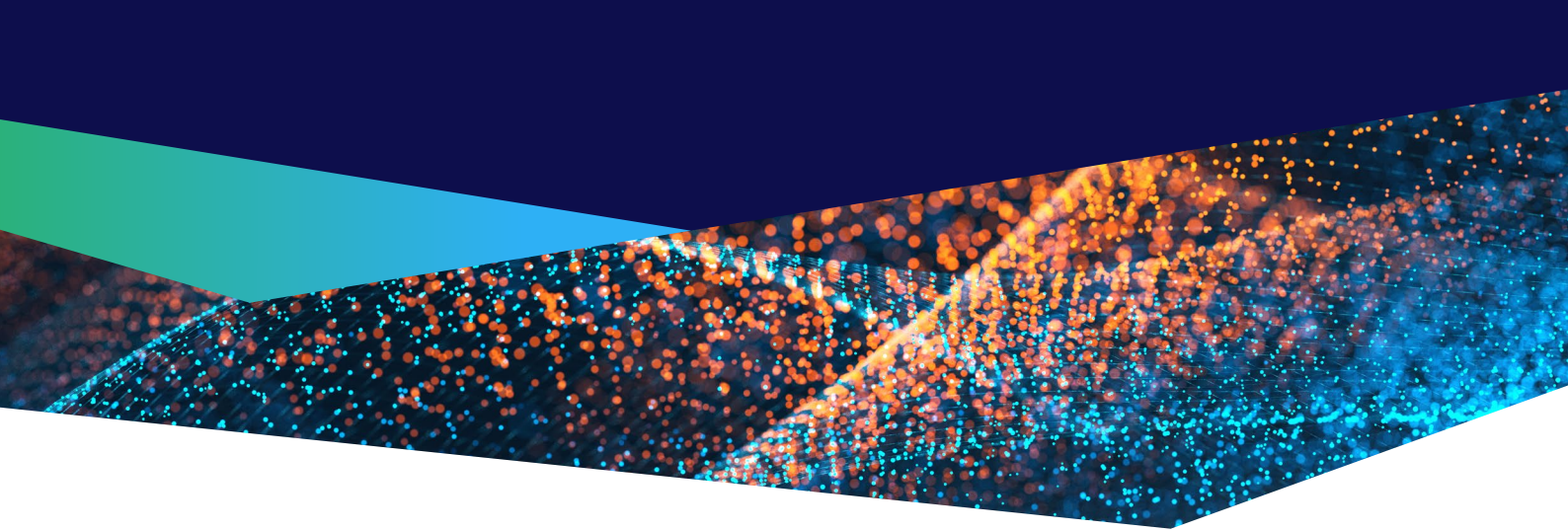


How to implement a successful cybersecurity strategy in an interconnected environment





Organisations are rapidly digitally transforming, and in most cases, the result is more productivity, flexibility, and resilience. As environments become more interconnected, team members can operate faster, collaborating more effectively for stronger business outcomes. However, as the number of interconnected devices increases within organisations, so too does the cybersecurity risk. Cyberattacks should now be considered a near certainty for organisations. As such, cybersecurity is no longer the responsibility of the IT team. It is now a critical board-level issue and a case of not 'if', but 'when' an attack will occur.

Digital assets and data are highly valuable to organisations, determining their ability to compete effectively. These assets and data are also extremely desirable to cybercriminals looking to sabotage operations, steal information for monetary gain, or lock up data and assets in so-called ransomware attacks. If an attack or data breach of any kind is successful, organisations could face significant financial losses and disruption, as well as reputational damage. As such, businesses need cybersecurity that underpins their daily operations and protects them as they digitally transform.

Not all cybersecurity solutions are alike. It's important for organisations to choose a solution that will map to their threat profile and risk appetite. Since security budgets are often limited, getting this decision right can have far-reaching impacts as the business continues to transform into the future. It's essential to work with a trusted provider who will support the organisation and deliver strategic, pragmatic advice relevant to the specific business requirements.

It's important for organisations to choose a solution that will map to their threat profile and risk appetite.

As a starting point, there are four outcomes that organisations must demand from their cybersecurity solutions:

1. Email threat protection with multiple layers of defence

Too many people inadvertently click on links or follow email instructions without realising they have fallen victim to a social engineering attack. Cyberattackers can use the information they gather from these users to mount additional attacks such as ransomware, or trick users into paying fraudulent invoices or transferring funds to the attacker's account. They can use the credentials they obtain through this method to access more corporate systems and even bank accounts.

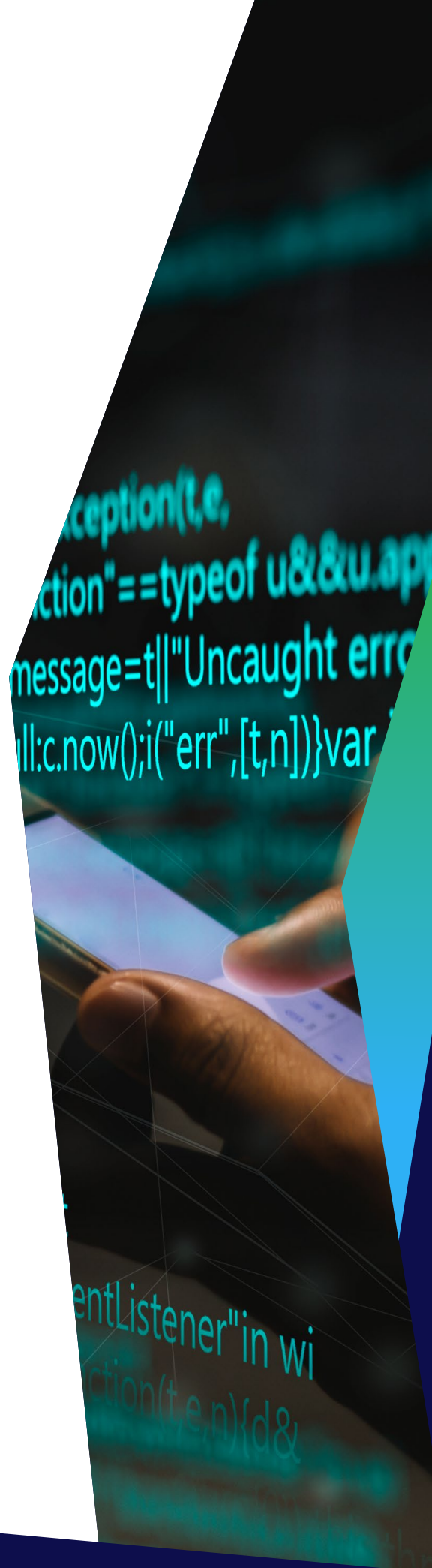
According to the Australian Cyber Security Centre (ACSC), phishing and spear phishing remain the most common attack methods. The ACSC's Annual Cyber Threat Report revealed that malicious emails (the vector for phishing and spear phishing attacks) accounted for 27% of all cybersecurity incidents in the past year.¹ While it's essential to educate staff members on what to look out for when it comes to malicious emails, an email threat protection solution can stop these threats in their tracks by preventing them from being delivered to staff members in the first place. Businesses should look for a solution that combats malware, viruses, spam, phishing, and advanced persistent threats.

2. Advanced threat reporting

Cyber threats are an unfortunate reality of doing any form of business online. Threats can come from inside or outside the organisation, making it difficult to determine where the most significant risk may lie. Advanced threat reporting can provide visibility into threats through threat analysis insights and per-user statistics that determine benchmarks for everyday activity, making it easier to quickly identify suspicious activity.

Early warnings delivered by advanced threat reporting can help stop cyberattacks before they impact the organisation. This avoids the cost and disruption incurred when a cyberattack succeeds and must be remediated.

¹ <https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>



3. A tailored system that covers all the security gaps in the organisation

A strong cybersecurity solution must target all areas of the digital landscape that present a security risk to the business. Often, security gaps go undetected due to a lack of visibility into the network. Last year, cybersecurity researchers discovered more than 800,00 unsecured printers were accessible online. They instructed 28,000 units to print cybersecurity advice, demonstrating the ease with which unsecured devices could be compromised.²

Printers are just one example of connected devices that present security gaps. The more interconnected an environment is, the more potential entry points there are for cybercriminals to exploit. This can include Internet of Things (IoT) devices and sensors and other end-user devices. It's essential to choose a solution that delivers visibility into all corners of the network for a comprehensive security posture.

A defence in depth strategy can overcome security gaps by adding third-party security tools to existing tools, and adding custom policies to these. Defence in depth adds more layers to security and can compensate for weaknesses and even, to some extent, for user error when doing business via email. Defence in depth means that if one tool or strategy fails, another one will be ready to back up that defence.

Last year, cybersecurity researchers discovered more than 800,00 unsecured printers were accessible online.

4. Awareness training for all employees

Studies show that human error accounts for 95% of successful cyberattacks, so equipping staff members with an adequate understanding of cybersecurity policies and procedures must be a priority for any business.³ Regular training programs must be implemented for employees at all levels and should cover external threats as well as internal risks. These training sessions must be consistent and evolve as the business grows. The threat landscape is never static, and the security advice that applies one week may not protect the organisation the following week, so it's essential to be adaptable and responsive to maintain security.

2. <https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/>

3. <https://www.cybintsolutions.com/cyber-security-facts-stats/>

Over the Wire is an industry expert that identifies the best cybersecurity options for organisations operating with highly connected environments. Over the Wire helps businesses remove the complexity of managing and integrating IT and telecommunications security systems so your business can thrive.

If you would like to discuss your organisation's cloud security strategy in more depth, please [contact the team](mailto:contact@overthewire.com.au) today. For more information visit overthewire.com.au/data-security.