Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

The lack of adoption of the reasonable care standard for security

As the risks and repercussions of cyberattacks have become more pronounced, so has the understanding of the importance of risk management around cybersecurity. Most organisations have successfully elevated cybersecurity to the board level and most directors understand that cybersecurity risk is a business risk like any other. However, this increased understanding of the importance of cybersecurity doesn’t necessarily mean that boards are well-equipped to tackle cybersecurity effectively, according to Wavelink.

Ilan Rubin, managing director, Wavelink, a Fortinet distributor, said, “When it comes to cyber resilience, the bar is only getting higher for organisations and their boards. The Australian Securities and Investment Commission (ASIC) expects directors to address cyber risk and not pass this responsibility off to IT departments. They need to take a leadership role and demand to be given the information they need to make effective choices around managing risk.

“It’s important for CISOs and business leaders to work closely together to ameliorate the risk of cyberattacks. However, there is often a disconnect between security experts and the rest of the organisation, especially as business users demand to use the latest technology to drive competitive advantage. These users can often perceive security-related checks and balances as a hindrance to business operations.”

One of the most serious disconnects between CISOs and other business leaders is their approach to the reasonable care standard for security and resiliency. This standard is widely referenced in best practices and regulatory frameworks such as Europe’s General Data Protection Regulation (GDPR), which affects many Australian organisations. It refers to the actions that, objectively speaking, the organisation should take to protect sensitive data and information.

While this sounds simple in theory, and most CISOs agree that it’s the right approach to cybersecurity, few boards have officially adopted reasonable care as their measure of security.

Ilan Rubin said, “The value of a ‘reasonable care’ metric is that it takes into account common-sense approaches to security. For example, if a company has extensive security monitoring tools but no one is reviewing those tools or acting in response to alarms, then a reasonable person would argue that the organisation has breached its duty of care. Therefore, to meet the ‘reasonable care’ standard, organisations simply have to take a logical approach to ensuring every vulnerability is addressed as well as possible.

“While the CISO is possibly the ideal person to determine whether all reasonable steps have been taken, it’s essential for business leaders and board members to get involved to make sure that all possible risks have been considered and addressed. When CISOs and boards can’t get together on this, security gaps are bound to be missed, leaving the organisation open to attack.”

Given most security breaches happen because of a gap in visibility, awareness, and control, it’s important for organisations to consider a security fabric approach to cybersecurity. This approach provides visibility and control, and leverages a zero-trust approach in which no traffic is trusted regardless of whether it originates inside or outside the network perimeter. Taking a more stringent approach to cybersecurity can help avoid charges of failing to meet ‘reasonable care’ standards and ensure companies are protected from catastrophic cyberattacks.