The Institute of Certified Bookkeepers
Volume 16 Issue 7
January 2025

Client eBrief

JKM MANAGEMENT SERVICES
HELPING BUSINESSES ASCEND

The Growing Cybercrime Landscape

2023–24 Annual Cyber Threat Report Summary

The 2023–24 Annual Cyber Threat Report highlights Australia's growing cyber threats. Global conflicts, rising tensions in the Indo-Pacific, and advancing technology are providing cybercriminals and state-sponsored hackers with new ways to target governments, businesses, and households. Key risks include espionage, spreading disinformation, and cyberattacks on critical infrastructure.

The Australian Signals Directorate (ASD) is a government agency dedicated to protecting Australia from cyber threats. The ASD monitors electronic communications, defends critical infrastructure, and conducts operations to support national security and military efforts.

In the past year, ASD received over 36,700 calls for help and handled 1,100 cyber incidents. Hackers, often backed by foreign governments like China and Russia, are using advanced tactics to disrupt networks and steal sensitive data. Critical infrastructure such as energy and healthcare are primary targets, as cyberattacks on these sectors can cause widespread disruption.

Cybercrime Continues to Grow

Cybercrime remains a significant threat, with criminals increasingly using advanced tools like artificial intelligence to carry out their operations more effectively. In FY2023–24, common cybercrimes reported in Australia included business email compromise, fraud, ransomware, and data theft extortion. These attacks have led to financial losses, significant disruption, and reputational damage for businesses.

ATO Lodgement Dates

These dates are from the ATO website and do not account for possible extensions.

You remain responsible for ensuring that the necessary information is with us in time.

See ATO Due dates by month to check monthly lodgment and payment dates.

BAS/IAS Monthly Lodgements
Final dates for lodgements and payments:

January Activity Statement
21 February 2025

February Activity Statement
21 March 2025

BAS Quarterly Lodgements
Final dates for lodgements and payments:

2nd Quarter 2025 Financial Year:
December Quarter 2024 (incl. PAYGI)
28 February, 2025

3rd Quarter 2025 Financial Year:
March Quarter 2025 (incl. PAYGI)
28 April, 2025

When a due date falls on a Saturday, Sunday or Public Holiday*, you can lodge or pay on the next business day.

*A day that is a public holiday for the whole of any state or territory in Australia.

Due date for super guarantee contributions:

2nd Quarter 2025 Financial Year:
October to December 2024 – contributions must be **in the fund** by 28 January, 2025

3rd Quarter 2025 Financial Year:
January to March 2025 – contributions must be **in the fund** by 28 April, 2025

Late payments of superannuation are ***not*** tax deductible. If your business has overdue superannuation guarantee payments and you are unsure of how to proceed, please contact us to discuss.

Ransomware: A Growing Threat

Ransomware remains one of the most significant cyber threats, particularly for small and medium-sized businesses. In this form of attack, cybercriminals encrypt data or lock systems, demanding a ransom for its release. Increasingly, attackers are stealing sensitive data and using it for extortion. Businesses that pay ransom do not guarantee data recovery, and often, the attack doesn't stop with one payment.

Small businesses are particularly vulnerable to these types of attacks, as they often lack the resources to implement robust cybersecurity measures. Ransomware can lead to significant financial losses, reputational damage, and operational disruptions, leaving businesses offline and unable to access critical data.

The ASD advises businesses not to pay ransoms, as it doesn't ensure data recovery or prevent further attacks. Instead, the focus should be on adopting strong security measures, including regular updates, secure backups, and proactive threat detection systems.

Cybersecurity Is an Ongoing Effort

Cybersecurity isn't a one-time fix – it's an ongoing effort that requires constant vigilance. Organisations must prioritise replacing outdated systems with secure-by-design products. These are built with security in mind from the start, reducing vulnerabilities. New technologies should be assessed with security as a key consideration. Following industry best practices, such as the Essential Eight, is crucial to mitigating risks. Regular updates and ongoing maintenance are also essential for strengthening resilience. For critical infrastructure organisations, preparing for a cyberattack should be assumed. Every organisation needs a tested response plan, an understanding of its systems, and a plan to recover from incidents quickly.

Reporting Cybersecurity Incidents

If you experience a cybercrime or security incident, it is vital to report it immediately. Cybercrime reports will be referred to the relevant law enforcement agency, while cybersecurity incidents should be reported through the ReportCyber portal.

Cybersecurity incidents can include:

- Denial of Service (DoS) attacks.
- Scanning and reconnaissance.
- Unauthorised access to a network or device.
- Data exposure, theft, or leaks.
- Malware or ransomware attacks.
- Phishing or spear-phishing attempts.
- Other suspicious cyber activity.

When reporting an incident, be ready to provide **indicators of compromise**, **logs**, **network traffic captures**, or other relevant analysis.

How The ASD Can Help

When you report an incident, ASD provides immediate assistance, including advice on how to contain and remediate the issue. They may also connect you with relevant Australian government organisations for further support. In more complex cases, the ASD may deploy a team of digital forensics specialists to assist with technical investigations.

The ASD encourages every organisation and individual who observes suspicious cyber activity, incidents and vulnerabilities to report to cyber.gov.au/report or the Australian Cyber Security Hotline **1300 CYBER1 (1300 292 371)**. ASD provides free technical incident response advice and assistance 24 hours a day, 7 days a week. ASD also offers guidance on managing public communications during an incident to protect the integrity of the investigation.

Source: *Cyber.gov.au – Annual Cyber Threat Report 2023-2024*

JKM Management Services Pty Ltd

Tel: 1300 627 688

office@jkms.com.au | **jkms.com.au | Facebook | Review us on Google**

This newsletter is produced by the Institute of Certified Bookkeepers and distributed by members.