HealthManagement
Promoting Management and Leadership

HIMSS Report on Healthcare Cybersecurity Threats

Already burdened by the unprecedented challenges from the COVID-19 crisis, healthcare organisations also were hit by a barrage of significant security incidents – i.e. phishing, ransomware and data breaches – during the past 12 months, says a new HIMSS report.

You might also like: 'Shielding' Against Cyber Attacks

These cybersecurity attacks often caused disruption to IT and business operations, but they also had impacts on clinical care, according to the report, titled "2020 HIMSS Cybersecurity Survey". In addition, there were monetary losses due to business email compromise, wire fraud, and extortion.

The survey study included 168 healthcare cybersecurity professionals, mostly performing a management role in IT operations (83%). Most of the respondents who reported patient safety impacts said that their organisations did not have effective mechanisms in place to detect patient safety issues related to cyberattacks.

"Because of the clear nexus between patient safety and cybersecurity, it is clear that more organisations need to have effective mechanisms for detecting patient safety issues," the report points out. "Healthcare cybersecurity professionals should be collaborating with patient safety professionals within their organisations and vice versa."

Survey results show phishing was the most common form of cybersecurity attack (57% of respondents), followed by credential harvesting attacks (21%), social engineering attacks other than phishing (20%) and ransomware/other malware (20%). Other security incidents that were reported include theft/loss, breach/data leakage, and malicious insider activity.

Another interesting finding: legacy systems remain prevalent in healthcare, such as Windows Server 2008, Windows 7, and Windows XP. In fact, the majority of respondents (80%) reported that their organisations are still using legacy systems, which are no longer supported by manufacturers and thus more vulnerable to attacks.

"Based upon these findings, it is likely that the legacy footprint will continue to grow," says the HIMSS report, citing the need for a modernisation plan to ensure that legacy systems are replaced or upgraded. However, technology modernisation is hindered by tight cybersecurity budgets, which generally did not change from the previous year. Indeed, only 6% or less of the IT budget is typically allocated for cybersecurity, the report notes.

The report says healthcare organisations should be more proactive in improving their cybersecurity posture by taking some important steps, including: increasing cybersecurity budgets, upgrading or replacing legacy systems, conducting end-to-end security risk assessments, and enhancing cybersecurity awareness and training programmes.

"It is time for healthcare organisations to improve their security postures. Robust cybersecurity is essential for normal operations, patient safety, and data protection," the report concludes.

Source and image credit: HIMSS

Published on : Thu, 26 Nov 2020