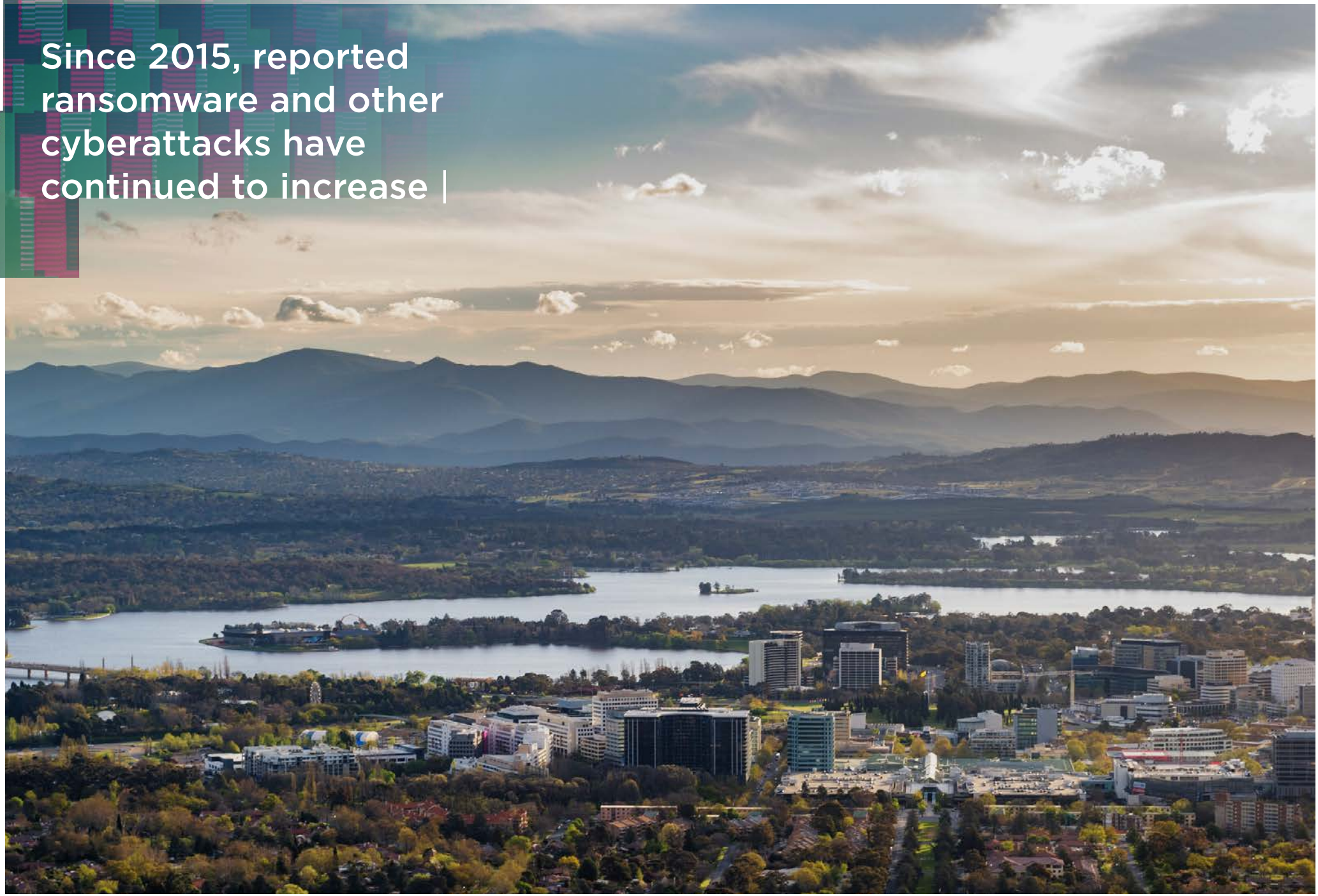
AUCLOUD

How confident are you that you can recover from a ransomware attack? |


Since 2015, reported ransomware and other cyberattacks have continued to increase |

THE RISE OF CYBERATTACKS AND RANSOMWARE

Ransomware and cyberattacks have increased in both scale and complexity in recent years. Each day, media reports detail yet another data breach, cyberattack, or ransomware incident. With experts predicting cybercrime damages could amount to trillions of dollars, implementing a robust cybersecurity strategy is vital in mitigating organisational risk.

IN THE BEGINNING

Although ransomware incidents and cyberattacks may be the scourge of the modern digital age, cybercrime theory, tools, and techniques have been around for decades. The first documented ransomware incident occurred in 1989. The AIDS Trojan, also known as the PC Cyborg virus, used social engineering to infect unsuspecting researchers. Created by a biologist named Joseph Popp, it targeted attendees at the World Health Organisation's AIDS conference. During that event, Dr Popp handed out over 20,000 malicious floppy disks. On infection, the malware embedded itself and lay in wait counting the number of computer restarts. On the 90th restart, it hid directories and encrypted or changed file names on the computer's C drive.

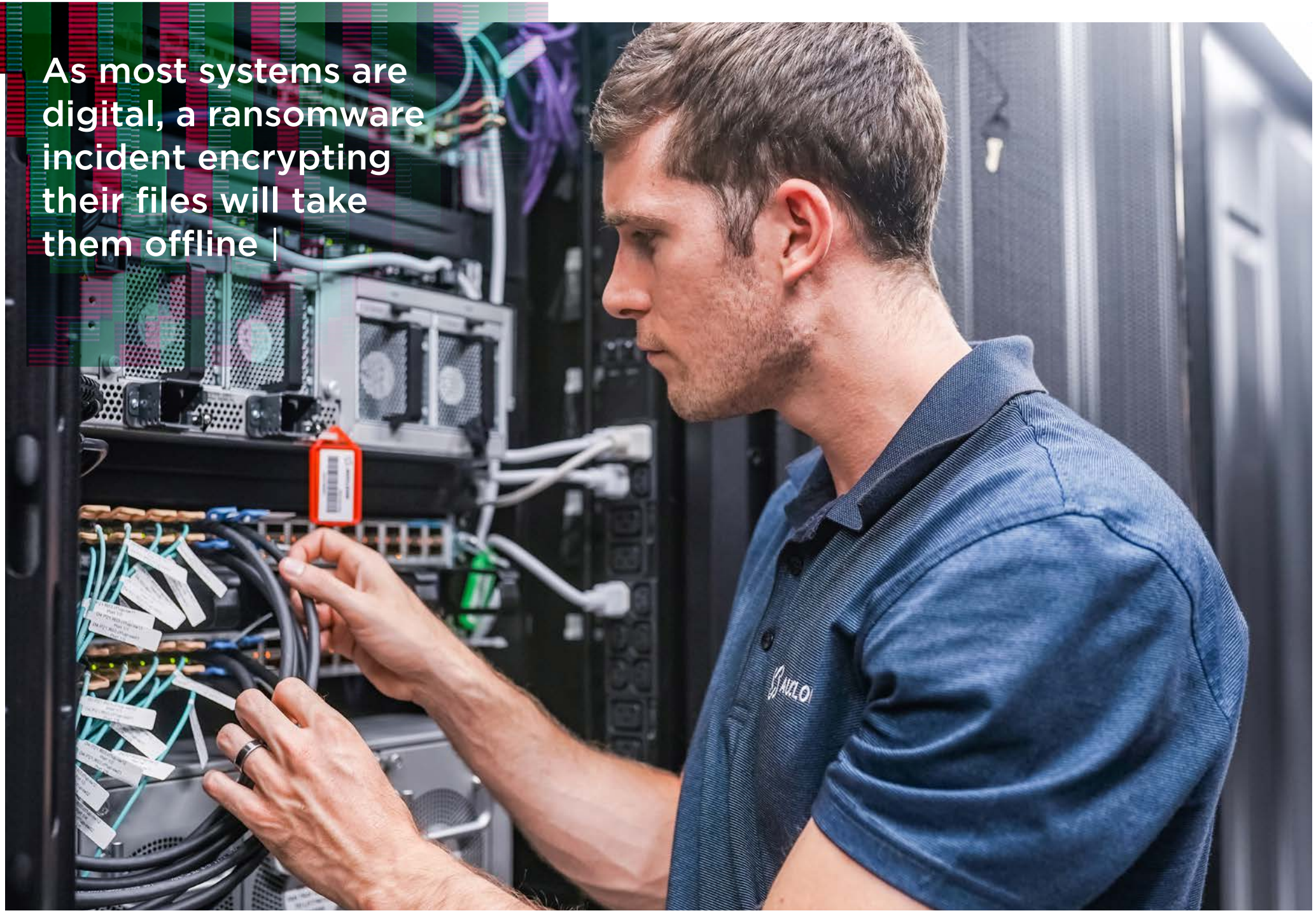
THE NEXT WAVE

In the mid-1990s the world changed. Sir Tim Berners-Lee created the HTTP protocol giving birth to the World Wide Web. Within a few years, organisations and individuals were online. Consequently, as the value of information increased, criminal elements targeted this new hunting ground. Leveraging the age-old human practice of extortion and adapting it to the digital realm, new ransomware variants such as the Archiveus Trojan and GPCode started their malicious campaigns in 2006. However, it was not until 2011 that ransomware became a daily threat to organisations and individuals everywhere. In Q3 of that year, security companies and malware researchers identified over 60,000 ransomware variants. This more than doubled in twelve months to over 200,000. By Q1 of 2015, there were over 700,000 ransomware variants.

THE MODERN ERA

Since 2015, reported ransomware and other cyberattacks have continued to increase. With organisations embracing digital transformation fuelled by the exponential consumption of cloud and mobile services, the amount of data created and stored by organisations and individuals mushroomed. In 2019, the Information Overload Research Group reported that online users generated over 90% of the world's data in the preceding two years. This explosive growth naturally drew the attention of criminal elements.

In addition to the dramatic surge in malicious code, a disturbing trend that has emerged with ransomware attacks in recent years is the additional danger of attackers threatening to leak stolen information. Information extracted before deploying the ransomware attack's encryption phase increases the potential harm for organisations considerably. Not only do they now need to contend with the operational fallout of inaccessible systems and data, but they also need to grapple with the repercussions of a data breach.


As most systems are digital, a ransomware incident encrypting their files will take them offline |

WHY ARE ORGANISATIONS VULNERABLE TO RANSOMWARE?

As organisations leverage digital platforms to communicate, operate, and compete in the economy, there is intrinsic value in the information they create. A data breach resulting in unauthorised access to this information would be damaging. Reputational harm and public liability are two potential consequences as well as the risk of punitive fines and criminal charges as many countries enact legislation to protect their citizens' private information.

Over and above the intrinsic value of data, organisations also risk a catastrophic impact on operations. As most systems are digital, a ransomware incident encrypting their files will take them offline. Should an enterprise store all its information in a central location, it also exposes them to the risk of a single point of failure.

THE IMPACT OF WORK FROM HOME

A significant factor in increasing the scale and reach of ransomware incidents in 2020 was the dramatic rise in people working from home due to the Covid-19 pandemic. Even though the number of employees or devices may not have increased, the complexity created by work from home was an additional security burden for IT. As employees left their corporate networks, criminal elements took this opportunity to launch attacks. With devices and corporate data not residing behind the corporate firewall, home networks and weakened security proved a tempting target to ransomware gangs. These criminal elements capitalised on the distributed workforce's larger attack surface. The added benefit of not needing to deal with enterprise-grade security made it easier for them to gain the foothold they needed to launch their attacks. Analysis conducted illustrates this, with Bitdefender's Mid-Year Threat Landscape Report 2020 claiming a 715% year-on-year increase in detected ransomware attacks.


A layered security posture is a good defence against potential attacks, there are instances where criminals have managed to circumvent these precautions |

PREVENTING AND MITIGATING AGAINST A RANSOMWARE ATTACK

Preventing and Mitigating Against a Ransomware Attack Organisations have typically mitigated the risk of ransomware by adopting a defence-in-depth cybersecurity strategy. Configuring and implementing a layered security approach should diminish both the threat and the impact of an incident. For example, subscribing to a mail and web filtering service reduces the potential attack vector of a phishing attack. Endpoint protection aims to prevent the execution of any malicious code. As hackers infiltrate networks using guessed or stolen login credentials, hardening security with multi-factor authentication (MFA) is another measure organisations have chosen to adopt.

However, the traditional first and last line of defence against ransomware is restoring data from a backup. When all preventative measures fail, and organisations end up with encrypted data, recovering vital information from a backed-up copy has always been the final fallback position.

TRADITIONAL MEASURES MAY NOT BE SUFFICIENT

Although a layered security posture is a good defence against potential attacks, there are instances where criminals have managed to circumvent these precautions. For example, running unsupported legacy applications with unpatched vulnerabilities can allow attackers unauthorised access to the most hardened network. Implementing network and security monitoring solutions is a step in the right direction. However, if the enterprise does not configure it correctly or act rapidly and decisively on alerts, the platform is ineffective against any attack. Anti-malware solutions do not provide any guarantees either. Most of these systems defend against malicious software by comparing some data to a sample it has in its database. If the ransomware is a previously undiscovered variant, anti-malware will not flag it, and it can enter the network unimpeded.

Even backups are not infallible. Ransomware gangs know that organisations will roll back to their last known good state to mitigate an attack. Advanced ransomware circumvents this control by attacking an organisation's network as the military would invade an enemy country - with a specially crafted strategy.

Targeting backups first, a ransomware gang can ensure the organisation has no fallback position.


Mitigating a ransomware threat requires the implementation of preventative measures at every phase of the attack. |

THE KEY REQUIREMENTS OF A RANSOMWARE MITIGATION SOLUTION

The four phases of a ransomware attack

A tailored ransomware cyberattack typically involves four distinct phases: infection, dissemination, extraction, and detonation. During infection, the malware gains exploits vulnerabilities to access to an organisation's network.

Once infected, the malware then moves into dissemination. It spreads by looking for poorly secured data to encrypt - including backups. During extraction, the ransomware agent extracts data the attackers can use to extort their victims further. Finally, during the detonation phase, the malware activates its malicious payload and encrypts all the information it can access. If the malware has found and targeted backups, there is no last line of defence. The organisation would be at the mercy of the cybercriminals.

Aligning measures with the four phases

Mitigating a ransomware threat requires the implementation of preventative measures at every phase of the attack. This layered, defence-in-depth approach protects the organisation by enforcing security at every possible malware infection, dissemination, or extraction point.

Prevention

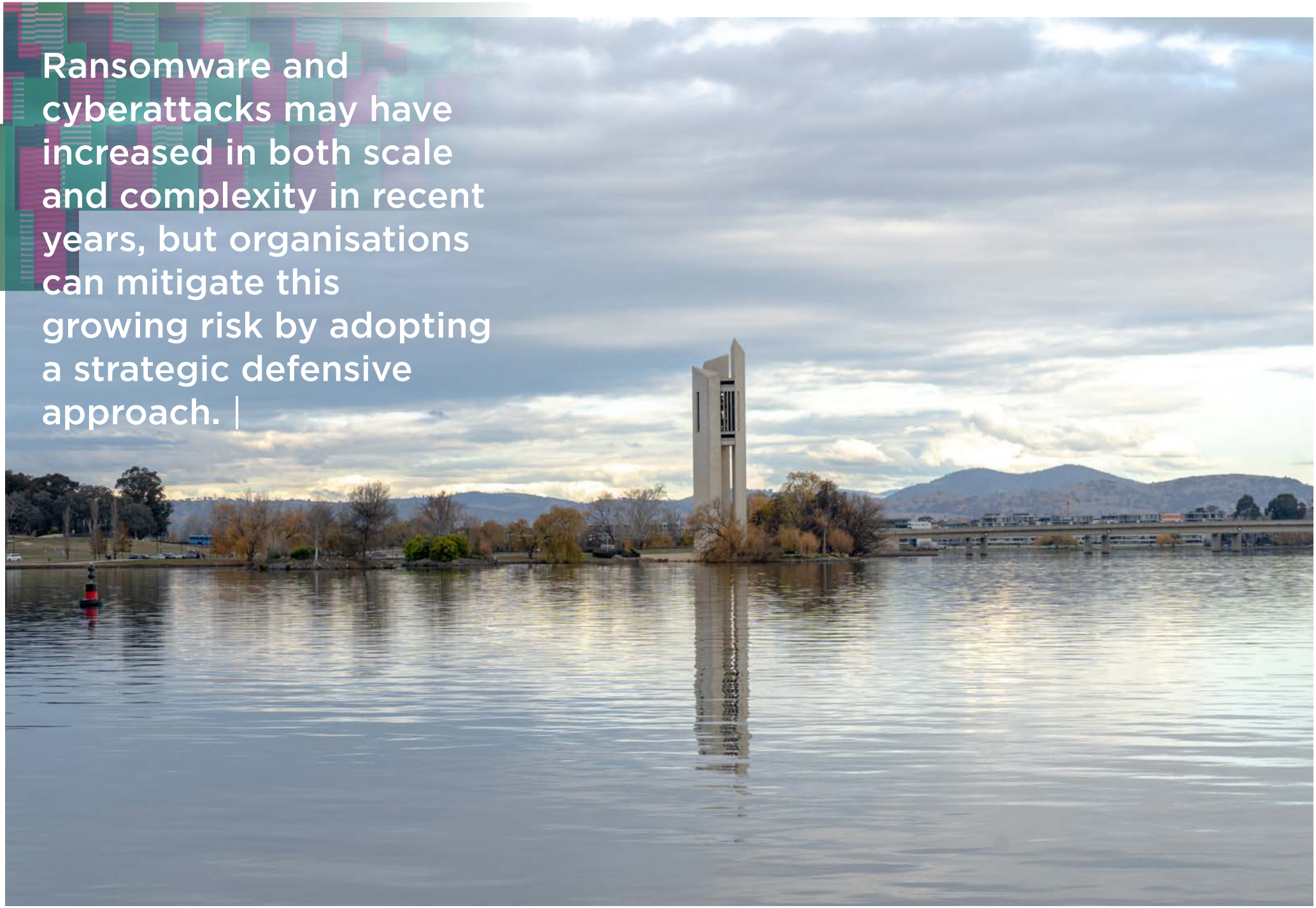
Preventing malware before it can infect a network must be the primary objective. Configuring a robust identity and access management solution with MFA can prevent unauthorised access. Patching applications and not operating unsupported legacy applications mitigates the risk entry via an exploit. Security awareness training to minimise the risk of social engineering attacks, like phishing, can also help prevent ransomware infection.

Zero Trust

Should preventative measures fail, organisations can fall-back to internal control measures to prevent the ransomware disseminating. Implementing a Zero Trust architecture that deems every network, person, workload, and device as untrusted, provides a framework for controlling access to data. As the traditional network perimeter is no longer the sole protective defence, with work from home being a good case in point, the Zero Trust model provides a sound data protection framework.

Protect Your Backups First

Traditionally, data backups have been the last line of defence against ransomware. As we have learnt, campaigns target backups so that organisations do not have a fallback position. Subscribing to an immutable backup service is a security measure that protects backups from ransomware. It permanently secures the state of the data so that no process or individual can modify it. This preventative measure ensures that an organisation can safely recover its information should it fall victim to a ransomware attack.



Ransomware and cyberattacks may have increased in both scale and complexity in recent years, but organisations can mitigate this growing risk by adopting a strategic defensive approach. |

DATA SOVEREIGNTY AND ONLINE BACKUPS

Cloud-based backups offer a secure, offsite capability to organisations. However, as the enterprise is effectively storing their data on an external platform, companies must also consider data sovereignty. In Australia, the Australian Cyber Security Centre (ACSC) and their Cloud Assessment and Authorisation Framework (CAAF) delineates the relationship between Cloud Consumers and Cloud Service Providers (CSPs). The CAAF highly recommends a rigorous risk analysis of a range of commercial, security and capability factors in advance of using a specific CSP. It explicitly calls out the risks of CSPs that are not owned, based and solely operated in Australia.

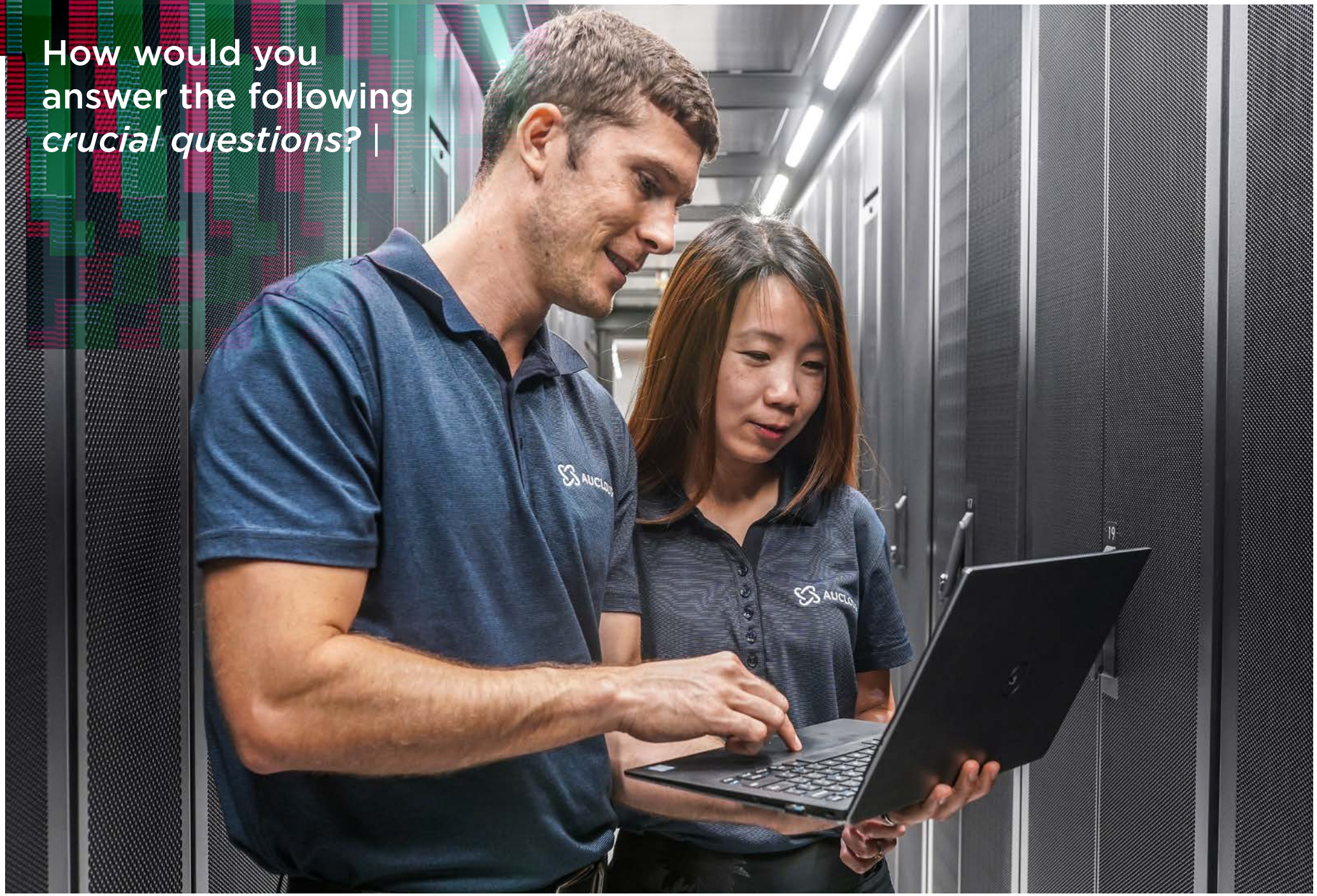
These CSPs are less likely to align to Australian standards and legal obligations and, unlike sovereign CSPs, more susceptible to extrajudicial control and interference by a foreign entity. Given the priority for data security and privacy, the CAAF requires that the additional risks associated with foreign-owned CSPs, including those located in Australia, are considered as part of the overall risk posture when assessing all cloud providers.

CONCLUSION

Ransomware and cyberattacks may have increased in both scale and complexity in recent years, but organisations can mitigate this growing risk by adopting a strategic defensive approach. A core component of this strategy should be the implementation of immutable backups – in a sovereign environment. Immutable backups permanently secure the state of the data so that no process or individual can modify it. Ensuring backup data is hosted in a sovereign cloud provides additional assurance that stored data (and the metadata, derived analytics, and support data etc associated with it) always remains in Australia.

Adopting these simple practices ensures the recoverability of valuableinformation in the event of any cyber event, including a ransomware attack.

How would you answer the following *crucial questions?* |



CRUCIAL QUESTIONS –

CAN YOU ANSWER THESE?

1

Are you confident that the security solution your organisation uses protects your data from Ransomware attacks?

Even if you use the most up to date security solution, such as endpoint protection, you may still be vulnerable. Employees that operate outside the corporate firewall increase this risk considerably. Traditionally, these workers have been targeted and are the most likely entry point for attacks.

Studies show that 75% of companies hit by Ransomware attacks use appropriate and up to date endpoint security software. During the 2019-2020 period, estimates are of a 715% growth in ransomware attacks, likely linked to the increasing number of remote workers.

Addressing this risk requires shifting from a focus on peripheral endpoint security to protecting the data after the network is penetrated - a shift broadly supported by industry experts.

◯ Yes ◯ No ◯ Unsure

2

If a ransomware attack penetrates your network, how confident are you that your data and your customers' data is genuinely safe?

Ransomware attacks can locate and encrypt both your production and backup data promising to provide the encryption key once the victim pays the ransom.

Forrester reports that creating an 'immutable' backup of your data that cannot be modified or deleted by anyone, even your administrator, is the 'last bastion of defence' in protecting against ransomware attacks. Knowing that backups are increasingly the target of hackers, typically attacked prior to disabling production data, protecting backup copies is vital in a modern ransomware solution.

◯ Yes ◯ No ◯ Unsure

3

Does your company host sensitive or valuable data (e.g., government, personal, healthcare, financial, legal, etc.)?

These organisations and data types are regarded by 'attackers' as 'high return' data targets.

Government, educational and financial institutions, healthcare organisations, and legal firms are among the ransomware attackers' top targets. They attract both higher instances of attack and higher ransom demands – sometimes demanding as much as ten times the average ransom. It is the reason why having a truly protected (immutable), backup copy is imperative.

◯ Yes ◯ No ◯ Unsure


AUCLOUD


AUCLOUD