Cyber Security & Digital Health

What the future may look like in a truly digital world

Paul O’Rourke
Global Cybersecurity & Privacy Leader
May 2019

Health Industries - In the Cyber Crosshairs

Be prepared for Cyber Threats

Cyber threats pose significant risk to the health industry ecosystem. Nation state actors, organized crime groups, hacktivists and insiders are gaining unauthorized access for malicious purposes. Ultimately this access may be used for economic espionage and generating profits from stolen intellectual property, Personally Identified Information (PII) and Protected Health Information (PHI).

Cyber criminals target healthcare companies because they:

Collect, transmit and store **large volumes of highly regulated information -** protected health information, personally identifiable information, payment card and **health insurance** information that can **be easily monetized on the black market.**

Generate highly sensitive **patient medical and diagnostic records, R&D data, valuable trade secrets**, and maintain access to connected and **wireless medical device technologies.**

Rely on **third-party vendors** for medical services and supply chain; employ large numbers of people with routinely high turn-over and need-to-know **access to patients, payors, providers, pharma and their sensitive data**.

Have increased **digitized** information in **electronic health records,** online appointment registrations, claims administrators, refill reminders, insurance forms, etc. with **less dedicated security spending** compared to other industries.

Cyber Threats and Implications - Today

Be prepared for Cyber Threats

$1.94 m

Average settlement amount received by HHS’ Office for Civil Rights in 2017

HIPAA Journal, Security Breaches in Healthcare in the last three years, March 2018

19 hours

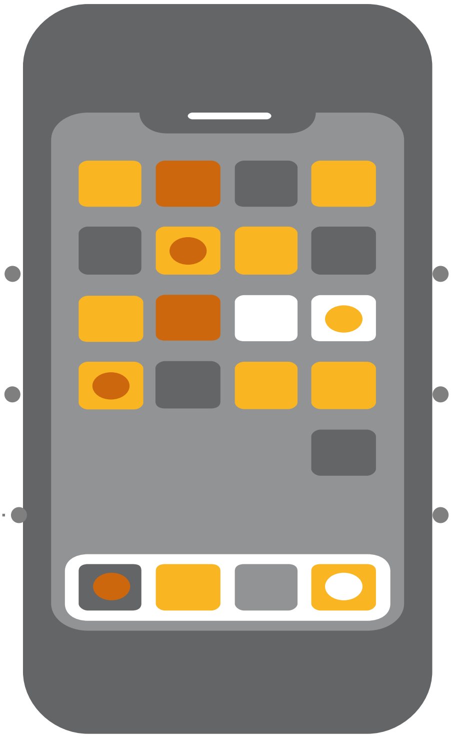
The total average downtime as a result of security incidents

PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 2017

6.1 m

Healthcare data breach victims in 2018 by August

Becker’s Healthcare & CIO Report, August 2018



525%

Increase in medical device cybersecurity vulnerabilities reported by the Department of Homeland Security’s Industrial Control Systems Cyber Emergency

U.S. Department of Health & Human Services

48

NHS health institutions in the UK, were impacted by the 2017 WannaCry attack, which resulted in disabled phone systems and cancellations of appointments and surgeries.

BBC World News, 19 Dec 2017

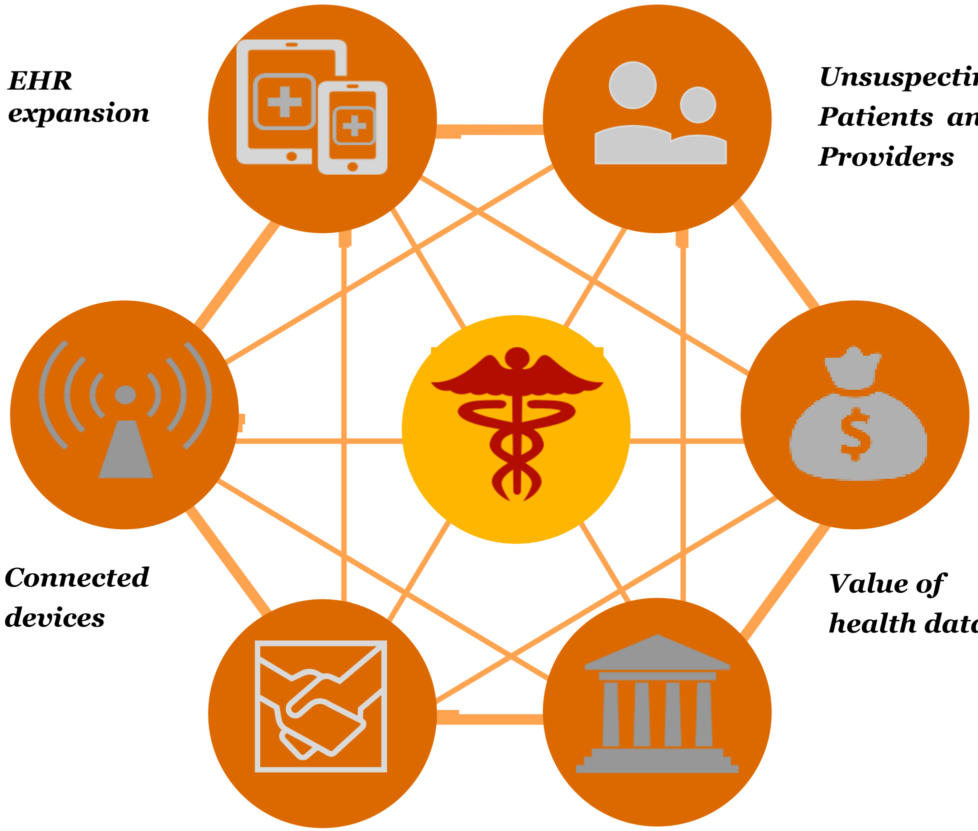
13%

Of businesses affected by cybercrime in the last 24 months report a “High” reputational impact

PwC, Global Economic Crime Survey 2016, February 2016

Health Industries - Convergence of risk factors

Convergence of risk factors makes healthcare a target



EHR expansion

Unsuspecting Patients and Providers

Connected devices

Value of health data

3rd party reliance

Regulatory change

Why anticipating a data breach event is important?

Cybersecurity is not just about securing your sensitive assets for compliance. Resilient cybersecurity is a strategic business advantage. As a cybercrime target, you should consider:

1. Full inventory of the **information** and data you have and how it is collected, used, maintained, and shared

1. The most **valued** information to your patients, your clients, your business, and your reputation - the '**crown jewels**'

1. How your **crown jewels** may be targeted or misused by malicious actor

1. The range of threat actor motives, tactics and where your **vulnerabilities** lie

1. Business impact of data leakage: loss of revenue, business interruption, reputational damage, competitive disadvantage, regulatory scrutiny and fines, litigation and third party liability, and, most crucial, **loss of trust**

Why is passing Threats onto providers / patients a concern?

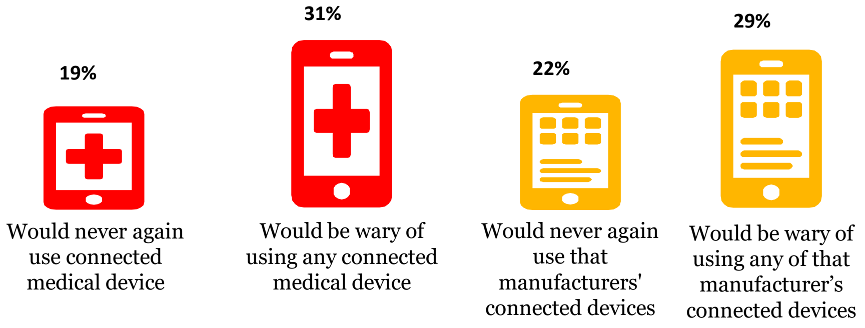
A breach or cyber incident will necessitate the need for a full investigation which will determine the vulnerability, how it was exploited, and ultimately who was responsible. The responsible party could be subject to criminal or civil action. Furthermore, there are several drivers in the industry that are placing a greater emphasis on medical device cyber security:

1. The Food and Drug Administration and the Federal Trade Commission have set the **expectation** that medical device manufacturers will identify and manage cybersecurity risks

1. Threat of civil and criminal penalties

1. The business impact of a cyber incident: loss of revenue, business interruption, reputational damage, competitive disadvantage, regulatory scrutiny and fines, litigation and third party liability, loss of trust, and, most crucial, **potential jeopardy of patient health**

Many healthcare consumers say they *would never use*, or would be wary of using, medical devices *known to have been hacked* or the or *healthcare facilities* where the hack occurred.[1]



1 HRI Consumer Health Survey, September 2015

Emerging Digital Health Challenges - Tomorrow

Be prepared for Cyber Threats

Technologically advanced medical devices

Technologically sophisticated medical devices are attractive to hackers as they expand attack surface of the increasingly connected health ecosystem.

Valuable personal health records

Personal health records are now more valuable than financial information as not only can criminals steal identities, they can gather medical details to commit insurance fraud.

Mobile phones as a source of security breaches

Patients use their mobiles to access remote healthcare services, such as GP consultations, expanding the potential for security breaches.

Device vulnerabilities increased more then ten fold

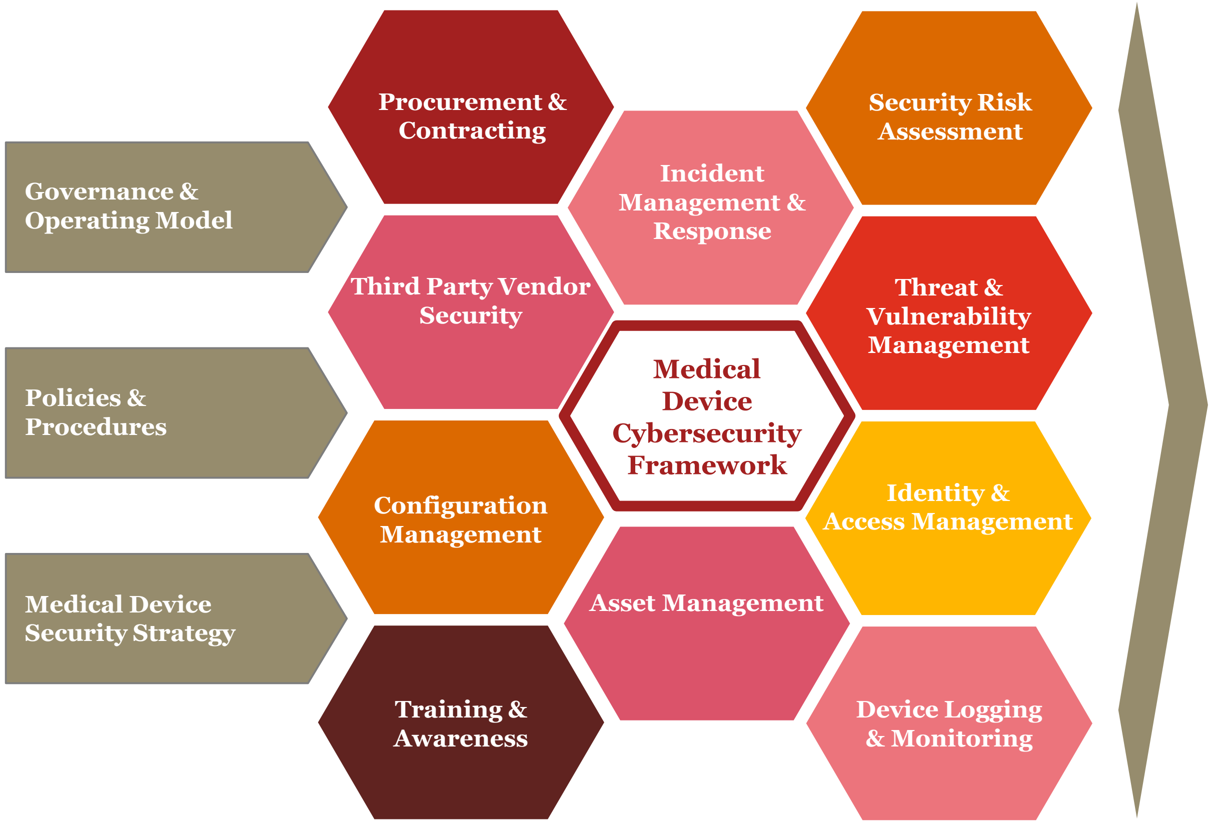
Thousands of devices connected to hospital networks, from MRI and x-ray machines to a host of smaller devices, are vulnerable to attack due to their lack of visibility.

Medical Device cybersecurity for providers

Making the complex simple

Providers need to develop and implement a proactive, risk based approach with cybersecurity in medical devices through a holistic management life-cycle approach. To help you keep your patients safe from cyber risks related to connected devices, our medical device cybersecurity framework is aligned to industry-leading practices and regulatory guidance.

Medical device cybersecurity framework


Governance & Operating Model
Policies & Procedures
Medical Device Security Strategy
Procurement & Contracting
Third Party Vendor Security
Configuration Management
Training & Awareness
Incident Management & Response
Medical Device Cybersecurity Framework
Asset Management
Security Risk Assessment
Threat & Vulnerability Management
Identity & Access Management
Device Logging & Monitoring

Governance & Operating Model

Defines a future state that addresses framework capabilities, incorporating the organisation’s structure, stakeholders, and unique needs.

Policies & Procedures

Sets enterprise-wide policy and procedures requirements aligned to framework capabilities and defines requirements across the medical device environment.

Medical Device Security & Strategy

A multi-year strategy and roadmap aligned to the framework capabilities to drive awareness and alignment to medical device security program development and execution.

Secure Digital Health Trends

Be prepared for Cyber Threats

Changing Consumer Demographic and Consumer Needs

More consumers than before are willing to receive care in a nontraditional settings including, virtual visits, health retail clinics, and urgent care centers.

*In order to meet consumer demand for alternative ways to connect with healthcare providers organizations will need to **secure consumer identities.***

Declining Healthcare Workforce

By 2035 there is projected to be a worldwide shortage of **12.9 million** healthcare professionals, creating a pathway for new technologies such as Artificial Intelligence to augment the workforce and facilitate increased efficiency.

*Healthcare organizations using AI to support an increasing number of critical business processes will need to protect their AI systems against adversarial attacks by **hardening infrastructure through Defense-in-Depth.***

Increasing Healthcare Costs

Global spending on healthcare is projected to increase to **US $18.28 trillion** by 2040. To reduce cost, healthcare companies are increasing use of technology to support with the administration of healthcare services (e.g., use of digital platforms to accelerate recruitment for clinical trials).

*Increased use of technology to combat the rising healthcare costs require organizations to **consider security implications earlier in the technology development /implementation lifecycle**.*

Increased Digitization and Reliance on IoT

Connected medical devices enable consumers to monitor their health and fitness, while allowing medical personnel to supervise health and control dosages of medications remotely.

*As adoption of connected medical devices becomes more prevalent, in addition to securing their networks, healthcare organization will **need to prioritize incident response readiness** through development and testing of incident response plans**.***

New Entrants

The health industry has long been a closed and highly-siloed system. But powerful global players, both new and traditional to healthcare, are transforming the industry into a nimble and modular ecosystem.

*Non-traditional healthcare players will need to **stay abreast on the evolving data protection and privacy regulatory requirements.***

The Future in Digital Health Security & Privacy

Be prepared for Cyber Threats

Secure Digital Interaction and Information Sharing

Need to secure digital interaction and information sharing among physicians, patients, payers and other business partners.

Mobile and embedded devices represent a significant and growing risk.

Secure IoT and Connected Devices

Improved technologies are foundational to improving healthcare outcomes, but the IoT and connected devices often lack cybersecurity and privacy safeguards.

Health providers need increased governance and safeguards over the deployment of IOT and connected devices

Increased use of real world data

The need to speed products to market is expanding the use of real-world data, including information gleaned from digital health apps, wearable devices and electronic health records (EHRs).

Increased sharing of sensitive data like patient and clinical trial results demands comprehensive data protection capabilities.

Proactive investments in security and privacy

New Entrants competing with new technologies to advance care and increased patient engagement.

Businesses see value in making strategic, long-term investments in security programs and technologies.

How to respond to the security challenges

Be prepared for Cyber Threats

It's clear that all hospitals and health organisations face some serious cyber security issues. So, what steps should you be taking to address them? The big challenge is that advances in medical technology are moving so fast, that the main concern is the delivery of the best care to patients.

What should healthcare institutions be doing?

Protect what matters most:
Patient data is the most sensitive data under the control of healthcare entities and must be safe from malicious and unauthorized uses. Proper safeguards are required to ensure privacy..

Get the basics right: Out-of-date and unpatched systems can provide an easy route in for attackers. The high turnover of staff at clinical sites must be carefully handled by managing user access privileges at all times.

It is difficult to protect what you can't see:
Proactively monitor and detect for cyber threats and activity across your network, endpoint and log all data access – and ultimately enhance visibility.

Plan for the inevitable:
Assess your response through simulations and regular testing, and develop your crisis and technical response plans and policies accordingly. It's better to fail at a simulation than in real life.

Awareness is key: Ensure your people are aware of the risks, trained in cyber security and understand their responsibilities. Also educate patients and clinicians on the tools and policies that exist to protect data privacy.

The Human Element in Digital Health Security

Be prepared for Cyber Threats

The cost of cyber damages in will continue grow to trillions of dollars by 2021. The **most successful cyber attacks in healthcare** are those that exploit the **human element**. **Security awareness** is a key mitigating factor.

31%
Phishing or Malware

24%
Employee Action or Mistake

17%
External Theft

14%
Vendor

8%
Internal Theft

6%
Lost or Improper Disposal

Source: 2016 Data Security Incident Response Report, Baker Hostetler

Risk-based Cybersecurity Strategy

Conduct a risk-based maturity assessment to develop a cyber security strategy and governance function to manage cyber risks

Security Culture & Awareness Program

Employ methodology that combines proactive phishing simulations with awareness workshops to increase awareness to cyber risks

Service-oriented Security Program

Map desired capabilities to distinct security services that will be fully operationalized over the next 2-3 years.

Assessments, Remediation, & Program Development

Resilient cybersecurity is a strategic business advantage that not only reduces the manufacturers liability but also helps their customers meet their cybersecurity goals.

Strategy Execution, Design and Implementation

Develop the privacy/security strategy in accordance with business, operational, risk and compliance needs. Design the program operating model, identify the resources to carry out the day to day activities and provide architecture and implementation support.

- Integrated Privacy and Security Strategy and Program Development
- Information Governance
- Data Identification, Classification, Use and Protection
- Software/Systems Development Lifecycle (SDLC) process

Information Risk and Incident Management

Comprehensive approach to identify and mitigate cybersecurity risks and evaluate the effectiveness of the privacy/security program

- Health Information Risk Mitigation
- Health Innovation and Product Risk
- Vendor Risk Management
- Data Breach Investigation and Cybercrime

Regulatory Compliance

Preparation for regulatory audits and assess the health of the overall privacy and security programs

- Mock Audits
- Risk Assessments
- Compliance Roadmaps
- Implementation

www.pwc.com.au

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

181213-171427