WHITE PAPER

GOAGILE.COM

Top tips for increasing cyber risk resilience

By James Crowther

GO AGILE

AGILE. Coverholder at LLOYD'S

AGILE.

Coverholder at LLOYD'S

Contents

Go AGILE

Cyber crime is big business

Hackers, spammers, bots and malware, including ransomware, are a threat to the integrity, availability and confidentiality of digital information.

Research by cyber security training provider DDLS found 7 in 10 businesses surveyed expect data breaches and cyber security to be their company's top IT priority. DDLS found about 60% of targeted attacks were on small-to-medium enterprises (SMEs).

In 2020, the Federal Government released Australia's Cyber Security Strategy 2020, pledging $1.67 billion over the next decade towards cyber safety. It said the Australian Cyber Security Centre (ACSC) responded to almost six cyber security incidents each day in the year to 30 June 2020.

DDLS's Australian Institute of ICT says global cybercrime is expected to cost $US6 trillion in 2021, double that of six years ago. In Australia, the annual estimate is $29 billion.

The Acronis cyber threats report shows the most commonly exploited applications globally are:

- Microsoft Office (74.83%)
- Internet browser (11.06%)
- Android (8.7%)
- Java (3.12%)
- Adobe Flash (1.54%)
- PDF (0.74%)

The Covid-19 pandemic, and accompanying and continuing trend for workforces to be offsite, has prompted an increase in due diligence for underwriting risk in the cyber portfolio.

The increase in remote workforces, coupled with more strident efforts from the perpetrators of cyber crime (threat actors), mean the threat landscape is shifting dramatically.

Basic security measures are no longer sufficient. Ransomware is now sophisticated enough to bypass minimal security so advanced protection is essential.

(and it's not just big business at risk)

The BDO and AusCERT annual cyber security survey identifies industry trends across private and public SMEs in Australia and New Zealand. The 2020 survey, published in March 2021, highlights that "to effectively manage cyber security threats and risks, organisations must understand where the threat is coming from, which assets adversaries are seeking to compromise, and the methods they'll use to do so. Without appropriate cyber threat intelligence, organisations risk ... exposing themselves to threats and risks without the resilience required to manage their impacts".

> **Seven in ten businesses surveyed expect data breaches and cyber security to be their company's top IT priority.**

BDO-AusCERT say cybercriminals are changing tactics and increasingly stealing sensitive data and threatening to disclose it unless a cyber ransom is paid. The technique is sometimes coupled with ransomware, known as 'double ransom', and an increase in those types of attacks is expected during the next 12 months.

Based on all respondent data, cyber attacks via supply chain are now more than 50% more likely than they were in 2016 when BDO-AusCERT conducted the first survey. State sponsored attackers remain active, with attacks rising 40% since 2019 and doubling since 2016. For public sector respondents, 30% indicated that state sponsored attacks were the most likely source of cyber security incidents during the past year.

Diligent, iterative risk management is the key means by which organisations, large and small, can keep the threat at bay. In addition to basic cyber security measures typically utilised, these four key factors are important to implement:

- Continuous cyber awareness training for employees
- Multi-factor authentication
- Data backup procedures
- Advanced endpoint protection.

This whitepaper explores these options and explains how they can assist in keeping your business cyber safe.

Continuous cyber awareness training

There is a well-developed marketplace for cyber awareness training providers. Services available include video training and simulated attacks to test organisations' depth of knowledge and responsiveness.

It can take just one phishing attack to wreak havoc.

Training provider KnowBe4 has developed a free phishing security test to find out what percentage of your employees are "phish-prone". Phishing occurs when a threat actor fraudulently attempts to obtain sensitive information or data by impersonating a trustworthy entity in a digital communication.

KnowBe4 also has created an Automated Security Awareness Program (ASAP) that enables organisations to create customised security training programs that include actionable tasks, helpful tips, courseware suggestions and management calendars.

Insurance brokers, as trusted risk advisers to their clients, need to alert them to the need for continuous training, which should include all employees, plus contractors.

It is likely underwriters will soon make resilience training mandatory for obtaining cyber risk insurance policies. It might be annual for SMEs, but quarterly for larger enterprises where the financial risk is greater.

> **Threat actors target organisations of all sizes, but appreciate that the larger the entity under attack, the higher their "prize pool" might be.**

It is vital to measure the success of your awareness training. Simulated phishing attacks help employees understand how to avoid them and provide stark reminders if they don't avoid the bear trap. Picture a pop-up on your screen with the words "You failed".

Most reputed training courses have high pass marks and employees must keep training until they achieve the pass mark.

Multi-factor authentication

Multi-factor authentication (MFA) is one of the most effective ways to protect against unauthorised access to your valuable information and accounts.

It is a security measure that requires two or more proofs of identity to grant you access.

The Federal Government's ACSC, explains it well: "MFA typically requires a combination of something the user knows (pin, secret question), something you have (card, token) or something you are (fingerprint or other biometric)."

MFA options include physical tokens, random pins, biometrics or fingerprints, authenticator apps, emails, and SMS messages.

ACSC provides useful guides to implement MFA on Facebook, Apple, Microsoft and Gmail platforms.

However, implementing MFA is not always achievable, particularly as automation can make systems more complex.

Remote desktop systems can be particularly vulnerable. Malware can be embedded into bring-your-own devices (BYOD) and can easily bypass less-secure networks, making it easy for threat actors to login and extract data.

Remote Desktop Protocol (RDP) is a built-in part of the Windows toolkit popular for facilitating remote work access. With a shift to remote working during the Covid-19 pandemic, cyber criminals have taken great interest in compromising RDP endpoints as they provide direct access into a victim's environment via a graphic interface.

Statistics from Coveware, a company that provides ransomware incident response and negotiation services, firmly ranked RDP as the most popular entry point for ransomware incidents it has investigated.

Businesses should have active discussions with their IT providers about RDP and consider whether it is completely necessary for operating the business. If it is, implement these best practices:

1 Ensure the RDP is not internet-facing but protected behind a virtual private network (VPN) service.

2 Use strong passwords: Do not use default credentials, passwords that are the same as the username, or other passwords that are simple to guess. Brute force attacks due to weak passwords have resulted in numerous breaches of RDP environments.

3 Patch your systems: Ensure the latest security patches are deployed and your business has a patch management policy in place.

4 Enable MFA: Whenever possible, enable MFA to ensure an additional layer of protection exists for your business.

Microsoft now makes it easy to add MFA to your Windows Remote Desktop. Many RDP environments also use third-party MFA solutions, particularly if their Windows edition does not support MFA for RDP.

Data backup procedures

Everyone backs up their data regularly, right? Let's assume most do. But, even those that do, frequently fail to ensure the integrity of the data.

How often does your organisation check data to ensure back ups are not corrupted. It's not just a question of how often you back up. How often do you test the integrity of the backup data?

Organisations need to develop recovery-time objectives. What if it takes a week to restore your data?

Is your backup 'air-gapped'? The backup must be separate from the corporate network to avoid malware breaching the network and infecting the backup as well as your storage area.

You need to backup all data that is essential to operating the organisation. Here are a range of options to help ensure business continuity if your main network is compromised:

- Use remote storage – off-site or at least off-server storage is essential. You can use cloud-based servers, portable hard drives, USB sticks, or dedicated servers, but maintain the distance to enable data recovery.
- Backup often and regularly – set a schedule (minimum daily) and test your system's integrity to ensure the backup has occurred as planned. For critical data, consider a continuous back-up solution.
- Determine your retention span – you can't keep backups forever, so set a schedule that works best for your business. There may be industry standards or regulatory requirements about data retention that must be followed, for example, for financial institutions. Ransomware can remain undetected in your network for some time, waiting to detect mission-critical data to encrypt, and it can infect backups.
- Encrypt and protect your backups – this provides an added layer of security. Consider redundancy, which in an IT sense means duplicating critical components or functions of a system to increase reliability.
- Use multiple backup solutions – this will multiply your chances of recovering data quickly and efficiently if a disaster strikes. The 3-2-1 backup strategy is a method of organising your backups securely. 3-2-1 means having three separate copies of your data stored on two different kinds of media, with at least one copy stored off-site. 3-2-1 means even if one copy of your data is damaged, there are always other, safe ones. You can implement the strategy manually by using cloud storages and hard drives or use a third-party backup tool that follows 3-2-1 best practice.

Advanced endpoint protection

Traditional, reactive endpoint security tools, such as firewalls and anti-virus software, depend on known threat information to detect attacks.

And that's a good starting point. Every system should scan for worms, Trojan horses, ransomware and other types of malware than can infect systems.

But advanced technologies go deeper by using more proactive technologies, such as machine learning and behavioural analysis, to identify potential new or complex threats.

Advanced endpoint protection (AEP) can isolate and shut down threats quickly and prevent them moving to another device on the network. An infected device can be restored before damage infiltrates deeply into an organisation's systems.

AEP protects a network by securing endpoint devices, like laptops, tablets, smart phones, and other wireless devices that connect to a larger network. These devices often introduce new entry points for hackers to exploit.

AEP supplements existing security software to secure endpoints against known and unknown attacks before they can compromise a system. Most AEP products typically offer integrated solutions with anti-malware, personal firewalls, and port and device control.

As businesses adopt new strategies to increase cost-effectiveness, like cloud security services and workplace policies like BYOD, which govern how employees' personal devices can connect to corporate networks, endpoint devices can become targets for hackers to infiltrate network systems.

Software security provider McAfee says AEP can include several, or all, of the following technologies or capabilities.

Machine learning is a category of artificial intelligence that analyses large amounts of data to learn the typical behaviours of users and endpoints. Machine learning systems can then identify atypical behaviour and alert IT staff or trigger an automatic security process, such as containing the threat, quarantining the endpoint or issuing an alert. Machine learning is a key way to identify advanced threats against endpoints, and new or zero-day threats. (A zero-day threat is an attack that exploits a weakness a vendor or developer was unaware of. The name comes from the number of days a software developer has known about the problem.)

Security analytics tools record and analyse data from endpoints and other sources to detect potential threats. Security analytics can help IT professionals investigate security breaches or anomalous activity and determine what damage may have been done. IT departments can use security analytics to understand what vulnerabilities may have led to a breach and the actions IT can take to prevent future attacks.

Real-time threat intelligence – Advanced security has the ability to use real-time threat intelligence from outside security vendors and agencies. Real-time updates on the latest types of malware, zero-day threats, and other trending attacks reduce the time from first encounter to threat containment.

Examples of intelligence feeds are:

- The Cyber Threat Alliance, an independent organisation whose members share cyber threat information in near-real time.
- VirusTotal, an Irish security site that aggregates data from online scan engines and anti-virus products.
- McAfee Global Threat Intelligence, a service that develops reputation scores for billions of files, URLs, domains, and IP addresses.

IoT security – Smart, connected devices, such as industrial controls, medical imaging systems, office printers, and network routers, are ubiquitous. Many internet of things (IoT) devices lack security and are vulnerable to cyber attacks. A single unprotected device can provide a hacker entry to an entire network.

For industrial controls, a vulnerable device can enable an attacker to cripple key systems, such as electricity grids. Security solutions for these emerging endpoints may include white-listing to block unauthorised software or IP addresses and file integrity monitoring to scan for unauthorised changes to configurations or software.

Endpoint detection and response – EDR is not new technology, but it is more important today as threats increase in sophistication. EDR continuously monitors for suspicious endpoint or end-user behaviour and collects endpoint data for threat analysis. EDR solutions may provide automated response features, such as cutting off an infected endpoint from the network, ending suspicious processes, locking accounts, or deleting malicious files.

AEP is a critical element of IT security, because any endpoint – whether a desktop PC, a printer, or an industrial control – is a potential gateway into a network.

Conclusion

You can never protect against everything, but the more secure you are, the better your chances of recovery if disaster strikes.

Reducing the risk means a better price on your cyber insurance. As the threats increase, Agile Underwriting's risk selection includes increased due diligence and a greater understanding of potential insureds' business and cyber security practices.

Agile Underwriting conducts deep-dive audits into clients' business operations to identify areas of vulnerability and suggest remediation.

In high-risk areas, we take a mature approach to eliminating 90% of the risk and developing a premium for the other 10% that remains potentially vulnerable.

Implementing these four key factors can make a major difference in keeping your business cyber safe:

- Continuous cyber awareness training for employees
- Multi-factor authentication
- Data backup procedures
- Advanced endpoint protection.

James Crowther

Head of Cyber and Emerging Risks
Agile Underwriting

James is a highly innovative cyber risk and governance specialist, with experience spanning two decades in cyber and risk management, and commercial portfolio management gained at Lloyd's of London. His specialisations include risk review and assessment, raising cyber resilience awareness, and working with key stakeholders to ensure enterprise cyber security risks are well understood and managed.

Building on his career at Lloyd's, James has progressed to lead multiple cyber insurance start-ups in Australia, gaining experience in pre-risk identification; post-risk response services; data breach response framework development; cyber risk identification; impact assessments' crisis management; risk mitigation; public relations; and business continuity planning. James is an acknowledged industry specialist on cyber insurance, dealing with IT security incidents and data breaches effectively. He is regularly sought to provide an industry focus and his views.

~~Admin.~~
~~Proposal forms.~~
~~Busy work.~~
~~Spreadsheets.~~
~~Capacity.~~
~~Policy wording.~~
~~Digital payments.~~
~~Claims.~~
~~Regulations.~~
~~Reporting.~~

AGILE.

Coverholder at LLOYD'S

Go AGILE

and move from proposal to policy without the grind.

AGILE takes care of the admin, capacity, policy wording, claims, and more, leaving you to nurture your client relationships.

Go AGILE

Want to do more with less?

Go AGILE by getting in touch with us at:
hello@agileunderwriting.com

Agile Underwriting Services Pty Ltd
Level 5, 63 York Street, Sydney, NSW 2000
www.agileunderwriting.com
ABN 48 607 908 243   AFS Licence No. 483374

Coverholder at LLOYD'S