Compliance Today - September 2020

Tackling health IT challenges with a proven risk management strategy

By Gerry Blass and Jason Tahaney

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, NJ, and **Jason Tahaney** (jason.tahaney@comop.org) is Director of Technology at Community Options Inc. in Princeton, NJ.

- linkedin.com/in/gerry-blass-917a482/
- linkedin.com/in/jason-tahaney-91653618/

Whether we want to believe it or not, healthcare data breaches are prevalent throughout the industry. Even more alarming, an evaluation of recent cyber and ransomware attacks indicates that the size or type of healthcare organization is immaterial to would-be attackers. Hospitals, clinics, long-term and elderly care providers, dental and optometry practices, plastic surgeons, and medical testing facilities have all experienced cyberattacks since 2016.[1] In fact, a Ponemon Institute study cited that 89% of healthcare organizations have experienced a data breach.[2]

Malware, ransomware, phishing attacks, third-party vendor negligence, insider fraud, improper data access and disposal—all common sources of data breaches—can wreak havoc on a health system's daily operations, negatively affect patient care, and threaten the safeguarding of protected health information. Ransomware attacks, one of the fastest-growing cybersecurity threats, are expected to quadruple by the end of 2020.[3]

In this article, we will use this analysis of the current healthcare cybersecurity landscape to:

- Explore the most threatening risks in healthcare information technology (IT) and cybersecurity;
- Discuss the critical role of a chief information security officer (CISO) in developing and maintaining strategic direction;
- Identify the essential components of a comprehensive risk management strategy required to protect healthcare organizations from common security and compliance inconsistencies; and
- Apply real-life strategies—including governance, oversight, data analysis, and field observation—to identify and respond to risk, maintain transparency, set budgets, and effectively track risk registries, assessments, and the mitigation process.

Healthcare cybersecurity challenges and risks

CISOs and other healthcare IT leaders experience a complex and constantly evolving set of challenges every day. The digitization of healthcare has had an exponentially significant impact on the value of healthcare data over the past two decades. Let's explore the most common scenarios that cause inherent high risk at healthcare organizations.

Data silos everywhere

Continued merger and acquisition activity throughout the healthcare industry has led to a ubiquitous presence of data silos. The result of such operational changes yields a complex portfolio of systems that typically do not talk to each other. The merged organization ends up with a variety of software, which requires more servers, more configuration, more interface engines, more related patient systems, and more third-party vendors. All of these applications and systems are their own data silos, leading to an inventory of unstructured data and an associated high inherent risk. Providers are beginning to move data to the cloud using software-as-a-service models, which can improve overall data security.

Legacy electronic medical record applications

Legacy electronic medical record applications were written in the late 1990s with very little built-in security. Many of these are still in production today. But to meet current data security standards, the technology must be compatible with newer applications and systems. As a result, IT and security teams are left with developing their own workarounds to secure gaps with legacy systems.

Limited qualified staff

Healthcare has generally lagged behind other industries in funding and staffing for cybersecurity. According to a 2017 Thales data threat report, nearly 40% of healthcare organizations surveyed said they lack the staff to manage cybersecurity defenses.[4] Chuck Brooks, former legislative director of the Science & Technology Directorate at the Department of Homeland Security, states, "Cybersecurity workforce training of a next generation of technicians and SMEs will continue to be both a challenge and a priority in 2020. The risk environment is growing every day and there have not been enough resources [3 million talent shortage] dedicated to keeping up with governments' cybersecurity requirements.... As connectivity permeates every aspect of our lives, being cyber secure is an imperative and developing more cybersecurity workers is critical to cybersecurity success."[5]

Lack of an empowered CISO

Too often in healthcare we see that cybersecurity is assigned to the operational directors of IT. This organizational structure does not allow for the proper checks and balances needed to properly find, document, and report security threats. In this structure, the CISO is generally not empowered to audit IT controls or to provide unbiased feedback that would affect IT operations, leading to potential conflicts of interest or undue political pressure to whitewash audit results.

Misconceptions about cybersecurity insurance

Healthcare leaders may fall into a trap by thinking, "We have cyber insurance, so we're covered if anything happens." However, like other types of insurance, cyber insurance will not protect healthcare organizations that are negligent in performing security controls and policies. Cyber insurance will mitigate the majority of the more expensive costs related to cybersecurity breaches, but it does not typically cover all costs related to reputational harm, loss of business, business continuity, or regulatory authority audits.

Lack of a working governance model

Without executive oversight and governance, cybersecurity efforts tend to go unfunded. Healthcare organizations that lack an IT governance model may not have a transparent understanding of all security risks, and therefore do not have all the information required to make informed decisions on how to prioritize risk mitigation efforts. In addition, lack of governance impedes the growth of an enterprise culture of compliance where all departments share in the education, training, and enforcement of cybersecurity processes.

Insufficient workforce training

How many healthcare organizations are prepared to deal with risks that are constantly changing and evolving, especially when many attacks prey on unsuspecting employees? According to providers surveyed in a Ponemon study, 54% of healthcare associates say their biggest problem is employee negligence in the handling of patient information.[6] Leaders must prepare to continually train employees on cybersecurity processes and procedures.