What Healthcare Professionals Need to Know about Information Security

Theresa Meadows, RN, MS CHCIO, FHIMSS, FACHE
Senior Vice President and Chief Information Officer
Cook Children’s Health Care System

Objectives

• Understand the healthcare cybersecurity landscape
• Discuss the impact of culture
• Understand the key components of a cybersecurity program
About Cook Children’s

- Founded in 1918 – Fort Worth Free Baby Hospital
  - Cook Children’s Hospital
  - Fort Worth Children’s Hospital
- 1984 Merger: Cook-Fort Worth Children’s Medical Center
- 2013 Nationally recognized Integrated Delivery System
- 2018 Celebrating 100 years!

Cook Children’s Health Care System Today

- Eight Companies
  - CC Medical Center
  - CC Physician Network
  - CC Home Health
  - CC Health Plan
  - CC Health Foundation
  - CC Hurst Surgery Center (JV)
  - CC Pediatric Surgery Center (JV)
  - CC Health Services (for profit)
Current Cybersecurity Landscape

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Wanna Cry?

RANSOMWARE
Strikes UK Hospitals

Academic Medical Centers at High Risk

Study: Risk of data breaches at hospitals is greater at larger facilities, teaching hospitals

Johns Hopkins expert evaluates breaches reported from 2009 through 2016

The risk of data breaches at U.S. hospitals is greater at large facilities and hospitals that have a major teaching mission, according to a study led by a researcher at the Johns Hopkins Carey Business School.
# Largest Healthcare Breaches – 2017

<table>
<thead>
<tr>
<th>Entity</th>
<th>Number of Affected Individuals</th>
<th>Type of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airway Oxygen of Michigan</td>
<td>500K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Women’s Healthcare Group of PA</td>
<td>300K</td>
<td>Hacking of desktop and server</td>
</tr>
<tr>
<td>Urology Austin</td>
<td>278K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Pacific Alliance Medical Ctr.</td>
<td>266K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Peachtree Neurological Ctr. Of Georgia</td>
<td>176K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Tampa Bay Surgery Center</td>
<td>142K</td>
<td>Hacking of server – public posting</td>
</tr>
<tr>
<td>McLaren Medical Group</td>
<td>106K</td>
<td>Hacking of server</td>
</tr>
<tr>
<td>Emory Healthcare</td>
<td>79K</td>
<td>Hacking of server - extortion</td>
</tr>
<tr>
<td>Salina Family Healthcare Ctr.</td>
<td>77K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Stephenville Medical &amp; Surgical</td>
<td>75K</td>
<td>Unauthorized disclosure/email</td>
</tr>
<tr>
<td>ABCD Pediatrics</td>
<td>55K</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Torrance California Medical Ctr.</td>
<td>46K</td>
<td>Hacking of email</td>
</tr>
<tr>
<td>St. Mark's Surgical Ctr. in Florida</td>
<td>33K</td>
<td>Hacking of server</td>
</tr>
</tbody>
</table>

## Cyber Security and Data Breaches in the Health Care Organizations

Data breaches in healthcare remain consistently high in terms of volume, frequency, impact, and cost. Healthcare organizations are experiencing a greater volume and frequency of data breaches, suffering multiple data breaches each.

- **89%** of healthcare organizations experienced data breaches over the past two years.
- **79%** have experienced multiple breaches in the past two years.
- **34%** have experienced two to five breaches in the past two years.
- **45%** have experienced five or more breaches in the past two years.

While the majority of breaches are small (less than 500 records) and are not reported to the U.S. Department of Health and Human Services (HHS) and the media, the financial impact is significant.

**NEWEST CYBER THREAT FOR 2016**

**RANSOMWARE**

A type of malicious software designed to block access to a computer system until a sum of money is paid.

- 59% of healthcare organizations don’t think their security budget is sufficient to curtail or minimize data breaches.
Hackable implanted medical devices could cause deaths, researchers say

Medtronic, a manufacturer of pacemakers and implantable insulin pumps, won’t fix security vulnerabilities in its products

Security researchers have demonstrated that some implanted medical devices like pacemakers and insulin pumps can be hacked. Photograph: Ulrich Baumgarten/U. Baumgarten via Getty Images

The Guardian, US Edition, August 9, 2018

Healthcare Cybersecurity Challenges

• Unique Culture
• Digital Transformation
• Regulatory Environment
• Organizational Size Varies
• Patient Safety
• Complexity of types of exposure
• Lack of skilled resources

Healthcare Industry Cyber Security Task Force – June 2017
Healthcare Is Complex

Healthcare Regulatory Environment
Types of Risks

- Privacy
- Availability
- Integrity
- Patient Safety

Impact of Cybersecurity Risks in Healthcare

- **Competition** – patient privacy violations can influence where individuals choose to get their care
- **Reputation** – security incidents that lead to media coverage can significantly damage public perception of the organization
- **Culture** – outstanding care is also about how well the integrity and privacy of patient records and electronic transactions are maintained
- **Financial** – significant penalties, litigation for security incidents where protected patient health information, credit card or other information protected by federal laws is disclosed
Patients and Families Expect

MORE TECHNOLOGY  ENHANCED ACCESS  HIGHER AVAILABILITY

...in a secure and private environment

Impact of Culture
What is Culture?

- Amplified by behaviors of leaders
- Embedded in a network of organizational practices
- Visible in the way that work gets done on a day to day basis
- Shared beliefs, values and assumptions held by members of an organization
- Evident in the behavior of individuals and groups
"In most organizational change efforts, it is much easier to draw on the strengths of the culture than to overcome the constraints by changing the culture." – Edgar Schein

What are some challenges?
Myths and Perceptions

- It will never happen to us.
- It will decrease my productivity.
- Security is an IT issue.
- Security is only needed to meet regulatory requirements (HIPAA)
- Technology will protect us.

Education

- Strict definitions can be confusing, misleading and uninteresting...

“Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.”

- Complicated training/awareness concepts
Ever Changing Security Landscape

**Hacking Then**
- Individual or Computer Clubs/Groups
- Manual efforts with Social Engineering
- War Protesting and Civil Disobedience
- Anti-Establishment Rhetoric
- Social Rebels and Misfits
- Success = Badge Of Honor
- Personal Monetary Gain or to pay for / fund hacking activity
- Initially viewed as mostly a nuisance growing into Criminal Acts
- Telco, University and some Government sites primary focus

**Hacking Now**
- Automated / Sophisticated Malware
- Hactivism – Freedom of Speech, Statements to Influence Change, Sway Public Opinion and Publicize Views
- Criminal – Drug Cartels, Domestic and Foreign Organized Crime for Identity Theft and Financial Fraud
- Espionage – IP, Business Intelligence, Technology, Military / Political Secrets
- Terrorism – Sabotage, Disruption and Destruction
- Nation-State – Intelligence Gathering, Disruptive Tactics, Clandestine Ops, Misinformation, Warfare Strategies, and Infrastructure Destruction

**What’s Next?**

- All the technology in the world will not prevent security issues
- Awareness is key to success – focus on changing behavior vs strictly on compliance
- Employees are our most valuable asset
Keys to Success

• Executive Governance (aka Buy In)
  • Board of Directors
  • Organizational Leadership
• Risk Assessment, Planning & Technology
• Ongoing education and awareness
• Continuous monitoring and improvement

Executive Governance
Never waste a good crisis – Gaining buy-in

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Wanna Cry?

The Low-Down

Target

Cook Children’s Information Security Office
Threat Summary
September 2018
What boards should know?

• Understand that cyber security is an enterprise wide management issue, not an IT issue
• Understand the legal and financial implications of a security breach
• Understand the impact to reputation if security is compromised
• Boards should be included in cyber risk discussions
• Boards should ensure adequate resources are spent on security

Education and Awareness
CyberSecurity is a Patient Safety Issue

Making it real.....

• What if I say...

  “Cybersecurity is the people, processes and technologies that....
  • Keep our children safe from online predators and cyber bullying
  • Ensures someone doesn’t steal your identity and empty your bank account
  • Prevents someone from publicly posting your personal emails
  • Stops someone from gaining unauthorized access to medical records, social security numbers, and other sensitive data
Typical Month

- Average 35 privacy investigations/month
- Average 18–20 million transactions (hits)/month
- 2.6 million vulnerabilities
- Average 5–7 million attacks blocked w/ IDPS/month
- 100 DLP quarantined incidents/month

Staff - Awareness and Engagement

- Identify “grass roots” employee engagement committee
- Develop awareness materials and computer based training
- “Brown bag” luncheons and cyber security awareness sessions
- Contests and other promotions
Culture of Security at Cook Children’s

- New employee orientation
- Monthly security education
- Quarterly Ask the CISO blog posts
- Repeat Offenders Education

Interactive Simulations to Test Knowledge

- Package delivery
- Tax forms
- Mailbox storage
- Improving our password complexity
- Email from the CEO, CFO, etc.
Phishing Simulation

Risk Assessment, Planning & Technology
Risk Assessment

- Assess and mitigate risks
  - Internal Assessment
    - Annual Security State of the Union
    - Annual HIPAA Risk Assessment
    - Social Engineering
    - Internal Audit (Compliance) – IS specific
    - Periodic Policy Review
  - External Assessment
    - BKD Audit (annually)
    - PCI auditing (quarterly)
    - Overall Security Risk Assessment (every 2 – 3 years)

Technology Planning

- Create layered defenses
  - PC
  - Network
  - Domain
  - Server
  - Application specific
  - Location
Technical and Operational Vulnerabilities

1. Outdated operating systems and poor patch management practices
2. Application vulnerabilities
3. Lack of backups, enterprise IT capabilities
4. Lack of Two-Factor authentication, advanced security tools
5. Flat networks/lack of segmentation
6. Flat “identity model”
7. Supplier/business partner risk
8. Medical devices
9. ATP and Zero-day exploits

The Cybersecurity Skills Gap

Two new studies connect the dots between an organization’s lack of staffing and skills to its ability to fend off cyber threats:

- There are approximately one million unfilled cybersecurity jobs in the U.S.;
- Existing professionals struggle to keep up-to-date in their skills and training;
- 54% of organizations have suffered at least one security event in the past year; and
- The vast majority attribute this to a lack of security staff or training.
Develop an Incident Response Plan

• The Computer Security & Cybersecurity Incident Response Plan (CSIRP) will cover adverse events and incidents related to cybersecurity incidents.

• The CSIRP will not address other threats like natural disasters and power outages that are covered in existing Business Continuity and Disaster Recovery plans.

Incident Response Considerations

<table>
<thead>
<tr>
<th>Critical Capabilities</th>
<th>Regulatory, Tools &amp; Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Detection &amp; Analysis</td>
<td>Preventative Controls</td>
</tr>
<tr>
<td>Incident Investigation</td>
<td>Detective Controls</td>
</tr>
<tr>
<td>Incident Containment / Eradication</td>
<td>Cyber Insurance Coverage</td>
</tr>
<tr>
<td>Incident Response Team Charter</td>
<td>Incident/Breach Risk Assessments</td>
</tr>
<tr>
<td>Communication Plans, Internal &amp; Ext Evidence</td>
<td>Notification to affected individuals</td>
</tr>
<tr>
<td>Incident Command</td>
<td>Notification to the press</td>
</tr>
<tr>
<td>Computer Forensics</td>
<td>Alternate notification</td>
</tr>
<tr>
<td>Backup/Recovery, DR &amp; BC</td>
<td>Notification to government</td>
</tr>
<tr>
<td>Incident Documentation/Retention/tools</td>
<td>Law Enforcement</td>
</tr>
<tr>
<td>Public Relations</td>
<td>Corrective Actions (30 days)</td>
</tr>
<tr>
<td>Plan for reduction of harm</td>
<td>Lessons Learned</td>
</tr>
<tr>
<td>General Counsel: Privilege</td>
<td>Credit Monitoring</td>
</tr>
<tr>
<td>HR, IA, Compliance &amp; Risk</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
</tr>
</tbody>
</table>

Lessons Learned

Credit Monitoring
Incident Response Team Membership

Incident Response Team
- General Counsel
- Public Relations
- Compliance
- Cyber Security
- Risk
- CIO
- Client Systems
- CISO
- Vendor Partners
- DR

Elevator Pitch

- Media
- Patients
- Physicians, Employees, Executives
- Board Members
- Community
Monitoring & Continuous Improvement

“In God we trust, all others must bring data.”
W. Edwards Deming
Awareness Trend YTD

Questions?