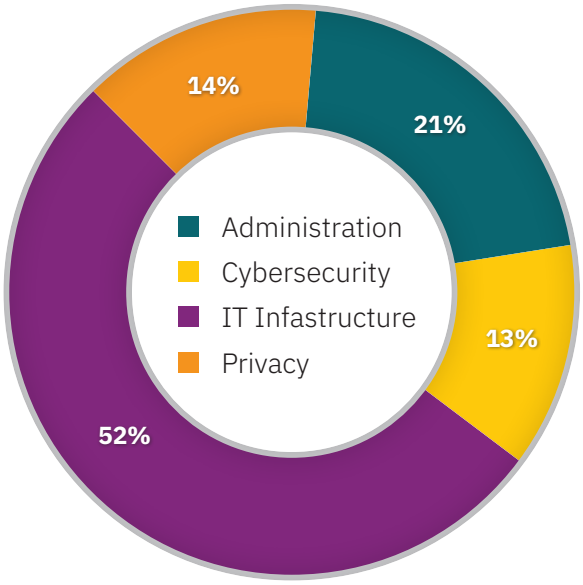
PONDURANCE

Cybersecurity Challenges for Midsize Healthcare Providers

INTRODUCTION

The healthcare industry continues to face challenges as the cybersecurity landscape evolves following the COVID-19 pandemic. Healthcare providers are facing an increase in cyberattacks and threats, offering greater digital technology options for patients, and encountering internal staffing shortages and low budgets. As a result, healthcare organizations are seeking viable solutions to their changing cybersecurity issues.

Pondurance commissioned Xtelligent Healthcare Media to survey IT, cybersecurity, administrative, and privacy professionals in hospitals, physician practices, and ambulatory care facilities for a better understanding of the cybersecurity challenges and needs of midsize healthcare providers in 2022. Pondurance and Xtelligent reviewed the responses of 52 professionals across a variety of midsize organizations, and the research study revealed significant changes in what these healthcare professionals experienced during 2022 versus 2021.



IN THIS REPORT, WE WILL ANSWER THESE QUESTIONS AND MORE:

- What are the cybersecurity and privacy challenges that midsize healthcare providers face?
- What internal changes have healthcare organizations made to adapt to the current cyber environment?
- What challenges do midsize healthcare providers anticipate moving forward?

ESCALATING ATTACKS

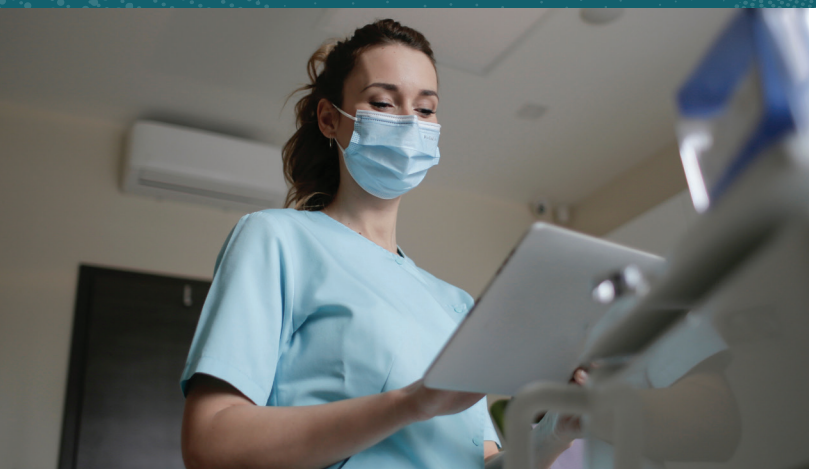
Over the past few years, midsize healthcare organizations have experienced cyberattacks and threats. In fact, all respondents in the study reported that they had been a victim of a cyberattack. Cyberattacks and threats have motivated 70% of healthcare organizations to prioritize privacy and cybersecurity, an increase from 40% in 2021. Three types of threats are currently the most prevalent:

- **Insider threats.** As much as 71% of healthcare organizations struggled with insider threats including negligent, malicious, or accidental activity from within their own organizations.
- **Ransomware.** These attacks typically harm a healthcare organization by halting online activity, exposing privacy information, and demanding high-dollar ransom payments. According to the study, 65% of healthcare organizations experienced a ransomware attack in 2022.
- **Business email compromise.** As many businesses know, it only takes one mistake to be vulnerable to an attack. Fifty-two percent of respondents experienced either fraud or business email compromise, such as credential harvesting, phishing, and impersonation.

PONDURANCE

"Healthcare is just a rich data trove, meaning that it has all of this valuable data and bad actors have recognized that," said Ron Pelletier, Chief Customer Officer at Pondurance, on the HealthITSecurity webcast Healthcare Providers Break Down Their Cybersecurity Practices. "It's not surprising that we see that these organizations made a leap from 40% to 70% now prioritizing privacy and cybersecurity."

While protecting on-premise environments and endpoints is still a priority, 87% of respondents named "cloud security" as the new top challenge.



EXPANDED ATTACK SURFACE

Every time a new medical device connects to an IT healthcare network, it expands the attack surface and increases the risk to patient safety, data privacy, and healthcare operations. Midsize healthcare organizations have greatly expanded the attack surface, including virtual services, cloud storage, and enhanced digital care practices, contributing to a complex cyber infrastructure that is increasingly vulnerable to attack. In fact, 56% of respondents stated that interoperability and connected device security are current challenges for their organizations, up from 42% in 2021.

The expanded attack surface has required healthcare providers to prioritize privacy and cybersecurity for their organizations. More than three-fourths of respondents reported that an increased number of digital offerings to patients have motivated them to prioritize security. In addition, 44% of respondents reported that their pandemic-related remote workforces pushed them to prioritize privacy and cybersecurity, which accounts for a 12% year-over-year increase. These healthcare organizations have sought new technology tools to support the expanded attack surface.

INTERNAL STAFFING AND CAPABILITIES

A massive talent shortage exists across the healthcare industry. Many organizations are struggling to find cybersecurity talent, and when they do, the qualified candidates demand competitive salaries. The expense is a strain on budgets. As a result, fewer organizations increased their cybersecurity staffing over the past year. The percentage of organizations that increased staffing was 42%, a drop from 50% in 2021. The most commonly hired positions included compliance or risk officers (73%), IT security analysts (60%), electronic health records (EHR) security analysts (42%), cybersecurity directors (12%), and chief information security officers (4%). Only 6% of organizations did not hire additional employees over the past year.

The study also found that most midsize organizations overestimate their internal capabilities. Ninety percent of organizations claimed to have threat hunting, including detection and analysis capabilities, yet only 56% claimed to have incident detection and analysis as part of their incident response (IR) strategy.

In addition, only 58% of respondents had alert triage and 75% had alert management, indicating a lack of understanding of the internal capacity for alert supervision.

On a positive note, 85% of organizations stated they had an IR strategy that included an IR policy, plan, and procedure. Not a single organization responded that it did not have an IR strategy in place. Also, respondents agreed that their organizations have increased monitoring and improved patch management in 2022.

Some of the staffing and capabilities issues stem from low budgets for cybersecurity needs. According to the study, 71% of all respondents agreed that their organizations have increased their budgets to support a digital health environment, up significantly from 2021. However, a whopping 98% of healthcare organizations dedicate less than 10% of their total budget to cybersecurity.

> "Security overall is a scarcity business because there just aren't enough people available to cover all of the needs out there," said Ron. "Organizations are thinking about rightsizing their programs. They don't want to be a technology company; they don't want to put all of their investment in security, nor do they need to be, to be as secure as they should be. So I think it's very smart for organizations to have value-driven partnerships with third parties that can be there at their side."

REGULATORY COMPLIANCE

HIPAA compliance dropped considerably in the rankings as a leading cybersecurity and privacy challenge for healthcare organizations. Only 15% of respondents agreed that HIPAA compliance was a challenge for 2022. However, regulatory compliance is still a motivation to prioritize privacy and cybersecurity. Application programming interfaces (APIs) often are used to exchange health information and are an important component of EHR. Apps that use APIs to share patient data as part of new legislation, including the Patient Access Final Rule, are increasingly targets for cybercriminals.

"Remember, compliance does not equal security,"

said Ron. He believes that people are waking up to that fact. After all, a ransomware event gets everyone's attention because it has the potential to bring healthcare operations to a stop and can become a public event. From there, the resulting business impacts can quickly mount.

OUTSOURCING

The cybersecurity landscape continues to evolve, and healthcare organizations are evolving with it. Increasingly complex systems, lack of staff, low budgets, and regulatory pressures have incentivized healthcare organizations to pursue outsourcing to keep up with their cybersecurity needs.

The research study found that 50% of midsize healthcare providers currently outsource their privacy and cybersecurity monitoring, up from 42%. Plus, an additional 42% of respondents plan to outsource this year. That represents a total of 92% of healthcare providers that either currently are outsourcing or plan to outsource in 2022. These providers view outsourcing as an advantageous strategy, particularly due to the talent shortage. Of those providers, 62% responded that they believe choosing a new cybersecurity vendor will be a challenge over the next six months.

Ron believes that healthcare organizations should be looking for a few specific attributes in a cybersecurity vendor. "You need a dedicated and strong security competency that never sleeps, never takes a vacation," he said. "And I think the key is to find a partner that will sit with you at the table, work with you, respond with you, learn with you, and grow with you."

PONDURANCE

CONCLUSION

Our survey reveals that healthcare providers in hospitals, physician practices, and ambulatory care facilities are facing important cybersecurity challenges, including escalating attacks, an expanding attack surface, internal staffing and capabilities issues, and regulatory compliance. These complex challenges are leading midsize healthcare organizations to use outsourcing as a plan of action to keep their patients, employees, and data safe from cyberattacks.

FOR MORE INFORMATION on midsize healthcare cybersecurity check out our healthcare services page.

READ HERE

ABOUT PONDURANCE

Pondurance delivers world-class managed detection and response services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your team can focus on what matters the most.

Copyright © 2022 Pondurance