



Risk and Compliance Concerns for Healthcare Providers

The healthcare industry continues to face challenges as cyber risk increases and regulatory compliance grows in complexity. Healthcare providers are experiencing frequent cyber threats and are working to implement viable solutions for issues involving multiple vendors, incident frequency and downtime, new technology, regulatory compliance, and spending and future plans.

Pondurance commissioned Xtelligent Healthcare Media to survey IT professionals in the healthcare industry for a better understanding of the cybersecurity objectives and needs of healthcare providers in 2024. Pondurance and Xtelligent reviewed the responses of information security, cybersecurity, and information technology respondents in organizations with 500 to 10,000 employees, and the research revealed how healthcare providers are responding to potential cyber threats now and moving forward.



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

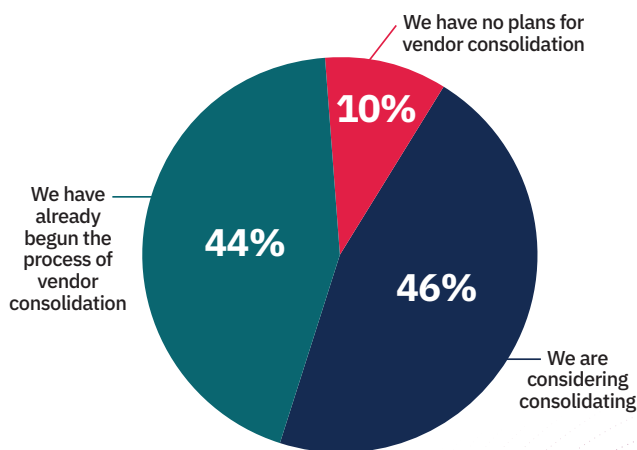
- How much do healthcare providers rely on third-party vendors for their cybersecurity operations?
- What are the current business priorities and future investment plans for healthcare providers?
- What are the gaps and inconsistencies in the cybersecurity posture of healthcare providers?

MULTIPLE VENDORS

Over the past few years, healthcare providers have had a greater reliance on cybersecurity solution providers, including managed service providers (MSPs) and point solution vendors. As much as 47% of respondents use four or more cybersecurity solution providers, and a small number of healthcare providers even use as many as 10 or more. Multiple vendors may increase the complexity of security protocols for each partnership, which may increase cyber risk.

However, the study also found that there is a strong push to consolidate vendor partnerships as healthcare providers seek efficiencies. Currently, 44% of healthcare providers have started the process of consolidation, and 46% are considering it in the next 12 to 24 months, leaving only 10% of respondents with no plans to consolidate vendors within that time frame.

HOW DOES YOUR ORGANIZATION PLAN TO APPROACH CYBERSECURITY VENDOR CONSOLIDATION IN THE NEXT 12-24 MONTHS?



INCIDENT FREQUENCY AND DOWNTIME

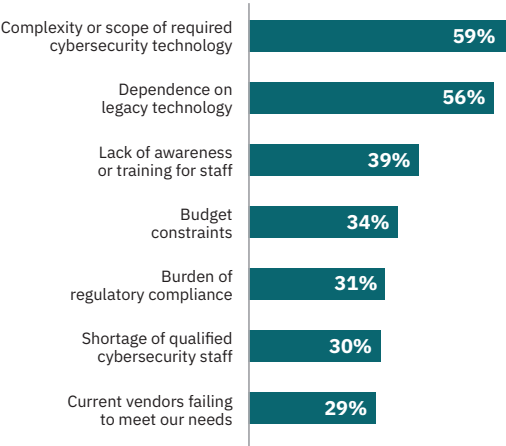
Healthcare providers have experienced multiple cyber incidents, such as system failures, cyberattacks, and breaches, that have resulted in significant downtime. Sixty percent of respondents in the study reported four or more incidents in the last year. As much as 18% of respondents reported 10 or more incidents, and those respondents said they struggle to implement successful cybersecurity programs and rely heavily on incident response.

The study also showed that healthcare providers are highly focused on proactive metrics when measuring cybersecurity posture. Survey respondents prioritize their key metrics as mean time to detect (66%), regulatory and compliance (61%), and mean time to respond (61%). These priorities suggest that healthcare providers cannot withstand any amount of downtime and that stringent industry regulations, including HIPAA, require significant resource dedication.

NEW TECHNOLOGY

Healthcare providers are challenged by the complexity of new technology and the resources needed to stay up to date. Nearly 60% of respondents stated that the complexity of new technology is a barrier, and 56% have a dependence on legacy technology. In addition, 39% of respondents believe they face a lack of awareness or training for staff. Respondents also cited budget constraints, regulatory compliance, and talent shortages as barriers. The results suggest that healthcare providers heavily rely on external vendors because employees' current knowledge base and dependence on older technology limit their ability to improve cybersecurity.

WHICH LIMITATIONS ARE KEEPING YOUR ORGANIZATION FROM EVOLVING WITH THE CHANGING CYBERSECURITY LANDSCAPE?



REGULATORY COMPLIANCE

Healthcare organizations take a comprehensive approach to regulatory compliance and technological advancement to assure that they stay in HIPAA compliance. The survey showed that 71% of healthcare providers prioritize HIPAA compliance above all other priorities. Other major goals include securing new systems (53%) and consolidating cybersecurity vendors (52%). Also, as the attack surface grows, 49% of healthcare providers have a goal of securing their Internet of Medical Things devices to reduce their risk.

For HIPAA compliance, 66% of healthcare providers prioritize the use of third-party consultants or auditors with a deeper knowledge of HIPAA than internal teams to validate their data security. In addition, 49% of providers focus on maintaining up-to-date policies and 47% conduct regular audits.

For assessments, 70% of healthcare providers use trusted third-party consultants, whereas only 21% of providers said they trust their internal teams to complete a HIPAA compliance assessment. The other 9% specifically use a managed detection and response (MDR) partner for assessments. Most providers conduct annual HIPAA assessments, while 37% conduct assessments more than once a year, even though regulations do not require the greater frequency.



SPENDING AND FUTURE PLANS

Healthcare providers place an importance on having dedicated resources and a more preventive, data-driven approach to cybersecurity. The survey found that a majority of healthcare providers plan to increase spending on MSPs, with risk assessments (69%), security analytics (66%), incident response (63%), and MDR (61%) seeing the highest anticipated investments over the next 12 to 24 months.

Spending on MSPs often happens in reaction to external events. As much as 71% of healthcare providers are likely to increase their MSP spending due to a change in HIPAA regulatory compliance. Healthcare providers also are likely to increase MSP spending when there's an emergence of a new type of ransomware or cyber threat (63%) or following an increase in the number of attempted or successful attacks (46%).

Specifically, the study found that healthcare providers plan to greatly increase spending on protective measures such as endpoint protection platforms, penetration testing, and vulnerability management. In fact, each of these categories is expected to receive a 45% increase in planned spending, while spending on older and more generalized security tools, such as email security, virtual chief information security officer service, and single sign-on, is on the decline.

The survey also showed that healthcare providers are motivated to improve their detection and response over the next 12 to 24 months, taking a proactive approach to threat management by emphasizing mean time to detect, detection rate, mean time to respond, and regulatory compliance, among others. The goal is to neutralize threats before they can inflict significant damage and cause downtime.

CONCLUSION

The survey revealed that healthcare providers are facing increasing and complex cybersecurity challenges and are seeking viable solutions. These challenges are leading healthcare providers to rely on external vendors, focus on proactive measures, prioritize HIPAA compliance, and dedicate greater resources to cybersecurity.

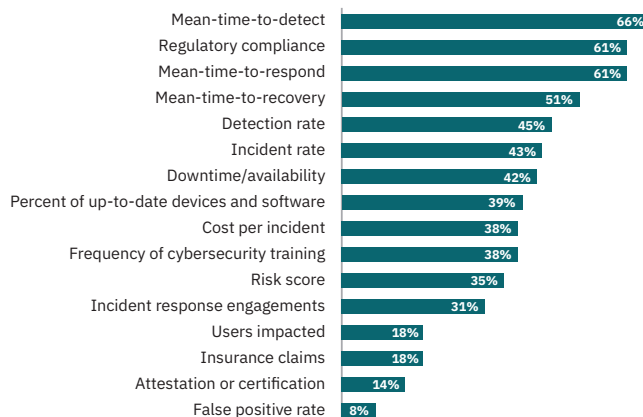
For additional report details and analysis, watch our [webinar](#).

For more information about cybersecurity for healthcare providers, check out our [healthcare services page](#).

ABOUT PONDURANCE

Pondurance delivers world-class MDR 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 most.

WHICH KEY PERFORMANCE INDICATORS (KPIs) DOES YOUR ORGANIZATION PRIORITIZE WHEN MEASURING CYBERSECURITY POSTURE?



HOW DOES YOUR ORGANIZATION PLAN TO CHANGE SPENDING ON MSPs ACROSS THESE AREAS IN THE NEXT 12-24 MONTHS, IF AT ALL?

