HIMSS Analytics and Symantec Study Shows While Risk Management Is Maturing, Cybersecurity Gaps Still Loom

Cybersecurity business risks call for enterprisewide solutions

Cyberattacks on healthcare providers and breaches of patient data continue to dominate the news. The constant media attention to these incidents has helped elevate healthcare's awareness of cybersecurity risks. Yet, the third annual *HIMSS Analytics IT Security and Risk Management Study*[1] found that healthcare providers' confidence in their ability to stop cyberattacks has not improved.

The realization that a provider's cybersecurity program is not where it should be, is an important first step, said Axel Wirth, Distinguished Healthcare Architect at Symantec and a member of the HIMSS Privacy and Security Committee. "Healthcare is a lucrative target, and at the same time, it has a relatively low security maturity level," he said. That means that every healthcare provider — from the largest urban academic medical center to the smallest rural hospital — is at risk of a cyberattack. "If a healthcare provider doesn't see itself as a target, that would indicate that it doesn't have a full understanding of what cybersecurity means in 2018," Wirth said.

"If a healthcare provider doesn't see itself as a target, that would indicate that it doesn't have a full understanding of what cybersecurity means in 2018."

Axel Wirth | Distinguished Healthcare Architect, HIMSS Privacy and Security Committee Member | Symantec

Moving cybersecurity out of IT and into the boardroom

The first step is being aware that all healthcare providers are at risk of a cyberattack. The next step is realizing that cyber risks are not just an IT problem or a compliance problem, but also a concern for the entire enterprise. "Cyberattacks aren't just technical risks anymore," said Wirth. "They are business risks."

Produced in partnership with HIMSS Media

Produced in partnership with HIMSS Analytics

> ***"One of the strengths of our approach to security is that we leverage external best practices by focusing on the NIST Cybersecurity Framework."***
>
> **CISO** | 500-Plus Bed Healthcare Organization

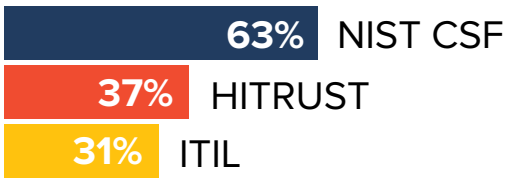
Two trends have contributed to this reality. First, during the past 10 years healthcare has undergone a digital transformation, and as a result, has become highly dependent on the availability of digital systems and data. Second, cyberattacks have become more sophisticated, targeted and focused on financial gain. Consequently, "hospital boards have begun to realize security affects their bottom line, their reputation, their ability to deliver care to their patients, and — in extreme cases — even their ability to keep their doors open," said Wirth.

A little more than one of four survey respondents (27 percent) indicated they have a standing security report at each board meeting. Another 40 percent indicated cybersecurity reports take place on an ad-hoc basis, upon the request of the board or executive management. Only 14 percent meet proactively to discuss risks.

Regular reporting to the board may seem like a trivial detail, but it's not. Consistent communication with the board is important. "The more systematic a board is in looking at cybersecurity from a business risk standpoint, the more mature an organization is," said Wirth. Organizations need to "take security out of the technical realm and into the business realm. They need to understand and articulate the business risk of security; define overall governance and risk tolerance; and then enable security through staffing and budgets. Most importantly, they need to establish a culture of security through all tiers of the organization."

One practice that helps organizations move security out of IT and into the broader enterprise is the adoption of a security framework. "One of the strengths of our approach to security is that we leverage external best practices by focusing on the NIST Cybersecurity Framework," said a CISO at a 500-plus bed organization. "NIST is the centerpiece of our security program and ongoing operational processes." The survey found the most commonly adopted frameworks include the NIST Cybersecurity Framework (CSF) (63 percent), HITRUST (37 percent) and ITIL (31 percent) (Figure 1).

FIGURE 1: The top three most commonly adopted frameworks:



Which framework a provider uses isn't as critical as the fact that an organization has adopted a framework. Frameworks give organizations a common language to talk about risk, and establish common goals and report on their progress. Frameworks also provide a way to standardize the way risk is measured and benchmarked across the enterprise. Industry-agnostic frameworks, such as the NIST CSF, can also be used to compare an organization not only to industry peers but also to other industries, which can be helpful for executive decision-making.

Healthcare continues to underinvest in cybersecurity compared to other industries

Healthcare consistently lags behind other industries when it comes to investing in cybersecurity. Previous studies have found most healthcare providers spend only 6 percent or less of their overall IT budget on security, compared to, for example, the financial services industry, which typically spends double that amount.[2] This is ironic in light of the fact that data breaches in the healthcare industry are actually costlier than data breaches in the financial services industry. A recent study found the average cost of a data breach per lost or stolen record was $380 for healthcare compared to $245 for financial services.[3]

"We don't use the public cloud. And we won't move to it until we are sure everything — including protected health information — is absolutely secure."

Vice President of IT | Healthcare Provider

The HIMSS Analytics survey confirmed a lack of investment in cybersecurity by healthcare providers. Nearly half of respondents (45 percent) reported allocating 3 percent or less of their total IT budget to security. Another 29 percent reported spending between 4 and 6 percent of their total IT budget on security. Overall, spending on IT security has remained relatively flat for the past three years.

Providers recognize that underinvestment is a problem. The director of security at an intermediate-size provider (251 to 500 beds) said: "In most other industries, about 10 to 15 percent of the IT budget gets spent on security. The commitment from our board and our CIO is that we want to be more consistent with other industries."

FIGURE 2:

73%

of providers identified "budget" as the most significant barrier to improving their security programs, with "staffing" and "skillsets" coming in 2nd and 3rd.

When asked about the top three barriers preventing their organizations from achieving a higher level of confidence in their security programs, respondents identified budget, staffing and skill sets, in that order (Figure 2). Seventy-three percent of respondents placed budget among their top three barriers; 63 percent ranked staffing among their top three; and 40 percent ranked skill sets in their top three. More than one of three (36 percent) also identified a lack of appropriate tools as a barrier.

Unique technology ecosystem creates additional challenges

In addition to the obstacles created by budget concerns, staffing, skill sets and tools, healthcare providers also deal with the challenge of managing risk in the context of a uniquely complex technology ecosystem. This complexity spans across technology generations from legacy equipment that is no longer supported on one end to the rapid adoption of cloud technologies on the other.

Seventy-seven percent of respondents indicated their organizations are using the cloud in some capacity. Sixty-three percent of those using the cloud are doing so with multiple systems or services. At the same time, 71 percent of respondents expressed several security concerns related to moving to the cloud (Figure 3). Concerns about data security have kept some providers from moving to the cloud at all.

The vice president of IT at one provider said: "We don't use the public cloud. And we won't move to it until we are sure everything — including protected health information — is absolutely secure."

FIGURE 3:

71%

of respondents have widespread security concerns related to moving information and/or applications to the cloud, even though

3 of 4

providers are already using the cloud in some way.

"Moving to the cloud offers a lot of advantages in terms of efficiency, cost and flexibility," said Wirth, "But it does impact your security posture. You have to look at security technology in a new way that gives you visibility into your infrastructure and your data and the way users are interacting with your data in the cloud. It makes security more complicated."

> ***"Security in this day and age is not a point problem anymore; it's an enterprise problem with the potential to affect the bottom line, care delivery and, most critically, patient safety."***
>
> **Axel Wirth** | Distinguished Healthcare Architect, HIMSS Privacy and Security Committee Member | Symantec

Network-connected medical devices represent another challenge. Ninety-five percent of respondents identified multiple obstacles to securing medical devices. A typical hospital may be dealing with hundreds – or even thousands – of different device types from multiple different vendors. Also, the longevity of equipment is a security concern. "Devices may be perfectly sound from a clinical perspective, but not from a security perspective," said Wirth. Most providers have to account for a significant number of insecure medical devices when conducting their security risk analysis. "I've seen hospitals that literally had to turn patients away when medical devices became infected by malware," he said.

Another aspect of the healthcare provider ecosystem that is often overlooked is equipment connected to the hospital network, which is neither IT nor a medical device, but is nonetheless critical to patient care. An example might be temperature controls for a suite of operating rooms. "If I can change the temperature up or down a little bit, I can basically cancel every single appointment in those rooms, because they are no longer in compliance with environmental requirements for the procedures. So even though those systems may appear fairly benign, you can do a lot of damage with them in terms of impacting the business," said Wirth.

Evolving cybersecurity challenges demand new approaches

"The challenge of managing risk in today's complex healthcare environment is an onion problem. You solve for one layer, and then you find there are more challenges below it," said Wirth. That is why every aspect of a provider's approach to cybersecurity — from keeping the board informed to adopting a framework, to budgeting for and managing risk — must be conducted from a business risk perspective.

To that end, many healthcare providers have begun looking at enterprisewide security platforms rather than relying on a collection of incompatible point solutions. Businesswide cyber risks require enterprisewide security solutions.

"All of an organization's security tools need to work together in order to optimize detection across the organization and to minimize the impact of security incidents." All the evidence points to the same conclusion, Wirth said, "Security in this day and age is not a point problem anymore; it's an enterprise problem with the potential to affect the bottom line, care delivery and, most critically, patient safety."

[1] I*T Security and Risk Management Study*, conducted by HIMSS Analytics, on behalf of Symantec, December 2017.
[2] Filkins, B., IT Security Spending Trends: A SANS Survey, Feb. 2016. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[3] 2017 Cost of Data Breach Study: Global Overview, Ponemon Institute, June 2017. Retrieved from https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states

Produced by HIMSS Media | www.himssmedia.com | © 2018