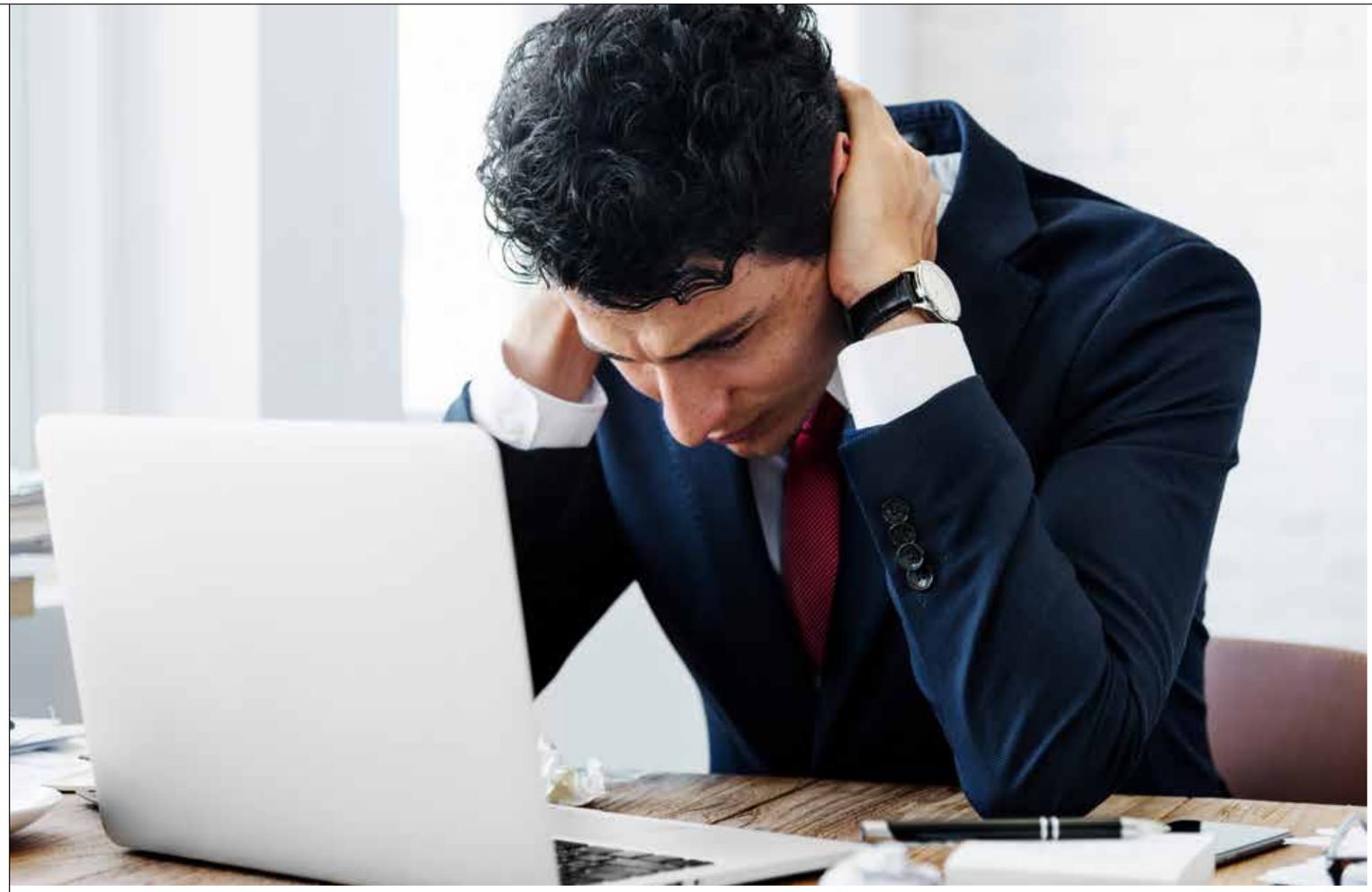

Picture credit: Adobe Stock

ARE YOU COVERED?

Leyton Jefferies *examines the importance of cyber insurance in the event of an attack*

The recent trend of insurance companies tightening their standards is a challenge for organisations. Recent research by CSI Ltd found that only two in ten (19 percent) security decision-makers are fully confident that their cyber insurance will cover their cyber risk in 2023. Less than a third (29 percent) are fully confident they're compliant with the new stricter terms that insurance companies are now stipulating.

Cyber insurance is designed to protect businesses against internet-based risks, such as data breaches, cyber-attacks and other threats. Policies generally cover expenses associated with a cyber incident such as investigation, legal fees, customer notification costs and regulatory fines.

Yet, the risk level only looks to increase. CSI's research found that 78 percent of organisations believe the current cost-of-living crisis will increase the risk of a cyber threat occurring in their organisation. When asked what factors they anticipate will increase due to the economic climate, 43 percent said fraud and phishing attempts, 45 percent said new and emerging threats, 39 percent said greater risk of supply chain partners being breached and 34 percent said reduced budgets leading to lack of third-party services and tools. So, what is the scale of the challenge in the cyber insurance industry?

Only two in ten security decision-makers are fully confident that their cyber insurance will cover their cyber risk

In 2021, ransomware disrupted infrastructure and brought down public and private networks as never before. These dramatic events and insurance companies paying hundreds of millions in cybersecurity-related claims each year are being blamed for organisations now facing rising cyber insurance rates, tightening of standards and limiting coverage.

With average ransom payments reaching $812,000 during 2021, the true cost of ransomware is in fact much more when the cost of downtime and reputational damage is included.

THE VOLUME, VELOCITY AND VARIETY OF CYBER ATTACKS IS GROWING EXPONENTIALLY

The uptick in cyber-attacks and pay-outs has meant mounting losses for cyber insurance companies and has forced change. Insurers are becoming much stricter about what risks they will underwrite in a "hardening of the market". One major insurer underwrote 80 percent of the risks presented to them last year. Now it's just 10 percent.

Despite this, cyber insurance isn't going anywhere, in fact, the market is set to grow drastically over the next few years. The global cyber insurance market was considered to be worth $6.15-billion in 2020. It's projected to grow from $7.60-billion in 2021 to $36.85-billion in 2028 at a CAGR of 25.3 percent during the period.

Digital transformation means that the attack surface is now larger and more diverse than ever. The traditional network perimeter no longer exists, *identity* is the new perimeter. The volume, velocity and variety of attacks is growing exponentially. Overall security spend is increasing to record highs, but unfortunately so are the costs of successful attacks.

With dynamic, personalised attacks, hackers will have significantly more power to cause damage. Then there are the unknown threats. Given the pace of technological development, it's likely we will be hit within the next few years by forms of cyber-attacks that are hardly conceivable today.

A single click or minor misconfiguration can lead to a major breach. And if your organisation fails to meet the security requirements defined by the insurance provider, your policy will be in jeopardy.

The huge shortage of cyber-security workers is also adding to the problem and means that it will only get worse as the risk can no longer be transferred to the insurance company.

To protect your organisation, satisfy cyber security insurance requirements and ensure rapid recovery if you are breached, security needs to be a continuous process. Companies need to demonstrate that they have taken adequate steps to safeguard their IT infrastructure before they are granted cyber insurance. It's essential to be proactive and implement effective security controls to thwart cyber-attacks. A reactive approach to identifying and responding to a cyber-attack is no longer acceptable and will make it difficult to obtain cyber insurance and put the company at significant risk of financial and reputational damage.

While the prospect of having no cover may be daunting, it perhaps serves as a point of reflection for companies to adequately reassess their own security posture and strengthen it where required. So how can organisations ensure they are operating on the front foot when it comes to cyber security?

IMMUTABLE BACKUP AND DISASTER RECOVERY

One of the essential controls for an organisation is immutable backup and disaster recovery. Backups allow companies to restore their systems and data quickly after a cyber-attack. While immutable backups guarantee that the data is not altered or deleted, even by an attacker with administrative privileges. This ensures that a company can quickly recover from an attack without losing data or compromising the integrity of it.

ENDPOINT DETECTION AND RESPONSE (EDR)

EDR is another control that should be included as part of an organisation's arsenal to reduce cyber risk. EDR technology provides real-time visibility and response capabilities into the endpoints of a company's network. This allows security teams to detect and respond to threats quickly.

MANAGED DETECTION AND RESPONSE (MDR)

MDR is a service that combines technology with human expertise to monitor a company's network and identify potential threats. It provides proactive defence against attacks by detecting and responding to them before they can cause harm.

PATCH MANAGEMENT

A significant proportion of external breaches are due to unpatched vulnerabilities. A poor regime can have catastrophic consequences on systems, personally identifiable information, and intellectual property.

Keeping software and operating systems up to date with the latest security patches is crucial to prevent known vulnerabilities from being exploited by attackers. Patch management as a discipline also plays a crucial role in improving stability and functionality.

ASSET MANAGEMENT

This involves conducting and maintaining an inventory of your network environment and all cyber-enabled technologies including software and hardware. This will help to identify all the technologies that can be hacked. Once you know what devices need to be managed and secured, you can then implement security around them.

MONITOR ADMIN RIGHTS

Linked to asset management should be the continuous and proactive investigation into

privileged accounts. This includes deciding whether old accounts are needed and looking at whether accounts can be restricted or disabled. It also comes down to investigating all the requests for access to certain files and applications and making sure that they are just being accessed by those that need it within an organisation. This action needs no other financial investment beyond the security team's time, but can reduce the attack surface area of an organisation significantly.

SECURITY OPERATIONS CENTRE (SOC)

This is a centralised function for the monitoring of threats in the network. It concerns people, processes and technology to continuously monitor and protect an organisation's assets including intellectual property, personal data, business systems and brand integrity. The SOC team is responsible for an organisation's overall cyber security strategy. It is the central point of collaboration in coordinated efforts to improve an organisation's security posture while preventing, detecting and analysing and responding to cyber incidents.

EMPLOYEE EDUCATION

Employees are your most important line of defence when dealing with social engineering attacks so it's crucial they are aware of the risks. Regular training can help to make complex cyber threat issues understandable for everyone. It's important that staff understand the 'why' behind the instruction to create a security-first culture.

Make security education consistent, give clear advice and make it very accessible, so that people know what to look for and what to do next, rather than decide for themselves. Reward employees when they do something security focussed. Let the reward be seen and continually build to a zero-trust culture.

MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires users to provide more than one form of authentication before providing access to a system or application. This additional layer of security helps to prevent unauthorised access and protects against phishing attacks.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

Businesses are using their imagination – along with practical security consultation – to identify and remediate risk. SOAR is an additional layer that enterprises are exploring as a way of stitching together disparate toolkits that are often labour intensive and require skilful calibration and configuration. For example, it enables you to integrate security, IT operations and threat intelligence tools to achieve a more comprehensive level of data collection and analysis – even across different vendors. This is important as simplifying and streamlining your toolset significantly reduces your likelihood of breach.

SOAR is a great example where companies are really trying to innovate their security posture.

Despite their best efforts, many businesses unfortunately will still be attacked, so having the right business continuity practices in place and cyber insurance will be critical to survival. Cyber insurance can bring peace of mind for organisations. Remember, it's not a case of 'if' but 'when' you may fall victim to a cyber-attack. Cyber insurance can help you recover from external attacks from bad actors as well as oversights from within the business, putting the focus back on the core operations. However, taking a proactive approach to reducing your risk profile will significantly increase your overall security stance – which is a win, regardless of whether you have cyber insurance or not ●

Leyton Jefferies is head of cyber security services, CSI LTD.

If your organisation fails to meet the security requirements defined by the insurance provider, your policy will be in jeopardy

Picture credit: Adobe Stock