HealthManagement
Promoting Management and Leadership

Strengthening Cybersecurity Training in Healthcare

Annual cybersecurity training has become a standard practice across many industries, including healthcare. These sessions, which often involve informational videos or phishing simulations, are important for compliance. Yet compliance does not necessarily equate to security. With cyber threats growing in frequency and sophistication, the healthcare sector faces particular challenges due to the sensitive nature of its data and the critical importance of uninterrupted patient care. A more effective approach is emerging: role-based cybersecurity training, designed to provide staff with knowledge tailored to their responsibilities. This shift acknowledges that safeguarding institutions requires more than ticking regulatory boxes; it demands training that aligns with the real-world risks staff encounter daily.

The Need for Role-Based Security Training
Healthcare workers are often placed in situations where risky digital behaviour is not negligence but part of their job. A 2024 survey found that 71 per cent of employees admitted to actions that compromised security, such as clicking on unfamiliar links or sharing credentials. For example, human resources may need to download resumes, IT help desks must confirm credentials, and researchers regularly access large volumes of sensitive data. These activities inherently create opportunities for malicious actors to exploit.

The problem is magnified for staff in specific roles. Help desk employees, driven by a desire to assist colleagues, may be manipulated into granting access to attackers posing as legitimate staff. Similarly, high-profile clinicians or researchers are particularly vulnerable due to the value of the data they handle and their public visibility. Attackers increasingly tailor their strategies to target such individuals and departments, especially in organisations conducting medical research that may be of interest to nation-state actors. Role-based training allows staff to recognise subtle warning signs that generalised training overlooks, building awareness that is essential to protect both institutional data and patient safety.

Approaches for Effective Training
Traditional annual training modules are often treated as a chore, delayed until deadlines approach and quickly forgotten. More effective programmes use shorter, frequent sessions, sometimes delivered in real time in response to emerging threats. These sessions act as refreshers, reinforcing lessons when staff are most receptive and making the content relevant to their daily tasks.

Must Read: ***The Future of Healthcare Security: Embracing Passwordless Authentication***

The growing use of artificial intelligence by attackers introduces new challenges. Techniques such as deepfakes and shallowfakes are increasingly used to manipulate trust. While deepfakes involve entirely fabricated videos, shallowfakes subtly alter real content in ways that make them more believable. Training must adapt to prepare staff to recognise these evolving tactics, complemented by technical measures such as sandbox technology that allow suspicious content to be examined before action is taken. Even with advanced tools, people remain the primary targets. Exploiting human behaviour is often easier and cheaper for cybercriminals than identifying software vulnerabilities, underscoring the continuing importance of human-centred training.

Building a Culture of Security in Healthcare
For healthcare organisations, effective cybersecurity is inseparable from their mission of providing safe and continuous care. In the past, staff often viewed security training as a distraction from clinical duties, and security protocols were sometimes resisted as obstacles to efficiency. That perception is gradually shifting. There is a growing recognition that inadequate security not only threatens data but can also interrupt patient care entirely. If systems are disabled or compromised, hospitals and clinics may be unable to deliver critical services, putting patients at risk.

Role-based training supports this cultural change by linking digital vigilance directly to patient outcomes. Staff begin to understand that their attentiveness to cybersecurity is not just about compliance but about protecting patients, colleagues and the institution itself. By reinforcing this connection, healthcare organisations can foster an environment where security is seen as integral to care, rather than as an external burden.

Cybersecurity in healthcare requires more than broad compliance exercises. As attackers refine their methods and exploit human behaviour, the sector must respond with targeted, role-specific training that equips staff to recognise and resist threats in the context of their daily work. Shorter, more frequent sessions enhance effectiveness, while preparation for emerging tactics such as shallowfakes keeps training relevant. Ultimately, embedding role-based security into organisational culture ensures not only stronger protection of sensitive data but also the uninterrupted delivery of patient care.

Source: HealthTech

Image Credit: iStock

Published on : Mon, 18 Aug 2025