FUTURE PROOFING HEALTHCARE:

The State of Healthcare Provider Cybersecurity 2017: Is Your Organization Keeping Pace with the Threat?

Cyberattacks have come fast and furious in healthcare in recent times. And, these assaults are expected to become even more frequent and sophisticated in the days ahead. In fact, 96 percent of healthcare IT professionals predict that ransomware/malware attacks will increase in the next two years, according to *Future Proofing Healthcare: Cybersecurity*, a survey of 101 healthcare IT professionals conducted by HIMSS Analytics and sponsored by Commvault.

Indeed, ransomware over the last three years has become a "big business" as cyberattackers have moved on from simply stealing data to encrypting it and forcing organizations to pay for it. And, it looks as if the attacks are poised to get even worse as cybercriminals "are going to look for opportunities to mess with the integrity of patient data by changing a couple of fields and not telling you which ones," said an IT security officer from a 500-plus-bed organization who participated in the study.

As threats escalate, healthcare organizations are mounting increasingly sophisticated defenses and investing more money and resources to combat the danger. But there's still that pit-in-the-bottom-of-the-organizational stomach, as leaders wonder if they are doing what it takes to protect their organizations in these perilous times. Insights from the study, which surveyed professionals at large- (500-plus beds), intermediate- (101 to 500 beds) and small- (100 beds or fewer) sized provider organizations across the country, illustrate just how far the industry has come and where it needs to go next to protect itself from cyberthreats. Perhaps more importantly, the study's results can help your organization assess its progress in comparison to other providers – giving you a better idea of how to identify and address the chinks in your armor.

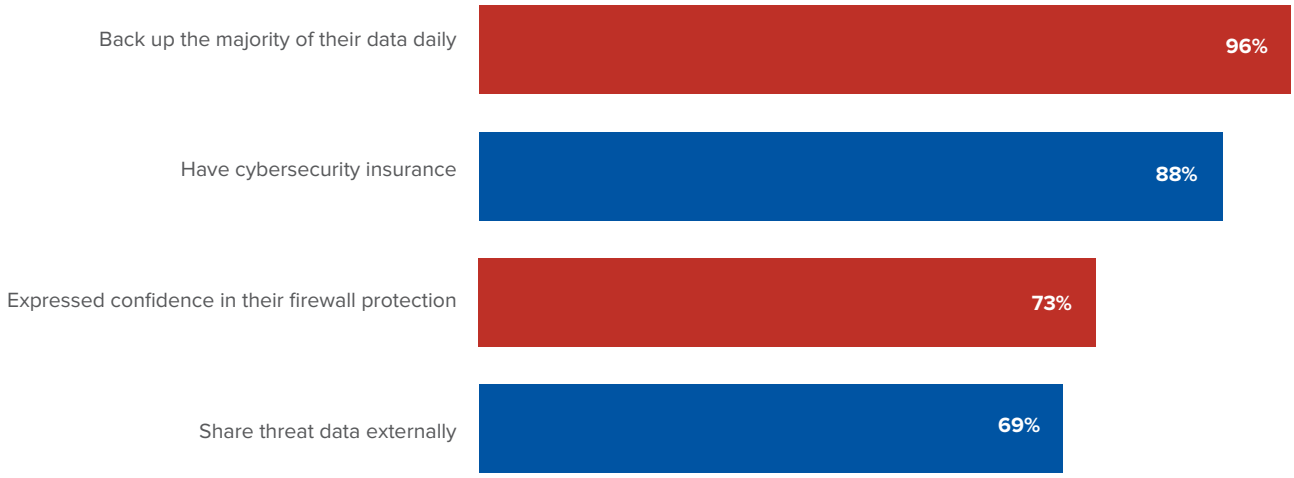
How far we've come

The survey shows that healthcare organizations have bulked up their cybersecurity defenses considerably, as 96 percent back up the majority of their data daily; 88 percent of respondents have cybersecurity insurance; 73 percent express confidence in their firewall protection; and 69 percent share threat data externally (Figure 1).

Produced in partnership with HIMSS Media

Produced in partnership with HIMSS Analytics

Figure 1. Organizations are taking measures to bolster their cybersecurity defenses.
Respondents stated that their organizations:



Yet, despite all this progress, less than half of healthcare IT professionals (48 percent) feel confident in their organizations' overall security levels. "To be honest, [healthcare organizations should] never feel totally comfortable with cybersecurity, because it's so dynamic and it's so complex. Things change very quickly and we have to be on top of that. Trying to make sure that our patients' data is safe and secure, and that we give our clinicians access to what they need to access to take care of people is really a big challenge," said a CIO from a large provider organization.

While healthcare organizations have progressed, security programs are still in their infancy. "Security, privacy and compliance models need to be much more holistic. They've got to go end-to-end, and those types of approaches right now are still lacking," said Hector Rodriguez, Microsoft's worldwide health chief information security officer.

Indeed, healthcare IT professionals are aware of a variety of shortcomings in their cybersecurity initiatives. Perhaps most perplexing is the fact that just 37 percent of the health IT professionals surveyed felt their organizations were using both cutting-edge technology and best training practices. Bringing technologies into the mix weighs even more heavily on smaller facilities, as 26 percent of small providers indicated that they follow best practices but lack adequate technology, compared to just 18 percent of intermediate organizations and 12 percent or large providers.

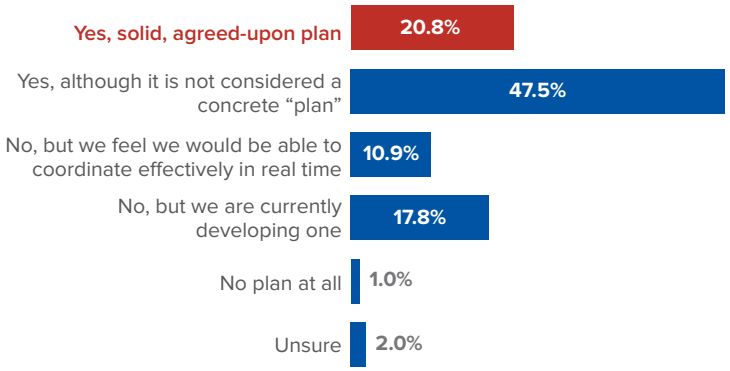
The gap, unfortunately, is not one that can be glossed over. Organizations must unequivocally "use both best practices and technology to be fully prepared," according to Ananth Balasubramanian, general manager at Commvault.

In fact, Mike Feld, acting CTO at Temple University Health System, contends that healthcare organizations should strive to coordinate their education and technology efforts. "When you look at a particular event such as malware being delivered through email, you have to teach employees that this is what a suspicious email looks like, and you have to educate them to eliminate the behavior that would lead them to clicking on the dangerous malware. At the same time, organizations need to then 'layer in' the appropriate technology, so they can say to employees, 'You have to pay attention to your email, but we're going to do our best to eliminate certain components and likely types of email that you might see,'" Feld explained.

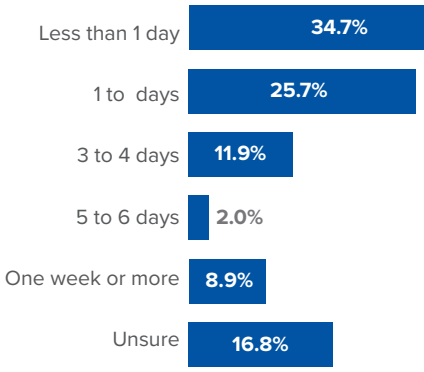
While it is important to simultaneously leverage education and technology to prevent attacks, organizations still need to be ready to recover in the wake of a security incident. Unfortunately, only 21 percent of providers surveyed have an agreed-upon plan for responding to a cybersecurity attack (Figure 2). "This is really disconcerting because it is not a question of *if* you are going to be attacked; it's a question of *when* you are going to be attacked," Balasubramanian warned.

Figure 2. Those with solid agreed-upon response plans can be fully functioning within two days.

Do you have an action plan ready in the event you fall victim to a cyberattack?
Cyberattack defined as: An attempt by hackers to damage or destroy a computer network or system, including but not limited to malware/ransomware.



In the event of your organization is successfully infected by ransomware, how quickly would your organization be able to be fully functioning again?



Of the respondents who have a solid agreed-upon plan
- 2/3's indicate their organization would be fully functioning in **less than a day**
- 90% indicate they would be up **within 2 days**

The fact that only 32 percent of organizations are backing up their data more than once daily and only 35 percent of IT professionals believed their organizations could recover within one day of an attack adds to the worry, according to Michael Leonard, senior director, healthcare product management at Commvault. "If you are only backing up your data once a day, that's not good enough. You want to be backing up your data as often as is practical for that particular application stack or that particular user base because the frequency of backup affects the time it takes to recover. Recovery point objective and recovery time objective are two key metrics that every organization should keep its eyes on," Leonard advised.

Moving forward

The good news is that healthcare organizations are bolstering their security efforts. In fact, the number of healthcare organizations dedicating more than 10 percent of overall IT budgets to cybersecurity has increased 139 percent over the past three years, according to the survey.

With more money earmarked for security, organizations are looking to increase employee awareness and training, as this bubbled to the top of the priority list with 64 percent of respondents citing it among their top three priorities for the next two years (Figure 3).

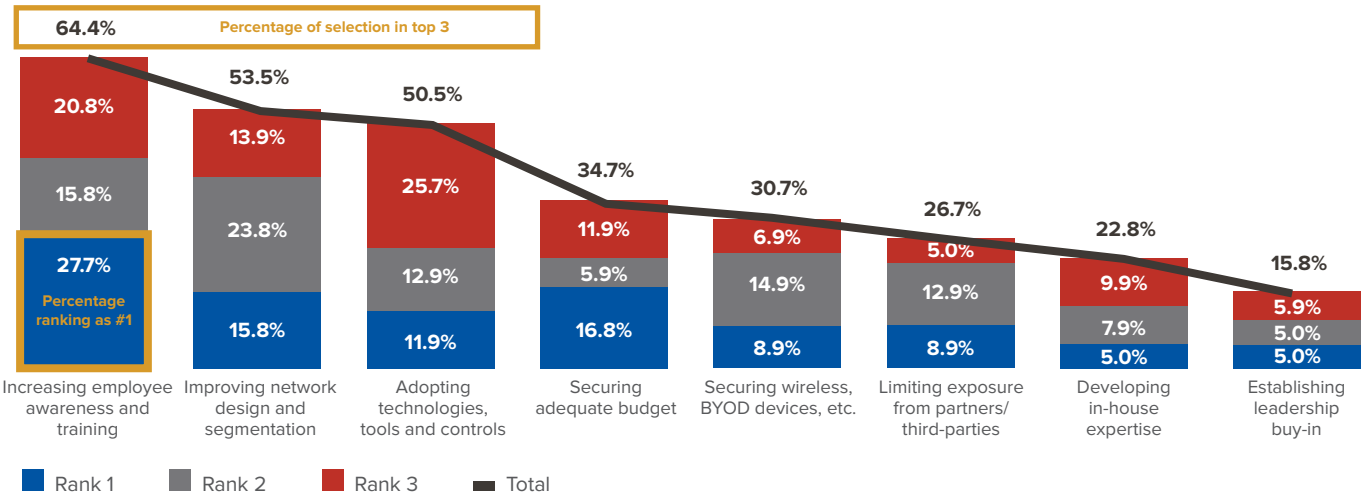
This training, however, must be done right, according to Balasubramanian. "Many times, organizations have training programs that happen once in a while or training that is performed remotely. The problem is that the learning doesn't really stick. The training needs to be done in person, in a classroom setting where people can understand from a live person that there may be a threat," he said. "The training programs need to incorporate the impact of what happens when you click on a phishing link or what happens when you click on a ransomware link because just telling people, 'don't click on links' is not really going to work."

In addition to raising awareness, organizations are looking to improve network design and segmentation (54 percent identified as a top three priority), and adopt technologies, tools and controls (51 percent). At the same time, using the cloud for backup and disaster recovery is becoming an increasingly popular option. Indeed, 60 percent of respondents in the *Future Proofing* survey, conducted in September 2017, cited using the cloud for these purposes, compared to just 38 percent of the healthcare professionals who participated in the *Essentials Brief: 2017 Cloud Study*, which was conducted by HIMSS Analytics in January of 2017.[1]

As organizations adopt new solutions, though, the importance of working with the right vendor cannot be underestimated. More specifically, the survey showed that organizations are looking for vendors who can respond to an evolving threat landscape (rated as very important or important by 95 percent of respondents) and vendors that demonstrate subject matter expertise (71 percent).

"Healthcare organizations need to look for vendors and partners who've done their homework, who understand what it truly means to be a covered entity, a healthcare provider, and the rules and regulations by which they must abide," Microsoft's Rodriquez said. "That means

Figure 3. Increasing employee awareness and training is the top cybersecurity priority for organizations.
Over the next 2 years, what do you expect will be the top cybersecurity priorities at your organization? Please rank the top 3 priorities 1 to 3 with 1 being the largest priority and 3 being the third largest priority.



working with vendors who have a focus on the industry. If the vendor doesn't truly understand the rules and regulations, it puts the onus back on the healthcare organizations to figure out the security, privacy and compliance capabilities of that solution."

While 61 percent of respondents also rated initial cost as very important, it should not be the determining factor. "The last thing we always look at in terms of a vendor, whether it's cybersecurity or anything else, is cost, said a CIO from a 500-plus-bed organization. "We look at cost maybe as a differentiator, but for the most part, if a vendor can do what we need it to do based on our functional requirements, then that overrides pretty much anything else."

Indeed, making sure that sophisticated cybersecurity defenses and recovery plans are in place is likely to loom as a top concern as organizations look to keep their data safe in the years ahead. With such technologies and plans in place, healthcare organizations can keep pace with the evolving threat landscape, prevent many attacks and, just as importantly, recover from those that penetrate. As such, leaders could be in the position to take it all in stride just as this well-prepared CIO has: "We've had 20 incidents where we have had to recover files that were encrypted. Many of those were ransomware, where they get the little box and say, 'Pay your 200 bucks' or whatever. But luckily for us, we haven't had a need even to consider [paying]; we just clean the machine … identify what [the ransomware] is … and then we just recover the encrypted files from a backup."

[1] *HIMSS Analytics*. 2017 Essentials Brief: Cloud. February 8, 2017.