Cybersecurity Trends for the Healthcare Industry

About This eBook

Implementing cybersecurity countermeasures is of great importance for healthcare organizations, ensuring that patient health information (PHI) remains protected and secure.

Failure to do so results in HIPAA-based ramifications, resulting in significant monetary losses for today's treatment centers and hospitals.

This eBook discusses the current state of cybersecurity operations, highlighting emerging threats and solutions to these malicious activities.

2019 Cybersecurity Challenges

Michael Zboray, Gartner's former chief information officer and OnPage's current information and cybersecurity advisor, states that the medical internet of things (m-IoT) poses the greatest cybersecurity threat to today's organizations.

Medical devices tend to be on-premise and internet connected. Available devices (e.g., monitors, laptops and tablets) are integrated into a common network, sharing important electronic health records (EHR). Device manufacturers create and develop technologies with vulnerabilities, allowing malicious parties to target clinics, hospitals and treatment centers.
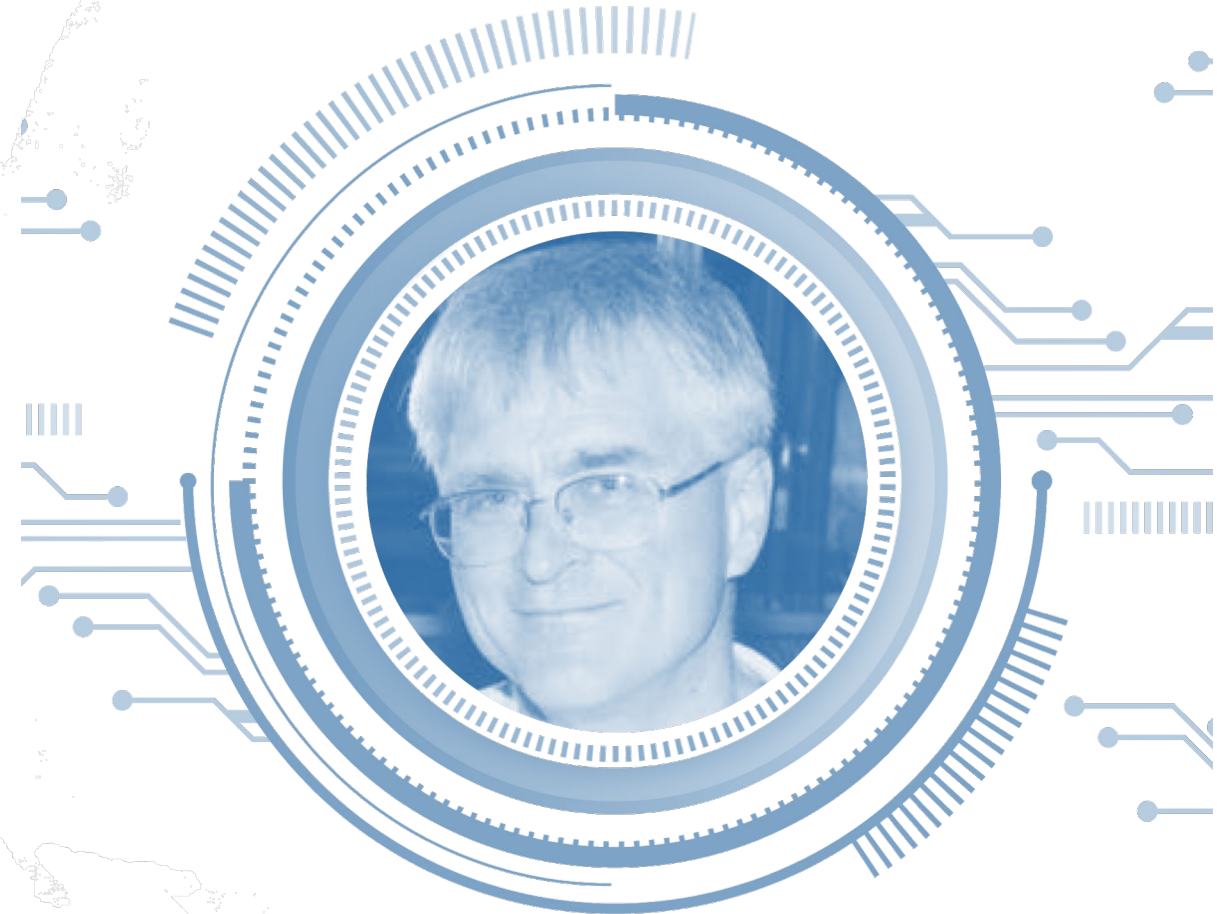
Michael Zboray,
information and cybersecurity advisor,
OnPage Corporation

CIA Triad for the Healthcare Industry

In addition to enhancing m-IoT security, Michael Zboray suggests that organizations need to better solidify the confidentiality, integrity and availability (CIA) of information.

At its core, CIA ensures that only the appropriate medical personnel receive and share important clinical information. This way, healthcare organizations can defend against malicious parties and anomalies.
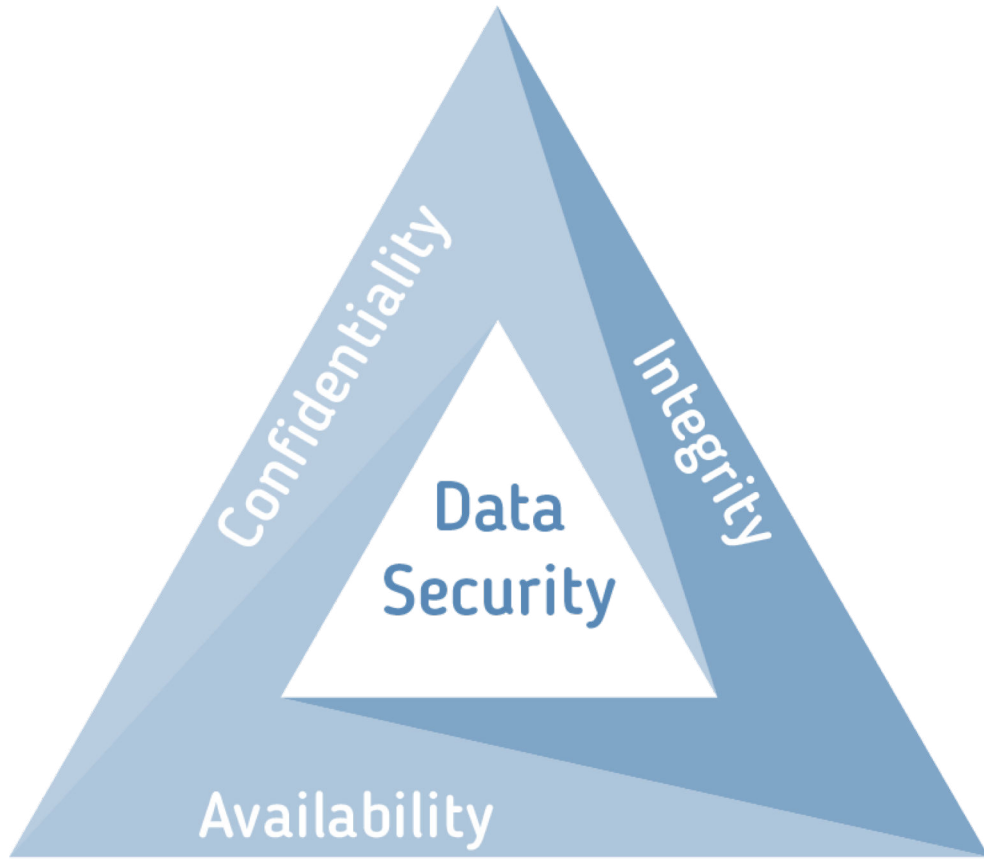
Monetary Ramifications

According to the Ponemon Institute, the average cost of a data breach is now **$3.86 million.**[1]

Even worse, healthcare organizations are common targets of malicious parties. The industry is now the second most targeted field of cybersecurity attacks.[2] For instance, the industry was required to pay a total of **$110,448,000** for data breaches occurring from 2013 to 2017.[3]

Healthcare organizations can avert these monetary ramifications by enhancing their security measures and practices.

1 https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/
2 https://netdiligence.com/portfolio/cyber-claims-study/
3 https://netdiligence.com/portfolio/cyber-claims-study/

Cybersecurity Solutions

Healthcare organizations can avert cybersecurity disasters by leveraging antivirus software, ensuring that important patient information isn't at risk.

Additionally, organizations need to place importance on security patches. This way, facilities can adopt software that eliminates technological security flaws.

Equally as important, healthcare organizations need to better solidify the CIA triad. For instance, confidentiality can be enhanced through access restrictions and password best practices.[4] Integrity can be improved through data consistency and data change detection, while availability requires constant maintenance of hardware and software systems.

4 https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Adopting a Clinical Communications Platform

A clinical communications platform such as OnPage, enhances an organization's cybersecurity operations.

Paging solutions offer HIPAA-compliant communications, ensuring that care team exchanges remain secure and protected.

Additionally, these solutions reduce delays in communication and enable physicians to securely exchange patient information (i.e., EHR).

On-call schedules and rotations can also be configured, ensuring that only the appropriate recipients (e.g., physicians) receive sensitive patient information.

By adopting a clinical communications solution, hospitals can benefit from a sign-in process and remote wipe capabilities to further enhance organizational security.

OnPage's award-winning, HIPAA-compliant incident alert management and clinical communications system for healthcare professionals, provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. Through its platform and smartphone app, OnPage helps streamline workflows and improve patient outcomes.

OnPage's escalation, redundancy and scheduling features make the system infinitely more reliable and secure than pagers, emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response.

Whether to minimize IT infrastructure downtime or to reduce the response time of healthcare providers in life-and-death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notification needs.

To learn more, contact OnPage at sales@onpagecorp.com, call (781) 916-0040 or visit www.onpage.com