Clean the house: Cyber-hygiene to safeguard patient information and ensure patient safety

October 31, 2017

Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
CEO

Sheetal Sood, CHC, CIPP, ESA, CRISC, CISA, GIAC, CISP, GSEC
Senior Executive Corporate Compliance Officer

Discussion Flow

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management

First Healthcare Risk Manager

“First, Do No Harm.”

- Hippocrates, 4th Century, B.C.E.
- OR
- Auguste François Chomel (1788–1858) Parisian pathologist and clinician
- OR
- ???

Digitization in Healthcare is Great AND We Can Now Create Harm from New Threat Sources
Very Real Need - Increasingly More Significant Business Risk

Damage to Brand
Compliance
Financial
Cyber
Patient Safety
Cyber and Compliance Risk Management is Not "an IT Problem"

Third Party Liability
Property Damage

Cyber criminals next deadly target: Grandpa's pacemaker

"We're going to have our digital D-Day, our cyber D-Day, if you will, in medical, and there's going to be patients that die. It's going to be a big deal," said Dr. Christian Dameff, an emergency room physician and expert on cyber vulnerabilities.

Fears of hackers targeting hospitals, medical devices | ABC News | June 29, 2017

https://www.youtube.com/watch?v=pU3NQ3GkC_0
**The Risk Problem We’re All Trying to Solve**

- What if my Sensitive Information is shared?
- What if my Sensitive Information, Systems, or Devices are not there when it is needed?
- What if my Sensitive Information, Systems, or Devices are not complete, up-to-date and accurate?


---

**Discussion Flow**

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management

---

**Must Include Every Information Asset in Every Location/LOB**

- Clinics
- Hospitals
- LTC Facility
- ASC
- CHC
- Hospice
- Imaging Center
- Home Health
- EMS
- Rehab Clinic
- Rural Clinic
- Dialysis Clinic
- Behavioral
- Research
Traditional Assets – IT Systems and Applications

- Electronic Health Record Applications
- Clinical Information Applications
- Lab And / Or Medical Specialty Applications
- Medical Billing/Claims Processing Applications
- Email Applications
- Company Intranet Websites
- HR Management Applications
- Network File Sharing Applications
- EDI Applications
- Fax Applications
- Payment Processing Applications
- Financial Management/Reporting Applications
- Any Other Software Used To Manage Sensitive Electronic Information

Biomedical Assets – Pumps, PACS, etc.

- Patient monitoring devices, monitors and smart rooms:
- Smart medical devices, infusion pumps, ventilators, incubators, telemetry, smart stethoscopes and medical imaging
- Electrocardiogram (ECG), heart rate, pulse, and eye telecom
- Ventilators, capnography monitors, depth of consciousness monitors, regional oximetry, biopatch technology and respiratory rate
- Smart beds, hand hygiene and fall detection
- Remote ICU telemetry, Tele-technology (any medical science done remotely — for example, tele-neurology or tele-dermatology)
- Remote wellness and chronic disease management:
- Wearable wristbands, bio-patches, smartwatches and ear buds
- Remote clinical monitor spirometer, pulse oximeter, ECG, glucometer and fall detection

IoT Assets – Facilities, Infrastructure, etc.

- Facilities Security, Building Management:
  - Video surveillance, door locks and entry systems, and fire alarms
  - Power monitoring, power distribution, energy consumption and management, and elevators
  - HVAC, lighting, room control, water quality, humidity monitoring, and tissue and blood refrigerators
  - Real-time location services (RTLS) for Assets, Employees, Patients and Visitors
  - Wheelchairs, infusion pumps, smart cabinets, medication carts, par-level management and rental management
  - Physicians, nursing staff and ancillary staff
  - Infant abduction and wandering systems
  - Wayfinding and digital signage
- Networking Hardware, Software, Security, Services
- Routers, Switches, LAN cards, Wireless routers
- Operating systems, IT Security and Services
Don’t Compromise CIA of any Traditional, Biomedical, IoT Assets

Confidentiality  Integrity  Availability

Quality and Safe Care  Access to Care  Timely Care

Patient Information AND Patient Health

Medical Device Security: An Industry Under Attack and Unprepared to Defend

- 67% of medical device manufacturers believe one of their devices will be attacked in the next 12 months
- Two-thirds of healthcare organizations are unaware of adverse effects to patients due to an insecure medical device
- Only 17% of medical device makers are taking significant steps to prevent attacks

Include Biomedical Devices in Risk Analyses

- NIST is increasing activity and work products
- First Practice Guide published May 2017
- Government and industry collaboration
- NIST-based risk assessment performed
Discussion Flow

1. Connecting the Dots
2. Beyond Traditional IT Assets
3. Bona Fide Risk Analysis and Risk Management

NIST Risk Management Process

1. Finalize Information Asset Inventory
2. Identify Threats & Vulnerabilities
3. Determine Likelihood & Impact
4. Determine Risk Level

What Are All the Possible Ways in Which We May Compromise Sensitive Information?

NIST Risk Assessment Process

1. Finalize Information Asset Inventory
2. Identify Threats & Vulnerabilities
3. Determine Likelihood & Impact
4. Determine Risk Level

What Are All the Possible Ways in Which We May Compromise Sensitive Information?
### Risk Assessment Example

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat Source / Action</th>
<th>Vulnerability</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Hacker exfiltrates data</td>
<td>No DB encryption</td>
<td>Med (3)</td>
<td>High (5)</td>
<td>15</td>
</tr>
<tr>
<td>Server</td>
<td>Hacker exfiltrates data</td>
<td>Weak passwords</td>
<td>High (5)</td>
<td>High (5)</td>
<td>25</td>
</tr>
<tr>
<td>Server</td>
<td>Malware encrypts data</td>
<td>Unpatched OpSys</td>
<td>Med (3)</td>
<td>Med (3)</td>
<td>9</td>
</tr>
<tr>
<td>Server</td>
<td>Careless IT changes data</td>
<td>Integrity checks</td>
<td>Low (1)</td>
<td>Medium (3)</td>
<td>3</td>
</tr>
<tr>
<td>Server</td>
<td>Hardware head crash</td>
<td>No data backup</td>
<td>Med (3)</td>
<td>High (5)</td>
<td>15</td>
</tr>
<tr>
<td>Server</td>
<td>Hacker DDoS</td>
<td>Insufficient capacity</td>
<td>Low (1)</td>
<td>High (5)</td>
<td>5</td>
</tr>
</tbody>
</table>

etc

### Risk Assessment Fundamentals

- Must be possible to have loss or harm
- Must have asset-threat-vulnerability to have risk
- Risk is a likelihood issue
- Risk is an impact issue
- Risk is a derived value (like speed is a derived value = distance / time)
- Fundamental nature of Risk is universal
- Risk assessment informs all other steps
- Not "once and done"
- Critical Output: Risk Register

### NIST Risk Response Process

1. Identify Risk Responses
2. Evaluate Alternatives
3. Make Risk Response Decision
4. Implement Risk Response

What decisions do we need need to make to treat or manage risks?
**Decide on Response or Treatment**

- Accept
- Avoid
- Mitigate
- Transfer

**Risk Response Fundamentals**

- **Real Risk Response Requires Real Risk Analysis**
- **All Risks Need a Response**
- **Not All Risks Must Be Mitigated**
- **Risk Response Requires Setting Your Risk Appetite**
- **Risk Response Requires Real Risk Framing**
- **Risk Management is Informed Decision Making – What’s New?**
- **Risk Response Informs All Other Steps**
- **Critical Output: Risk Management Plan**

**Thinking Like a Risk Manager**

- Risk Assessment
- Avoid / Transfer Risks
- Mitigate / Transfer Risks
- Accept Risks

Risk Response is making informed decisions on how to treat risks.
Key Elements of Risk Action Plan

- Control Gap
- Recommendation
- What is Affected? (assets, ePHI, etc.)
- Responsibility for Implementation
- Priority
- Due Date
- Actual Completion Date
- Current Status
- Documentation

Risk Assessment In Practice: Bio-medical equipment

- Scenario: A mid-size hospital system with one ambulatory care unit and a small long-term care unit wants to start an audit of their bio-medical devices. Such an audit has never been performed before.

Challenge: Where to begin? How do I assess risk?

<table>
<thead>
<tr>
<th>Issues</th>
<th>Resultant Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inaccurate Inventory</td>
<td>1. Scope and universe of assets not known, No baseline information, No view of what assets need protection</td>
</tr>
<tr>
<td>2. Improper Data Management</td>
<td>2. Unauthorized access, use or disclosure</td>
</tr>
<tr>
<td>3. Inadequate Security controls</td>
<td>3. Unauthorized access, use or disclosure</td>
</tr>
<tr>
<td>4. Insufficient Physical controls</td>
<td>4. Unauthorized access, use or disclosure</td>
</tr>
<tr>
<td>5. Lack of System Hardening</td>
<td>5. Unauthorized access, use or disclosure</td>
</tr>
<tr>
<td>6. Insecure transmission</td>
<td>6. Unauthorized access, use or disclosure</td>
</tr>
</tbody>
</table>
Risk Assessment In Practice: Bio-medical equipment

Audit methodology

- **Inventory**: Accurate, Current, Prioritized assets list
- **Data**: Nature, Quantity, Storage State
- **Security Capabilities of Device**: Access control, Logs, role-based access
- **Physical controls**: Locks, Secure spaces
- **System Controls**: Patches, updates, system hardening
- **Insecure Transmission**: Removable drive or solid-state drive, peripheral, printing, network connection

Final Outcome:

* Risk Chart with Assets Prioritized by Risk
* Short-term and Long-term Mitigation Plans

---

Information Risk Management Must Become a Team Sport

---

Four Critical Points

1. eHealth brings opportunities and new risks
2. It’s about safeguarding ePHI AND assuring Patient Safety
3. Information Risk Management Language is Business Risk Management Language
4. Information Risk Management Must Become a Team Sport
Compromise of Confidentiality on Patient Satisfaction

<table>
<thead>
<tr>
<th>How Does It Happen?</th>
<th>Ramifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Careless User</td>
<td></td>
</tr>
<tr>
<td>- Discussing treatment in an open environment</td>
<td></td>
</tr>
<tr>
<td>- Calling the wrong family about a patient’s status</td>
<td></td>
</tr>
<tr>
<td>- Emailing or faxing patient information to an unauthorized person</td>
<td></td>
</tr>
<tr>
<td>- Improperly disposing of paper records</td>
<td></td>
</tr>
<tr>
<td>Snooping</td>
<td></td>
</tr>
<tr>
<td>- Accessing records of a friend on behalf of a colleague</td>
<td></td>
</tr>
<tr>
<td>- Accessing records of an ex-spouse new partner</td>
<td></td>
</tr>
<tr>
<td>- Accessing records of a neighbor out of curiosity</td>
<td></td>
</tr>
<tr>
<td>Malicious</td>
<td></td>
</tr>
<tr>
<td>- Selling medical records of famous people for personal gain</td>
<td></td>
</tr>
<tr>
<td>- Using medical information for medical fraud</td>
<td></td>
</tr>
<tr>
<td>- Posting medical information on social media as revenge</td>
<td></td>
</tr>
<tr>
<td>- Using medical records to provide insurance to friends or family</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Theft</td>
<td></td>
</tr>
<tr>
<td>Reputational Damage</td>
<td></td>
</tr>
<tr>
<td>Relationship Damage</td>
<td></td>
</tr>
<tr>
<td>Employment Damage</td>
<td></td>
</tr>
<tr>
<td>Financial Damage</td>
<td></td>
</tr>
<tr>
<td>Anxiety</td>
<td></td>
</tr>
<tr>
<td>Depression</td>
<td></td>
</tr>
</tbody>
</table>
### Compromise of Integrity on Patient Safety & Quality of Care

<table>
<thead>
<tr>
<th>How Does It Happen?</th>
<th>Ramifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors or Omissions</td>
<td></td>
</tr>
<tr>
<td>• Patient identification errors</td>
<td>• Incorrect Diagnosis</td>
</tr>
<tr>
<td>• Use of temporary names</td>
<td>• Incorrect Treatment</td>
</tr>
<tr>
<td>• Input errors</td>
<td>• Incorrect Prescriptions</td>
</tr>
<tr>
<td>• Inadequate reporting of test results</td>
<td>• Incorrect Billing Charges</td>
</tr>
<tr>
<td>Inadequate Information “Hand Off”</td>
<td>• Contaminated Clinical Trial</td>
</tr>
<tr>
<td>• Poor coordination of care between primary and specialist care</td>
<td>• Identity Theft</td>
</tr>
<tr>
<td>• Poor care coordination with next level of care if not automated</td>
<td>• Reputational Damage</td>
</tr>
<tr>
<td>Inadequate Administrative Controls</td>
<td>• Death</td>
</tr>
<tr>
<td>• Inadequate role-based security on EMR system</td>
<td></td>
</tr>
<tr>
<td>• Unsecured maintenance networks linked to the infrastructure network</td>
<td></td>
</tr>
<tr>
<td>Inadequate Technology Controls</td>
<td></td>
</tr>
<tr>
<td>• Vulnerable networked medical devices</td>
<td></td>
</tr>
<tr>
<td>• Use of robotics supporting telemedicine/telehealth</td>
<td></td>
</tr>
</tbody>
</table>

### Compromise of Availability on Patient Safety & Quality of Care

<table>
<thead>
<tr>
<th>How Does It Happen?</th>
<th>Ramifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete or untested remediation plans</td>
<td>• Delayed Admission</td>
</tr>
<tr>
<td>• Disaster Recovery Plans</td>
<td>• Delayed Diagnosis</td>
</tr>
<tr>
<td>• Business Continuity Plans</td>
<td>• Delayed Surgery</td>
</tr>
<tr>
<td>• Business Continuity Plans</td>
<td>• Delayed Prescriptions</td>
</tr>
<tr>
<td>Inadequate Processes</td>
<td>• Delayed Discharge</td>
</tr>
<tr>
<td>• Unintentional or incomplete back-up procedures</td>
<td>• Diagnosis Errors</td>
</tr>
<tr>
<td>• Disconnected Systems</td>
<td>• Treatment Errors</td>
</tr>
<tr>
<td>• Unpatched applications</td>
<td>• Death</td>
</tr>
<tr>
<td>Inadequate Security Controls</td>
<td></td>
</tr>
<tr>
<td>• Back-up connected to infrastructure network</td>
<td></td>
</tr>
<tr>
<td>• Untrained workforce members on social engineering tactics</td>
<td></td>
</tr>
</tbody>
</table>