EXECUTIVE SUMMARY

EMEA Healthcare in 2019:

The Healthcare Industry in EMEA Seeks Cybersecurity Remedies

A Special Report

vmware® | Forbes insights

INTRODUCTION

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

The rise of digital healthcare makes robust cybersecurity in this area even more critical than in other industries, due to the extreme sensitivity of the data involved, combined with associated strict regulation intended to protect patient privacy. Healthcare systems and capabilities are expanding rapidly and becoming more and more distributed, which exposes larger attack surfaces which need protection. Central IT systems also need to be more secure on one hand, but paradoxically, easier to access by authorized personnel, using an expanding network of medical devices and end-user services. This specialist hardware also needs to be secured.

Vulnerabilities to cybersecurity attacks have been on the rise in healthcare organizations, says Richard Temple, vice president and chief information security officer for the Deborah Heart and Lung Center, which is based in Browns Mills, New Jersey, in the US. 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 … and distort the rightful owners' medical history by having the imposter's history co-mingled.**

Chris Gutmann, systems 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.

> **… A patient's record contains highly sensitive information, making health systems high value targets for cyber thieves. The unique challenges for 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, VMware, in partnership with Forbes Insights, surveyed 651 security practitioners and security executives throughout Europe, Middle East and Africa (EMEA). This report details the specific findings from the 130 respondents from within the healthcare industry. Where appropriate, healthcare results are contrasted with the overall EMEA market.

THE SITUATION

Digital transformation a norm in healthcare organization

For healthcare organizations across EMEA, digital transformation is seen as being at very much the mid point of the transformation journey. Exactly half of healthcare executives say infrastructure, security controls, and applications have significantly evolved as digital technologies have taken root. Much of this is concerned with cloud adoption. Whilst it is encouraging that a good proportion are taking action, it equally highlights that there is still work to be done for a significant number of healthcare organizations in EMEA that are unnecessarily exposing themselves to cyber risks. (Figure 1)

Cybersecurity Strategy Alignment an issue in Healthcare Organizations

More concerning, the urgency of transforming cybersecurity in healthcare organizations does not yet appear to have fully engaged business leaders in this sector. Healthcare security leaders say major stakeholders are less aligned with their security strategy than is typically the case in other industries. Overall, only just over half of respondents in EMEA say their business leaders are intimately involved in their organization's security processes. Across other industries, over two thirds report close alignment, so healthcare in the EMEA has some urgent catching up to do. (Figure 2)

Budgetary Constraints are Top Barrier to Improving Security

The challenges faced by healthcare security professionals are both organizational and technical. Unsurprisingly, in an EMEA market dominated largely by state-funded healthcare systems, the greatest organizational challenge reported is budgetary — 44% indicate they face budget headwinds in their efforts to secure solutions and resources to ensure security. (Figure 3) The proliferation of new and diverse systems and mobile end-user devices present the greatest technical challenges. (Figure 4) Interestingly, healthcare respondents seem to be less sensitive to many of the issues that other industries face. For example, healthcare executives are significantly less concerned with the proliferation and viability of their installed security products — only 31% cite the number of discrete security point products as an issue, versus 40% overall. In addition, while 38% of healthcare respondents see their security tools as outdated, this is less than the overall sample (44%).

Healthcare organizations see more incidents and attacks than other industries

The survey shows that EMEA healthcare respondents report seeing a greater number of incidents or intrusions than their counterparts in other industries. Social engineering-based threats are a fundamental issue for healthcare as in other heavily people-based industries: nearly two in five say they have experienced cyberattacks as a result of password phishing (versus 34% in the market overall), with socially engineered malware, ransomware and social media-based cyberattacks at 31%, 27% and 26% respectively (all of which are significantly higher than the overall market). (Fig 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.**

Figure 1:
Healthcare Enterprise Areas Seeing Transformational Change

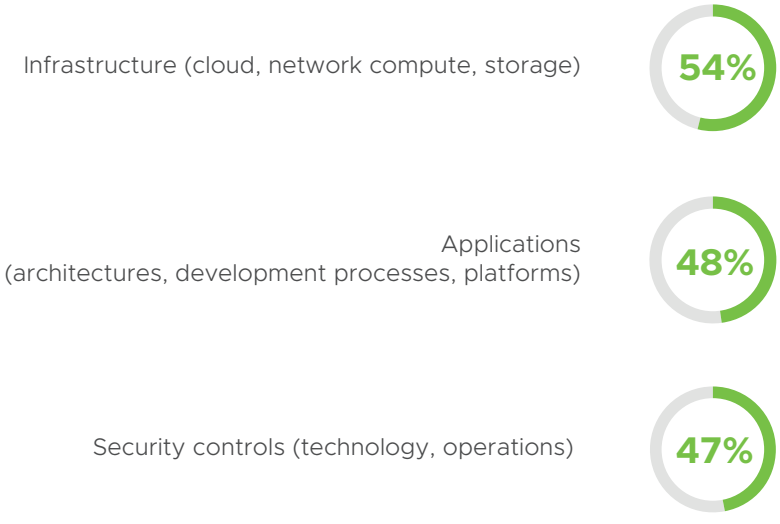


Figure 2:
Stakeholder Alignment In Security Strategies

	Healthcare	Overall
C-suite	63%	67%
Functional directors	57%	69%
Lines of business, SVP, GM	56%	67%
Chief Security Officer	55%	69%
Board of directors	52%	65%

Figure 3:
Healthcare Cybersecurity Organizational Pain Points
(Represents/highly represents)

	Healthcare	Overall
Need more budget	54%	49%
Need more coherent enterprise approach and strategy	43%	43%
Need for stronger policies and guidelines	43%	42%
Lack of end-user training or awareness	47%	41%
Lack of visibility (e.g. we don't know what we don't know)	50%	42%
Lack of skilled staff	49%	43%
Lack of top executive support	42%	37%

Figure 4:
Healthcare Cybersecurity Technology Pain Points
(Represents/highly represents)

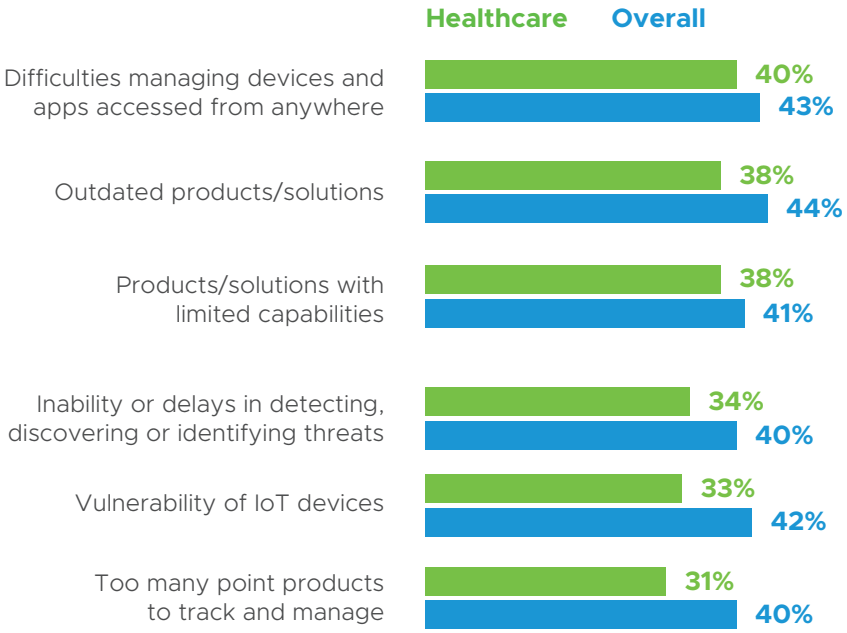
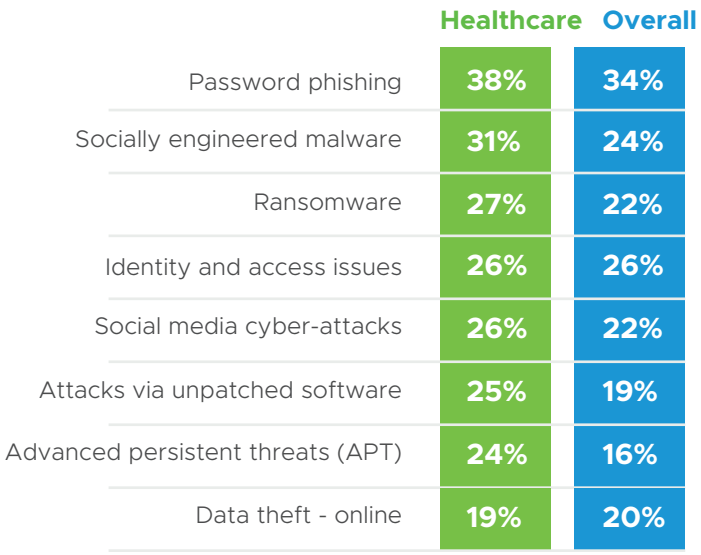


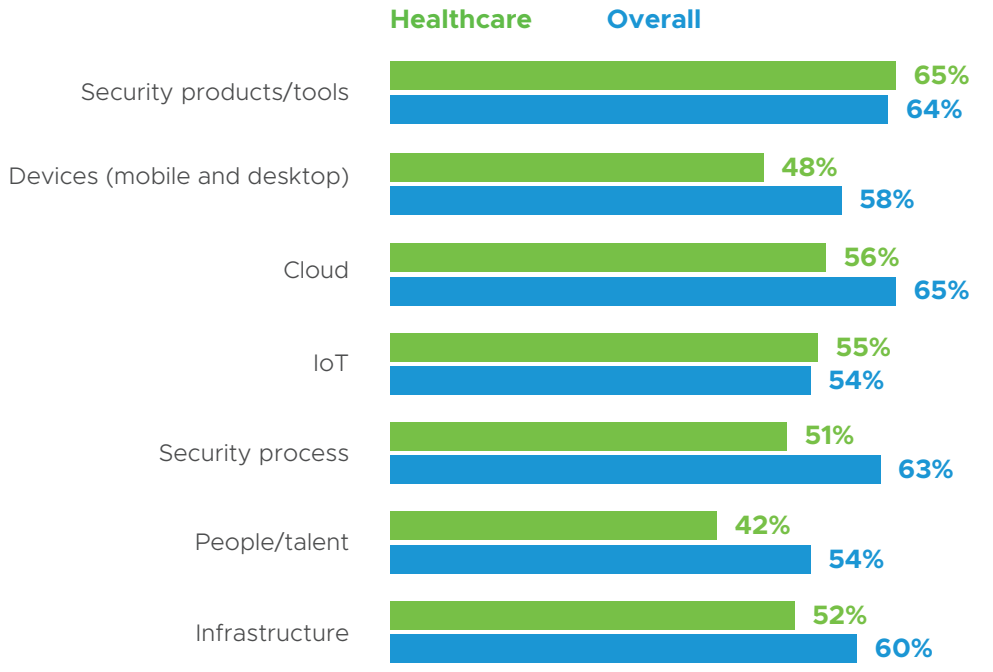
Figure 5:
Top Incidents Experienced Over The Past Three Years



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

Tellingly, healthcare leaders express less confidence than their peers in other industries that they are sufficiently prepared to address emerging security challenges. EMEA respondents in the healthcare sector indicate high levels of confidence in their security products, tools and devices — yet this is the only area where respondents are more confident than the overall average (Fig 6)

Figure 6:
Confidence In Addressing Emerging Security Challenges



THE TECHNOLOGY

It's absolutely 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 comprehensive way. The healthcare sector lags even further behind—only 17% of EMEA healthcare organizations fully involve their security organizations in decisions across their tech stack from the start, compared to 22% overall. This means just under nine in 10 healthcare organizations do not holistically 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 way 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.**

However, healthcare industry investments in the use of advanced analytics for security (eg. AI and machine learning) are slightly ahead of the overall average - 30% plan to invest in artificial intelligence for their security strategy, versus 29% overall. As is the case in other industries, healthcare leaders are focused on cloud, device security and threat security as their infrastructures transform and workloads gradually move into the cloud. (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, also play an important role in the mix.**

Across the technology spectrum, healthcare values network, public cloud, and storage infrastructure to improve their security capabilities. Close to eight in 10 in EMEA indicate they pay a lot of attention to their networking infrastructure to achieve heightened states of security—above the overall industry average. In addition, close to three-quarters now see public cloud services as essential to their cybersecurity posture as well. (Figure 8) Around 70% of healthcare respondents indicate that at least some security measures are now handled by cloud providers, which although lower than the overall sample, still represents a huge vote of confidence in public cloud and a rapid turnround from the apparently entrenched attitudes of only a few years ago. (Figure 9) Identity services is the most common function delivered by cloud providers.

Cloud Strategies are shifting security strategies

Cloud is helping companies within healthcare 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 only 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 hand the hosting baton over to a third-party organization whose sole raison d'etre is maintenance of healthcare systems. We could never afford 24x7 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 7:
Top Areas For Security Investment Over The Next Three Years

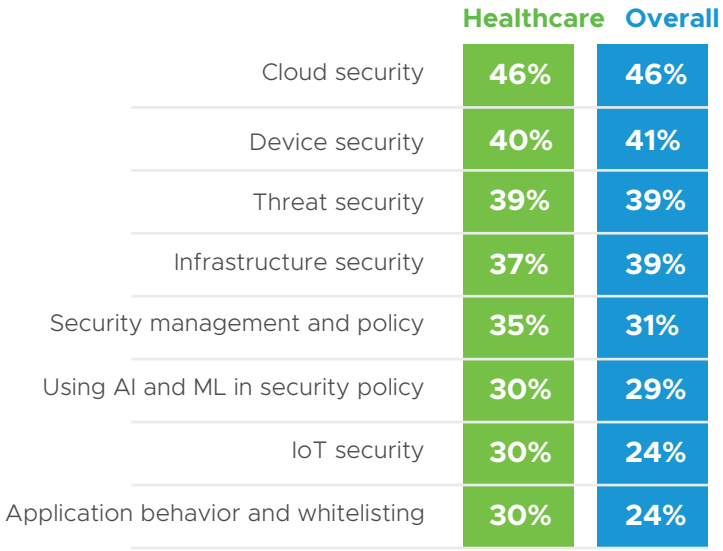


Figure 8: How Valuable Are The Following Technologies And Solutions To Your Cybersecurity Strategy?

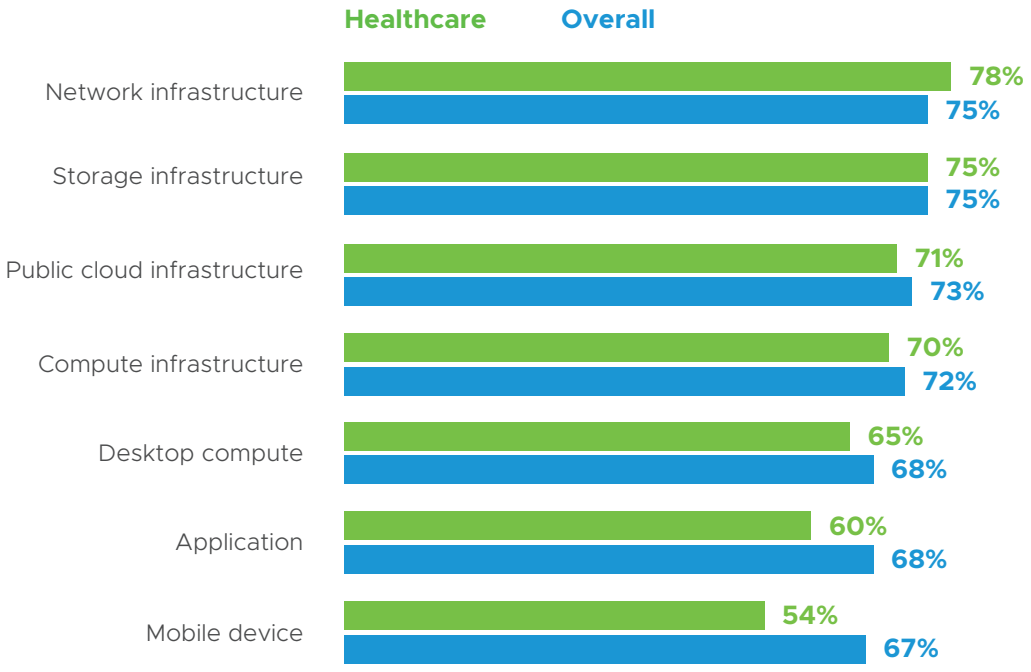
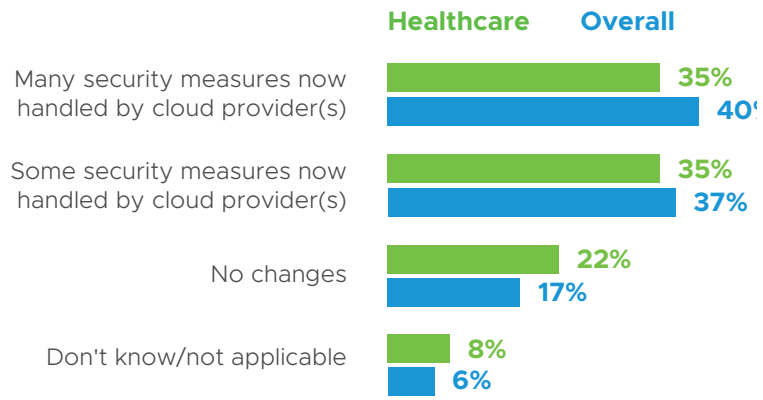


Figure 9:
How Cloud Adoption Has Changed Security Strategies



THE PEOPLE AND 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.

According to the survey, while EMEA healthcare organizations tend to be able to resolve security issues at a faster pace than other industries overall, they express just as much impatience with the time it takes them to do so. (Figures 10 and 11)

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 is roughly on par with other industries in EMEA. The fact that Implementing new or additional policies and procedures are is also seen as being important to healthcare organizations seeking to secure their data and systems, shows that there is a broad understanding that modern cybersecurity cannot be just be left to technology.

Action to upgrade the skills and capabilities of their cybersecurity teams is given a high priority in healthcare organizations across EMEA (41%), but similar training for end-users is not seen as anywhere near as important, only cited by 31%. The diversity of end-users in healthcare settings make such training a challenge, but given the preponderance of insider risk arising from social engineering oriented attacks, this is both short sighted and potentially an quick win if corrected. (Fig 12)

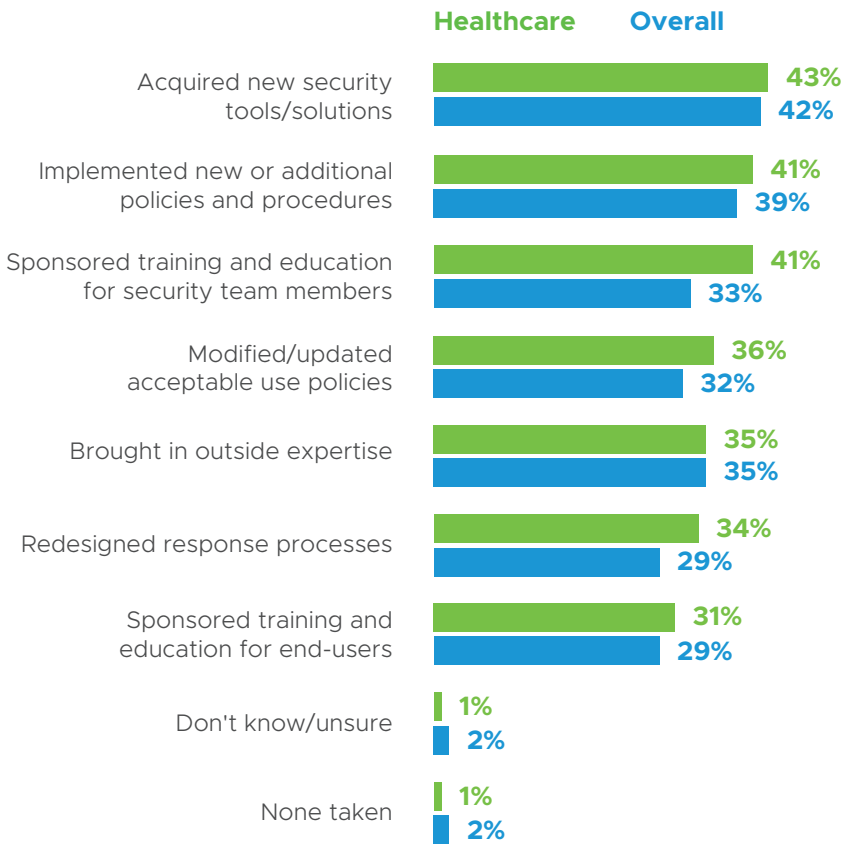
Figure 10:
Length Of Time To Resolve A Security Issue

	Healthcare	Overall
Less than 1 hour	5%	8%
Multiple hours to 1 day	46%	43%
Multiple days to 1 week	27%	31%
More than 1 week	22%	18%

Figure 11:
Satisfaction With Length Of Time To Resolve A Security Issue

	Healthcare	Overal
Not satisfied at all	4%	5%
Somewhat satisfied	26%	31%
Mostly satisfied	51%	45%
Highly satisfied	19%	18%

Figure 12:
Actions Taken To Improve Responsiveness To Security Issues



THE FUTURE

Healthcare security executives and practitioners in EMEA need to prepare for the transformative changes that are sweeping through organizations. Here are the key trends that will shape the healthcare industry over the coming years.

1 **The concept of zero trust-based security for application behavior, devices and access needs to be universally adopted.**

When it comes to implementing this form of security, healthcare lags behind all other industries we surveyed in EMEA (55% versus 61% overall). In addition, EMEA healthcare organizations rank lowest in their confidence in strategies to identify 'known good' application behavior for an effective zero-trust application strategy (63% versus 67% overall), as opposed to the traditional and increasingly ineffective tactic of 'chasing known threats'. Against an almost exponentially worsening threat landscape, it's imperative that healthcare organizations move to adopt zero trust across all applications and interfaces, based on an intimate knowledge of what the application infrastructure should look like ('the known good'), and mandate that systems, networks and applications should all automatically verify all requests for connectivity or access, and not trust anything by default from within or without.

2 **End-user and IoT devices will proliferate within healthcare settings, challenging security efforts.**

This is an important area for security investments. However, healthcare has lower intrinsic security within IoT compared to other industries in EMEA. Only 57% say security is built into their IoT infrastructures, versus 65% 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 or edge systems.

3 **Develop a cybersecurity risk profile.**

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 cyber-attack 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 great deal 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."

4 **Increasing consideration of cloud or third-party options to deliver security capabilities.**

Until recently, the perception of inherently lower levels of security was seen as being a significant negative when it comes to moving healthcare workloads to the cloud. Now, the favorable economics of the cloud model, combined with the fact that cloud providers can demonstrably deliver far higher levels of security and investment in security than any single healthcare organization could hope to achieve with on-premises infrastructure, is changing the market's collective mind. However, it's still notable that 54% of healthcare respondents in the survey cite an "inability to control the elements of the infrastructure end to end" as a risk factor for cloud deployments, versus 46% 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."

5 **Healthcare business, security, and medical team leaders need to foster open and frequent communication on security concerns and to work collaboratively.**

Cybersecurity is now an ongoing cross-disciplinary challenge that affects every part and function of the healthcare enterprise. This requires that processes and work habits across the whole organization 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 healthcare is conducted in a wider sense.

METHODOLOGY

Forbes Insights surveyed 651 executives from across EMEA representing manufacturing, retail, financial services, healthcare, government and education. Within this group, 130 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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com