Cybersecurity – The Increasing Threat
Health Care Compliance Association (HCCA) Regional Conference
31st May 2019
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting with you</td>
<td>2</td>
</tr>
<tr>
<td>Health care industry: Emerging risks &amp; threat landscape</td>
<td>3</td>
</tr>
<tr>
<td>Cyber risk as a business imperative</td>
<td>4</td>
</tr>
<tr>
<td>Witnessing transformation in health care</td>
<td>5</td>
</tr>
<tr>
<td>Risks from emerging technologies</td>
<td>6</td>
</tr>
<tr>
<td>Regulatory drivers for cyber</td>
<td>7</td>
</tr>
<tr>
<td>Impact of the Rule for Interoperability and Information Blocking</td>
<td>8</td>
</tr>
<tr>
<td>Use case: PCI implementation</td>
<td>9</td>
</tr>
<tr>
<td>PCI program</td>
<td>10</td>
</tr>
</tbody>
</table>
Meeting with you

Thomas J. Balcavage  
VP Information Security  
Thomas Jefferson University Hospitals  
Thomas.Balcavage@jefferson.edu

Jimmy Joseph  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
jijoseph@deloitte.com
Health care industry: Emerging risks & threat landscape

**Cyber skills shortage** is a major problem faced within the industry:

53% of survey respondents reported a problematic shortage of cybersecurity skills in their organization¹

There will be as many as 3.5 million unfilled positions in the industry by 2021.²

4 in 5 U.S. physicians have experienced some form of a cybersecurity attack³

Health care data is predicted to reach 35 zettabytes by 2020⁴

$2.2 Million is the average cost of a data breach for health care organizations³

$408 cost per record (data breach cost) in healthcare vs. $206 in financial services³

$2.2 Million is the average cost of a data breach for health care organizations³

$408 cost per record (data breach cost) in healthcare vs. $206 in financial services³

**Industry disruptors**

- **Technology is Everywhere**
- **Diversity/Generational change**
- **Jobs vulnerable to automation**
- **Artificial Intelligence, Cognitive Computing, Robotics**
- **Explosion in Contingent work**

Cybercrime damage cost:

- $3 trillion in 2015
- $6 trillion by 2021

14 seconds

Businesses will experience ransomware attacks every 14 seconds by 2019⁸

60% of digital businesses will suffer major service failures by 2020 due to the inability of IT security teams to manage digital risk⁵

30% of organizations targeted by major cyberattacks will spend more than two months cleansing backup systems and data, resulting in delayed recoveries⁶

---

2. https://cybersecurityventures.com/jobs/;
5. Gartner "Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack" 3 September 2017; 6. CSO "Top 5 cybersecurity facts, figures and statistics for 2017" 15 June 2017; 7. Cybersecurity Ventures "Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019"
Cyber risk as a business imperative

When it comes to cyber risk, the threat is only one side of the equation. Oftentimes, organizations do not consider the implications of their strategic decisions on creation of new or proliferation of existing cyber risks. Leadership must build a cyber organization that is tailored to the unique risks of the business. Cyber security should be considered a business enabler, rather than a detractor.

Three key business dimensions that may impact an organization’s cyber risk landscape:

**Increased Connectivity**
Organizations have become more connected with technologies designed for sharing. It's critical that leadership evaluates the growing cyber risk due to increased connectivity.

**People**
Leaders have to trust that the people within their organization will do the right thing. Risk is often derived from complacency and rarely out of malice.

**Business Strategy Drivers**
Initiatives and activities tied to the business strategy often create the most risk. Moves like entering new markets, expanding third-party networks, or business model transformation; all of the above drive value for the business, however, may create additional cyber risk.
Witnessing transformation in health care

The use of these technologies have skyrocketed as health care payers aim to modernize their core infrastructure through the use of data and analytics in order to improve the overall member experience.

Increased use of these technologies are bringing patients, providers, payers and pharmaceutical organizations closer.

Increased use of cloud services are enabling both provider and payer IT environments to use “only what they need”, improving the reliability, scalability, efficiency and effectiveness of business critical applications as well as securing the use, transfer and storage of electronic Protected Health Information (ePHI).

Integration of sensitive health care data between providers and payers to improve the overall member experience and deliver value-based care.
## Risks from emerging technologies

### Technology

**AI, Machine Learning and Automation**

- Audit complications
- Inadequate recovery processes
- Operational inefficiencies

**Connected devices and wearables**

- Increased attack surface
- Ineffective access control for sensitive data

**Cloud**

- Ineffective cloud asset governance
- Malware / Ransomware
- Legal and regulatory fines
- Vendor lock-in

**Data sharing and interoperability**

- Compliance Violation
- Data exfiltration

### Emerging Risks

**Insights on emerging technology and the risk it poses.**

- Bots may act in ways that violate existing laws (e.g., failure to satisfy Medicare or Medicaid certification and licensure requirements)
- Inadequate recovery processes may introduce delays in use of emergency medical devices
- Third-party risks emanating from partners operating in AI technology landscape
  - More than 50% of all connected medical devices are considered at “risk” of security composure
  - 20% of organizations have observed at least one Internet of Things (IoT) – based attack in the past three years
  - 45% of increase in the number of medical devices requiring security hardening by a healthcare provider, by 2020
- 60% of cloud services do not specify that the customer owns the data in their terms of services
- Approx. 81% of cloud services do not support encryption of data at rest
- Approx. 11.5 M dollars is spent on an average by healthcare organizations due to cloud data breaches
- 51% of the organizations are not vigilant in ensuring their partners and other third parties protect patient information
- Approx. 40% of enterprise data is either inaccurate, incomplete, or unavailable

[9] [https://go.forrester.com/blogs/arm-yourselves-for-healthcares-cybersecurity-war/](https://go.forrester.com/blogs/arm-yourselves-for-healthcares-cybersecurity-war/)
Regulatory drivers for cyber

- **Access to ePHI must be controlled and authorized while data is at rest, in use, and in transmission.**
  - **HIPAA / HITECH**
  - **PCI DSS**
  - **Critical infrastructure program**
  - **GDPR**
  - **Interoperability**
  - **CCPA**

- **Provides guidance on health care and public health critical infrastructure protection to ensures continuity and availability of health care system, especially during disasters and emergencies.**
- **Advance access of health information through digital and automated channels directly to plan members and patients receiving care**
- **Stringent data privacy regulation**
  - **Alert authorities within 72 hours of data breach.**
  - **Violation may attract fine of €20 million or 4 percent of an organization’s annual global revenue.**
- **US’s strictest consumer privacy and data protection measure for-profit healthcare firms.**
  - **Similar to GDPR in terms of right of access, deletion, know, opt in/out, and equal service.**

*Definitions: Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH); Payment Card Industry Data Security Standard (PCI DSS); General Data Protection Regulation (GDPR); California Consumer Privacy Act (CCPA)*
Impact of the interoperability and information blocking rule*

1. **As a payer**
   - Use of application programming interfaces (APIs) for retail segment products
   - Electronic Health Information (EHI) Export

2. **As a care provider**
   - Automated, electronic patient event notification from hospitals
   - Information blocking

3. **As a post-acute care (PAC) provider**
   - Promoting interoperability among other health care settings such as long-term, PAC, behavioral health settings, and home and community-based services

Use case: PCI implementation

- Third-party processes
- Assessment
- Remediation Roadmap
- Executive Leadership (Steering Committee)
- Funding

Enterprise-wide Cyber Transformation
PCI program - A high-level approach

- Provide PCI Advisory and PMO Support
- Establish PCI Service Provider Management program
- Develop PCI compliant policies, processes & standards
- Build detailed PCI System Inventory
- Develop PCI compliant business and technology integration processes
- Implement PCI compliant system hardening configurations
- Conduct PCI compliant IAM processes
- Conduct PCI compliant training documents
- Conduct PCI compliant policies, processes & standards
- Conduct vulnerability scans & remediate vulnerabilities
- Identify scope reduction opportunities
- Implement network segmentation
- Conduct penetration tests
- Implement multi-factor authentication
- Implement file-integrity monitoring
- Align logging and monitoring controls in accordance with PCI
- Build detailed PCI System Inventory
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.