ANATOMY OF AN ATTACK & KEY SECURITY TRENDS
Kevin Dunnahoo

HEALTHCARE CYBERSECURITY TRENDS
CERTAINTIES...

Death
Taxes
Breaches
Government Audits

SNAPSHOT

195,415,696
Patients Impacted

2500+
# of reported breaches

75%
records breached from hacking / IT incident

Statistics as of 2/15/2019 from OCRPortal.hhs.gov
ENFORCEMENT

Key Recent HIPAA Settlement Agreements

21st Century Oncology – $2.3M December 2017

- What: Hacker compromised 2.2M records
- How: SQL databases through RDP from an exchange server
- Issues: Risk Analysis, data protection, monitor activity/logs, BAAs
- When: Identified in 2015 – Ch. 11 Bankruptcy 2017

MD Anderson Cancer Center – $4.3M June 2018

- What: Failure to remediate known security risks
- How: Unencrypted laptop and USB drives
- When: Breaches occurred in 2012 and 2013

2018 BREACHES

- Alive Hospice – Phishing
- Med Associates – Workstation compromise
- Cass Regional – Ransomware
- Manitowoc County – Phishing
- Aultman Health Foundation – Phishing
- LifeBridge Health – Malware/Network compromise (2016-2018)
- Center for Orthopaedic Specialists California – Ransomware
OCR’S RECURRING ISSUES

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g., Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal [of PHI]
- Insufficient Data Backup and Contingency Planning

ELEMENTS OF A RISK ANALYSIS

- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures
- Determine the Likelihood of Threat Occurrence
- Determine the Potential Impact of Threat Occurrence
- Determine the Level of Risk
- Finalize Documentation
- Periodic Review and Updates to the Risk Assessment

Nine key risk analysis elements that must be incorporated according to OCR
ANATOMY OF AN ATTACK

- Recon
- Foothold
- Escalate
- Lateral Movement
- Action
ANATOMY OF AN ATTACK

1. Recon
   - Build a deep understanding of the target

2. Foothold
   - Obtain initial access to the network or system

3. Escalate

4. Lateral Movement

5. Action
ANATOMY OF AN ATTACK

1. **Recon**
   - Build a deep understanding of the target

2. **Foothold**
   - Obtain initial access to the network or system

3. **Escalate**
   - Establish persistence on the network and gain elevated access

4. **Lateral Movement**
   - Move throughout the network to locate sensitive systems/data

5. **Action**

---

13 protiviti
ANATOMY OF AN ATTACK

- **Recon**: Build a deep understanding of the target
- **Foothold**: Obtain initial access to the network or system
- **Escalate**: Establish persistence on the network and gain elevated access
- **Lateral Movement**: Move throughout the network to locate sensitive systems/data
- **Action**: Perform action on the objective

PLANNING A PREEMPTIVE STRIKE
THINKING LIKE THE ATTACKERS

- **Attacker Objective:** What are we going to attack?
- **Testing Objective:** What attack surface do we need to secure?
- **Example Approach:** Open-Source Intelligence Gathering and Network Scanning

---

**Challenges**

- Do we know our entire attack surface?
- What about our vendors/partners/joint ventures?
- External and Internal, Cloud, Devices, M&A

**Regulatory tie in**

- HIPAA Security Risk Analysis §164.308(a)(1)(ii)(A) – Scope and Data Collection
- Business Associate Agreements §164.308(b)(1) & Contractual Agreements
THINKING LIKE THE ATTACKERS

- **Attacker Objective:** Can we break into a network?
- **Testing Objective:** Are we protected from external unauthorized access?
- **Example Approach:** External network assessments, social engineering/phishing assessments.

---

THINKING LIKE THE ATTACKERS

- **Challenges**
  - Limited Multi-Factor Authentication (MFA) capabilities
  - Legacy systems/devices unable to be patched timely
  - Complex network environments
  - Complex user access needs

- **Regulatory tie in**
  - HIPAA Security Risk Analysis §164.308(a)(1)(ii)(A) – Identify Threats and Vulnerabilities
  - HIPAA Security Evaluation §164.308(a)(8) – Technical Assessment
THINKING LIKE THE ATTACKERS

- **Attacker Objective**: Can we leverage our foothold to gain additional, more critical access?
- **Testing Objective**: Are our most critical systems and accounts properly protected from compromise?
- **Example Approach**: Internal network assessments, workstation compromise assessments, privilege access management review.

**Challenges**

- Non-centralized user access management
- Management of vendor support accounts
- Management of elevated privilege accounts
- Monitoring of user activity

**Regulatory tie in**

- HIPAA Security Person or Entity Authentication §164.312(d)
THINKING LIKE THE ATTACKERS

**Attacker Objective:** Can we use our current access to move throughout the network and gain further access and data?

**Testing Objective:** Is our network designed to detect or minimize the impact of ongoing breaches?

**Example Approach:** Network segmentation review, cyber defense capabilities review, purple teaming.

---

**Challenges**

- Flat networks
- Inability to identify anomalous activity
- Who is responsible for detecting and can they?
- Lack of drills/testing

**Regulatory tie in**

- HIPAA Security Risk Analysis §164.308(a)(1)(ii)(A) – Assess Current Security Measures
THINKING LIKE THE ATTACKERS

- **Attacker Objective:** How can we leverage access to impact the organization or obtain financial reward?
- **Testing Objective:** What are our most critical assets and how are we protecting them?
- **Example Approach:** Data exfiltration simulation, ransomware test, attack simulation, incident response exercise.

Challenges

- Ability to identify what is sensitive data
- Understanding of what authorized traffic is vs. unauthorized (encrypted traffic = free pass?)
- Vast number of data exchanges used (gov't., vendors, JVs, partners, care continuum, etc.)

Regulatory tie in

- HIPAA Security Incident Response Procedures §164.308(a)(6)(ii)
SUMMARY

REALITY OF TODAY

Key Cybersecurity Challenges in Healthcare

- Attracting and retaining Cybersecurity talent
- Large population of vendors
- Cloud environments
- Medical Devices / IoT
- Digital everything
- Growing M&A creating super systems
- Value of data, need for use, sharing
- Ever-changing threat landscape

Trending Risk Areas

- IT Vendor Management
- Medical Devices
- The Internet of Things (IoT)
- User Authentication / Passwords
- Business Continuity / Disaster Recovery
- Vulnerability Management
- Social Engineering
- Ransomware

---

protiviti
Kevin Dunnahoo
CISPP, HCISPP, ABCP, ITIL
Associate Director
kevin.dunnahoo@protiviti.com
Phone: (972) 788-8529

Kevin is an Associate Director with Protiviti’s National Healthcare Practice, and is a key lead for Healthcare IT, Cybersecurity, and HIPAA Compliance services. In the Healthcare industry, Kevin has provided value to his clients through his insights and understanding of how IT works in the Provider environment, how to navigate and comply with HIPAA, assessments against various security frameworks, business continuity readiness, as well as deep expertise in providing IT audits. He has also authored various Protiviti thought leadership pieces and presents at national and regional conferences and webinars.