Risk Management Strategies for Limited Budgets

Session # 151, February 22, 2017

Stephanie L. Tatum, Director of Health Information and Informatics Management, Privacy Officer, Oakland Regional Hospital

Jeff Bell, Chief Information Security Officer, CareTech Solutions
Stephanie L. Tatum, BS
Director Health Information and Informatics Management, Privacy Officer
Oakland Regional Hospital
- Responsible for policies that meet all laws and regulations
- Led ORH’s attestation of MU Stage 2
- “Proactive Security Measures Essential to Preventing Data Breaches,” Health IT Outcomes
- Highlighted in HealthITSecurity.com’s “How a Mich. Hospital Stays Proactive in Health Data Security”
Jeff Bell, BS  
Chief Information Security Officer  
CareTech Solutions  

- 30 years in Health IT and Cybersecurity  
  - PricewaterhouseCoopers  
  - CareTech Solutions  
  - Visiting Nurse Association of S.E. Michigan  
  - Detroit Medical Center  
- Previous chair of HIMSS P & S committee  
- Certifications: CISSP, GSLC, CPHIMS  
- Member of InfraGard and SANs Advisory Board
Stephanie L. Tatum, BS
And
Jeff Bell, BS
Have no real or apparent conflicts of interest to report.
Disclosure

• This handout contains excerpt(s) from “The CERT Top 10 List for Winning the Battle Against Insider Threats” by Dawn Cappelli © 2012 Carnegie Mellon University, with special permission from its Software Engineering Institute.

• Any material of Carnegie Mellon University and/or its Software Engineering Institute Contained herein is furnished on an “as-is” basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from the use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom of patent, trademark, or copyright infringement.

• CERT ® is a registered trademark of Carnegie Mellon University.
Agenda

• Current healthcare privacy and security threats and risks
• HIPAA requires a risk-based approach
• The role of a security framework
• Security foundations for a small business
• Oakland Regional Hospital’s story:
  – What the assessment revealed
  – Progress and strategies to address top risks
• Cybersecurity and Compliance roadmap
• Risk management strategies for a limited budget
Learning Objectives

• Identify current healthcare privacy and cybersecurity risks

• Discuss the importance and key components of developing an information security guideline after undergoing a risk assessment

• Explain the most effective precautions to reduce the risk of the most common types of threats and information security events
An Introduction of How Benefits Were Realized for the Value of Health IT

Satisfaction
• Data privacy & security are needed for patient satisfaction

Treatment/Clinical
• Trust is essential for patients to disclose their health condition

Electronic Secure Data
• Cybersecurity risk management reduces risk of breaches

Patient Engagement and Population Management
• Trust is essential for patients to utilize patient portals

Savings
• Estimated average cost of a data breach is > $2.2 million

¹Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2016, Sponsored by ID Experts
Healthcare Privacy and Cybersecurity Risks

• Hacking and cybercrime
• Ransomware
• Medical identity theft
• Insiders
• Third parties
• Medical device vulnerabilities
• IoT vulnerabilities
For the second year in a row, criminal attacks are the leading cause of data breaches in healthcare.

- 50 percent of healthcare organizations say the nature of the breach was a criminal attack.
- 13 percent say it was due to a malicious insider.

*Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May, 2016, Sponsored by ID Experts*
What was the root cause of the healthcare organizations’ data breach?

<table>
<thead>
<tr>
<th>Cause</th>
<th>CE 2016</th>
<th>CE 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal attack</td>
<td>50%</td>
<td>45%</td>
</tr>
<tr>
<td>Third-party snafu</td>
<td>41%</td>
<td>39%</td>
</tr>
<tr>
<td>Stolen computing device</td>
<td>39%</td>
<td>43%</td>
</tr>
<tr>
<td>Unintentional employee action</td>
<td>36%</td>
<td>40%</td>
</tr>
<tr>
<td>Technical system glitch</td>
<td>29%</td>
<td>31%</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Intentional non-malicious employee action</td>
<td>8%</td>
<td>7%</td>
</tr>
</tbody>
</table>

*Risks & Threats: Hacking and Cybercrime*

*Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May, 2016, Sponsored by ID Experts*
OCR Fact Sheet: Ransomware and HIPAA, July 2016

- Ransomware is malware that denies access to data until ransom is paid
- 4,000 daily ransomware attacks since early 2016
- 300% increase from 2015
- HIPAA compliance is relevant to prevent and recover from ransomware attacks
  - Risk analysis, management, user training, access controls
  - Backups, DR plans, contingency plans, incident response plans
- OCR advises that ransomware attacks should be presumed a breach and reportable unless analysis shows a low probability that data was compromised
Risks and Threats: Ransomware

Talos (Cisco) recommendations:
• Prevent initial access
  – Harden the DMZ (public facing services)
  – Mitigate phishing / social engineering
• Impede lateral movement and propagation
• Backup / recovery

US CERT recommendations:
• Backups
• Risk analysis
• Staff training
• Vulnerability patching
• Application whitelisting
• Incident response
• Business continuity
• Penetration testing

See the following link to the Talos blog for more detailed recommendations.

Risks & Threats: Medical Identity Theft

- More than 2.3 million Americans have been victims
- Average cost: $13,453
- How victims learn of the crime:
  - Hospital invoice
  - Collection letter
  - Insurance statement
  - Errors in health record
  - Credit report
- Difficult for victims to prove the theft
- 65% of victims spent money to resolve
- Incorrect medical records could jeopardize patient safety

*Fifth Annual Study on Medical Identity Theft*, Sponsored by the Medical Identity Fraud Alliance, conducted by Ponemon Institute LLC, February 2015
See also: Medical Identity Fraud Alliance: http://medidfraud.org/
Risks & Threats: Insiders

• “Insiders” refers to your workforce; those trusted with access to your systems
  – They make mistakes
  – They violate policies (snooping, shortcuts)
  – Some have criminal intentions

• According to US-CERT:
  “…Cyberattacks from employees and other insiders is a common problem that you should be planning for and preventing…Insiders pose a substantial threat to your organization because they have the knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means. The nature of insider threats is different from other cybersecurity challenges; these threats require a different strategy for preventing and addressing them.1”

1https://www.cert.org/insider-threat/
Risks & Threats: Insiders

The Cert Top 10 List for Winning the Battle Against Insider Threats¹
1. Learn from past incidents
2. Focus on protecting the crown jewels
3. Use your current technologies differently
4. Mitigate threats from trusted business partners
5. Recognize concerning behaviors as a potential indicator
6. Educate employees regarding potential recruitment
7. Pay close attention at resignation / termination!
8. Address employee privacy issues with General Counsel
9. Work together across the organization
10. Create an insider threat program NOW!

¹ The Cert Top 10 List for Winning the Battle Against Insider Threats¹.
Risks & Threats: Third-Parties

• Third parties were the source of 9% of breaches reported in 2015¹

• Healthcare providers need to manage third party risks:
  – Evaluate the risk profile for each third party
    • What is the level of access to PHI?
    • Where is the PHI stored and how is it accessed?
  – For high-risk third parties, perform a thorough evaluation of their security program before contracting and periodically thereafter

• Contract terms to manage third party risks
  – Request the right to audit and require cybersecurity insurance
  – Require notification of security incidents affecting your data
  – Require third party audits, such as SOC 2, and reporting of results
  – If you are a HIPAA CE or BA, include the HIPAA required business associate agreement

¹ Identity Theft Resource Center: http://www.idtheftcenter.org/Data-Breaches/2015databreaches.html
Cybersecurity threats to medical devices are a growing concern. The exploitation of cybersecurity vulnerabilities presents a potential risk to the safety and effectiveness of medical devices.

While manufacturers can incorporate controls in the design of a product to help prevent these risks, it is essential that manufacturers also consider improvements during maintenance of devices, as the evolving nature of cyber threats means risks may arise throughout a device’s entire lifecycle.
FDA recommendations for mitigating and managing cybersecurity threats include:

• Medical device manufacturers and health care facilities should take steps to ensure appropriate safeguards.

• Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

• Hospitals and health care facilities should evaluate their network security and protect their hospital systems.¹

¹http://www.fda.gov/medicaldevices/productsandmedicalprocedures/ucm373213.htm, Accessed 12/3/16
INTERNET OUTAGES all over on and off today. DDOS attacks on US domain host "Dyn.". Twitter, Reddit, Spotify, and...

Major DDoS attack knocks Twitter, Reddit, Spotify offline
Is the internet acting weird today? It’s not just you. A major cyberattack rendered websites and online services inaccessible across the East Coast on Friday morn...
dailypost.com
Risks & Threats: Medical Device and IoT Vulnerabilities

Security practices to address medical device and IoT vulnerabilities:

• Manufacturers must design in security

• Manufacturers must provide ongoing management of cybersecurity vulnerabilities

• Systems must be securely configured and installed in a secure network environment

• Providers must maintain a secure network environment, apply patches and follow vendor recommendations
HIPAA Requires A Risk-Based Approach

Ensure Confidentiality, Integrity and Availability:

• Ensure the **confidentiality, integrity, and availability** of all [ePHI] the covered entity or business associate creates, receives, maintains, or transmits.

• Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

• Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required [by the Privacy Rule].

• Ensure compliance with [the Security Rule] by its workforce 164.306(a)
HIPAA Requires A Risk-Based Approach

- **Risk analysis**: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by the covered entity or business associate 164.308(a)(1)(ii)(A)

- **Risk management**: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level 164.308(a)(1)(ii)(B)
Given the level of Cybersecurity Risk how can an organization:

- Decide on an appropriate cybersecurity program?
- Assure stakeholders, regulators, customers, the public?
- Demonstrate due diligence?

Cybersecurity frameworks are descriptions of a required or recommended set of controls (security safeguards).

Third party validation can provide an additional level of assurance.

Some security frameworks offer third party certification.
NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0
National Institute of Standards and Technology
February 12, 2014

**Identify:** Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

**Protect:** Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures

**Detect:** Anomalies and Events, Security Continuous Monitoring, Detection Processes

**Respond:** Response Planning, Communications, Analysis, Mitigation, Improvements

**Recover:** Recovery Planning, Improvements, Communications
## Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETECT (DE)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE.CM-3: The network is monitored to detect potential cybersecurity events</td>
<td></td>
<td></td>
<td>CCS CSC 14, 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS01.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2015 SR.6.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SG-7, SI-4</td>
</tr>
<tr>
<td>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20</td>
</tr>
<tr>
<td>DE.CM-1: Personal activity is monitored to detect potential cybersecurity events</td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2015 SR.6.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11</td>
</tr>
<tr>
<td>DE.CM-4: Malicious code is detected</td>
<td></td>
<td></td>
<td>CCS CSC 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS01.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.4.3.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2015 SR.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SI-1</td>
</tr>
<tr>
<td>DE.CM-5: Unauthorized mobile code is detected</td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2015 SR.2.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SC-11, SL4, SC-44</td>
</tr>
<tr>
<td>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</td>
<td></td>
<td></td>
<td>COBIT 5 APP07.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.2.1, A.15.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 CA-7, PPE-7, SA-4, SA-9, SI-4</td>
</tr>
<tr>
<td>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4</td>
</tr>
<tr>
<td>DE.CM-8: Vulnerability scans are performed</td>
<td></td>
<td></td>
<td>COBIT 5 BAB03.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.12.6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 EA-5</td>
</tr>
</tbody>
</table>

**Framework Core:** a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

---

*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014*
Benefits of using the **Cybersecurity Framework**:

- Improves cybersecurity: the NIST Framework core is up to date in terms of cyber threats / risks / effective controls – with an emphasis on Detect, Respond, Recover – not just Protect. It is much more up to date and comprehensive than the HIPAA Security Rule.

- Reduces legal exposure: this process can demonstrate due care in case of a breach and federal / state investigation or even law suit. The NIST Framework is founded on a presidential order and represents a baseline of good cybersecurity practices.

- Improves collaboration and communication of security posture with executives and others.
Security Fundamentals for Small Business

• Identify
  – Identify and control who has access to your business information
  – Conduct background checks
  – Require individual user accounts for each employee
  – Create policies and procedures for information security

• Protect
  – Limit employee access to data and information
  – Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Security Fundamentals for Small Business

• Protect (Continued)
  – Patch your operating systems and applications
  – Install and activate software and hardware firewalls on all your business networks
  – Secure your wireless access point and networks
  – Set up web and email filters
  – Use encryption for sensitive business information
  – Dispose of old computers and media safely
  – Train your employees

Security Fundamentals for Small Business

• Detect
  – Install and update anti-virus, spyware, and other malware programs
  – Maintain and monitor logs

• Respond
  – Develop a plan for disasters and information security incidents

• Recover
  – Make full backups of important business data/information
  – Make incremental backups of important business data/information
  – Consider cyber insurance
  – Make improvements to processes / procedures / technologies

• 71-bed physician-owned hospital in Southfield, MI
• A destination center for hand and orthopedic surgery serving Oakland, Wayne and Macomb counties
• Member of both the American Hospital Association and Michigan Health & Hospital Association
• Received Healthcare Facilities Accreditation Program Seal of Excellence
• Recognized as one of U.S. News & World Report’s Best Nursing Homes in 2012 and 2013
ORH Top Risks

- Lack of a formal risk assessment process
- Unmanaged VPN accounts
- Use of unsecure remote support tools
- Sending ePHI un-encrypted
- Not adhering to minimum necessary distribution
- IT Security Officer (ISO) and Privacy Officer roles not identified or assigned
- Absence of antivirus software
Risk Description

• Lack of a formal risk assessment process
  – Had not conducted a formal, documented risk assessment
  – Did not have the expertise to conduct a risk assessment
Risk Description

Unmanaged VPN Accounts
• Lack of a formal request and approval process
• Lack of proactive, consistent account review
• Accounts not being properly named and tracked

Unsecure remote support tools
• Allows users to bypass security controls
• Could be used to gain unauthorized access
Risk Description

- Sending ePHI unencrypted by email over the Internet
  - Communication of ePHI with vendors
- Distributing reports with PHI (surgery schedule) too broadly in the organization
  - Reports sent to a large email distribution list
Risk Description

• IT Security Officer and Privacy Officer Roles not identified or assigned
  – Required by HIPAA
  – Lack of adequate HIPAA and IT Security training
  – Absence of established programs, policies and procedures

• Antivirus software not fully deployed or operating properly
  • 9 servers infected with over 1,500 viruses
  • Increased risk of hospital data security breach
Lack of a formal risk assessment process - RESOLVED

- Formal third-party risk assessment in 2014
- Reviewed and updated risk assessment in 2015 and 2016
- Developed plan and mitigated the top risks
• Unmanaged VPN Accounts – RESOLVED
  – ORH fully implemented the Virtual Private Network (VPN) option for remote access
• Unsecure remote support tools –RESOLVED
  – A network management software program was used to identify and remove unauthorized remote access tools
  – A secure remote support tool was identified and implemented as the hospital standard
  – Web filters were put in place to block websites that allow downloading of unauthorized remote connection tools
• Sending ePHI Un-Encrypted – RESOLVED
  – Implemented a cloud-based email system with built-in encryption capabilities
  – Provided facility-wide education on how to properly send and retrieve encrypted messages

• Distributing reports with PHI (surgery schedule) too broadly in the organization - RESOLVED
  – Reviewed and reduced the distribution of reports with PHI to “Minimum Necessary”
Status

• IT Security Officer and Privacy Officer Roles not identified or assigned - Resolved
  – Job descriptions were created
  – Roles were assigned
  – Each designee obtained HIPAA and IT security training and certifications
• Antivirus software not fully deployed or operating properly – IN PROGRESS
  – An internet security software was installed to monitor and protect the data from emerging threats
  – A network management tool is used to identify devices on the network without anti-virus
Compliance Roadmap

• Evaluate current state – Compliance and Risk
  • Compare to HIPAA, NIST CSF, or other security frameworks)
• Identify what you already do –
  • The costs are already in the budget
  • Make sure the functions are maintained
• Identify gaps
• Identify what must be done to address gaps
  • Estimate costs – people, process, technology
  • Make sure to hardwire the new processes
• The cost of HIPAA compliance and security is not ZERO
Risk Management Strategies - On a Limited Budget

• All organizations have a limited budget
• Some budgets are more limited than others
• A budget of zero is a non-starter
• Skilled resources in cybersecurity and HIPAA compliance are necessary
### Risk Management Strategies - Three options for staffing cybersecurity

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use current staff</td>
<td>Know the organization</td>
<td>May not have skills</td>
</tr>
<tr>
<td></td>
<td>No additional cost</td>
<td>May not have time</td>
</tr>
<tr>
<td>Hire new staff</td>
<td>Can hire the needed skills</td>
<td>Additional cost</td>
</tr>
<tr>
<td></td>
<td>Long-term commitment</td>
<td>Long-term commitment</td>
</tr>
<tr>
<td>Contract security services</td>
<td>Can gain the needed skills</td>
<td>May be additional cost</td>
</tr>
<tr>
<td></td>
<td>Can flex staff level</td>
<td>Possible conflict of interest or divided interest</td>
</tr>
</tbody>
</table>

**Pros:**
- Know the organization
- No additional cost
- Can hire the needed skills
- Can gain the needed skills
- Can flex staff level

**Cons:**
- May not have skills
- May not have time
- Additional cost
- Long-term commitment
- May be additional cost
- Possible conflict of interest or divided interest
Implementing cloud-based systems can reduce costs, improve service level and security.

OCR Guidance on HIPAA and Cloud Computing, October 2016
- Business Associate Agreement required
  - Regardless if the data is encrypted in the cloud
- Need clarity and agreement on how each HIPAA security rule requirement is addressed by the cloud service provider (CSP) and/or the cloud customer
- Conduct a risk assessment of the CSP
Cloud Security Provider risk assessment

- Has the CSP completed the Cloud Controls Matrix from the Cloud Security Alliance?
  
  https://cloudsecurityalliance.org/group/cloud-controls-matrix/

- Is the CSP FEDRAMP Authorized? FedRAMP has a Security Assessment Framework for CSPs
  
  https://www.fedramp.gov/

- Cloud Security Framework Audit Methods by Diana Salazar
  
  https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-framework-audit-methods-36922

- HITRUST Certification -  https://hitrustalliance.net/

- CSA STAR has a public repository of CCM/CAIQ documents
  
  https://cloudsecurityalliance.org/star/#_registry
<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM V3.0 Control ID</th>
<th>Updated Control Specification</th>
<th>Architectural Relevance</th>
<th>Corr Gov Relevance</th>
<th>Cloud Service Delivery Model Applicability</th>
<th>Supplier Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity &amp; Access Management Audit Tools Access</td>
<td>IAM-01</td>
<td>Access to, and use of, audit tools that interact with the organization’s information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.</td>
<td>Phys: X</td>
<td></td>
<td>SaaS: X</td>
<td>Provider: X</td>
</tr>
<tr>
<td>Identity &amp; Access Management Credential Lifecycle Provision Management</td>
<td>IAM-02</td>
<td>User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizational-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must</td>
<td>Phys: X, Network: X, Compute: X, Storage: X, App: X, Data: X</td>
<td></td>
<td>SaaS: X, PaaS: X, IaaS: X</td>
<td>Provider: X, Consumer: X</td>
</tr>
<tr>
<td>Identity &amp; Access Management Diagnostic/Configuration Ports Access</td>
<td>IAM-03</td>
<td>User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.</td>
<td>Phys: X</td>
<td></td>
<td>SaaS: X</td>
<td>Provider: X</td>
</tr>
</tbody>
</table>
A Summary of How Benefits Were Realized for the Value of Health IT

Satisfaction
• Data privacy & security are needed for patient satisfaction

Treatment/Clinical
• Trust is essential for patients to disclosure their health condition

Electronic Secure Data
• Cybersecurity risk management reduces risk of breaches

Patient Engagement and Population Management
• Trust is essential for patients to utilize patient portals

Savings
• Estimated average cost of a data breach is > $2.2 million\(^1\)
Questions

Contact information:
Jeff Bell, BS
Chief Information Security Officer
CareTech Solutions
jeff.bell@caretech.com
https://www.linkedin.com/in/jeffbellcybersec
Twitter Handle:@JeffBell_CTS

Stephanie L. Tatum, BS
Director Health Information and Informatics Management, Privacy Officer
Oakland Regional Hospital
statum@orhmi.com
https://www.linkedin.com/stephanie-tatum-bs-rhia-b523a8103

Please let us know what you think by completing the online session evaluation!