Deloitte.

Cybersecurity – The Increasing Threat

Health Care Compliance Association (HCCA) Regional Conference

31st May 2019

Content

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 organization[1]

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 attack[3]

Health care data is predicted to reach **35 zettabytes** by 2020[4]

$2.2 Million is the average cost of a data breach for health care organizations[3]

$408 cost per record (data breach cost) in healthcare vs. **$206** in financial services[3]

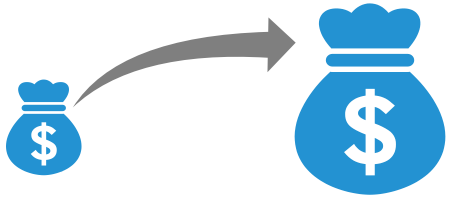
Industry disruptors

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

14 seconds

Businesses will experience ransomware attacks every 14 seconds by 2019[8]

Cybercrime **damage cost**[7]

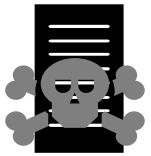


$ 3 trillion in 2015

$ 6 trillion by 2021

60%

of digital businesses will suffer major service failures by 2020 due to the inability of IT security teams to manage digital risk[5]



30%

of organizations targeted by major cyberattacks will spend more than two months cleansing backup systems and data, resulting in delayed recoveries [6]

1. https://www.valuewalk.com/2018/10/cybersecurity-talent-gap-infographic/ 2. https://cybersecurityventures.com/jobs/; 3. Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
4. "Largest Healthcare Data Breaches of 2017." HIPAA Journal, 8 Mar. 2018; 5.Gartner "Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk" 6 June, 2016; 6. Gartner " Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack" 3 September 2017; 7. CSO "Top 5 cybersecurity facts, figures and statistics for 2017" 15 June 2017; 8. 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.

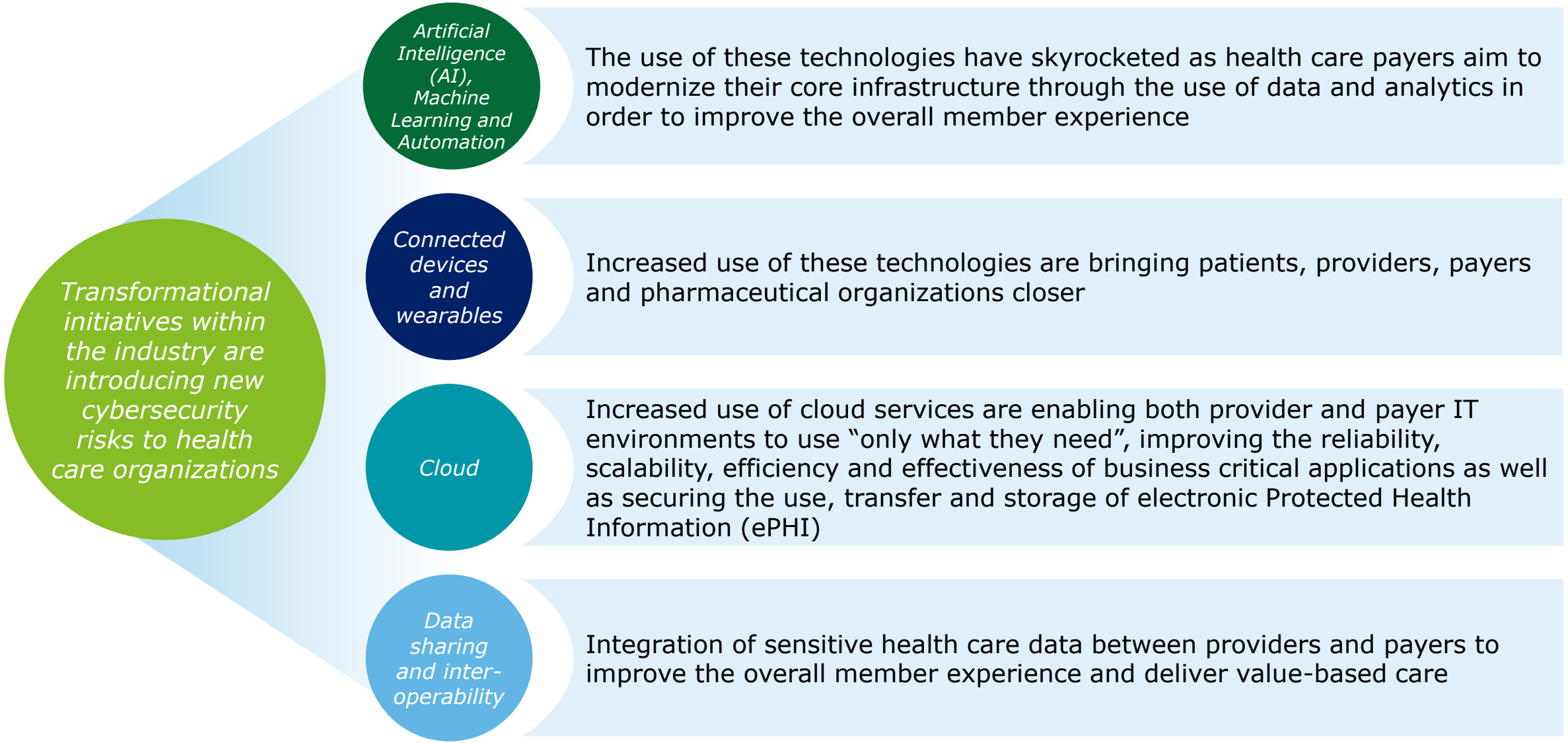
People

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



Risks from emerging technologies

Technology	Emerging Risks
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

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[9]
- 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[10]

- *60% of* cloud services do not specify that the customer owns the data in their terms of services[11]
- Approx. 81% of of cloud services do not support encryption of data at rest[11]
- 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[12]

[9] https://go.forrester.com/blogs/arm-yourselves-for-healthcares-cybersecurity-war/[10] Gartner:Top Three Security and Privacy Impacts of Connected Medical Devices on Healthcare Providers/27Sep2017 [11] https://www.cio.com/article/3217020/data-management/your-data-accessibility-problem-is-costing-you-65-million.html [12] https://www.dataversity.net/bad-data-crippling-data-analytics/

Regulatory drivers for cyber

HIPAA / HITECH*

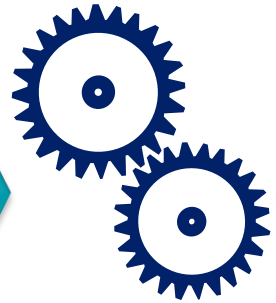
- Access to ePHI must be controlled and authorized while data is at rest, in use, and in transmission.

PCI DSS*

- Specifies how merchants and acquirers must protect card holder data from point of creation to destruction or obsolescence.

Critical infrastructure program

- 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.



GDPR*

- 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.

Interoperability

- Advance access of health information through digital and automated channels directly to plan members and patients receiving care

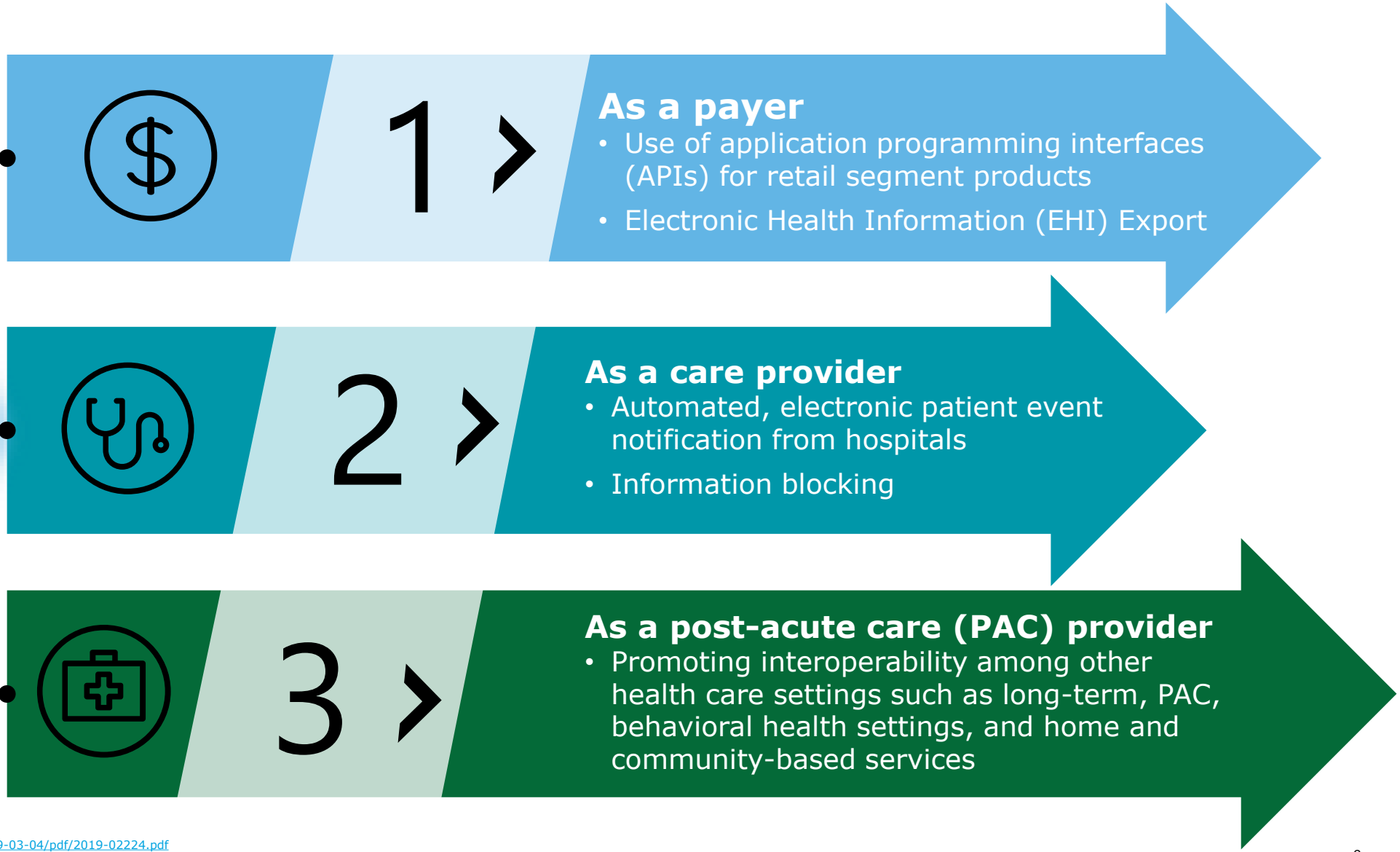
CCPA*

- 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)

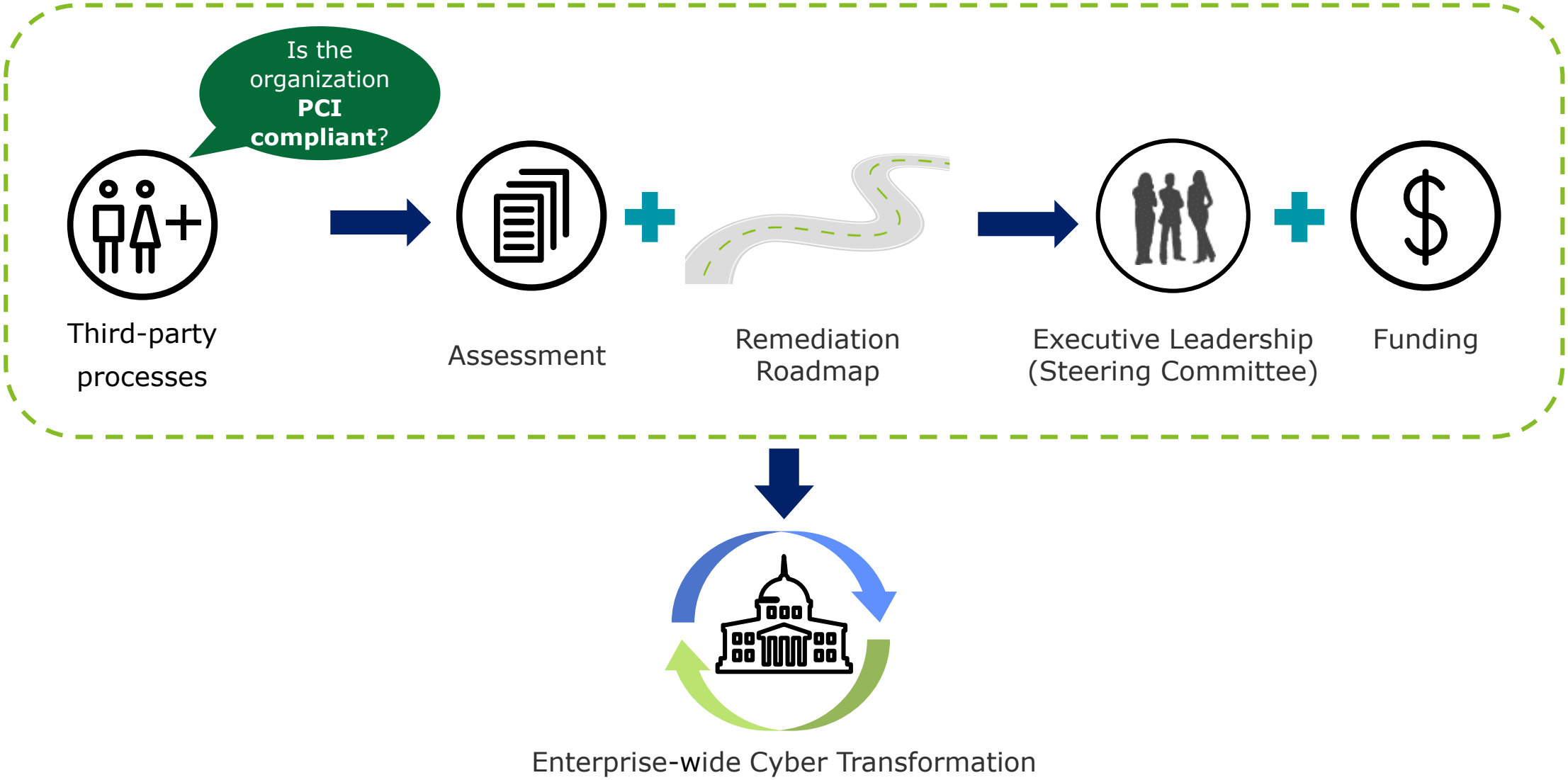
Impact of the interoperability and information blocking rule*

Proposed rule on Interoperability, and information blocking

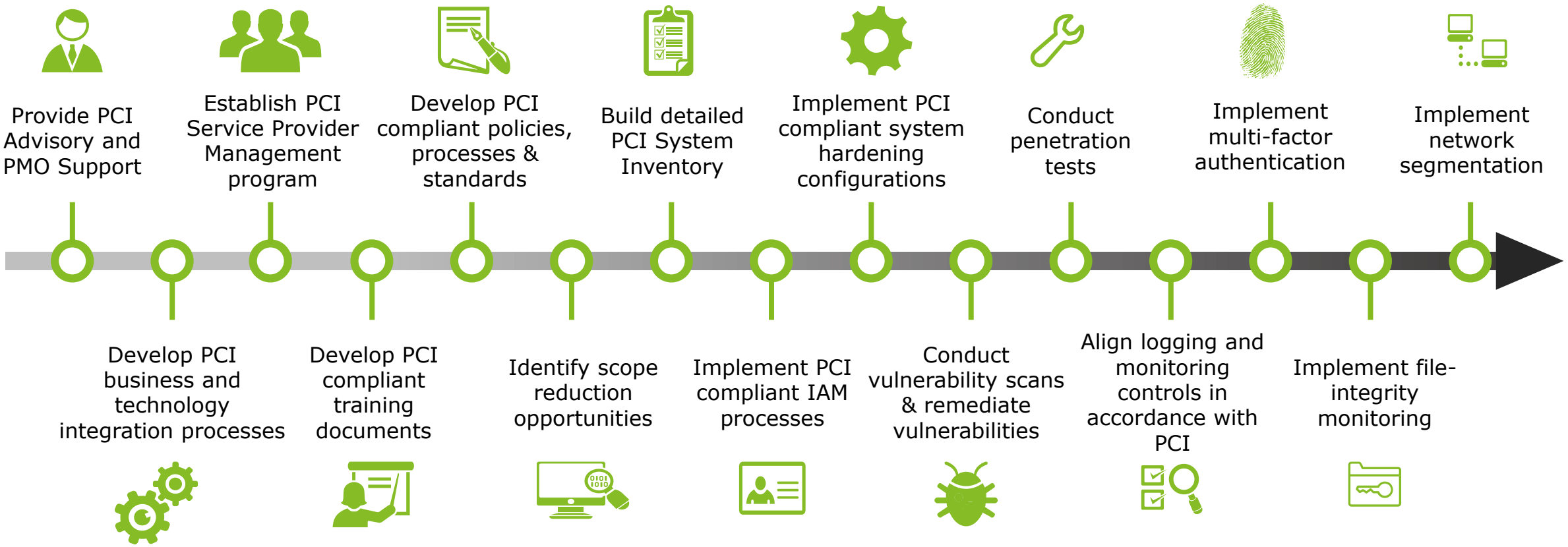


*Rule Source: https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf

Use case: PCI implementation



PCI program - A high-level approach



Deloitte.

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.

Official Professional Services Sponsor

Professional Services means audit, tax, consulting, and advisory.