Forbes insights

The Healthcare Industry Seeks Cybersecurity Remedies

In association with

vmware®

Across the healthcare industry, medical diagnoses, patient care, and back-office administration are being digitized—driven by both the need for greater efficiency in a highly inefficient patchwork of systems as well as government mandates. With a range of other digital initiatives occurring on many levels, from intelligent devices and monitors to telemedicine, new vistas are opening for healthcare, providing physicians and caregivers real-time access to patient data and appropriate therapies, as well as connecting patients directly to clinicians and organizations. Ultimately, digital transformation will lead to improved patient outcomes—a top priority for every healthcare organization.

The rise of digital healthcare makes cybersecurity even more critical, particularly with the strict regulations intended to protect patient privacy. Healthcare systems and capabilities are expanding rapidly, which means larger attack surfaces that need protection. Central IT systems need to be secure, along with an expanding network of medical devices and end-user services. Hardware also needs to be secured along with highly sensitive patient data.

Vulnerabilities to cybersecurity attacks have been on the rise at healthcare organizations, according to Richard Temple, vice president and chief information security officer for the Deborah Heart and Lung Center, which is based in Browns Mills, New Jersey. The threat of attacks has increased since "the value of a stolen medical record is so much greater than the value of, say, a credit card number or a Social Security number. A stolen medical record contains so many unique data points that comprise an individual's identity, and, at its worst, could allow an imposter to impersonate someone in order to get medical care at no cost and distort the rightful owner's medical history by having the imposter's history commingled."

Chris Gutmann, system director of information technology for clinical engineering at Yale New Haven Health, agrees that the greatest cybersecurity threat in healthcare is access to patient and employee information. "For verification of billing, a patient's record contains highly sensitive information, making health systems high-value targets for cyberthieves. The unique challenges to healthcare are the nature and volume of implantable devices in patients, and the never-ending need for real-time data to maintain patients' healing journeys."

To better understand how organizations are approaching cybersecurity, Forbes Insights surveyed 1,001 security practitioners and security executives, in partnership with VMware. Data from this survey, which covers a range of industries, is presented in our report "Cybersecurity Trailblazers Make Security Intrinsic To Their Business," which also outlines how organizations can improve their enterprises' security posture.

This brief details the findings among the 150 healthcare respondents. Where appropriate, healthcare results are contrasted with the overall sample.

The average annualized cost of cybercrime to healthcare organizations is estimated at $12.5 million.[1]

[1] "Cost of Cyber Crime Study," Accenture, June 26, 2018.

The Situation

For healthcare organizations, digital transformation has become the norm. A majority of healthcare executives say infrastructure, security controls and applications have significantly evolved as digital technologies have taken root. Most report their security controls have been keeping pace with their digital controls (Figure 1).

The urgency of cybersecurity in healthcare organizations has not fully engaged business leaders in this sector. Healthcare security leaders say major stakeholders are less aligned with their security strategy than other industries. Overall, approximately two out of three respondents say their business leaders are intimately involved in their organization's security processes. However, this shows that one in three have yet to be engaged. Across other industries, more than seven in 10 report close alignment (Figure 2).

FIGURE 1

Healthcare Enterprise Areas Seeing Transformational Change

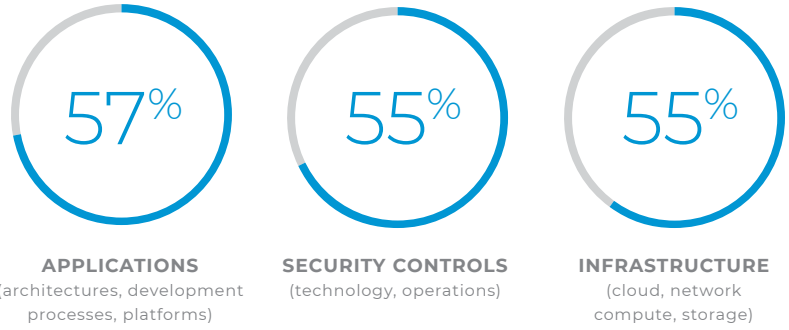
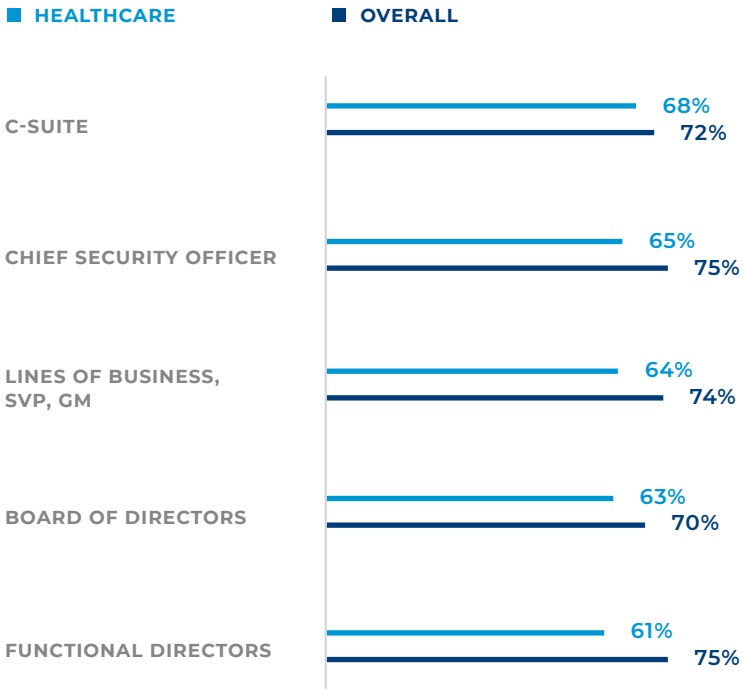


FIGURE 2

Stakeholder Alignment In Security Strategies

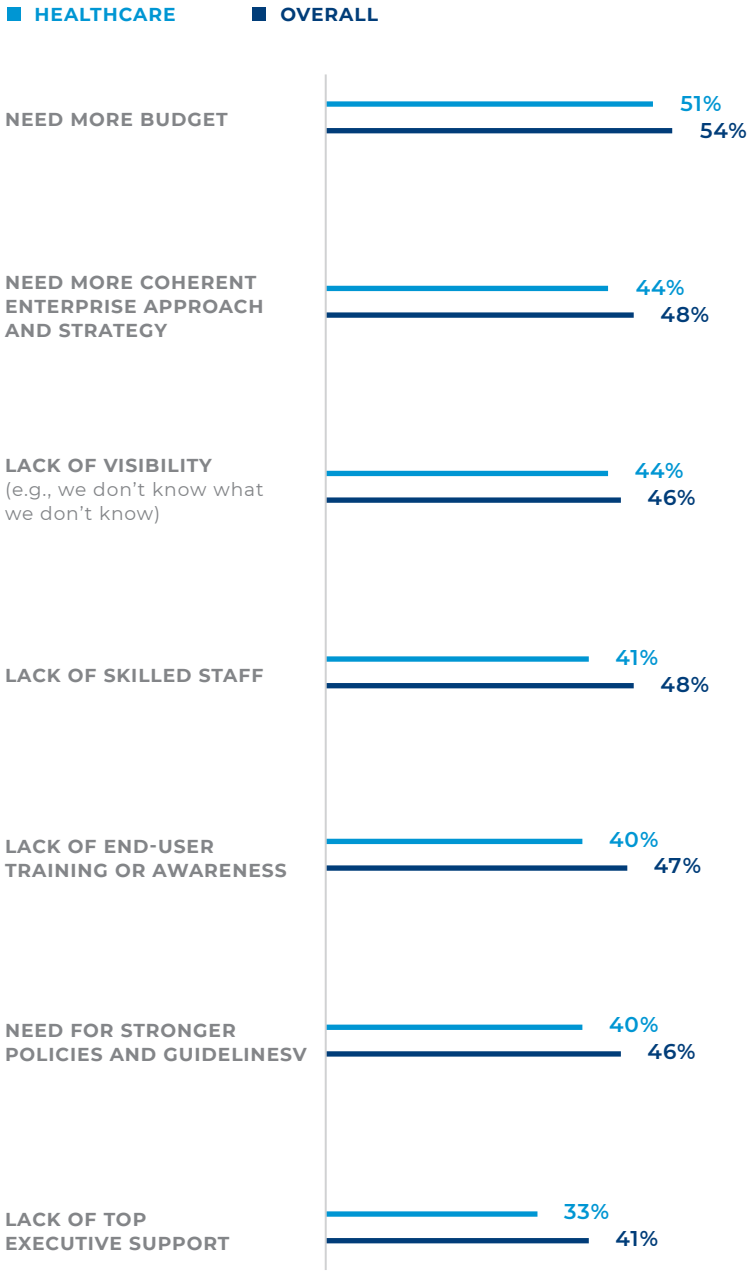


The challenges faced by healthcare security professionals are both organizational and technical. The greatest organizational challenge is budgetary—more than half indicate they face budget headwinds in their efforts to secure solutions and resources to ensure security (Figure 3).

FIGURE 3

Healthcare Cybersecurity Organizational Pain Points

(Represents/highly represents)



The proliferation of systems and end-user devices presents the greatest technical challenge (Figure 4). Interestingly, healthcare respondents are less sensitive to many of the issues that other industries face. For example, healthcare executives are less concerned with the proliferation and viability of their installed security products—39% cite the number of products as an issue, versus 45% overall. In addition, while 38% see their security tools as outdated, this is less than the overall sample (43%).

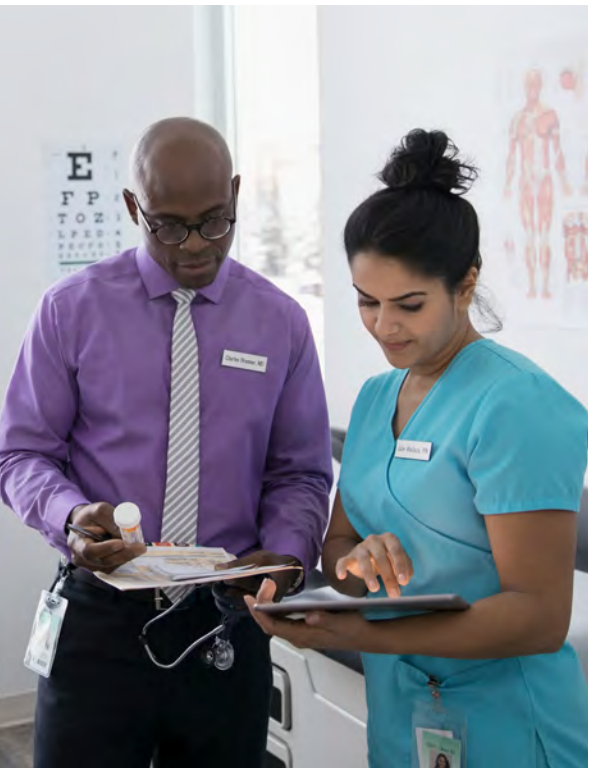
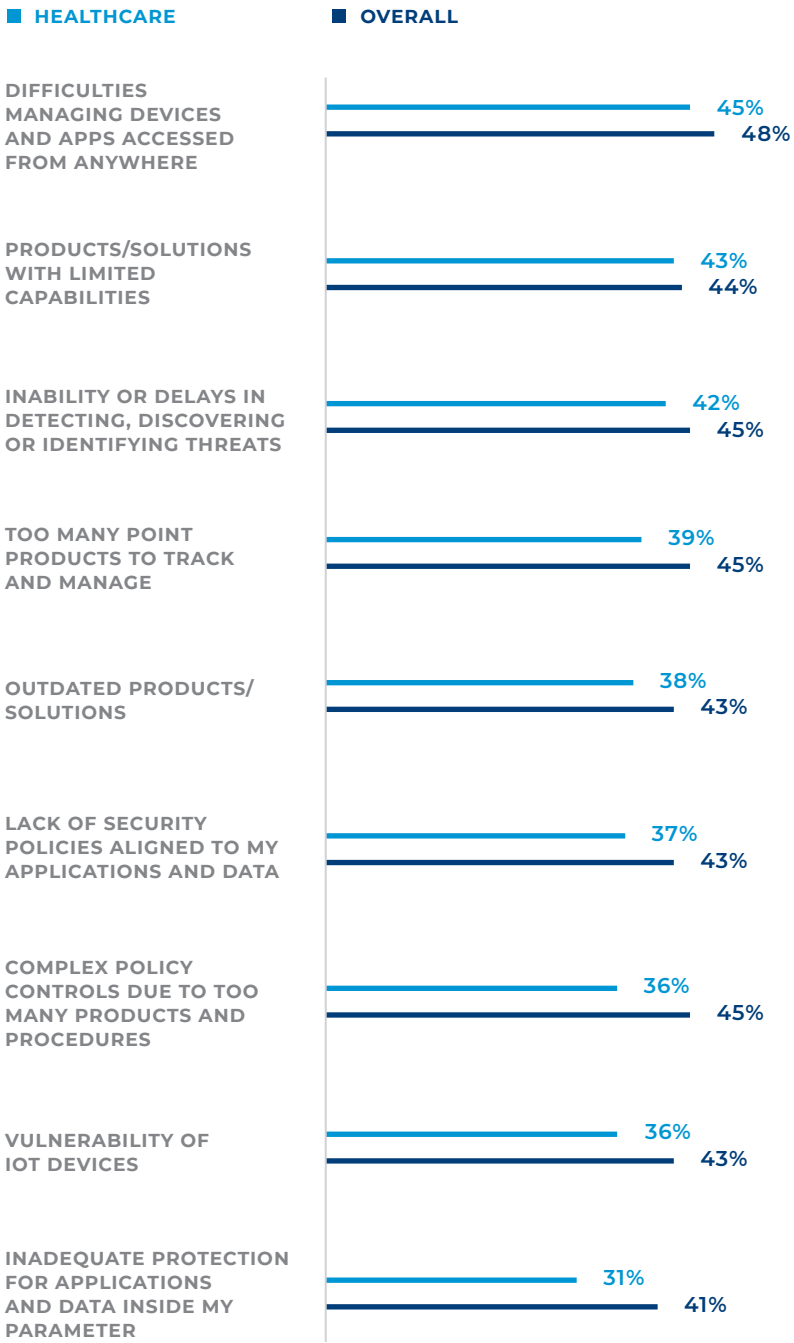


FIGURE 4

Healthcare Cybersecurity Technology Pain Points

(Represents/highly represents)



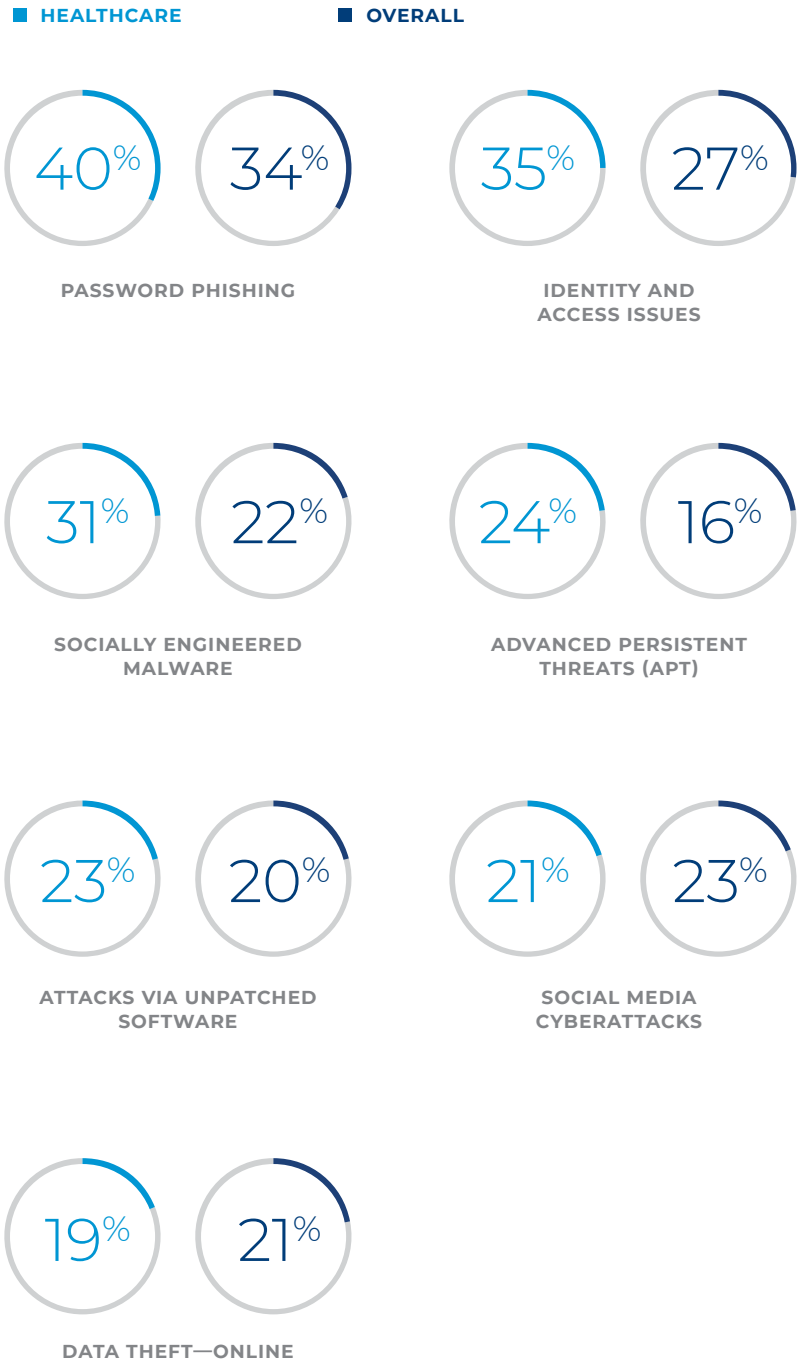
Healthcare respondents report seeing a greater number of incidents or intrusions than their counterparts in other industries, the survey shows. Two in five, 40%, say they have experienced attacks as a result of password phishing among their end-users, versus 34% overall. Another 35% of healthcare executives report having identity and access issues, versus 27% overall. In addition, socially engineered malware attacks have been more widely reported among healthcare organizations, versus only 22% overall (Figure 5).

"There really are many different vectors through which bad actors can infiltrate hospital systems," Temple says. "There is the potential for brute force hacking into the hospital's network, accessing IoT devices such as security cameras, medical devices like X-ray machines, and many others. But the biggest vulnerability point is end-users who are not attentive."

Healthcare organizations see more incidents and attacks than other industries.

FIGURE 5

Top Incidents Experienced Over The Past Three Years



> “There really are many different vectors through which bad actors can infiltrate hospital systems. There is the potential for brute force hacking into the hospital’s network, accessing IoT devices such as security cameras, medical devices like X-ray machines, and many others. But the biggest vulnerability point is end-users who are not attentive.”

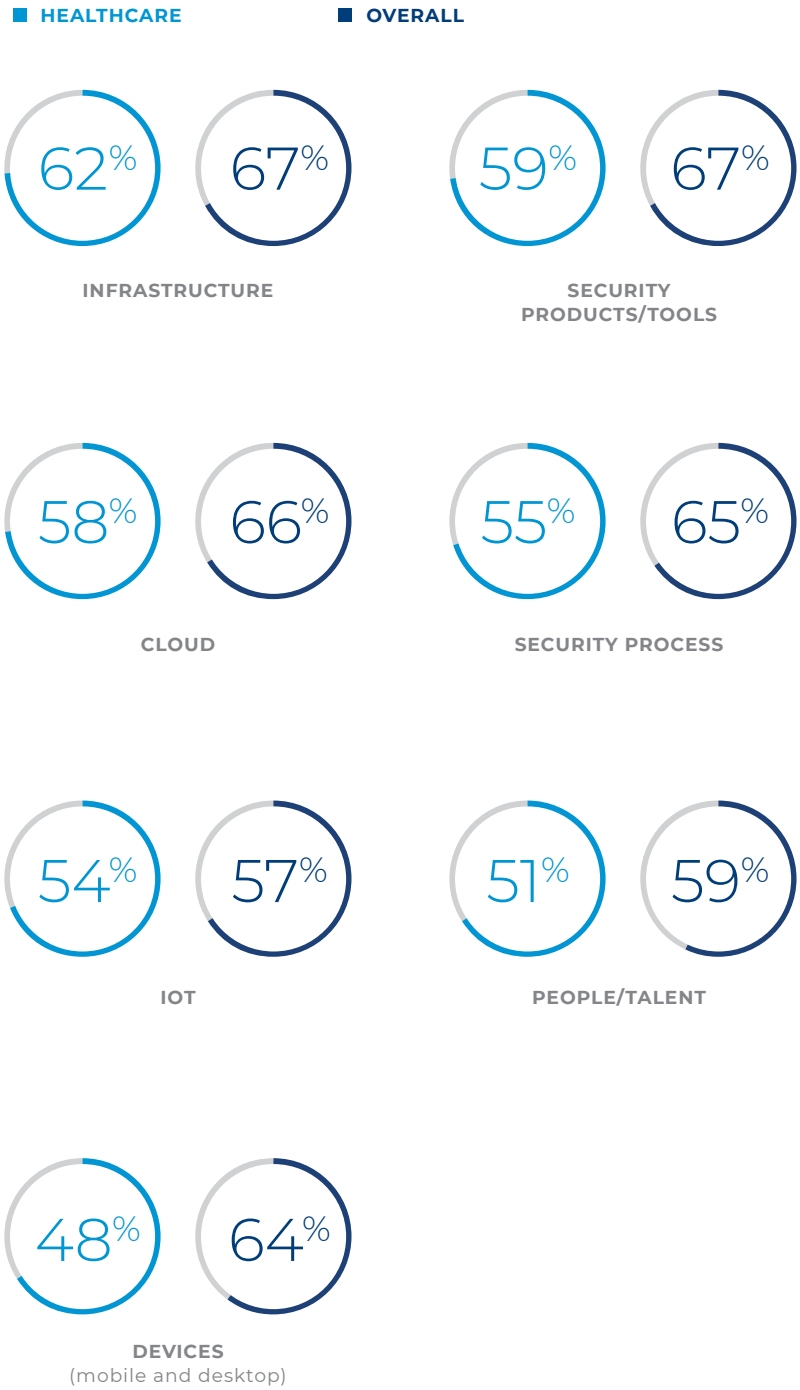
Richard Temple,
Vice President and Chief Information Security Officer,
Deborah Heart and Lung Center

For security executives and practitioners in healthcare, there is a long road ahead. Government regulations demand strict privacy and accountability, mandating security processes be woven into every application and data store. At the same time, very diverse sets of end-users need to be accommodated and educated to achieve alignment and encourage security best practices.

Tellingly, healthcare leaders express less confidence than their peers in other industries that they are prepared to address emerging security challenges. Respondents in the healthcare sector indicate high levels of confidence in their infrastructure—yet this lags the overall cross-industry survey group (Figure 6).

FIGURE 6

Confidence In Addressing Emerging Security Challenges



The Technology

It's key to bake security into technology stack design, development and deployment from the start, but most industries have yet to adopt this approach in a complete and comprehensive way. The healthcare sector lags severely behind—only 9% of healthcare organizations fully involve their security organizations in decisions across their tech stack from the start, compared with 25% overall. This means close to nine in 10 healthcare organizations do not inherently build security into their technology-driven processes.

At the same time, healthcare organizations may not be investing enough in cybersecurity technologies and programs. "Investing in cybersecurity technologies is certainly more top of mind than it ever has been, and there has been a trend toward increased funding in this area. But we still have quite a ways to go," says Temple. To accomplish this, he advocates that cybersecurity investments within the healthcare sector "go beyond merely technological solutions and be targeted toward all aspects of preventative protection and incident planning and response."

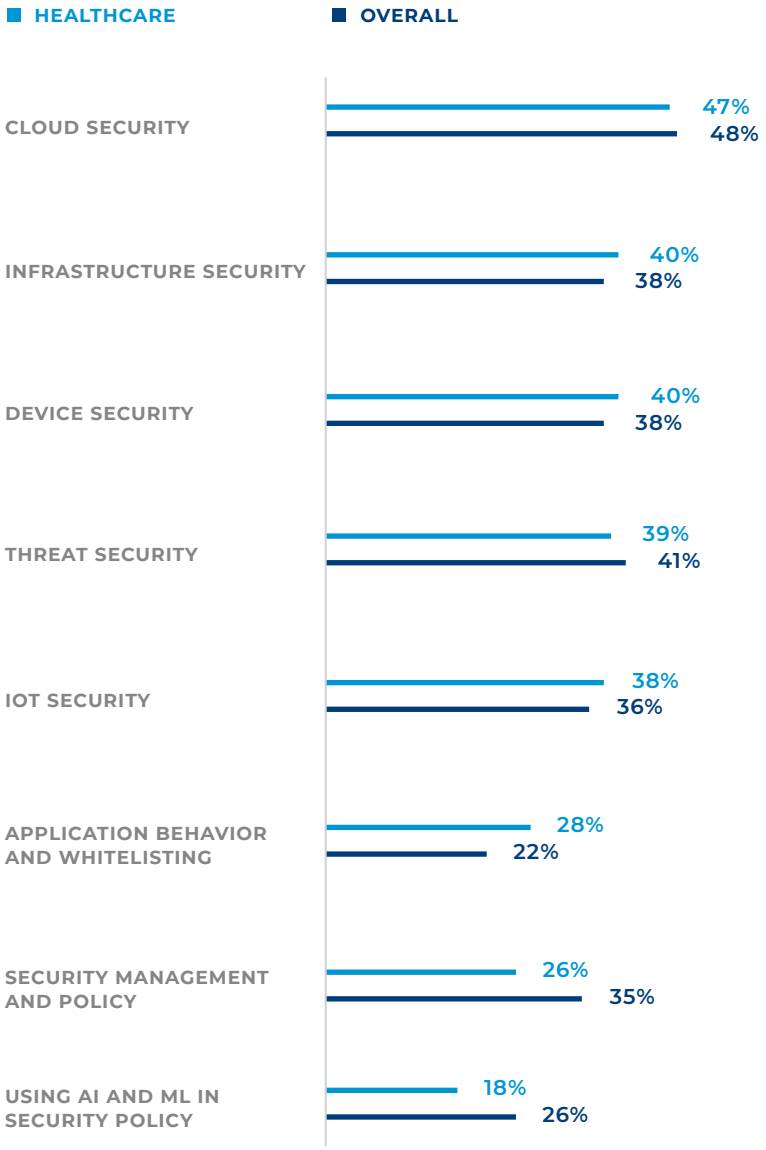
Close to nine in 10 healthcare organizations do not inherently build security into their technology-driven processes.

Healthcare industry investments in advanced analytics approaches also lag. Only 18% of respondents plan to invest in artificial intelligence for their security strategy, versus 26% overall. As is the case in other industries, healthcare leaders are focused on cloud, infrastructure and device security (Figure 7).

What's needed are "investments in monitoring systems that, through artificial intelligence, can understand behavior of particular devices and flag and alert someone if it observes behavior that significantly deviates from the norm," says Temple. "For example, if the system were to see an X-ray machine sending files to an overseas country when it has never sent a file outside the country before, that would constitute a major red flag, and an urgent alert would be sent to someone so it can be looked at as soon as possible. Other ongoing security initiatives, such as firewalls, need to play an important role in the mix."

FIGURE 7

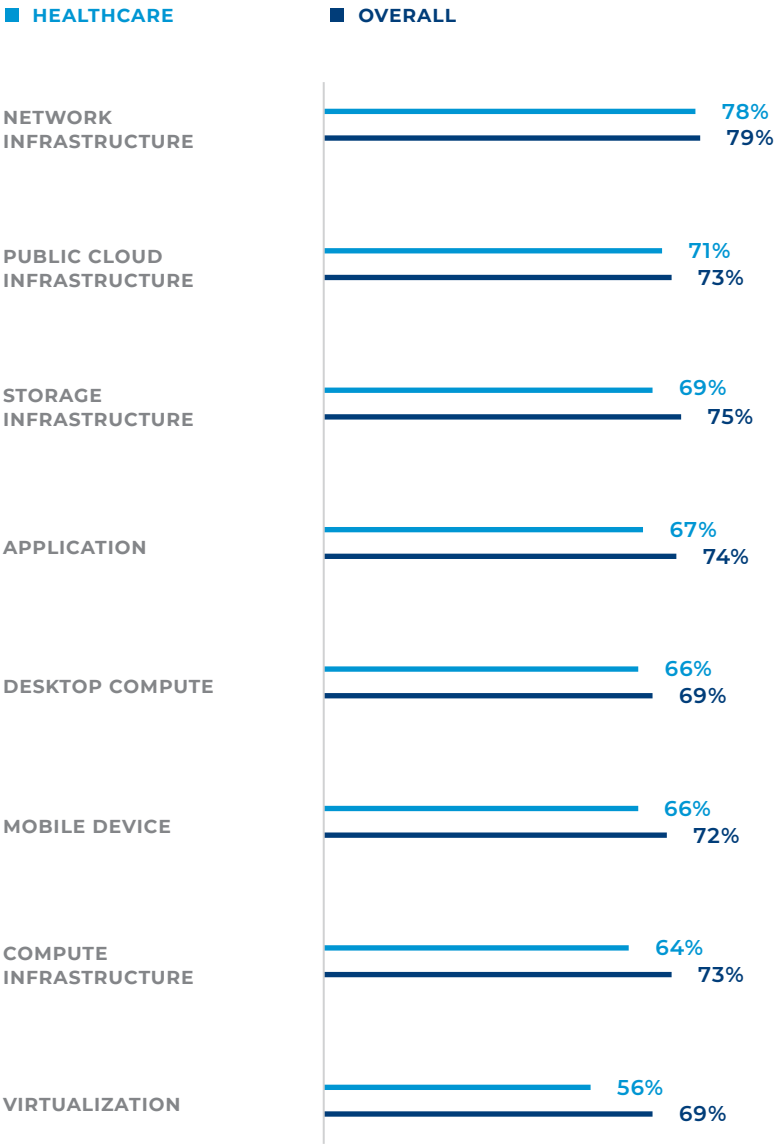
Top Areas For Security Investment Over The Next Three Years



Across the technology spectrum, healthcare values network, public cloud and storage infrastructure to improve security capabilities. Close to eight in 10 indicate they pay a lot of attention to their networking infrastructure to achieve heightened states of security—in line with the overall industry average. In addition, close to three-fourths now see public cloud services as essential to their cybersecurity posture as well (Figure 8). Two-thirds of healthcare respondents indicate some security measures are now handled by cloud providers, which is less than the overall sample (Figure 9). Identify and firewall services are the most common areas delivered by cloud providers.

FIGURE 8

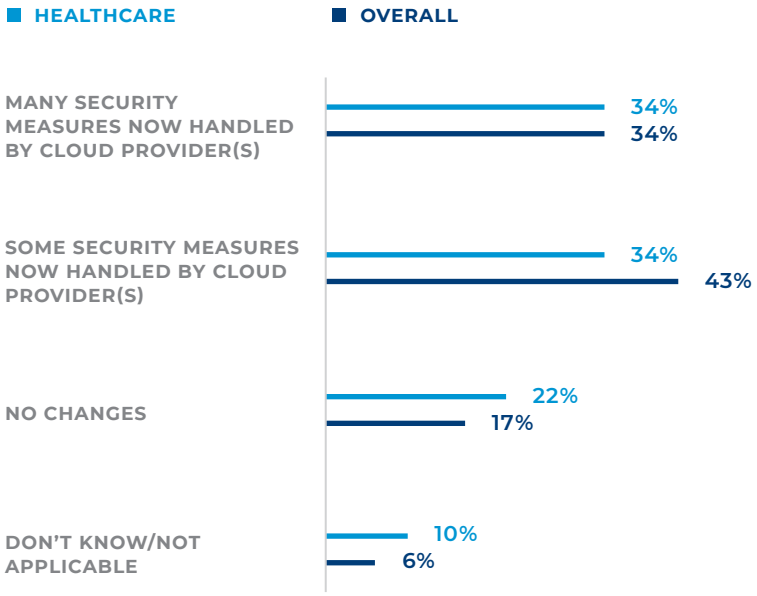
How Valuable Are The Following Technologies And Solutions To Your Cybersecurity Strategy?



Cloud is helping companies within healthcare to address security issues that may have been too complex for on-site staff to manage. "Our organization has moved its electronic medical record hosting to the cloud, and it was a very conscious decision as we have a small, but mighty, team of network engineers," says Temple. "With the magnitude of the potential impact of a data disaster, we thought it wise to turn the hosting baton over to a third-party organization whose sole raison d'être is maintenance of healthcare systems. We could never afford 24/7 constant system monitoring while maintaining local systems and handling the day-to-day, so we were able to get ourselves access to an army of resources to swarm on the system in the event disaster strikes. A real win for us."

FIGURE 9

How Cloud Adoption Has Changed Security Strategies



The People & Processes

Healthcare organizations have many moving parts, but in just about every case, people—clinicians, administrators, technologists and patients—are essential links in the chain. Time is critical as the ability to deliver data and diagnosis can be a matter of life and death. Healthcare organizations cannot afford to have their systems down or compromised for any length of time. In addition, unlike a financial breach, in which the victim can be made whole, once patient data is breached and compromised, the impact may be permanent.

While healthcare organizations are able to tend to security events at a faster pace than industries overall, they express just as much impatience with the pace of progress (Figures 10 and 11).

FIGURE 10

Length Of Time To Resolve A Security Issue

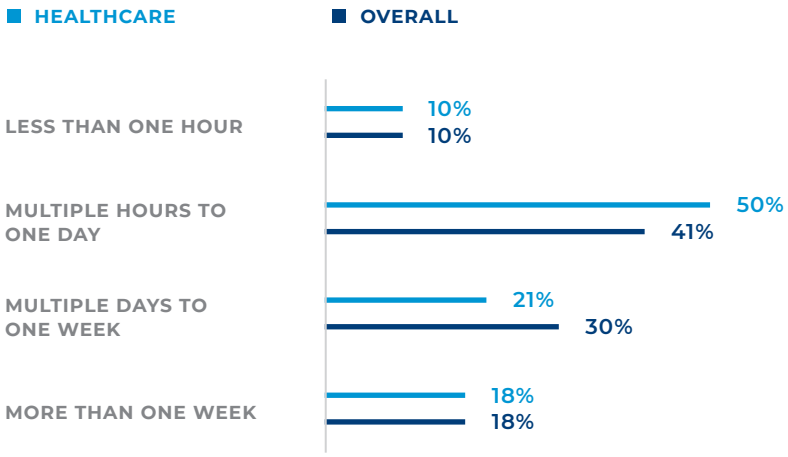
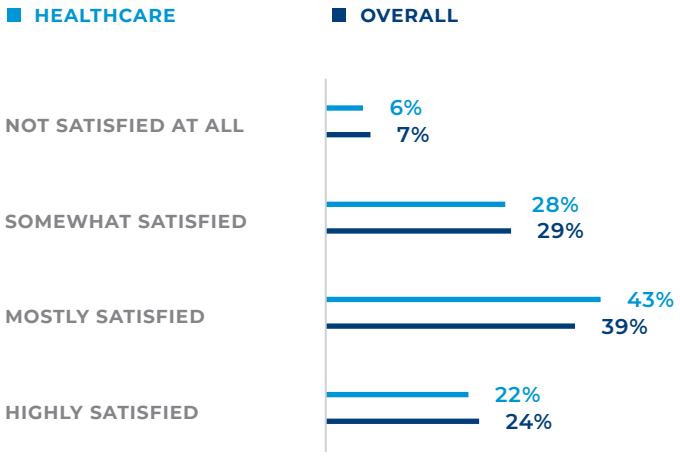


FIGURE 11

Satisfaction With Length Of Time To Resolve A Security Issue

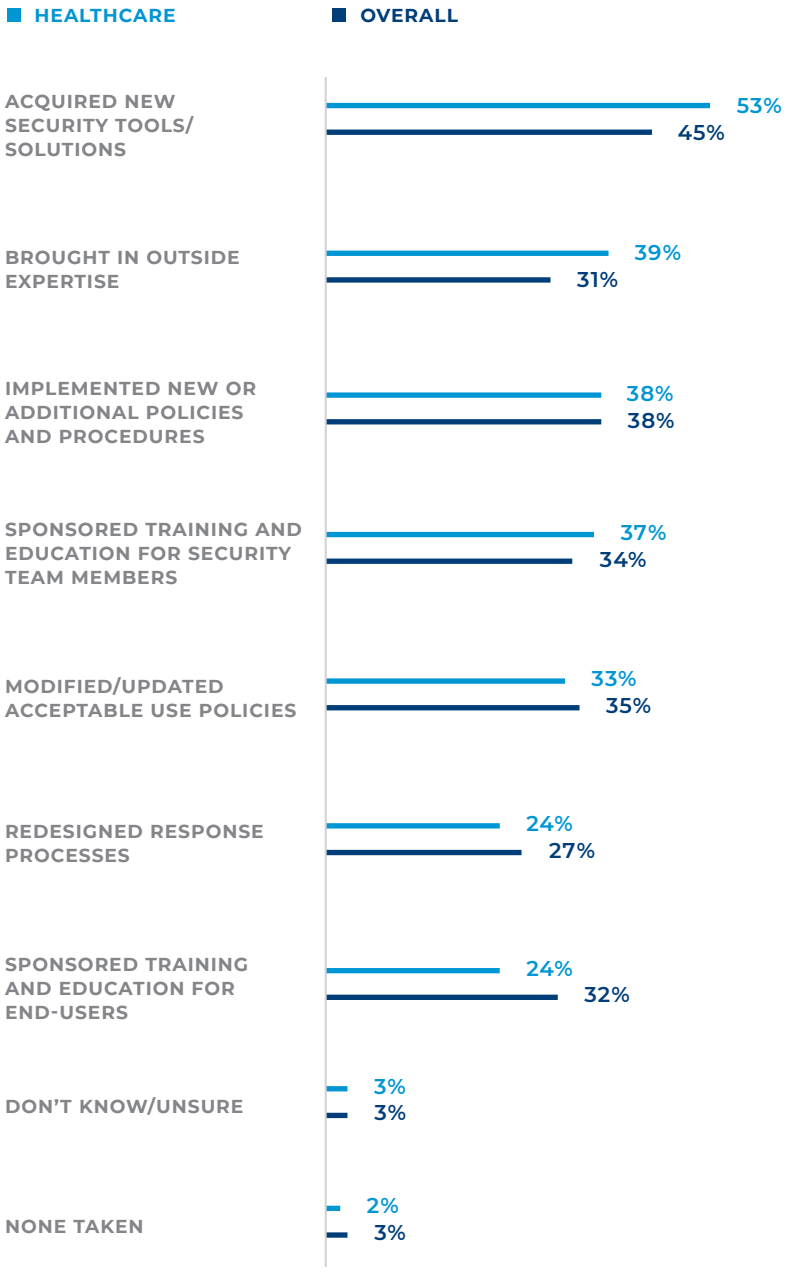


To be able to quickly and effectively deal with security challenges, healthcare organizations leverage both technology and partners. A majority of healthcare leaders indicate they rely on the latest security tools and technologies to address their security challenges. This exceeds the reliance on new technologies from other industries. Partnerships are also important to healthcare organizations seeking to secure their data and systems, as indicated by 39%. Again, this is a higher level of reliance than what is seen across the broader survey group.

Changes to internal processes and ways of doing business also figure prominently as remedies in healthcare settings, mentioned by 38%, who implemented new or additional policies and procedures to manage cybersecurity threats. A similar number have also taken action to upgrade the skills and capabilities of their cybersecurity teams. However, end-user training is relatively low on the list, cited by only 24%, which trails the overall industry average. The diversity of end-users in healthcare settings makes such training a challenge (Figure 12).

FIGURE 12

Actions Taken To Improve Responsiveness To Security Issues



The Future

Healthcare security executives and practitioners need to prepare for the transformative changes that are sweeping organizations.

Here are the trends that will shape the industry over the coming years.

There needs to be a zero-trust policy for application behavior, devices and access. When it comes to this form of prevention, healthcare is the lowest of all industries, the survey finds (58% versus 66% overall). In addition, healthcare organizations rank lowest in their confidence in strategies to identify "known good" application behavior for an effective zero-trust application strategy (12% versus 26% overall). It's imperative that healthcare organizations move to adopt zero trust across all applications and interfaces, which stipulates that systems should automatically verify all requests for connectivity or access, and not trust anything from within or without.

End-user and IoT devices will proliferate within healthcare settings, requiring more intrinsic security. Endpoints are an important area for security investments. However, healthcare has lower levels of security within IoT compared with other industries. Only 60% say IoT is built into their security infrastructures, versus 71% overall.

Devices—both personal and corporate—will continue to advance in healthcare settings, carried by physicians, nurses and allied health professionals, as well as by business-side administrators. In addition, patients are increasingly relying on health services delivered via the web and mobile apps for scheduling appointments and accessing online diagnostic services. Smartphones and tablets already proliferate.

On the horizon are wearable and attached devices that will automatically stream or upload data to centralized systems. While end-user training will help, attacks are bound to get through, which is why, from a technology perspective, organizations need to lower the attack surface with security built into the infrastructure so that when it bypasses users, potential damage can be limited.

Healthcare organizations need to ensure that their staffs and clinicians are prepared to address cybersecurity events. With the wide attack surface and the complexities of digital interactions, end-users serve as the first line of defense. As shown in the survey, most attacks in healthcare organizations arrive via phishing attacks and socially engineered malware—all preventable to a large degree through end-user awareness and education.

"In healthcare, we are highly aware of the sensitivity of information," says Gutmann. "Employees in every department understand we have the privilege and responsibility to serve our patients. We are most vulnerable as an organization when the cyberattack exploits the kindness and attentiveness of staff through phishing emails."

"Since we know that no system can offer complete protection at all times, hospitals need to invest in developing clear, unambiguous methodologies for how they will respond in the event of a major system compromise," says Temple. "Who would be on the rapid-response committee? What one-time capabilities might we grant someone lower in the organization to make decisions to cut certain computers off from the internet to minimize the spread of malware? How does the organization handle media inquiries? Although these pieces do not cost a ton of money, per se, they involve having key leaders in drills on a periodic basis and having to drop what they are doing to address the unfortunate situation."

Increasing consideration of cloud or third-party options to deliver security capabilities. Until recently, security was seen as a drawback of moving to the cloud. Now, cloud providers can deliver far more security than on-premises sites. However, it's notable that 60% of healthcare respondents in the survey cite an "inability to control the elements of the infrastructure end to end" as a high-risk factor for cloud deployments, versus 45% of their counterparts across all industries.

Yale New Haven Health sees cloud as a long-term cybersecurity strategy. "The choices of which vendors and the security used by those providers is a focus we are currently looking at to better understand the landscape," says Gutmann. "There are business advantages for putting computer power and storage in the cloud, although making sure that all companies along the data chain of custody align to our security protocol has consumed tremendous resources during due diligence."

Healthcare business, security and medical team leaders need to foster open and frequent communication on security concerns. Cybersecurity is an ongoing challenge that affects every part of the enterprise. This requires that processes and work habits be constantly examined and adjusted to meet security needs. The enhanced attention to processes that occurs within a robust and holistic cybersecurity strategy can help streamline and improve the way business is conducted.

For more information on how to turn security into a competitive advantage, read:

Cybersecurity Trailblazers Make Security Intrinsic To Their Business ⟶

METHODOLOGY

Forbes Insights surveyed 1,001 executives from across the globe representing manufacturing, retail, financial services, healthcare, government and education. Within this group, 150 respondents were with healthcare organizations. From the overall sample, more than four in 10 respondents were from the C-suite (including chief information security officers, chief information officers and chief technology officers), and nearly a quarter were in security management roles. Responses were weighted to reflect market size.

ACKNOWLEDGMENTS

Forbes Insights and VMware would like to thank the following individuals for their time and expertise:

Chris Gutmann
Systems Director, Information Technology: Clinical Engineering, Yale New Haven Health

Richard Temple
Vice President/Chief Information Officer, Deborah Heart and Lung Center

Forbes insights

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis.

By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes'* social and media platforms.

Report Author:
Joe McKendrick

499 WASHINGTON BLVD. | JERSEY CITY, NJ 07310 | 212.367.2662 | FORBES.COM/FORBES-INSIGHTS