Beyond HIPAA: Improving Cybersecurity for Healthcare Organizations

**POWERFUL INSIGHTS**

**Issue**

Cyberattacks against healthcare organizations are on the rise – and bound to escalate even more. While retail and financial sector organizations, victimized by a spate of high-profile cybercrimes, have bolstered their security measures aggressively, their healthcare counterparts, traditionally focused on compliance rather than security, have lagged behind.

For hackers, healthcare records are a treasure trove of bankable data – prescription drug information as well as addresses and Social Security numbers, which hackers can use for identity theft or insurance fraud. This data is 10 to 20 times more valuable to cybercriminals than credit card numbers, according to some estimates (with others estimating it as high as 50 times more valuable). The relatively easy access to such “low-hanging fruit” makes healthcare organizations today far more vulnerable to cybercrime than other data-rich organizations.

Yet, the responses of healthcare leaders who participated in Protiviti’s *2015 Internal Audit Capabilities and Needs Survey* indicate healthcare organizations can make significant improvements in cybersecurity. Asked if evaluating and auditing cybersecurity risk was part of their audit plan, 43 percent said no (20 percent of those did indicate they planned to include it in next year’s audit plan).

Among the 57 percent of respondents who said they do address cybersecurity as part of their audit plan, nearly half (47 percent) said internal audit does not evaluate the organization’s cybersecurity program against the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

**Challenges and Opportunities**

The numbers cited are concerning, but they are not without reasons. For one, HIPAA (the Health Insurance Portability and Accountability Act of 1996) compliance – a top priority for healthcare organizations – can provide a false sense of security when it comes to cybercrime. Because risk analysis efforts are covered under HIPAA and there appears to be a broad disconnect across the industry as to what constitutes a sufficient risk analysis (despite guidance being available from the Office for Civil Rights (OCR)), leaders assume they have addressed information security issues adequately. That is rarely the case. HIPAA risk analyses are not sufficiently prescriptive – meaning they don’t require best-practice execution of security controls and adversarial resiliency. In addition, the risk analyses that are currently being done are frequently not comprehensive enough, often omitting much of the organization’s electronic protected health information from the scope or inadequately evaluating issues, such as privileged access, network configuration, incident response, biomedical device security, etc.

Another factor – the availability of cyber insurance – may play a role as well, reducing the motivation for healthcare organizations to conduct proper risk analyses. It is important to note, however, that insurance companies have denied claims on the basis that basic security controls were not in place before a cyberattack occurred.

Healthcare organizations that take steps to address cybersecurity weaknesses will avoid much more than reputational harm; they will also be less likely to incur regulatory penalties or legal costs stemming from violating patient privacy. However, more importantly, they will be better positioned to protect their patients’ sensitive information. Compromising patient privacy is not a gamble.
healthcare organizations want to take, especially since reasonable and effective ways to demonstrate due care do exist. Because attacks and security incidents now are viewed as common occurrences rather than exceptions, it is imperative for healthcare executives to take appropriate countermeasures, deploying best practices and frameworks in their efforts – or meet with little sympathy from their regulators and consumers when a breach does occur. With OCR’s looming Phase 2 HIPAA audit program soon to be released, scrutiny and regulatory activity will only continue to increase and is not going away.

Our Point of View

Protecting patient information begins with effective risk analysis. To this end, healthcare leaders need to initiate risk discussions among their boards and the technology, medical and legal stakeholders within their organizations. In some cases, the discussions may require outside expertise to bridge the knowledge gap among those entities.

It is also essential for healthcare organizations to realize that HIPAA is not a security framework, and that the adoption of a legitimate cybersecurity framework, such as the one from NIST, is necessary. The NIST Critical Infrastructure Cybersecurity Framework was released in February 2014, following an executive order by President Obama to protect critical infrastructure.1 Although the framework is voluntary, its risk-based approach to managing cybersecurity risk is accepted widely. The framework’s emphasis on balancing cybersecurity with civil liberties and privacy is also important and timely. By following the framework’s standards, guidelines and practices, organizations will be able to:

- Describe their current cybersecurity posture
- Describe their target state of cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk and posture

The NIST framework consists of three components:

1. **Framework core**: A set of best practices for cybersecurity activities, outcomes and references to aid in developing an organization’s risk profile. The core consists of five functions: identify, protect, detect, respond and recover.

2. **Framework implementation tiers**: A mechanism for organizations to understand their risk management rigor and approach to managing cybersecurity risks. There are four tiers, reflecting a progression from an informal, reactive response, to an approach that is agile and risk-informed. Tier selection considers factors such as the threat environment, legal and regulatory requirements and organizational constraints.

3. **Framework profile**: This component assists in articulating an organization’s current state and targeting activities to reach a desired state. The use of a risk-based approach enables the organization to gauge resources (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.

Mitigating cybersecurity risks introduces new investment costs that healthcare leaders will need to consider. But it is imperative that they do not shortchange the process. Leaders should be prepared to respond appropriately to emerging threats and federal agency advisories so they are not faced with the difficult situation of having to explain their inaction in the face of exposed patient information or compromised patient safety.

---

1 As defined by the executive order, critical infrastructure consists of “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”
How We Help Companies Succeed

Protiviti offers a unique blend of technical and healthcare industry talent and can assist organizations in making informed decisions on how best to limit their liability and ensure patient privacy.

Our team includes healthcare information security experts with significant industry expertise as well as hands-on researchers and thought leaders who consult regularly with government agencies on healthcare security. This ensures that our clients receive first-hand guidance from those with the most current information.

Our services include:

- Medical device risk assessments
- HIPAA program development, gap evaluations, and security risk analyses
- Vulnerability management program development and remediation
- Privileged account management
- Breach detection and incident response
- Security program and framework development and assessment
- Payment card industry (PCI) assessment

Contacts

Susan Haseley
+1.469.374.2435
susan.haseley@protiviti.com

Jeff Sanchez
+1.213.327.1433
jeffrey.sanchez@protiviti.com

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 Fortune 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.