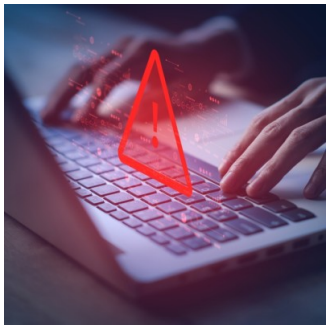
HealthManagement
Promoting Management and Leadership

Healthcare Cybersecurity: Insights from the HIMSS Survey



Recent cyberattacks in France and Romania, as well as the Change Healthcare ransomware, have brought attention to the growing issue of healthcare cybersecurity, and the steps needed to mitigate this risk. The Healthcare Information and Management Systems Society (HIMSS) recently released a survey presenting insights from 229 healthcare cybersecurity professionals, with a focus on their roles, challenges, and budget trends. Nearly half of the respondents had primary responsibility for healthcare cybersecurity programmes, reflecting the critical role these professionals play in safeguarding sensitive data and ensuring patient safety. These professionals were employed across various sectors, including healthcare providers, vendors, consulting firms, and government entities, with diverse roles in executive and non-executive management.

Hiring qualified professionals remains a challenge

A pervasive challenge highlighted in the survey is the difficulty in hiring qualified cybersecurity professionals (74,16% of respondents). This issue is not unique to healthcare but is exacerbated by the growing demand for cybersecurity expertise globally. Factors contributing to the hiring challenge include the lack of cybersecurity experience or skills among candidates, budget constraints, and the need for healthcare-specific knowledge due to the direct correlation between cybersecurity and patient safety. Regulatory aspects are also a healthcare-specific complexity that adds to the difficulty of recruiting the right profiles. Moreover, non-competitive compensation and concerns about job security further complicate recruitment efforts. Retaining qualified professionals is equally challenging, with factors such as limited growth opportunities, a lack of executive support, and stress contributing to dissatisfaction among cybersecurity professionals.

Stronger cyber defence requires greater investment

Effective cybersecurity measures require substantial investment, yet many healthcare organisations operate on constrained budgets. Chief Information Security Officers often face limitations in implementing robust cybersecurity strategies due to financial constraints. However, increased funding enables organisations to adopt cutting-edge solutions and better prepare for evolving threats. Encouragingly, the survey indicates a positive trend, with a majority of respondents (55%) reporting budget increases compared to previous years. Historically, healthcare organisations have allocated a small portion of their IT budgets to cybersecurity, but recent trends show a shift towards higher cybersecurity expenditures, reflecting the growing recognition of its importance.

The lasting impact of the COVID pandemic

The COVID-19 pandemic has further emphasised the need for robust cybersecurity measures, particularly with the rise of telework and telemedicine. While the pandemic officially ended in 2023, remote work remains prevalent, necessitating ongoing adjustments in cybersecurity strategies towards decentralised and virtual ways of working. Telemedicine visits comprise a growing number of patient interactions, changing deeply the healthcare landscape. Healthcare organisations have responded by increasing their cybersecurity budgets, with an average allocation of at least 7% of the overall IT budget. This increase is expected to continue in 2024, indicating a recognition of the evolving cybersecurity landscape and the importance of proactive investment.

In conclusion, the 2023 HIMSS Healthcare Cybersecurity Survey sheds light on the challenges and trends shaping the cybersecurity landscape in the healthcare industry. While recruitment and retention of qualified professionals remain significant hurdles, increasing budget allocations demonstrate a growing commitment to strengthening cybersecurity measures. With adequate support from executives, meaningful work, and contributions to the organisation that are valued, cybersecurity professionals will thrive and build up healthcare capabilities to safeguard patient data and maintain operational resilience.

Source: HIMSS

Image Credit: iStock

Published on : Tue, 5 Mar 2024