ASD Cyber Threat Report

What it means for SMEs in 2024

Introduction

Each year, the Australian Signals Directorate (ASD) publishes a Cyber Threat Report, which discusses the current state of cybersecurity, cybercrime, and cyber resilience in Australia. In this whitepaper, we summarise and analyse their key findings relevant to small and medium enterprises (SMEs).

The full report, published in November 2023, can be found on the ASD's website.[1]

Risk and Impact Continue to Increase

The number of cyber incidents in Australia, and the cost of each incident, are maintaining their upward trend. In FY23, approximately 94,000 cyber incidents were reported to the ASD, a 24% increase from the 76,000 reported in FY22—and a rate of growth that greatly outstrips the growth in operating businesses.

Total Reported Cyber Incidents[2]

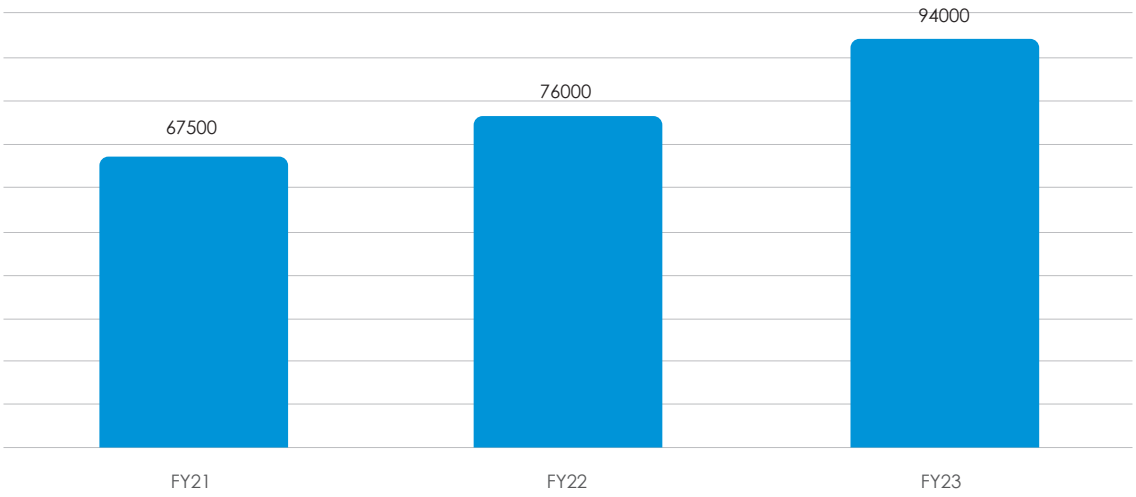


Figure 1: *Total Reported Cyber Incidents*

[1] https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
[2] The ASD points out that this figure only represents reported incidents, and that they suspect the majority of incidents go unreported each year.

The ASD also tracks the average cost incurred by small, medium and large enterprises due to a cyber attack, which continues to increase year on year. In FY23, small businesses saw an average cost per cyber incident of $46,000; for medium businesses, the number was $97,200. This represents an 18% and 10% increase from FY22 respectively.

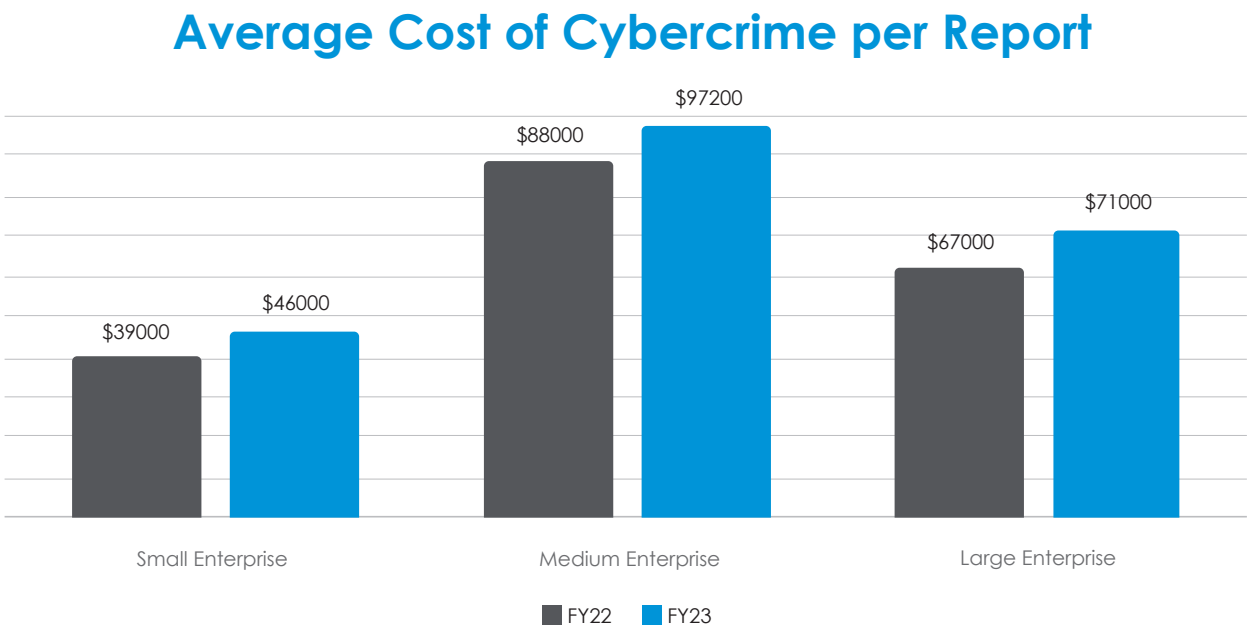


Figure 2: *Average Cost of Cybercrime per Report*

With the growing likelihood of a cyber incident, and the increasing cost when one does occur, cyber risk has never been higher for Australian SMEs.

Growing Threats

While the cost of each incident increases, so does the threat businesses face.

As businesses continue to leverage digital systems and processes, their attack surface grows larger. Cybercriminals and malicious actors look for vulnerabilities to exploit in digital systems. These are known as common vulnerabilities and exposures (CVEs), and are tracked by the US Government via the US National Vulnerability Database. FY23 saw a 20% increase to the number of new known vulnerabilities, from 24,266 to 29,019.

It's important to note that this is the number of new vulnerabilities added to the database in FY23; old vulnerabilities do not expire, meaning cybercriminals' arsenal only grows each year. The ASD noted that in some FY23 incidents, vulnerabilities as old as seven years were being actively exploited.

Number of published Vulnerabilities (CVEs)

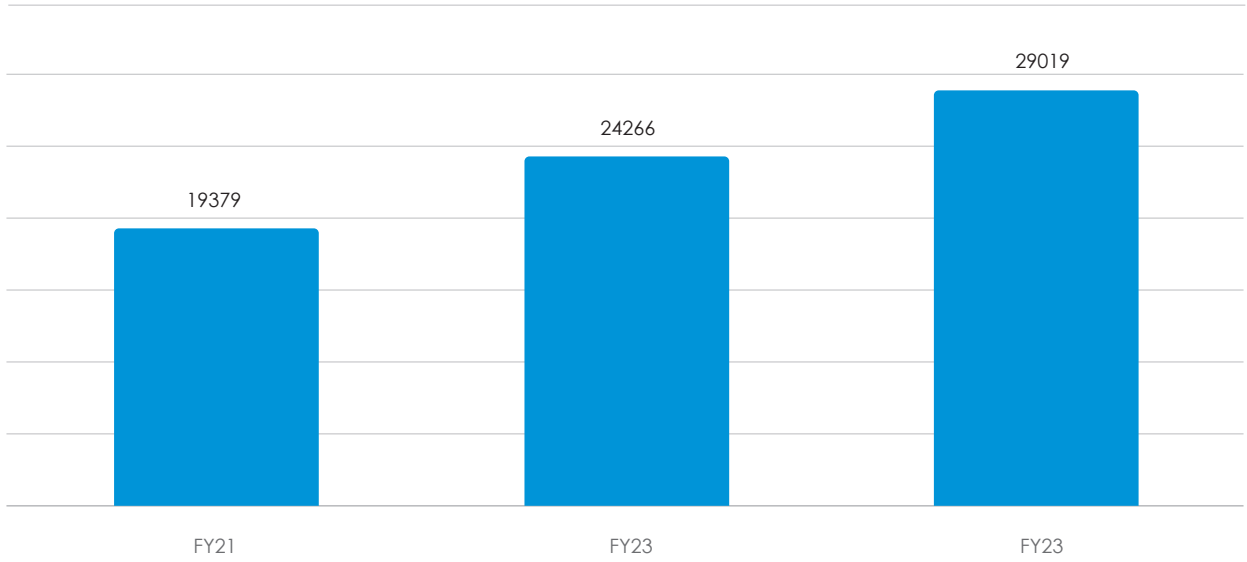


Figure 3: *Number Of Published Vulnerabilities*

Vulnerabilities are typically mitigated through the installation of patches provided by vendors and software developers. Unfortunately, as malicious actors become more advanced, they're frequently using vendor disclosures and patches as signals of a new vulnerability, reverse-engineering them with increasing speed.

The ASD report found that one in five vulnerabilities (21%) are being exploited within 48 hours of patching or mitigation advice being released, and half of all vulnerabilities were exploited within 2 weeks.

Vulnerabilities by Time to Exploit

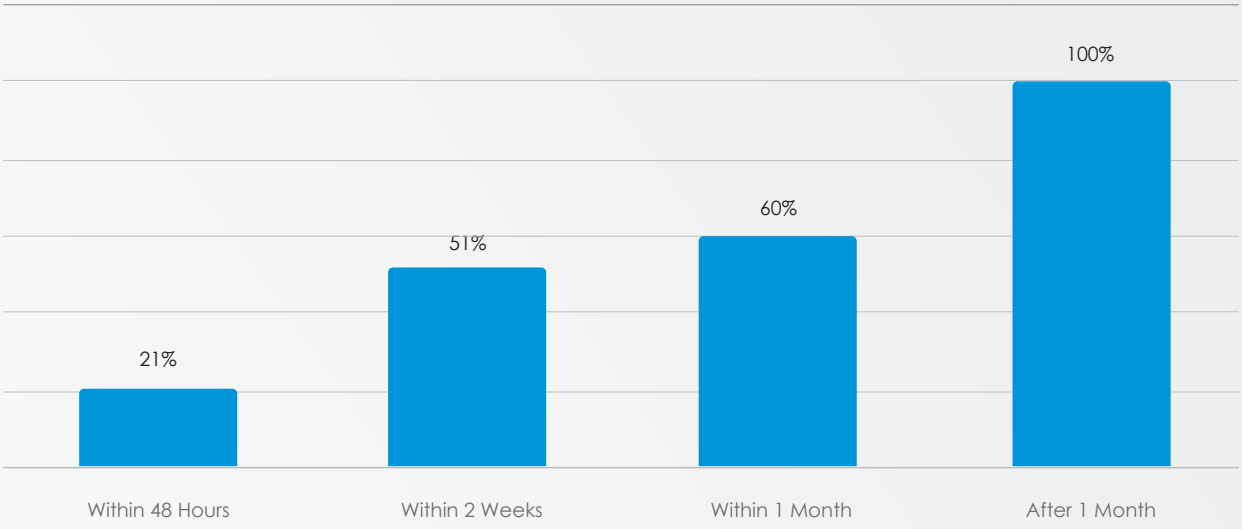


Figure 4: Vulnerabilities by Time to Exploit

Given this alarming landscape, it is more crucial than ever for businesses to prioritise rapid patching of vulnerabilities. The escalating number of CVEs, combined with the sophistication and speed of cybercriminals, means the window for safely implementing these fixes is ever shrinking. SMEs must stay vigilant in monitoring for new vulnerabilities and act swiftly in applying patches. The cost of delay is increasingly high, as older vulnerabilities continue to be exploited. In essence, the speed of response in patching is now a pivotal factor in maintaining cybersecurity and safeguarding digital assets in the modern environment.

Social Engineering Attacks

In addition to technical attacks leveraging vulnerabilities and exploits, malicious actors continue to use social engineering to target employees of Australian businesses. This type of attack opens opportunities for less technically skilled actors by targeting people—which are perceived as easier to exploit than technology.

Phishing

Phishing is an attempt to trick recipients into clicking on malicious links or attachments to harvest sensitive information, like login details or bank account details, or to facilitate other malicious activity.

Phishing continues to be the most widely used social engineering attack, as it allows malicious actors to launch potentially hundreds of thousands of potential attacks at once. Using this scattergun-style approach also allows them to identify the most vulnerable targets to focus their effort on.

Phishing may be used as a precursor to another attack—such as gathering credentials for later use to deposit malware—or as a vector itself, tricking employees to open attachments that contain malware.

Business Email Compromise

Business email compromise (BEC) is a form of email fraud. Cybercriminals target organisations and try to scam them out of money or goods by attempting to trick employees into revealing important business information, often by impersonating trusted senders.

Another form of social engineering is business email compromise (BEC). While less common than phishing, it's often far more lucrative for the malicious actor. BEC exploits trust in business processes and relationships for financial gain; it's often used as part of payment redirection attacks, where employees are tricked into paying fake invoices, or legitimate invoice or salary payments are diverted to bank accounts controlled by a malicious actor.

Australian organisations self-reported more than 2,000 successful BEC attacks in FY23. 'Successful' here means attacks that led to a financial loss, with an average loss per incident of over $39,000.

The best defence against social engineering and BEC attacks, according to the ASD, is to train staff to recognise social engineering attempts. This is best achieved through an ongoing process of training and regular simulated phishing exercises.

Ransomware

The ASD report notes that ransomware continues to be the most destructive cybercrime threat to Australians—and that the tactics employed by malicious actors keep evolving. Whether introduced via a vulnerability, social engineering, or a combination of the two, ransomware attacks can be devastating for businesses, particularly SMEs.

While backups provide a robust defence against data encryption and destruction, most cybercriminals today use data extraction, where they first take copies of data and store it in their own systems. This means they can extort payments by threatening to publish confidential and/or sensitive data.

In addition, due to the lucrative nature of this form of attack, ransomware groups have become more sophisticated and developed a black-market ecosystem. Ransomware-as-a-service (RaaS) offerings have become increasingly common, making these attacks accessible even to low-level criminals. Ransomware groups often operate affiliate programs, where access to a business's network can be purchased through initial access brokers, ransomware is deployed using RaaS tools, and ransom negotiations are handled by a centralised group that leverages its reputation to increase payment rates.

The ASD continues to recommend that Australian businesses do not engage with or pay ransom demands. Instead, it advocates for good cyber hygiene to prevent such attacks, including turning on multi-factor authentication (MFA), implementing access controls, performing and testing frequent backups, regularly updating devices, and disabling Microsoft Office macros.

Ensuring remote work cyber security

With remote work becoming a mainstay of the modern workplace, even an expectation for many workers, the ASD report recommends that all organisations, and especially SMEs, pay special attention to cybersecurity controls in this environment.

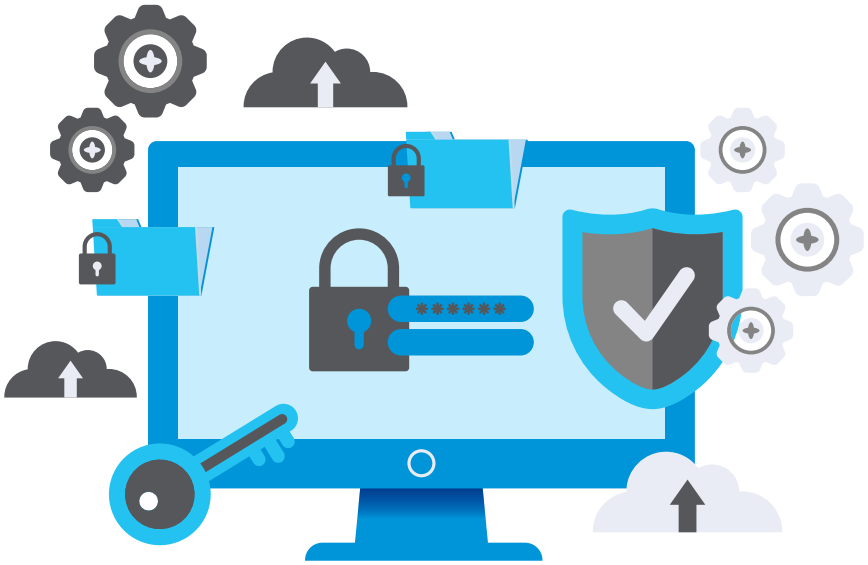
The ability to work from home is often supported by bring your own device (BYOD) implementations, which see employees using their personal laptops, phones and routers to complete work. If not managed correctly, this can introduce significant additional risk to an organisation, particularly when employees' devices store sensitive and confidential data.

In FY23 the ASD helped several organisations recover from extensive corporate network breaches that originated from employees conducting work from compromised personal devices. The report also mentions the high-profile incident suffered by US security company LastPass, which suffered a breach due to credentials being stolen via keylogger malware installed on the home computer of one of its employees.

Conclusion

The ASD Cyber Threat Report for 2023 is a stark reminder of the ever-growing cyber threat to Australian businesses in 2024. The escalating number of cyber incidents, alongside the rising costs associated with these attacks, underscores a critical need for increased cybersecurity awareness and preparedness—especially among SMEs.

The report's key takeaway is the need to invest in strong cybersecurity measures, including technical ones such as cybersecurity software, backups, patching and updates, but just as importantly, training for employees. Any investment in cybersecurity is money well spent, as cyber threat to operations is only set to increase in the years to come.



Contact info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au