Addressing Healthcare Cybersecurity Strategically

Healthcare organizations are awash with data. However, electronic health records (EHRs) and digital clinical systems in many healthcare organizations have been deployed without strategic data and IT infrastructure security planning. As a result, chief information security officers (CISOs) frequently have limited authority, sparse staffing and tight budgets. Data security spending in healthcare lags behind other top cybercrime targets such as financial services, according to new research by HIMSS Analytics on behalf of Symantec Corporation.

All of this makes healthcare organizations rich targets for cybercriminals. Stolen patient data fetches up to 50 times more than a Social Security or credit card number,[1] because a patient's EHR contains data that can be used for medical or identity theft, or other fraud. As a result, criminal attacks on healthcare information systems have increased 125 percent in the past five years.[2]

"No doctor leaves his car unlocked at the hospital, but we're pretty close to doing that with ePHI (electronic protected health information)," said David Finn, Symantec's health IT officer. Each patient record should be treated as if it were an actual patient. "We would no more send patients to the wrong specialist or give them the wrong diagnosis, yet we leave computers unlocked and use unprotected jump drives," he said.

Adding more security products to an enterprise is not the solution. And managing data security with after-the-fact tactical responses instead of proactive strategies to prevent incidents contributes to the enormous financial consequences of each privacy breach. Banks and retailers face costs of about $215 and $165, respectively, for each lost or stolen record, while healthcare privacy breaches cost businesses as much as $398 per lost or stolen record.[3] CISOs need to guide hospitals, including their leadership, on making the best business decisions given the realities of risk today, according to Finn.

"No doctor leaves his car unlocked at the hospital, but we're pretty close to doing that with ePHI."

David Finn
Health IT Officer
Symantec

The HIMSS Analytics Healthcare IT Security and Risk Management Study of healthcare IT security leaders found:

- Most organizations conduct IT security risk assessments only once a year;
- Many security leaders have only occasional interactions with top-level leadership;
- Medical-device security is only in the planning stages at many organizations.

The survey polled 115 IT and security personnel responsible for data security in hospitals with more than 100 beds. Organization size ranged from standalone hospitals to integrated delivery networks. A subset was selected for in-depth interviews.

Symantec™

Featuring industry research by

HIMSS Analytics®

"The irony is that information technology and data in healthcare are clearly critical to the mission of providing care, yet data security is an afterthought."

Mac McMillan
Chairman
HIMSS Privacy & Security
Policy Task Force

Struggling for resources

Unlike industries such as insurance or banking that rely on personal data, few healthcare organizations allocate more than 6 percent of IT budgets to data security. Half of survey respondents (52 percent) said their organizations allocate between zero and 3 percent of IT budgets to IT security; 28 percent said budgets were between 3 percent and 6 percent (Figure 1).

Staffing is another limitation. Among respondents, 72 percent have five or fewer IT employees allocated to data security, and only 10 percent have 21 or more. Even when employees outside of IT with data security responsibilities are included, the adjusted average total number of employees allocated is 10.[4]

"The lead challenge is talent and acquisition," said one CISO. Competition for talent with other industries puts healthcare at a disadvantage, said another. "The rest of the cybersecurity world is retaining good talent," he said.

"The irony is that information technology and data in healthcare are clearly critical to the mission of providing care, yet data security is an afterthought," said Mac McMillan, chair of the HIMSS Privacy & Security Policy Task Force and CEO of CynergisTek, Inc., an information security and privacy consulting firm. He agreed that recruiting and retaining data security professionals is one of the biggest challenges in healthcare. "We don't have enough of them, and we don't have enough who are qualified to do their job," he said.

Reporting structure and leadership challenges

Organizational structure compounds underfunding and understaffing challenges. In most healthcare entities, CISOs report to the chief information officer (CIO), and in effect, police their bosses. More than 65 percent of data security officers are part of IT departments, and only about 20 percent are independent. Most (69 percent) report collaborative relationships between security and IT.

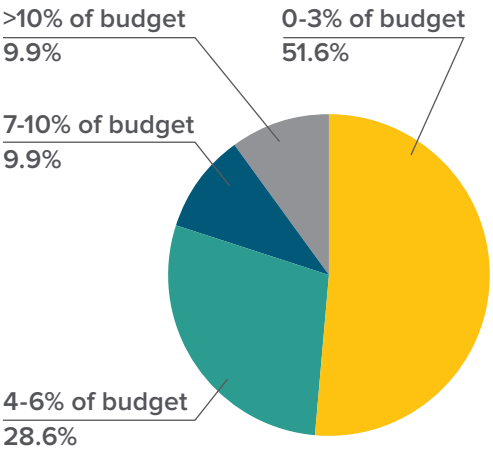
Corporate leadership's attention to data-security strategy is another factor. While 10 percent said data security is on every board of directors meeting agenda, 54 percent said regular schedules for board review don't exist. Furthermore, 8 percent of respondents said that data security reports are "never" on board agendas (Figure 3).

That structure stymies data security. "The technology belongs to IT, but the information belongs to the patient," Finn said. By relegating data security to IT departments, healthcare leaders focus too much on preventing the next breach when they could instead implement better, more reliable systems that yield business advantages.

Compliance is not assurance

Respondents ranked the importance of a cybersecurity strategy for their organizations 4.23 on a 5-point scale. However, only 23 percent of respondents said they have ongoing, consistent risk-management programs, and 44 percent conduct risk

Figure 1 **Less than six percent of budget is allocated to security.**
What percent of your total IT budget (operating and capital) is allocated to IT security?



Out of 91 survey participants responding to this question, only 10 percent spend more than 10 percent of their total budget for security.

"We are dealing with a different threat profile… and a different level of sophistication from three or five years ago."

assessments just once a year. Survey results also showed the National Institute of Standards and Technology (NIST) framework is the most common methodology (57 percent) used for HIPAA assessments.

While frequency of these risk assessments and budgets remains low, the volume of threats keeps growing. CISOs surveyed expressed concerns about their ability to keep up with ever-changing efforts to hack into their networks. "We are dealing with a different threat profile… and a different level of sophistication from three or five years ago," said one respondent. "That has been one of the key drivers of our increased investment in new technologies and employee awareness."

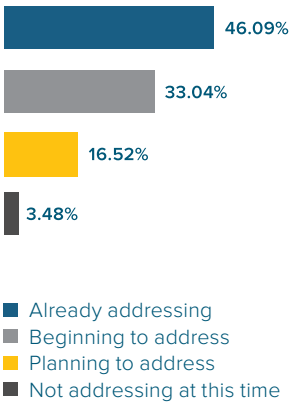
Adding to the challenge, respondents reported only mid-level agreement on the prioritization of data security measures, and the need for remediation and mitigation of incidents ranked higher than having a unified view of controls and vulnerabilities that might prevent incidents from happening.

Medical devices are another concern. Because manufacturers traditionally have not put a focus on incorporating cybersecurity features in their devices, the growing network of connected devices emerges as an attractive cybercrime target.[5] And healthcare organizations are not filling the gap: 50 percent of respondents are only planning and beginning to address medical-device security (Figure 2).

The CISO's evolving role

Protecting data security requires CISOs to gain authority and resources, which can happen when they translate technical risks into business risks and data security plans into business opportunities. "We need to be able to present our findings and our risks in the same context (as other business units), so that when the board looks at our recommendations, they realize that this is something worth investing in," said a CISO of a mid-size healthcare organization.

Figure 2 **IT security most likely not addressed for medical devices**

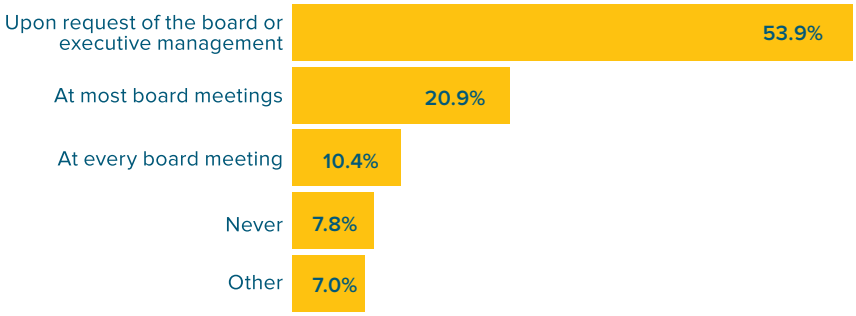


McMillan said CISOs have to be strategic themselves to win support for long-term data security plans. "CISOs have to understand the business, know what the leaders are aiming to accomplish and put together a business plan for security that ties into those business goals," he explained. This is an opportunity for CISOs is to be recognized for more than tactical responses and individual incidents. "We have seen a similar evolution of CIOs over the past 20 years," said Finn. "They aren't the 'IT guy' anymore."

Partnerships between CISOs and CIOs help make the business case, a respondent noted. "It is absolutely critical that the CISO and CIO work together to understand how technology is used, the strategy of technology in the organization and how technology is spread across the organization," said the CISO of a large children's hospital, adding that the CISO is "the partner to help (the CIO) do things in the least-risky manner."

"It is absolutely critical that the CISO and CIO work together to understand how technology is used."

Figure 3 **Security's seat in the board room.**
How often is security (plan, metrics, status, incidents) discussed at board meetings?



Continuous vigilance required

Finn emphasized that organizations need to stop relying on annual HIPAA compliance risk assessments as measures of data security. "The measure should be: Are we making the best, rational decisions (business and clinical) given the risks we face? And that has to be asked every time there is a change in the system — people, process or technology."

McMillan said healthcare organizations should scan their external IT environment quarterly and internal environment twice a year, but periodic risk assessments are secondary to continuous monitoring of user IDs, firewall logs, software patches and other points where risks can be spotted. "Those active risk-management practices that go on day-in and day-out are the things that need to be solid, so that CISOs can stay ahead of threats," he said.

Once organizations deploy base security controls and comply with key mandates such as HIPAA and HITECH, they can let their risk assessments drive priorities and business priorities drive the security strategy. By developing a sustainable risk-management program, CIOs and CISOs can help their organizations shift their security mindset from tactical and reactive to strategic, robust and long term.

That culture change is critical. "Healthcare is a very open, caring and trusting business," which makes some people in healthcare organizations less receptive to addressing data security, said McMillan. "They don't understand that you cannot have privacy without good data security," he said. Finn concurred, adding, "Privacy and security have to be part of the system. You cannot do it after the fact. It's never as effective and it costs more to do it that way."