CSOHIMSS Spring Conference

Cybersecurity and Privacy challenges in the Healthcare Ecosystem

May 2016
Objectives

1. Define Cybersecurity
2. Recognize the inherent vulnerabilities
3. How to operate in a new health ecosystem
4. Consideration for addressing the new reality
The new reality
The new reality...
Our perspectives

• Developed based on our interactions with CISOs, CIOs, CAEs, Corporate Suite Leadership, and Boards of Directors
• Shaped through knowledge and experience of developing strategies, implementing solutions and executing programs, and responding to security crises
• Supported and enhanced by years of healthcare industry, federal law enforcement, foreign intelligence and forensic experience
• Pragmatic insight and a balanced view of how to prioritize investments in people, processes and technology solutions needed to address the cybersecurity challenge
• Updated and refined based on healthcare industry trends, law enforcement alerts and key learnings from other industries (financial services, manufacturing and retail)
The new reality...
Highlights from PwC Global Information Security Survey

Technology Advances
86% of Healthcare CEO’s believe technological advances will transform their business

Cyber Attacks a Serious Global Concern
53% of Healthcare CEO’s are somewhat or extremely concerned by cyber attacks

Financial Loss from Security Events
283% increase in the financial losses stemming from events in 2014, at an average of $2.9M per organization

Investing in Cybersecurity
66% increase in organization’s investment in cybersecurity spending since 2013.

Sources:
1 - PwC 17th Annual Global CEO Survey
2 - PwC 6th Annual Digital IQ Survey
3 - 2015 Global State of Information Security
The new reality...
What is cybersecurity?

- Cybersecurity represents many things to many different people
- Key characteristics and attributes of cybersecurity:
  - **Broader** than just information technology and **extends** beyond the enterprise
  - **Increasingly vulnerable** due to technology connectivity and dependency
  - An ‘outside-in view’ of the **threats** and **business impact** facing an organization
  - Shared responsibility that requires **cross functional disciplines** in order to plan, protect, defend, react and respond

*It is no longer just an IT challenge – it is a business imperative!*
The new reality... Beyond the enterprise

**The Evolution:**
- Technology-led innovation has enabled business and care delivery models to evolve.
- The extended enterprise has moved beyond technology and patient-provider integration.
- Connectivity and collaboration now extends to all facets of business.

**Leading to:**
- A dynamic environment that is increasingly interconnected, integrated, and interdependent.
- Where changing business drivers create opportunity and risk.
# The new reality...

Technology domain convergence

<table>
<thead>
<tr>
<th><strong>Information Technology</strong></th>
<th>Computing resources and connectivity for processing and managing data to support organizational functions and transactions such as user workstations, reporting repositories, data warehouses, web applications, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Technology</strong></td>
<td>Systems and related automation assets for the purpose of monitoring and controlling physical processes and events or supporting the creation and delivery of products and services such as EHRs, nurse stations, hospital scheduling machines, drug allocation devices, etc.</td>
</tr>
<tr>
<td><strong>Medical Devices</strong></td>
<td>The healthcare industry includes a unique convergence of operational and consumer technology in the field of medical devices. These systems control physical processes and events supporting the delivery of medical services, while being external end-user focused, such as pacemakers, insulin pumps, CPAP machines, etc.</td>
</tr>
<tr>
<td><strong>Consumer (Products and Services) Technology</strong></td>
<td>Computing resources and connectivity integrated with or supporting external end-user focused products and services such as wearable medical devices, Health &amp; Well-Being Rewards sites, etc.</td>
</tr>
</tbody>
</table>

**Cybersecurity** encompasses all four technology types
The new reality...
Threat actors and the information they target

**Adversary**
- Nation State
- Hacktivists
- Organized Crime
- Insiders

**What’s most at risk?**
- PHI, PII, HIPAA, and other regulatory
- EHR, EMR, and Cloud solutions
- CPOE and Mobile EHR
- Health Information Exchange (HIE) integration
- Physical theft and loss
- Emerging technologies and BYOD
- ERA/EFT and Provider Payments
- Online Consumer payments and PCI-DSS
- Fraud and Anti-Money Laundering
- Business deals and strategic information
- Patient safety monitoring
- Medical devices

**Motives and tactics** evolve and what adversaries target vary depending on the organization and the products and services they provide.
### The new reality...

#### Why target healthcare?

1. **Electronic Health Records are changing the information game**
   - The healthcare business model has evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.

2. **Health records are now worth more than credit cards and SSN**
   - With Financial Services and Retail having long been targets for cyber attackers, the black markets are flooded with credit card and social security numbers, increasing the value of verified health records and identifiers for use in fraudulent access to healthcare as well as identity theft.

3. **Healthcare, and new medical research, is a focus of developing nations’ economic plans**
   - Several developing nations have targeted existing healthcare technologies, including patient care and clinical improvements, and intellectual property for further “co-innovation” or “re-innovation” in order to jump start their national economic development plans.

4. **Healthcare is less prepared to handle cyber events than FS and Retail**
   - Traditional healthcare information security programs have long been narrowly-focused, compliance based efforts that have yet to adapt to the emerging and ever-changing threat landscape presented by these advanced threats.

5. **Cybersecurity is seen as a barrier to patient care**
   - Cybersecurity is not an just an IT issue; rather it requires attention and input from key business leaders, including executives, board or directors, legal, media relations, and others.
The new reality... and adapting to it.

<table>
<thead>
<tr>
<th>Historical Perspective</th>
<th>Today’s Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope of the challenge</strong></td>
<td>Limited to your “four walls” and the extended enterprise</td>
</tr>
<tr>
<td><strong>Ownership and accountability</strong></td>
<td>IT led and operated</td>
</tr>
<tr>
<td><strong>Adversaries’ characteristics</strong></td>
<td>One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain</td>
</tr>
<tr>
<td><strong>Information asset protection</strong></td>
<td>One-size-fits-all approach</td>
</tr>
<tr>
<td><strong>Defense posture</strong></td>
<td>Protect the perimeter; respond if attacker</td>
</tr>
<tr>
<td><strong>Security intelligence and information sharing</strong></td>
<td>Keep to yourself</td>
</tr>
</tbody>
</table>

The shift is necessary because, healthcare data breaches today are less about accidental disclosure and more about targeted acquisition and unauthorized access to health records.
Events from the new reality
Events from the new reality...
Lessons learned from recent breaches in health industry demonstrate vulnerability and need to address core fundamentals...

- **Attack Method** - organized and coordinated efforts to use social engineering (phishing exploit), exploit Internet connectivity (fake infrastructure), and compromise system access (backdoor malware) for theft of business credentials

- **Awareness** - adversaries tested and enhanced their approach over the course of months before executing their campaign; intelligence sources communicated threat elements

- **Detection** - technical indicators were undetected during the attack sequence; additionally, as is often the case, third parties (e.g. law enforcement or the banks) detect the compromise first, *not* the company

- **Security Posture** - known companies compromised were assumed to be compliant with industry standards (e.g. HIPAA, PCI DSS) -- compliance does not equal security

- **Industry Exposure** – attacks are often not limited to a single company; many companies within an industry sector share the same / similar profile and it is highly likely there are other targets and victims
Events from the new reality…
Meeting the HIPAA Privacy and Security Rules may not be (is not) sufficient to prepare an organization for today’s threats

- **HIPAA** - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is implemented by **covered entities and business associates** through adoption of the **HIPAA Privacy Rule** and the **HIPAA Security Rule**

- The HIPAA Privacy Rule – **only addresses** appropriate use and disclosure of protected **health information (PHI)** in physical or electronic form

- The HIPAA Security Rule – only addresses **administrative, physical, and technical safeguards for a subset of PHI** that is created, received, maintained, or transmitted, in **electronic form** (ePHI)

- **Limitations of scope**
  - **Data** - other types of critical data, for example, **intellectual property, authentication credentials, or non-public financial information**, are **not** necessarily protected, even if an organization meets the HIPAA rules
  
  - **Threats & Vulnerabilities** – requirements **do not** specifically address evolving threats and vulnerabilities, and as such, the required Security Rule controls only provide a baseline for implementing safeguards and do not specifically address Advanced Persistent Threats and the evolving threat landscape.

- **But, HIPAA Risk Assessments**, done properly, can provide insight regarding the threats and vulnerabilities that relate to the risk surrounding PHI for a covered-entity or business associate.
Events from the new reality...
Once a security and compliance activity, incident response is now a board level and audit committee issue

- The industry has faced regulatory scrutiny for data loss / breaches previously; however these cybersecurity attacks are significantly different in their objectives, execution and impact. For instance these new cyber attackers are:
  - Seeking PHI/PII data for resale on black market for fraudulent access to healthcare products and services (i.e. Medicare, which is not reimbursable)
  - Targeting intellectual property including clinical trial data for new pharmaceuticals
  - Utilizing sophisticated threat actors with exceptional technical skills and experience
  - Employ advanced persistent threats to avoid detection and propagate your network seeking valuable information including intellectual property, trade secrets, etc.
- While some companies are thinking about proactive actions and some will operate reactively; PwC belief is to lead your response with a business impact based approach

Risks

- **Financial**: fines, remediation, cost to defend
- **Reputational**: brand impact, loss of confidence
- **Operational**: inaccurate or unavailable data, systems, or devices
- **Regulatory**: active federal and state regulators, increasing enforcement
- **Legal**: lawsuits, class action
- **Compliance**: evolving domestic & international laws
- **Contractual**: compliance with “promises” made – yours and your vendors/third parties
Adapting to the new reality
Adapting to the new reality...

Operating in the new health ecosystem requires you to think differently about your security program and investments.

Engage and commit with operations
- Leadership, ownership, awareness and accountability for addressing the cyber-risks that threaten operations
- Alignment and enablement of business objectives

Rationalize and prioritize investments
- Critical assets are constantly evaluated given they are fundamental to the brand, business growth and competitive advantage
- Threats and impact to the business are considered as investment activities are contemplated

Transform and execute the security program
- New and enhanced capabilities are needed to meet the ever-changing cybersecurity challenges
- A comprehensive program must be built on a strong foundation and include proactive coordination and collaboration with the business
- The security implications related to the convergence of Information Technology, Operational Technology and Company Products and Services are addressed
Adapting to the new reality...

Questions to consider when evaluating your ability to respond to the new challenges.

Identify, prioritize, and protect the assets most essential to the business
- Have you identified your most critical assets and know where they are stored and transmitted?
- How do you evaluate their value and impact to the business if compromised?
- Do you prioritize the protection of your crown jewels differently than other information assets?

Understand the threats to your industry and your business
- Who are your adversaries and what are their motivations?
- What information are they targeting and what tactics are they using?
- How are you anticipating and adapting your strategy and controls?

Evaluate and improve effectiveness of existing processes and technologies
- Have you patched and upgraded your core platforms and technology?
- How are you securing new technology adoption and managing vulnerability with your legacy technology?
- Have you evolved your security architecture and associated processes?

Enhance situational awareness to detect and respond to security events
- How are you gaining visibility into internal and external security events and activities?
- Are you applying correlation and analytics to identify patterns or exceptions?
- How do you timely and efficiently determine when to take action?

Develop a cross-functional incident response plan for effective crisis management
- Have your business leaders undertaken cyberattack scenario planning?
- Do you have a defined cross-functional structure, process and capability to respond?
- Are you enhancing and aligning your plan to ongoing business changes?

Establish values and behaviors to create and promote security effectiveness
- How is leadership engaged and committed to addressing cyber risks facing the business?
- What sustained activities are in place to improve awareness and sensitivity to cyber risks?
- How have your business practices evolved to address the threats to your business?
Adapting to the new reality...
Key points to consider

1. The global business ecosystem has changed the risk landscape
   Business models have evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.

2. Focus on securing high value information and protecting what matters most
   Rather than treating everything equally, you should identify and enhance the protection of your “crown jewels” while maintaining a consistent security baseline within their environment.

3. Know your adversary – motives, means, and methods
   Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary or political gain – requiring threat intelligence, proactive monitoring and deep response capabilities.

4. Embed cybersecurity into board oversight and executive-level decision making
   Creating an integrated, business aligned security strategy and program requires awareness and commitment from the highest executive levels of the organization – in order to apply the appropriate resources and investments.
## Adapting to the new reality...
### Questions Boards and CEO’s should be asking

<table>
<thead>
<tr>
<th>Enhancing their cybersecurity strategy and capability</th>
<th>1. Is our cybersecurity program aligned with our operational strategy?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Do we have the capabilities to identify and advise on strategic threats and adversaries targeting us?</td>
</tr>
<tr>
<td>Understanding and adapting to changes in the cybersecurity risk environment</td>
<td>1. Do we know what information is most valuable us? Our providers? Our patients?</td>
</tr>
<tr>
<td></td>
<td>2. Do we know what our adversaries are after / what would they target?</td>
</tr>
<tr>
<td></td>
<td>3. Do we have an insider threat program? Is it inter-departmental?</td>
</tr>
<tr>
<td></td>
<td>4. Are we actively involved in relevant public-private partnerships? Information sharing?</td>
</tr>
<tr>
<td>Advance their cybersecurity posture through a shared vision and culture</td>
<td>1. How was our last security crisis identified; in-house or government identified?</td>
</tr>
<tr>
<td></td>
<td>2. Who leads our incident and crisis management program? Is our program cross functional / inter-departmental?</td>
</tr>
<tr>
<td></td>
<td>3. How often are we briefed on our cyber initiatives? Do we understand the cyber risks associated with certain business decisions and related activities?</td>
</tr>
<tr>
<td></td>
<td>4. Have we made investments into prevention? Response? Resilience?</td>
</tr>
</tbody>
</table>
Addressing the new reality
Strategic steps to address cybersecurity risks

Organizations can’t eliminate the risk of cyber attacks, but they can minimize their consequences. Here are 5 things leading organizations do to combat cybersecurity risks.

1. Own the Risk
   - Cyber risk is owned by leadership and is not relegated to the IT function.
   - Periodic cybersecurity briefings are provided to the Board and C-Suite.

2. Prioritize Initiatives
   - Leadership prioritizes and monitors cybersecurity investments.
   - Investments are made in new capability, not just technology.
   - Crown jewels have been identified and their protection prioritized.

3. Learn and Incorporate
   - Leading organizations work with various external parties, share information on current threats and incorporate learnings into their own cybersecurity strategy and tactics.

4. Enhance Culture
   - A security culture and mindset is established through training, measurement and evaluation.
   - Behaviors and capabilities of the organization are established and reinforce the importance of cybersecurity.

5. Secure the Business
   - Security of the business value chain including suppliers, third party providers and high-risk interconnection points has been considered.
   - Adapt to the challenges of new and emerging digital business models.
Tactical Information Security actions to consider

Here are 4 actions to consider in the short term to determine the current state of your environment and cybersecurity program.

1. Establish on-call incident response agreement(s) with forensic experts and outside counsel.

2. Conduct a Breach Indicator Assessment and Threat Model to determine “Are you compromised and don’t know it?”

3. Perform a gap analysis and security risk assessment to determine your cybersecurity program’s current maturity.

4. Review your cybersecurity program strategy and incident readiness at the Board level.
**Tactical Internal Audit actions to consider**

**Perform a cybersecurity audit**
- To gain an understanding of the current state and maturity of the information security (IS) and privacy programs.
- Identify information security and privacy risks and gaps using a chosen framework (NIST, ISO, HITRUST, PwC).
- Provide recommendations for enhancement and improvement.

**Scope of Audit**
- Assess the current state information security and privacy programs across relevant processes and systems,
- Identify potential risks and process gaps based on review of policies and procedures and program governance, and
- Provide a current state maturity level with recommended enhancements to improve the information security and privacy programs.

**Assessment Elements**
- Process to identify, assess, and mitigate security threats and vulnerabilities.
- The capture, processing, storage, and distribution of data and information.
- Alignment and incorporation of operational domains within information security and privacy programs.
- Correlation of information security and privacy programs to strategic and operational IT and business objectives.
- Consideration and integration of identified future information security and privacy initiatives within the security organization and privacy & compliance teams.
For more information on cybersecurity...

www.pwc.com/cybersecurity

- 10Minutes on the stark realities of cybersecurity
- Answering your Cybersecurity Questions
- 2014 US State of Cybercrime Survey Whitepaper
- Why you should adopt the NIST cybersecurity framework
- Results of 2015 Global State of Information Security
- Cybersecurity risk on the board’s agenda
- A response to the President’s Cybersecurity Executive Order
- Cyber Video Series