Putting Your Money Where Your Healthcare Risk Is

Gaining greater value from healthcare-focused cybersecurity technology

Cybersecurity is now a universal concern among U.S. healthcare leaders, with virtually everyone worried about outside intrusions and insider threats that can expose private data, take down critical systems, destroy reputations, and launch compliance audits.

These executives have reason to fear what's next: 82% of U.S. hospitals experienced a significant security event in the prior year, according to the 2019 HIMSS Media research report *Securing Healthcare Transformation: Cybersecurity Trends and Insights*. No doubt threats are expanding as health systems meet growing demand for mobile health and secure data-sharing. These and other market mandates require more options for accessing data, opening closed systems, retrofitting legacy systems, integrating more third parties, maintaining regulatory compliance, stimulating innovation, and of course, addressing the human element.

Needless to say, things quickly get complicated, and expensive — even with most health systems in the mood to shop. "We talk to a lot of customers that buy a lot of technology, but the integration of that technology and the ability to map it to real-time dataflows is still a process," explained Lee Field, Director of Healthcare, Insurance & Life Science Solution Architecture for Verizon Business Group.

> *"Having the ability to maintain visibility for all the links in the chain is really challenging in healthcare. This is particularly true with IoT. That ability to keep up with so many potential blind spots is going to be a major focus."*
>
> **DAVID J. GRADY** | CYBERSECURITY EVANGELIST VERIZON

Do you see what I see?

Each year, Verizon releases its popular Data Breach Incident Report, which offers insights into the changing cybersecurity landscape, both globally as well as by industry. In the 2019 report, healthcare stood out as an outlier in that more than 50% of threats came from internal actors, namely snooping or vengeful employees and partners with lax security practices, as opposed to the more common bad actors from outside an organization.

Even more unique is the increasing complexity of healthcare IT ecosystems. "It's not just one federated system. It's incredibly distributed now. It's incredibly mobile. And any chain is only as strong as its weakest link," said Verizon Cybersecurity Evangelist David J. Grady. "Having the ability to maintain visibility for all the links in the chain is really challenging in healthcare. This is particularly true with IoT. That ability to keep up with so many potential blind spots is going to be a major focus."

The 125 healthcare cybersecurity and IT security stakeholders who took part in the recent HIMSS Media survey believe protecting personal health information and other patient data is top of mind. Seventy-two percent ranked it first, compared to securing

"It comes down to having a great design and a good security model, and following security basics," he said. Having such a strong foundation also will help manage the many smart devices and mobile applications now reshaping the patient and clinician experience."

LEE FIELD | DIRECTOR OF HEALTHCARE, INSURANCE & LIFE SCIENCE SOLUTION ARCHITECTURE
VERIZON BUSINESS GROUP

connected devices, preventing fraud, and addressing ransomware (Figure 1). To address these concerns, 1 in 2 of those surveyed predicted email security will be a priority in 2020. That was followed by data loss prevention (46%); mobile device security, threat intelligence, and identity and access management (each at 38%); and encryption (34%).

Field believes that healthcare IT leaders need to nail down data security basics before heading down a particular buying path. Those basics include having established policies, procedures, and processes for identity and access management, authorization, two-factor authentication, and other hallmarks of good cyber hygiene. "It comes down to having a great design and a good security model, and following security basics," he said. Having such a strong foundation also will help manage the many smart devices and mobile applications now reshaping the patient and clinician experience.

Selecting the right solutions can help alleviate the anxiety permeating IT departments trying to keep pace with consumer expectations. But those purchases also add intricacy to an already data-rich IT ecosystem. "Sometimes that complexity introduces risks, especially if you aren't entirely sure how these tools fit together," Field said. "It comes back to visibility that lets you know when you have an incident, and having procedures in place to know how to respond when something does happen."

Lea Sims, Global Practice Lead for Verizon Business Group's Healthcare Practice, believes healthcare IT shops need a more meaningful view into their own risks. "Many are relying on general breach statistics to direct their security spend, and what they really need are intelligent risks insights that are unique to their industry and specific to their organizations," she said. "They can't address what they can't understand and anticipate. Beyond those insights, they need sophisticated threat detection capabilities that can give them the assurance that if they are vulnerable somewhere across their networks, they are going to be alerted to it quickly so that they can pivot and respond to that threat."

The looming impact of 5G

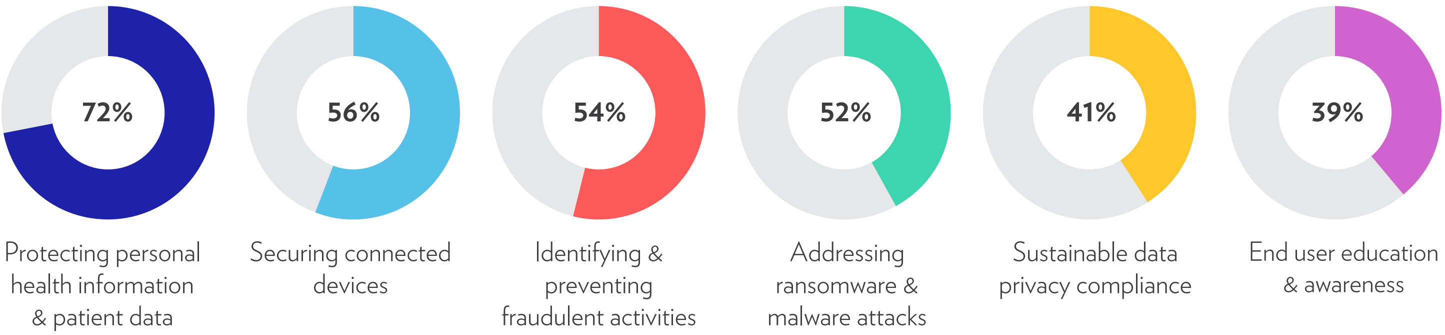
There's no doubt that the introduction of 5G networks will transform healthcare as we now know it. "We're going to see the way people interact with different systems shift, the way clinicians interact with technology materially change," Field predicted. "We're going to see the opportunity for automation, whether through artificial intelligence or other systems, and that's going to change the way the industry works."

The HIMSS Media report showed healthcare IT stakeholders are most excited by the faster connectivity and more reliable uptime and improved workflows these next-generation networks can provide, making it easier to bring more connected devices online to assist in care delivery. That excitement, though, is tempered by new cybersecurity risks all these mobile and medical devices will pose (Figure 2).

Grady believes the impact of 5G on security plans is an issue of scale. "5G has an incredible amount of security hardwired into it. It's going to open the floodgates to innovation. We can't even imagine some of the use cases that are coming. When that innovation comes, those

Figure 1: Protecting PHI and patient data are biggest concerns for healthcare IT professionals.

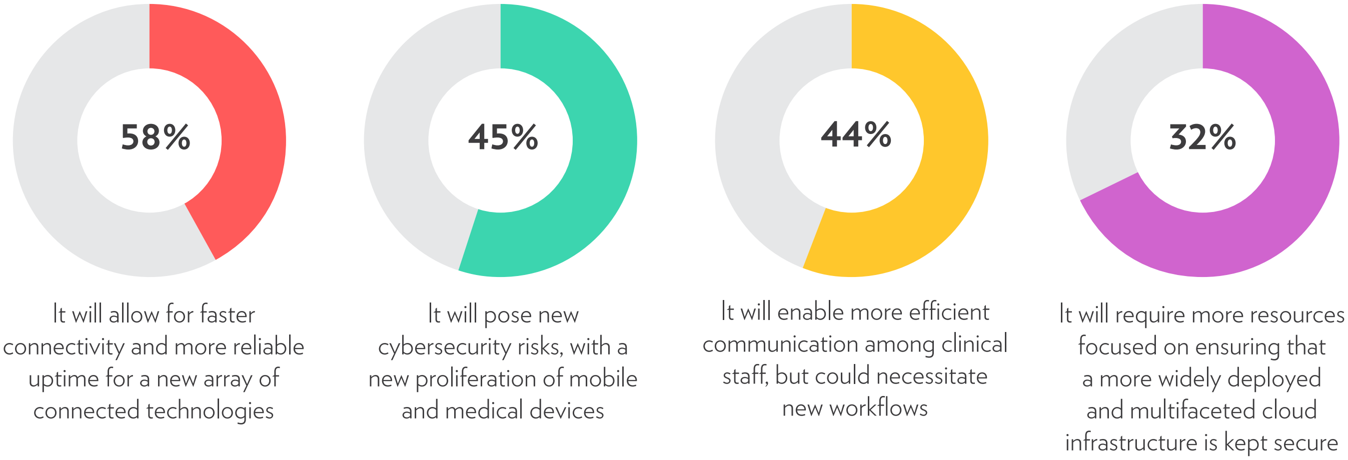
What are your top IT security or cybersecurity concerns?



> *"The complexities of the security landscape in this industry mean security solutions can't be a 'one size fits all.' These organizations need a security partner that recognizes that a 'healthcare anywhere' model will necessitate a security blueprint that meets that need both now and in the 5G-enabled future when this will be even more complex for healthcare."*
>
> **LEA SIMS** | GLOBAL PRACTICE LEAD | VERIZON BUSINESS GROUP'S HEALTHCARE PRACTICE

Figure 2. Healthcare IT stakeholders are excited by 5G's potential to improve connectivity, communications, and workflows, but also worry about broader cybersecurity implications.

How will 5G impact your security planning?



processes that move data around might outpace the security team's ability to gain visibility into that dataflow and outpace the scale for all the devices expected to come online. 5G is going to blow the door off IoT in healthcare settings, and if an organization is struggling now to keep an eye on the security of their laptops and cell phones, how are they going to keep an eye on 10,000 IoT devices that are enabled overnight because 5G makes it more effective?"

He concluded: "You need to be in good shape before you run a marathon; 5G will be a very demanding 26-mile run. People need to realize you can't go into this out of shape; you need to have done your basics and prepare for this."

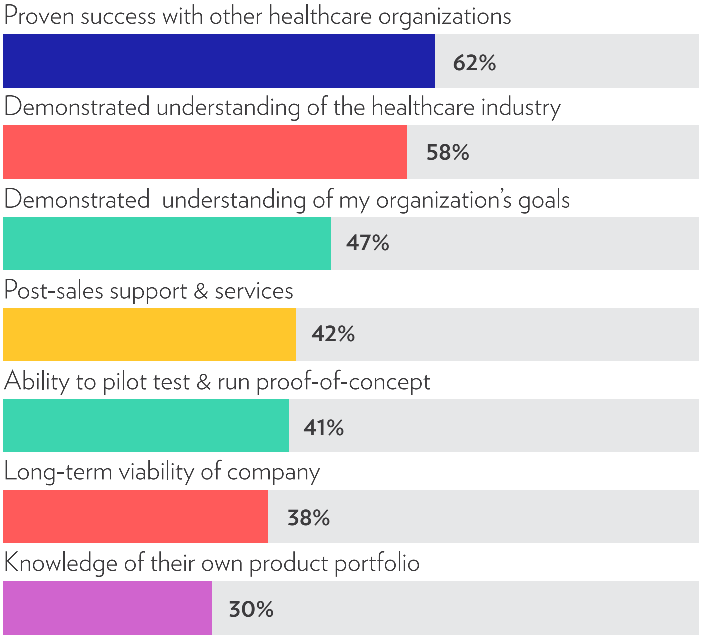
Where and with whom to invest

The top factor for IT security vendor selection in the HIMSS Media survey was a strong track record with other healthcare organizations. This was followed by a demonstrated understanding of the healthcare industry and an organization's goals (Figure 3).

"The first questions you need to ask are not 'What should we be buying and from whom?' They're, 'What do we want to do, and why do we want to do it?'" Grady said. "Once you have that clarity about what you want to achieve, you can talk to organizations that can help you get there."

Figure 3: Healthcare leaders want assurance a chosen vendor really understands their unique industry.

What are the critical factors for short-listing IT security vendors?



For the majority of HIMSS survey respondents, vendors with the ability to deliver standards-based APIs and integrated security platforms are most important to their vendor selection process (Figure 4).

This makes sense, given healthcare's collective digital transformation now well underway, Sims said. "The complexities of the security landscape in this industry mean security solutions can't be a 'one size fits all.' These organizations need a security partner that recognizes that a 'healthcare anywhere' model will necessitate a security blueprint that meets that need both now and in the 5G-enabled future when this will be even more complex for healthcare."

The cybersecurity talent shortage

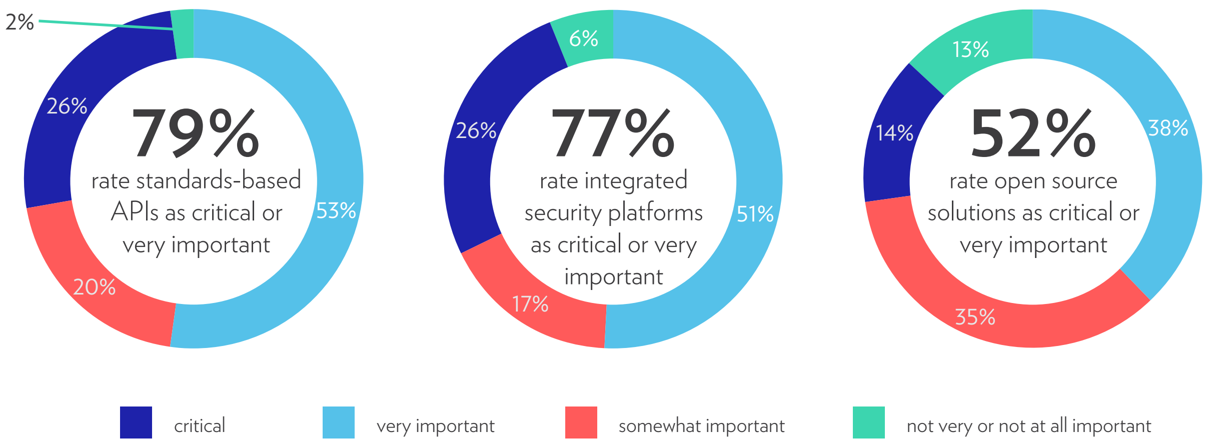
She and her Verizon colleagues noted the global shortage of cybersecurity professionals not only makes talent acquisitions more difficult and expensive, but also stretches current workforces as duties continue to expand but technological resources do not.

"The critical shortage of security expertise we're seeing across industry means something's got to give," Sims said. "The burden of keeping up with security definitions, protocols, and programmatic upgrades is untenable for this space. Shifting that burden to a managed services model is a go-forward approach these organizations would be wise to consider."

Fields warned now is not the time to kick the can down the road. "The technology market is evolving. The healthcare market is evolving. Your competitors are evolving," he said. "That procrastination some of us are prone to? That's a really bad place to be now." On the other hand, "if you have a strategy and are taking the right steps to develop good cybersecurity hygiene and the right partners to help you develop the building blocks toward that vision, then you're in a really good place."

Figure 4: Healthcare buyers want robust, standards-based APIs and integrated security platforms, even if they aren't from open sources.

How important are the following capabilities when selecting IT security solutions?



About Verizon Enterprise Solutions

Verizon Enterprise Solutions helps clients improve customer experience, drive growth and business performance and manage risk. With industry-specific solutions provided over the company's secure mobility, cloud, strategic networking, Internet of Things and advanced communications platforms, Verizon Enterprise Solutions helps open new opportunities around the world for innovation, investment and business transformation.

Visit www.verizonenterprise.com to learn more.