HealthManagement
Promoting Management and Leadership

How to Fix Internal Cybersecurity Vulnerabilities

Healthcare remains a favourite hunting ground for hackers. The month of April (2019) saw a record high number of 44 healthcare data breaches, affecting information of 686,953 individuals. Common tactics employed by hackers were phishing, ransomware and distributed denial-of-service (DDoS) attacks.

However, in addition to external threats, there were also a number of internal cybersecurity failures, ranging from unauthorised employees accessing patient records to coding errors that unintentionally exposed data. A case in point: the accidental sharing of 37 patients' email addresses in an invitation to a support group distributed by NHS Highland.

Indeed, poor internal risk management and lax security measures (59%) are more likely than external threats (42%) to cause data leaks, according to Verizon's 2019 Data Breach Investigations Report.

Because internal cultural and technological issues are often more to blame for this cycle of healthcare data breaches, experts are now emphasising the need for institutions to make a dramatic cultural shift to enhance cybersecurity management.

Healthcare, a soft target of attackers, is made softer by the nature of "businesses" that have never considered themselves to be technology companies, according to Jason Gillam, CIO at Secure Ideas, adding that such mindset breeds technical incompetence when it comes to cybersecurity.

"In healthcare security, we're taught above all else that life and limb are important," Gillam says. Because data and personal information are not always the top priority, a lot of activity that might be considered suspicious in any other industry tends to be ignored. "We need to make a cultural shift from cybersecurity as a compliance check-box to doctors treating the protection of their patients' personal data as a priority," he points out.

For his part, Dave Kennedy, TrustedSec's founder and senior principal security consultant, says a number of his healthcare clients have made significant cultural adaptations and many of them now give much attention to cybersecurity management. He notes though that this issue is not something that can be solved overnight by throwing more people and resources at it.

You might also like: Common Healthcare Cyber Threats

"Being more proactive means having the ability to fix issues as they are identified over time," Kennedy explains. "The biggest challenge for a hospital CIO is being able to communicate the likelihood and impact of a breach and introduce whatever is necessary prevent it. And describing possible impact to a board is difficult."

With regard to technological vulnerabilities, Kennedy has these core recommendations: A more frequent patch management programme for applications and systems, combined with enhanced multifunctional password management.

The cultural challenge of managing cybersecurity risk takes on more importance given the increased connectivity in healthcare operations.

“These are such highly connected environments,” says Elliott Frantz, CEO of Virtue Security. “A lot of employees need access to a lot of systems – and this creates inherent risks. Traditionally, a hospital has wrapped technology around its business, leading to multiple segregated pieces. Instead, they need to use technology to solve security by design. The positive sign is that a lot of new network and virtualisation technology is helping to create less exposed infrastructures.”

He hopes to see more efforts being exerted to improve application security. “We have seen a lot more hospitals taking a bigger interest in tackling application security problems, and that’s a good thing,” Frantz says. “But the picture has not improved substantially.”

Source: Healthcare IT News

Image: iStock

Published on : Tue, 29 Oct 2019