Top Security Threat Trends in Healthcare and How You Can Learn from Incidents to Reduce Risk

Mac McMillian, FHIMSS, CISM, CEO/Co-Founder CynergisTek
Dr. Cris V. Ewell, Ph.D., CISO Seattle Children’s
Mahmood Sher-Jan, CHPC, EVP/GM ID Experts
April 19, 2015

Agenda
• Top Security Threat Trends in Healthcare
• Growing Regulatory Complexities
• Trends in Healthcare: Incidents & Breaches
• Keys to Being Prepared for Managing Incidents
• Real World Incident Response Cases
• Insights From Analysis of Real Incident Data
• Tools and Methodologies for Correlating Incidents and Managing Incident Response

The Face of Cybercrime Today
• 12 y/o learning computers in middle school
• 14 y/o home schooled girl tired of social events
• 15 y/o in New Zealand just joined a defacement group
• 16 y/o in Tokyo learning programming in high school
• 19 y/o in college giving course work to work
• 20 y/o fast food employee that is bored
• 22 y/o in Mali working in a carding ring
• 24 y/o black hat trying to hack whoever he can
• 25 y/o soldier in East European country
• 26 y/o contractor deployed overseas
• 28 y/o in Oregon who believes in hacktivism
• 30 y/o white hat who has a black hat background
• 32 y/o researcher who finds vulnerabilities in systems
• 35 y/o employee who sees a target of opportunity
• 37 y/o rogue intelligence officer
• 39 y/o disgruntled admin passed over
• 42 y/o private investigator
• 44 y/o malware author paid per compromised host
• 45 y/o pharmacist in midlife crisis
• 55 y/o nurse with a drug problem

4/15/2015
### Accidents, Mistakes & Deliberate Acts
- 4M medical records maintained on four workstations
- Physician loses laptop with psychiatric patients records
- Neurologic institute accidentally emails 10,000 patient records to 200 patients
- Phishing/hacking nets nearly $3M from six healthcare entities
- University reports laptop with patient information stolen out of a student's car
- Vendor sells hospital's knives (RFM) to third party
- Resident loses track of USB with over 500 orthopedic patients information
- Portable electronic device with patient data stolen from hospital
- Physician has laptop stolen from vacation home
- Printers returned to leasing company compromise thousands of patient records
- Health System reports third stolen laptop with 13,000 patient records
- 2200 physicians victims of ID theft lose head
- Physician notified at gun point, phone and computer taken, thief demands passwords
- International hacking group uses phishing, then steals information on almost 80M people
- And, on and on it goes...

### The Emergent Threat
**Black Hat 2014**
- Snatching passwords w/ Google Glass
- Screen scraping VDI anonymously
- Compromising AD through Kerberos
- Remote attacks against cars
- Memory scraping for credit cards
- Compromising USB controller chips
- Cellular compromise through control code
- Free cloud botnets for malware
- Mobile device compromise through MDM flaws
- Cryptographic flaws and a Rosetta Stone

### Black Market Driven
- Darknets will be more active, participants will be vetted, cryptocurrencies will be used, greater anonymity in malware, more encryption in communications and transactions
- Black markets will help attackers outpace defenders
- Hyperconnectivity will create greater opportunity for incidents
- Exploitation of social networks and mobile devices will grow
- More hacking for hire, as-a-service, and brokering
Increased Reliance

More than 98% of all processes are automated, more than 98% of all devices are networkable, more than 95% of all patient information is digitized, accountable care/patient engagement rely on it. The enterprise is critical to delivering healthcare. Any outage, corruption of data, loss of information risks patient safety and care.

Insider Abuse: Trust, But Verify

- It is estimated that more than half of all security incidents involve staff
- 51% of respondents in a SANS study believe the negligent insider is the chief threat
- 37% believe that security awareness training is ineffective
- Traditional audit methods & manual auditing is completely inadequate
- Behavior modeling, pattern analysis and anomaly detection is what is needed

Questionable Supply Chains

- Greater due diligence in vetting vendors
- Security requirements in contracting should be SLA based
- Particular attention to cloud, SaaS, infrastructure support, critical service providers
- Life cycle approach to data protection
- Detailed breach and termination provisions
Devices Threaten Safety & Information

In June 2013 the DHS tested 300 devices from 40 vendors, ALL failed. In response the FDA issued guidance for manufacturers and consumers addressing design, implementation and radio frequency considerations.

“Yes, Terrorists could have hacked Dick Cheney’s heart.”
- The Washington Post
October 21, 2013

Malware & Persistent Threats

- 3.4 million Botnets active
- 20-40% of recipients in phishing exercises fall for scam
- 26% of malware delivered via HTML, one in less than 300 emails infected
- Malware analyzed was found undetectable by nearly 50% of all anti-virus engines tested
- As of April 2014 Microsoft no longer provides patches for WN XP, WN 2003 and WN 2000, NT, etc.
- EDL systems still prevalent in healthcare networks
- Hardening, patching, configuration, change management…all critical

Mobility & Data

- Medical staff are turning to their mobile devices to communicate because its easier, faster, more efficient...
- Sharing lab or test results, locating another physician for a consult, sharing images of wounds and radiology images, updating attending staff on patient condition, getting direction for treatment, locating a specialist and collaborating with them, transmitting trauma information or images to EDs, prescribing or placing orders
- Priority placed on the data first and the device second
- Restrict physical access where possible, encrypt the rest
ID Theft & Fraud

- Medical identity theft increased 21.7% in 2014, Ponemon Institute
- US CERT estimates 47% of cybercrime aimed at healthcare
- More than 70% of identity theft and fraud were committed by knowledgeable insiders – physicians, nurses, pharmacy techs, admissions, billing, etc.
- Healthcare-directed attacks have increased more than 20% a year for the last three years running
  - Insiders selling information to others
  - Hackers exploiting systems
  - Malware with directed payloads
  - Phishing for the "big" ones

Theft & Losses Thriving

- 68% of healthcare data breaches due to loss or theft of assets
- 1 in 4 houses is burglarized, a B&E happens every 9 minutes, more than 20,000 laptops are left in airports each year...
- First rule of security: no one is immune
- 138%: the % increase in records exposed in 2013
- 6 – 10%: the average shrinkage rate for mobile devices
- Typical assets inventories are off by 60%

"Unencrypted laptops and mobile devices pose significant risk to the security of patient information." – Sue McAndrew, OCR

Hacking & Other Cyber Criminals

- Defenses are not keeping pace
- Three most common attacks: spear phishing, Trojans & Malvertising
- API's, phishing, water cooler attacks, fraud, etc.
- Most organizations can't detect or address these threats effectively
  - An advanced incident response capability is required
  - Results in loss of time, dollars, downtime, reputation, litigation, etc.
  - Conduct independent risk assessments regularly

"I feel like I am a targeted class, and I want to know what this institution is doing about it!" – Anonymous Doctor
More Compliance

- OIG shifts focus to funds recovery
- OIG’s permanent audit program will resume in FY 2015 with new capabilities
- Improvements and automation in reporting and handling complaints
- Meaningful Use audits are evolving in scope and impact
- The FTC remains committed to enforcement of privacy and security
- States continue to create new laws
  - Florida Information Protection Act
  - New Jersey Health Insurers Encryption Law
  - SB1353 seeks to establish common framework for security and create universal requirement for notification.

Agenda

- Top Security Threat Trends in Healthcare
- Growing Regulatory Complexities
- Trends in Healthcare: Incidents & Breaches
- Keys to Being Prepared for Managing Incidents
- Real World Incident Response Cases
- Insights From Analysis of Real Incident Data
- Tools and Methodologies for Correlating Incidents and Managing Incident Response

Today’s Regulatory Complexity

- 47 state + 3 territory breach notification laws
  - Differ with respect to:
    - Definitions
    - Risk of harm
    - Safe harbor
    - Exemptions
    - Timing
    - Content
    - Notice to regulators, agencies, etc.
- A plethora of federal laws & other standards
  - HIPAA Omnibus Final Rule
  - GLBA, PCI
Stages of “Omnibus Breach Notification Rule” Compliance

Growing Regulatory Complexity
- Proposed Federal Breach Notification Laws
  - The Personal Data Notification and Protection Act
  - “You may wish to go back to 47 state laws!” - McDonald Hopkins PLC
- Proposed State Laws and Amendments
  - Indiana (SB 413) Tentative Effective Date 7/15
  - New Mexico (HB 217) Passed House on 2/19
  - New Hampshire Education Data Privacy Bills (HB 322, HB 607, HB 530)
  - Maryland (SB 548) Tentative Effective Date 10/1/15
  - Montana (HB 74) Tentative Effective Date 10/1/15
  - Wyoming (SF 35) Tentative Effective Date 7/1/15
  - Michigan (SB 33) Education Data Disclosure Reporting Bill

What security threats is your organization most concerned about?

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, April 2015.
Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months?

- No
- Yes, 1 breach
- Yes, 2 to 5 breaches
- Yes, more than 5 breaches

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, April 2015.

How the data breach was discovered?

- Accidental Loss prevention
- Patient complaint
- Law enforcement
- Legal complaint
- Employee detected
- Audit/assessment

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, April 2015.

Nature of the breach

- Unintentional employee action
- Intentional non-malicious employee action
- Technical systems glitch
- Criminal attack
- Malicious insider
- Third-party snafu
- Lost or stolen computing device

Source: Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, April 2015.
Agenda

• Top Security Threat Trends in Healthcare
• Growing Regulatory Complexities
• Trends in Healthcare: Incidents & Breaches
• Keys to Being Prepared for Managing Incidents
• Real World Incident Response Cases
• Insights From Analysis of Real Incident Data
• Tools and Methodologies for Correlating Incidents and Managing Incident Response

Incident Response: What are the things we should be considering?

• Keys to being prepared for managing incidents, including dealing with media and information dissemination.
• Tools and methodologies for correlating incidents and managing incidents
• Real world cases

What are the basics?
Have a Plan

- Remember – this is not just a privacy or security issue

Incident Response Process

- Preparation
- Identification
- Containment
- Remediation
- Follow Up
- Recovery

Overall Process
Define accountability

<table>
<thead>
<tr>
<th>Designated Official</th>
<th>Type of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>PHI</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>ePHI, PII, or other information related to IS incidents</td>
</tr>
<tr>
<td>Corporate Compliance Officer</td>
<td>Corporate compliance issues</td>
</tr>
<tr>
<td>Research Integrity Officer</td>
<td>Research compliance issues</td>
</tr>
</tbody>
</table>

Incident Management Team

- Chief Information Officer
- Chief Information Security Officer
- Chief Medical Officer
- Corporate Compliance Officer
- Privacy Officer
- Risk Management
- General Counsel
- General Counsel
- President
- Research Integrity Officer
- VP Human Resources
- Marketing & Communications
- Leaders from affected departments

Document and Review

- Show your work
- The burden of proof has shifted
- You need to show that the information has a low probability of compromise
Besides an incident management process ...
Complete asset inventory

Do you know what you have on the internet?

Who knew?
What would happen if you had to disconnect from the internet?

Could you communicate without email?

Too much information?

• How often do our meeting announcements include the passwords or codes for the meeting?
Daily Safety Brief

- Seattle Children’s huddles at the start of every day to maintain situational awareness of immediate problems impacting safety and quality of patient care.

What about outside communication?

- Assemble the team
- Gather and confirm as much information as possible
- Identify key internal and external audiences who need to be informed
- Develop simple and concise key messages
- Develop and implement a plan to communicate to key audiences
- Assess ongoing communications
- Do not speculate

Crisis Communication Plan
Questions to consider

- What is currently known about the issue?
- What needs to be done now to take care of any affected patient, family member, or member of the public?
- Now do we avoid a repetition of the incident?
- When, where, and how did the incident happen?
- Who was involved in the incident?
- What other sources of information can be accessed?

Questions to consider

- What is the worst case scenario?
- What are the short/long term implications?
- Who will be affected? Who needs to know the status of the situation?
- What steps should be taken to protect and support any involved provider or staff member?
- How will key audiences be impacted?

Potential communication mediums

- Phone calls and email
- Notifications to internal audiences
- News conferences
- Written statements
- In-person and phone interviews
- Website bulletins and updates
- Twitter and Facebook posts
- On the ground staff messages they can use with patients, families, etc.
Well trained professionals

You can not do this alone …
Example Cases

Case background

- The help desk receives a call from one of the Clinical Psychologist. She is requesting a password reset.
- The user reveals that she suspects that there is a key logger program installed on her personal laptop.
- The help desk reset the user’s password and turned the case over to the information security department.

Significant Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/30/10</td>
<td>Unauthorized OWA authentication for userid XXXX (04:36)</td>
</tr>
<tr>
<td>08/07/10</td>
<td>Unauthorized OWA authentication for userid XXXX (08:07)</td>
</tr>
<tr>
<td>08/27/10</td>
<td>Unauthorized OWA authentication for userid XXXX (08:27)</td>
</tr>
<tr>
<td>13/50/16</td>
<td>Unauthorized OWA authentication for userid XXXX (13:50)</td>
</tr>
<tr>
<td>16/30/16</td>
<td>Unauthorized OWA authentication for userid XXXX (16:30)</td>
</tr>
<tr>
<td>16/50/16</td>
<td>Unauthorized OWA authentication for userid XXXX (16:50)</td>
</tr>
</tbody>
</table>

Email - 133MB in overall size and included 1891 individual emails in 41 different folders.
The problem …

- Based on incidents and regular walkthroughs – we saw increased evidence of PHI issues with:
  - Visible spaces
  - Printing and faxing
  - Disposal

Awareness Campaign

- Cover it up or turn it over. If you leave the immediate area, cover up or turn over the PHI so no information is visible
- Know where it’s going. Check destination when printing or faxing
- Shred it or park it. If you find papers on printer, fax or another location, find a Shred-It bin or place in a “PHI deposit here” container.

Sign examples
Agenda

- Top Security Threat Trends in Healthcare
- Growing Regulatory Complexities
- Trends in Healthcare: Incidents & Breaches
- Keys to Being Prepared for Managing Incidents
- Real World Incident Response Cases
- Insights From Analysis of Real Incident Data
- Tools and Methodologies for Correlating Incidents and Managing Incident Response

Paper Plays a Big Role in Healthcare PHI Incidents

<table>
<thead>
<tr>
<th>Category</th>
<th>Paper</th>
<th>Electronic</th>
<th>Web</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providers (Hospitals)</td>
<td>30%</td>
<td>30%</td>
<td>15%</td>
<td>75%</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>8%</td>
<td>8%</td>
<td></td>
<td>16%</td>
</tr>
<tr>
<td>Insurance/Finance</td>
<td>44%</td>
<td>26%</td>
<td>2%</td>
<td>72%</td>
</tr>
</tbody>
</table>

Misdirected Mail, Paper Record, Prescription Order/Label, Manual File(s)

Paper PHI/PII Incidents

- Paper Record
- Electronic/Cloud/Internet
- Web Access
- Print
- Fax

- Paper Sub-Categories
- Paper vs. Other Categories

ID Experts Data Analysis

Electronic: 29%
PAPER: 63%
Verbal/Visual: 8%
Misdirected Mail, Paper Record, Prescription Order/Label: 43%
Electronic PHI/PII Incidents

- Electronic
- Paper
- Verbal/Visual
- Email
- Online Portal
- Electronic Medical Record
- Application
- FTP Site
- Network Access
- Posted Online
- Decommissioned Office Machines

Electronic vs. Other Categories

Electronic Sub-Categories

- Electronic
- Paper
- Verbal/Visual
- Email
- Online Portal
- Electronic Medical Record
- Application
- FTP Site
- Network Access
- Posted Online
- Decommissioned Office Machines

PHI/PII Data Controls

- Paper Incidents
- Electronic Incidents

- Information was in plain text
- Information was under physical safeguard
- Information was statistically de-identified
- Information was redacted

- No controls were present
- Information was not identifiable or recipient has ability to re-identify

- Password protected & password was not compromised
- Encrypted to NIST standard; key was not compromised
- Encrypted but evidence of access with valid credentials
- Information was encrypted; key was not compromised

Incident Cause or Intent

- All Incidents
- Intentional Malicious Incidents

- Unauthorized Access
- Theft of Information
- Unauthorized Use
- Hacking/Malware
- Exposure of Information
- Unintentional
- Malicious
- Other

- Unauthorized Access
- Theft of Information
- Unauthorized Use
- Hacking/Malware
- Exposure of Information
- Unintentional
- Malicious
- Other

Electronic PHI/PII Incidents

- Electronic
- Paper
- Verbal/Visual
- Email
- Online Portal
- Electronic Medical Record
- Application
- FTP Site
- Network Access
- Posted Online
- Decommissioned Office Machines
Data Risk Mitigation

(Proportion %)

<table>
<thead>
<tr>
<th>Reason for Inability to Mitigate Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health by design</td>
</tr>
<tr>
<td>Confirmed storing or destruction</td>
</tr>
<tr>
<td>Confirmed improper use</td>
</tr>
<tr>
<td>Unresolved last amount of backup copy</td>
</tr>
</tbody>
</table>

Data Risk Mitigation Frequency

- Risk Mitigated: 31%
- Risk Mitigated, Confirmed: 69%
- Risk Mitigated, Confirmed: 8%
- Risk Mitigated, Confirmed: 5%
- Risk Mitigated, Confirmed: 0%

Notification Frequency by Incident Category

Electronic Incidents
- Mandatory: 22%
- Voluntary: 10%
- None: 68%

Paper Incidents
- Mandatory: 22%
- Voluntary: 10%
- None: 78%

Notification Frequency by Industry

Insurance / Financial
- Mandatory: 21%
- Voluntary: 1%
- None: 78%

Hospital
- Mandatory: 21%
- Voluntary: 1%
- None: 78%
Notification Frequency by Industry

- Business Associate
  - Mandatory: 2%
  - Voluntary: 98%
  - None: 0%

- Pharmacy
  - Mandatory: 1%
  - Voluntary: 99%
  - None: 0%

Notification Frequency by Business Associates (BA)

- BA Notification
  - Mandatory: 11%
  - Voluntary: 89%
  - None: 0%

- BA Risk Assessment Outcome
  - High Risk: 7%
  - Med Risk: 93%
  - Low Risk: 0%

Know your incidents
Incident Response Complexity

Incident Response Life Cycle

Incident Risk Assessment is Complex
Compliance Challenges

Organizations struggle to effectively manage incidents. A recent Ponemon study found:

- Only 35% of respondents are using automated processes
- Almost half say they are not in compliance with federal rule
- Lack of consistency is top complaint with current process

Incident Risk Assessment Needs Consistency & Automation

Multiple regulations
Multiple factors & time critical

RADAR® Incident Response Management Platform

- Federal Laws (HIPAA/HITECH, GLBA)
- State & Territorial Laws
- International Laws
In Conclusion

1. Regulatory environment is complex and getting more complex

2. Prepare and practice for real world incident scenarios

3. Use the right tools designed for threat intelligence, incident correlation and response management

Know the rules

Follow the rules

Prove it!