million
  - Names, birth dates, email addresses
  - Encryption protected social security#, credit card and financial data

- **Hollywood Presbyterian Hospital**
  - Ransomware
  - Hackers holding data hostage for $3.4 million
  - Everything from emails to CT scans – providers using paper

© 2016

Statistics

- 81% of healthcare organizations have experienced a cyber attack but only 53% considered themselves ready to defend themselves. *(2015 KPMG Cybersecurity Survey)*

- 40% of consumers said they'd leave a health system that's been hacked and 50+% said they'd hesitate to use a health system if they were breached *(Healthcare Finance)*.

- A breach is estimated to cost $363+ per patient. *(2015 Cost of a Data Breach Study, Ponemon Institute)*

© 2016

Being Proactive

- Risk Analysis
- Education and Training
- Marriage between IT and the Privacy Officer/HIM Department

© 2016

Being Proactive

- Established and Implemented Plan

- Access Control
  - Process
  - Types of Access
  - Roles

- Remote Access
  - When/when not
  - Who
  - What

- Auditing and Monitoring – how you monitor
  - Identify gaps and loop holes
  - Make sure you're seeing what you need to see

© 2016

Being Reactive

- Putting the plan into action!
- Timeliness to respond and act
- Sanctions
- Mitigate! Mitigate! Mitigate!

© 2016

Impacts of Privacy/Cybersecurity

Effective

- TRUST from patients
- TRUST from workforce
- TRUST from/between vendors

- Reputation in the community

Lack of

- Lose trust
- Lose reputation
- Open to incidents and breaches
- Open up to government audits

© 2016

Incident Response and Investigation

1. Potential privacy/security violation reported
2. Investigate and document
   a) Did a breach occur?
3. If breach determined, perform a *breach risk assessment*
4. Notify individuals
5. Report to HHS accordingly
6. Mitigation/Sanctions
7. Feedback

© 2016

Guidance Solutions

Free to the Industry

- Practice Briefs
  - Understanding Cybersecurity *(Coming in April!)*
  - Navigating a Compliant Breach Management Process
  - Performing a Breach Risk Assessment
  - Security Risk Analysis and Management: An Overview (Updated)
  - Privacy and Security Audits of Electronic Health Information (Updated)
  - E-Discovery Litigation & Regulatory Investigation Response Planning

© 2016

More Guidance Solutions

- Advanced Breach Management Virtual Meeting | April 6
- Privacy and Security Institute | October 15-16
- Various webinars

© 2016

Questions

© 2016