Healthcare moves to mitigate cyber risk

Thanks to digitisation across the sector, the advent of internet of things (IoT) and wearables, and the increasing sophistication of cyber criminals, the security risks facing the healthcare sector have never before been so broad or so complex.

"The healthcare sector's exposure to risk has increased exponentially," says Paul Williams, country manager – Southern Africa at Fortinet.

Where South African healthcare service providers once lagged their international counterparts in mitigating information security risk, they are now moving to implement more comprehensive security measures.

He points out that while the next generation healthcare enterprise stands to gain significant benefits from digitised and interconnected operations, they also face an intensified threat landscape.

In the digital realm, the risks in the healthcare sector include medical identity theft, unauthorised access of personal information, ransomware, denial of service attacks, malware and fraud.

"Hackers could access networks to divert funds or pharmaceutical stock, forge prescriptions, change treatment regimens or even access connected and critical equipment in an ICU ward, for example. It may sound far-fetched, but in a highly connected, digitised environment, it could even become possible to target individual medical devices on individual patients," he says.

More comprehensive approach

The SA Protection of Personal Information (POPI) Act, the US Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS), along with an increased focus on compliance and accountability, are driving local healthcare sector organisations to take a more comprehensive approach to security across their ecosystems, says Williams.

“Traditionally, many healthcare organisations have tended to approach information security and risk management in a piecemeal fashion and plugged holes only after they come under attack. Now, we are seeing a more strategic approach to information security and risk management,” he says.

“The most effective way to mitigate this broad range of threats across the ecosystem is to centralise the security architecture to make it easier to protect patient data; ensure robust clinical security through an advanced threat protection (ATP) framework, enhance the protection of medical devices through use of internal segmentation firewalls, and introduce single pane of glass management of security, wireless access points, and LAN switches.

"In South Africa, the sector is only at the start of a long road, particularly in the public sector, but there are encouraging signs that it is taking information security and risk more seriously,” he says.