# Operationalizing Cybersecurity in Healthcare Organizations

2017 IT Security & Risk Management Study

Symantec

HIMSS Analytics

*"Many healthcare organizations continue to view cybersecurity as an IT problem, rather than as a business risk management issue."*

**David Finn**
Health IT Officer
Symantec


# Cybersecurity in healthcare is improving, but not fast enough

Healthcare organizations continue to make headlines as the target of cyberattacks, ransomware threats and the source of large data breaches. In fact, the healthcare industry now holds the unwelcome distinction of being the most cyberattacked industry, ahead of manufacturing, financial services, the government and transportation.[1]

In spite of this, many in the industry continue to view cybersecurity as simply a HIPAA compliance issue. HIMSS Analytics recently conducted research that drove this point home. One hundred C-suite, business, IT and clinical leaders participated in HIMSS Analytics' recent survey, "Healthcare IT Security & Risk Management," conducted on behalf of Symantec.

The survey data showed healthcare organizations are incrementally increasing governance, staffing and budgetary resources dedicated to cybersecurity. However, "many healthcare organizations continue to view cybersecurity as an information technology (IT) problem, rather than as a business risk management issue," said David Finn, health IT officer at Symantec.

This narrow view of cybersecurity can blind an organization to the larger risks that cyberattacks pose. "Progressive healthcare organizations are starting to view cybersecurity as a patient safety and quality-of-care issue," said Bob Chaput, chief executive officer of Clearwater Compliance.

"The HIMSS Analytics research showed that most organizations continue to treat cybersecurity on a tactical level and merely as a technical matter," Chaput said. "There is a lot of 'spot welding' going on, as opposed to taking a more architectural approach and treating cybersecurity as an organization-wide risk management issue." Finn and Chaput agree that healthcare organizations need to operationalize their cybersecurity strategies across the enterprise in order to defend themselves from increasing numbers and types of cybersecurity attacks.



[1] Morgan, S. (2016, May 13). Top 5 industries at risk of cyber-attacks. *Forbes*. Retrieved from: http://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#55ef62753954

*"People used to think cybersecurity was an IT issue. But now we are trying to cast cybersecurity in the same light we cast things like patient safety: everybody is responsible for this."*

**Survey Respondent**
CIO

# Who owns cybersecurity in the organization?

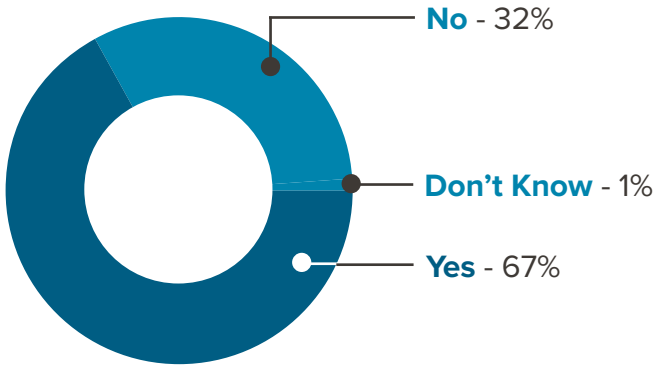
The cybersecurity leadership structure offers a clue as to whether or not cybersecurity has been operationalized. A majority (67 percent) of the survey respondents indicated their organization had a dedicated/full-time chief information security officer (CISO) (Figure 1).

It's good news that two-thirds of survey respondents represent organizations that take cybersecurity seriously enough to allocate dedicated leadership. On the other hand, said Finn, "The fact that nearly one-third of respondents still don't have a dedicated security officer — more than ten years after the security rule for HIPAA went into effect — is not a good reflection on the industry."

Although there is a need for CISOs in healthcare, the mere existence of a CISO is not enough. Reporting structure can impact the CISO's effectiveness. Sixty-six percent of respondents indicated the senior security officer reports to the chief information officer (CIO), a set-up with built-in conflicts. "The CIO's job is to keep the business up and running. The security officer's job is to make sure the business is secure; operations are therefore secondary to the CISO. If the CISO reports to the CIO, there are going to be conflicts. Organizations have to be aware of that and manage it," said Finn.

Regardless of whether leadership rests with the CISO, the CIO, or another position, healthcare organizations understand that ownership for cybersecurity risk is shared across the institution. As one survey respondent, the CIO of a 500-plus bed facility, said, "People used to think cybersecurity was an IT issue. But now we are trying to cast cybersecurity in the same light we cast things like patient safety: everybody is responsible for this."

**Figure 1.**
Only 2/3 of responding organizations have a dedicated CISO role.
*Does your organization have a dedicated/full-time Chief Information Security Officer?*



*"When you treat cybersecurity as a risk management issue, as opposed to a security operations issue, there are different sets of skills and knowledge and experiences that you need to apply."*

**Bob Chaput**
Chief Executive Officer
Clearwater Compliance

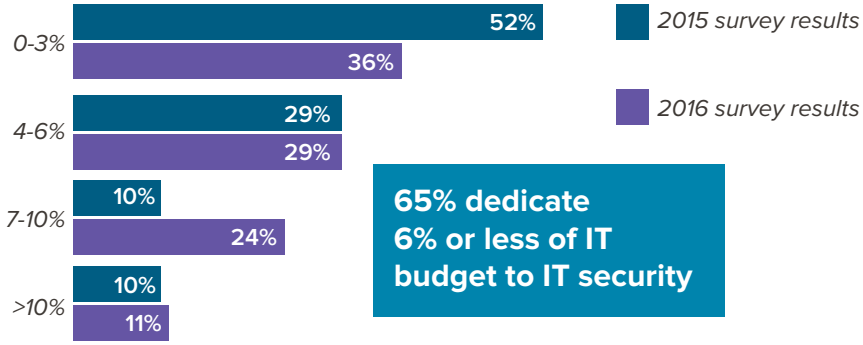
# Budgeting and staffing for cybersecurity

The survey data shows some improvement over the 2015 survey findings in budgeting and staffing for security, "but there is still a lot of room to grow," said Finn. Sixty-five percent of survey respondents indicated their organization allocated 6 percent or less of their IT budget to IT security (Figure 2). "I would contrast that to other highly regulated industries like government, or finance, where we see between 12 and 15 percent of the IT budget allocated to security," he added. "Until the industry understands that security is the business of healthcare today, we are not going to see an increase in that number."

The survey data also showed that operating expenses are increasing as a part of the IT security budget, while capital expenditures are decreasing. Finn noted that this is not surprising, as more and more organizations are relying on outside sources to assist in managing cybersecurity risks. "There are very few healthcare organizations that could actually build their own security operations center and staff it 24/7 by 365," Finn said.

Staffing related to security is one of the areas in which healthcare organizations saw increases over last year. What is less clear, is whether or not the right type of staffing choices are being made. "Are organizations hiring savvy, cybersecurity leaders with risk management experience?" asked Chaput. "Often organizations throw resources at security operations rather than risk management, which is like throwing resources at accounting rather than financial analysis. When you treat cybersecurity as a risk management issue, as opposed to a security operations issue, there are different sets of skills and knowledge and experiences that you need to apply."

**Figure 2.**
IT security budgets have increased since 2015 but still tend to be 6% or less of the IT budget.
*What percent of your total IT budget is allocated to IT security?*



*"That's really what security in the provider setting is: it's about taking care of your patients."*

**David Finn**

# Drivers for cybersecurity investment

The HIMSS Analytics survey identified risk assessment and HIPAA compliance as the top drivers for cybersecurity investments. Survey respondents' perspectives on which of these drivers were most important varied by the respondent's role in the organization. Business respondents were more likely to cite risk assessment as the primary driver, whereas clinical and IT respondents were more likely to cite HIPAA compliance as the primary driver (Figure 3).

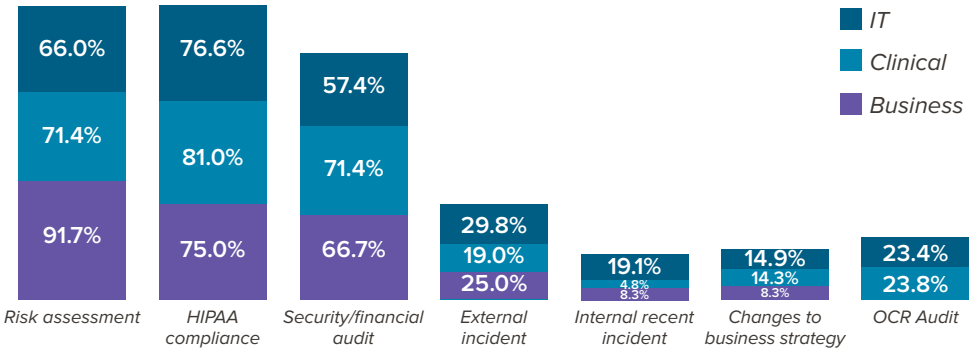
As drivers for cybersecurity investment, security and compliance are related, but not synonymous. "Many organizations believe, 'If we are compliant, we are going to be secure' or 'if we are secure, we are going to be compliant,'" said Chaput. "It's not true. You can be very secure, but not compliant, and vice versa. Organizations need to think about how compliance and security are inextricably linked, and then evolve their thinking to appreciate the significant differences."

Several survey respondents said the increasing reach of digitization and internet connectivity across the organization has contributed to an increased awareness of the need for cybersecurity investments. One survey respondent, the CMIO of a health system with 600-plus beds across multiple facilities, said, "I think there's a realization on the part of the Board, the CEO and our operating folks that the more dependent you are on electronic and internet-connected systems, the less you can afford to be shut down for any period of time due to external threats."

Finn believes that the view of cybersecurity as a business risk issue goes hand-in-hand with the understanding that weaknesses in an organization's cybersecurity strategy can impact patients. "That's really what security in the provider setting is: it's about taking care of your patients," said Finn.

**Figure 3.**
Business respondents more likely to cite risk assessment as driver; clinical and IT respondents more likely to cite HIPAA compliance as driver

*What is driving your decisions on where investments are being made in IT security? Total % choosing in top 3*



*"You have to have a cybersecurity framework to measure yourself against what actions need to be performed and an information risk management process to guide how to assess and monitor your risk posture on a day-to-day basis."*

**Bob Chaput**

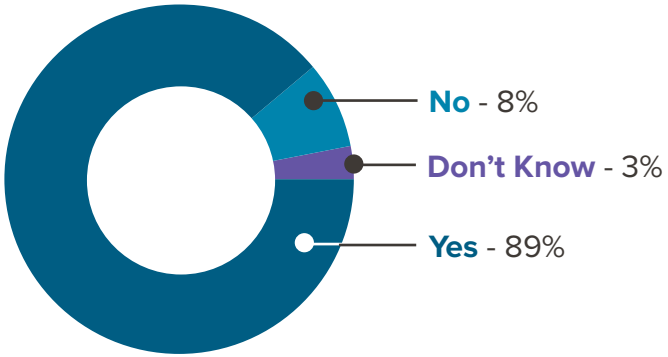
# Governance, framework and scope

In the areas of governance, framework and scope, the survey results gave mixed messages. Eighty-nine percent of respondents said cybersecurity is part of their organization's enterprise risk management strategy or Governance, Risk and Compliance (GRC) program (Figure 4). However, in response to a separate question, only 34 percent of respondents said a standing security report is presented at each board meeting. "There is definitely a disconnect there," Finn said. "But I think it shows we are seeing the beginning of understanding in the healthcare space of what GRC really is in relation to cybersecurity."

With respect to HIPAA-based security frameworks, 46 percent of respondents adhere to the National Institute of Standards and Technology (NIST) cybersecurity framework, while 30 percent of respondents use the HITRUST Common Security Framework (CSF). Finn and Chaput agree that while adopting a framework is important, it is how you use it that makes the difference. "You have to have a cybersecurity framework to measure yourself against what actions need to be performed and an information risk management process to guide how to assess and monitor your risk posture on a day-to-day basis," said Chaput, "but really, at the end of the day, it comes down to how you use the framework and the process."

Survey respondents were asked about security initiatives related to mobile devices, medical devices, and non-IT managed (shadow IT) information technology. Most respondents stated they were addressing these issues. But simply implementing a mobile device initiative, or a medical device initiative, is not sufficient because new cyberattack surfaces continue to emerge. "The list of cyberattack surfaces is going to be different next year and the year after that," said Chaput. "That is why it is important to take a risk management posture that transcends specific media types and devices."

**Figure 4.**
Majority address cybersecurity in enterprise risk management strategy or governance, risk, compliance (GRC) program.



*"The clinician may not think about the fact that a syringe pump can be an attack vector, because it is the easiest way to get onto the hospital's network."*

**David Finn**

# How prepared is your healthcare organization?

Preparedness for cyberattacks extends beyond having the right leadership, budget, staff, framework and governance in place. One critical aspect of an effective enterprise-wide cybersecurity strategy is a commitment to enhancing cyberawareness, education and training across the organization.

"Everyone in the organization understands there are risks, but the clinical and business people tend to be a little more confident on their organization's ability to fend off an attack because they don't understand the scope of those risks," said Finn. "The clinician may not think about the fact that a syringe pump can be an attack vector, because it is the easiest way to get onto the hospital's network."

In fact, clinicians were more likely than either business or IT survey respondents to identify employee awareness and training, or lack there of, as a significant barrier to achieving a higher level of confidence in their security program (Figure 5). The CMIO of one institution pointed out, "The end-user education is important because that's often the initial point of failure, where somebody gets through and then gets to deeper information." A number of the survey respondents said they periodically send out phishing emails to staff to see who bites, and then use that as an opportunity for further education and training.

One CISO stated, "I think the human training is the most important element. If I had to make a choice about the one thing to spend money on, it would be about getting the word out, talking to people and training people about the risks."

Finn noted that survey respondents' awareness of education and training as an issue demonstrates "we're actually getting a more enlightened view of security and understanding that it's training and processes and policies and people-oriented matters — not just hardware and software."

**Figure 5.**
Business and clinical respondents more confident in organization's preparedness for cyberattacks
*How confident are you in your organization's preparedness for cyberattacks?*
*Please use a scale of 1 to 7 with 1 being no confidence at all and 7 being very confident*
*Average rating*

*"If organizations continue to ignore the strategic importance of information risk management, we are going to continue to see an upsurge in breaches, an increase in failed audits and additional successful cyberattacks."*

**Bob Chaput**


# Moving toward strategic preparedness for cyberattacks

Healthcare organizations are beginning to understand cybersecurity is more than just an IT problem. Cyberattacks threaten an organization's reputation and brand; lead to financial consequences including fines, penalties and settlements; put regulatory compliance at risk; and affect operations, even to the extent of impacting quality of care and patient safety.

"We need to think about information risk management (IRM) as part of the organization's overall enterprise risk management and governance/risk/compliance (GRC) programs," Chaput advised. "If organizations continue to ignore the strategic importance of information risk management, we are going to continue to see an upsurge in breaches, an increase in failed audits and additional successful cyberattacks. Ultimately, these things are going to limit the ability of an organization to grow."

That's why it is so important to assess your risk before something bad happens. "If you can only do one thing, conduct a comprehensive risk analysis," said Chaput. "If you do it properly, you'll be going to the head of the class. Office for Civil Right (OCR) data shows over and over again that nine out of 10 organizations either audited or investigated by OCR are failing to do this very basic, fundamental requirement of any good cybersecurity program."

The bigger picture, however, is that healthcare organizations must understand, "these are not just IT or security risks – they are business risks and have the potential to slow down, or shut down, patient care," said Finn. "IT and security leaders cannot fix those problems, even from a cyber perspective, without the entire organization getting behind that initiative financially, staffing-wise, from a control perspective, and certainly not without training, education and awareness for everyone."

**To learn more about how your organization can operationalize cybersecurity, visit www.symantec.com/healthcare.**

Symantec

**About Symantec:**
Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, is defining the future of cybersecurity by solving the industry's toughest challenges of securing mobile workforces, protecting the cloud, and stopping advanced threats. Organizations around the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Symantec operates the world's largest civilian cyber intelligence network, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.