BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Safeguarding Healthcare: Addressing Cybersecurity Risks in a Connected Bioscience Era

April 23, 2026 | Opinion

Pamela Ong, Country Manager for Singapore and Asia, ESET Healthcare is consistently one of the most targeted sectors globally because it combines high-value data with a low tolerance for disruption. Ransomware remains one of the most serious threats,

The healthcare sector is increasingly interconnected and data-driven, making it a critical yet vulnerable part of modern bioscience. Health care organizations face increased cybersecurity risks due to the increasing use of health data pooling and artificial intelligence. These include ransomware, operational disruptions, and the exploitation of human error, all of which can have far-reaching consequences for patient care and ecosystem-wide resilience. As cybercriminals target the sector for its high-value data and low tolerance for disruption, strengthening cyber resilience through prevention, organizational awareness, and streamlined security measures is inevitable than ever before. Addressing the risks related to operational continuity and patient outcomes, ***Pamela Ong, Country Manager for Singapore and Asia, ESET*** shared comprehensive insights with

Biospectrum Asia at the GITEX AI summit in Singapore.

- **What are the biggest cybersecurity risks facing healthcare organisations today**

The biggest risk is that healthcare is no longer operating in silos. It is becoming far more connected, data-driven, and dependent on digital workflows across institutions, platforms, and partners. For example, the Health Information Bill (HIB) will connect more of Singapore's clinics, labs and hospitals through the National Electronic Health Record (NEHR). While this strengthens care delivery, it also means cyber risk is no longer contained. A vulnerability in one part of the ecosystem can have wider operational consequences.

Ransomware remains one of the most serious threats, but the real issue is not just encryption or financial loss. In healthcare, ransomware can quickly become an operational disruption. When systems are disrupted, access to records is delayed, workflows are interrupted, and patient care may be affected, which makes the stakes far higher than in most other sectors.

Human risk also remains a major issue. Attackers continue to exploit phishing, social engineering, weak access controls, and unpatched systems. In high-pressure clinical environments, even small lapses can have an outsized impact. That is why cybersecurity in healthcare needs to be treated not just as a technology issue, but as a core part of operational resilience and continuity of care.

- **Why is the healthcare sector such an attractive target for cybercriminals?**

Healthcare is consistently one of the most targeted sectors globally because it combines high-value data with a low tolerance for disruption. Healthcare organisations manage large volumes of sensitive patient information, including personal health records, identity data, financial details, and other confidential information that can be monetised in multiple ways, including fraud, extortion, and follow-on attacks. To put this into perspective, medical records can have up to 10 times the value of credit card data, which makes the sector especially attractive to cybercriminals.

On top of that, healthcare is becoming more interconnected. As patient data flows more freely across providers, labs and digital platforms, the attack surface expands. This means risk is no longer isolated to a single organisation and a weakness in one part of the environment can have wider consequences across the broader healthcare ecosystem.

- **What practical steps can healthcare providers take to strengthen cyber resilience?**

A prevention-first approach needs to be the starting point. In healthcare, the priority is to stop compromises before they escalate into operational disruption. This starts with getting the fundamentals right - specifically, strong access controls, multi-factor authentication, timely patching, endpoint and email protection, vulnerability management, and good cyber hygiene across the organisation. These remain the most effective ways to reduce exposure early and limit entry points.

Equally important is investing in people. Human error remains one of the most common entry points for attackers, so ongoing staff awareness is essential. Healthcare teams need to be equipped to recognise phishing and social engineering attempts in real-world and high-pressure situations.

Finally, organisations need to reduce complexity and improve visibility. Simply layering more tools onto existing systems is not the answer, especially for organisations with limited cyber resources. What matters is having clear oversight across the environment, from endpoints to cloud to identity, supported by automation and, where needed, managed detection and response to close capability gaps

Cyberfender Healthcare was designed with this in mind to help providers strengthen baseline cybersecurity controls while addressing operational and financial risks associated with cyber threats. As healthcare systems across Asia continue to digitise and adopt technologies like AI to manage rising demand, cybersecurity will increasingly underpin both resilience and patient outcomes. Prevention is no longer optional - it is foundational.