CYBERSECURITY OVERVIEW

Doug Shackelford
Information Security Officer
The Queen's Health Systems

Agenda

- Introduction
- HIPAA Security Rule
- Risk Management
- Security Challenges
- Security Program & Trained Workforce
- Key Risks & Mitigation
- Summary

Introduction

THE QUEEN'S HEALTH SYSTEMS

- Security program covers The Queen's Health Systems (QHS)
  - *The 4 hospitals (Punchbowl, West Oahu, Molokai General Hospital & North Hawaii Community Hospital)*
  - *Diagnostic Laboratory Services & CareResource Hawaii*
  - *The Queen Emma Land & Development entities*
- This includes approximately
  - *7,000 employees*
  - *1,900 medical staff (a portion of which are employees)*
  - *Vendors & contractors with access to sensitive information*

3

Introduction

THE QUEEN'S HEALTH SYSTEMS

- Security group
  - *Technical team (5, includes the Manager) – manages technical controls and incident response*
  - *Privacy Analyst (1) – data loss monitoring & prevention program*
  - *IT Disaster Recovery Coordinator (1) – IT disaster recovery & business continuity planning*
  - *Together, group also responsible for risk management, vendor management, awareness & training, reporting*
- Information Technology (IT) Relationship
  - *A part of QHS IT reporting to the Chief Information Officer (CIO)*
  - *Work closely with affiliate IT staff*

4

HIPAA Security Rule
Overview

- A Covered entity must
  - *Ensure the Confidentiality, Integrity & Availability (CIA) of ePHI*
  - *Protect against any reasonably anticipated threats to CIA*
  - *Protect against any reasonably anticipated unauthorized ePHI disclosures*
- Includes two types of standards
  - *Required. These must be implemented*
  - *Addressable. There is some flexibility based on if the requirement is reasonable and appropriate*

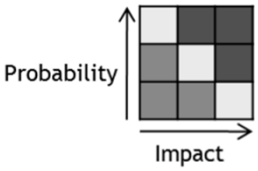
5

HIPAA Security Rule
Overview

- Managing 'reasonable', 'anticipated', 'appropriate'
  - *Risk assessment*
  - *Required standard*
- In addition to HIPAA, QHS Security Program
  - *Ensure compliance to the Hawaii breach notification requirements*
  - *Cover all sensitive data including PII, financial information, QHS proprietary*
  - *Cover physical and electronic media*
  - *ISO 27001 Standard was used to initially develop the program*

6

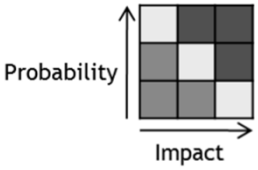
Risk Management
Overview



- What HIPAA states
  - *Conduct a thorough assessment of the risks to CIA*
  - *Implement security measures (i.e. controls) to reduce risks to a reasonable and appropriate level*
  - *Security measures must be review/modified as needed*
- QHS approach
  - *Risk management drives the security program*
  - *Ongoing process with continual updates as threats change, controls are implemented and new services are evaluated.*
  - *Do produce an annual HIPAA Risk Assessment report which is a point-in-time view of QHS risk posture*

7

Risk Management
Approach



- The basics
  - *Identify threats and risks (real-world examples to follow)*
  - *Assess existing controls for applicability and effectiveness to mitigate risks*
  - *Rate risks based on likelihood and potential impact*
  - *Develop plans to address any risks rated above tolerance*
- Considerations
  - *This is purposely a simple approach to facilitate easy training and maximum involvement of IT & non-IT experts and stakeholders*
  - *Executive management and/or oversight involvement key in developing impact thresholds (i.e. risk appetite). Example, how much financial loss would be considered 'high' impact.*
  - *The FFIEC IT Handbook (for financial institutions) has practical information on how to develop a risk management program.*

8

Security Challenges

- New controls may be met with resistance
  - *May mean additional steps to perform one's job*
  - *Monitoring may be seen as intrusive*
  - *May be seen as an impediment to business*
- Risk Management Benefits
  - *Ensure risk is evaluated by objective criteria*
  - *Ensure proposed control will reduce the risk*
  - *Encourages participation and input*
  - *Facilitates communication and therefore understanding & buy-in on why the control is necessary*

9

Security Program & Trained Workforce

Trained employees are arguably the most important component of a successful security program.

- Security policies and procedures
- New hire and annual Compliance training incorporates security training
- Communication opportunities when incidents occur (QHS-specific or broad issues such as ransomware attacks)
- Targeted training on specific threats (see 'phishing' below)
- Counseling on policy violations (see 'data loss' below)

10

Key Risks & Mitigation

In addition to a trained workforce:

- The following slides detail the key threats that QHS faces (as determined by the Risk Management program)
- Included with each threat are some of the steps QHS has taken to mitigate the risks
- None of these risks are unique to QHS

11

Data Loss

Inappropriate transmission of sensitive data

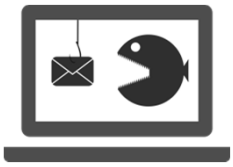
- E-mail to unauthorized recipient
- Internet uploads (Dropbox, attached to Gmail/Yahoo)

Data loss monitoring (aka Data Loss Prevention – DLP)

- Monitoring all outbound e-mail and Internet traffic
- DLP system uses rules to identify certain fields (such as SSN)
- System also utilizes 'fingerprinting' which involves uploads of QHS-specific information (such as medical record numbers)
- Violators are notified and asked to ensure deletion of the data
- Violations are escalated based on data quantity

12

Phishing



E-Mails crafted to entice the recipient to perform a risky function

- Click malicious links or attachments
- Send a wire or provide confidential information to the fraudster

Mitigate with a combination of user training and filtering controls

- Workforce trained during compliance training and with periodic fake phishing campaigns (those who succumb are auto-enrolled in additional training)
- Workforce procedures to report the phish so that we may block links and other actions to eliminate the threat
- E-Mail filtering to blocks the majority of malicious e-mail (on average QHS blocks 65% of external e-mail)
- Adding a banner to indicate e-mail originated from an external source to encourage diligence

13

Loss or Theft

Lost or stolen laptop, phone, USB drive

- Company owned or employee device
- Concern if device houses sensitive information or is set up to access company resources

Tight controls over devices that are not in physically secure locations

- Full disk encryption of all desktops & laptops
- Mobile device management for any device that can access e-mail
- Restrict USB access to only approved devices (i.e. those encrypted with password protection)

Note: While HIPAA lists encryption as an addressable control, history shows that fines & penalties can be large when lack of encryption leads to a breach.

14

Malware (including Ransomware)

Malware is broad term to include malicious programs, including virus and ransomware

- Create a path for hacker to control a system, exfiltrate data
- Ransomware encrypts files and requires payment in order to retrieve the unlock key
- Other mischief such as logging passwords or denial of service attacks

Common delivery method is e-mail so previously mentioned e-mail filtering & phish controls, plus

- Web filtering to block malicious sites
- Workstation controls such as anti-virus software
- Patching and backups

15

Web Browsing

Overlaps with other risks (see Malware, Data Loss); additionally

- Known bad sites
- Legitimate sites that have been compromised
- Inappropriate (gambling, adult) or abuse of company resources (excessive bandwidth usage)

Additional use of filtering tools

- Multiple layers to detect 'bad' or compromised sites
- Policy enforcement for inappropriate sites
- Logging for forensics or when bandwidth utilization research needed

16

Unauthorized Access

Access to applications & infrastructure

- Employee, contractor or other workforce member accesses resources inappropriately
- Terminated/disgruntled workforce member with intent to do harm
- Hacker

Various controls

- Manage terminations – timely access removal
- Periodic revalidations
- Monitoring (see 'Undetected Event')
- Password complexity, idle timeout, dormant account disable
- Multi-factor authentication (when warranted by risk)

17

Undetected Event

Event occurs that breached other defenses

- Hacker
- Malware
- Physical Intruder

Security Operations – monitoring & incident response

- Sensors at key points of infrastructure & applications
- Logs from malware and web/e-mail filtering tools
- Authentication systems logs
- Security Incident & Event Management (SIEM) tool combined with 24x7 Security Operations Center (SOC) monitoring.

18

Vendor, 3rd Party Risk

Risk that a vendor is compromised

- Susceptible to any of the above risks
- Breach of our data entrusted to their care
- Launching point to hack QHS systems

Vendor Security Management

- Accredit the security program of vendors that will receive sensitive information and/or perform high risk functions
- Periodically review accreditation (period set by risk)
- Tightly limit access to internal resources

19

Summary

Key takeaways

- Risk management program is essential to validate controls, identify gaps and prioritize remediation.
- Understand the HIPAA Security Rule and ensure requirements are met/addressed
- Additional standards available to guide program development such as ISO & NIST
- Various tools are available to validate a security program: HHS Risk Assessment tool, HITRUST cross reference spreadsheet, security consultants, etc.
- Balanced approach; ensure business needs are met and that security does not place an onerous burden on the organization.

20