

Cyber Crime Trends 2025

Find Out About The Biggest
Global Trends And How Australia
Is Measuring Up



SOSAFE

Europe's largest Security Awareness & Human Risk Management player

...now in Australia!



HOUSE OF FRASER
SINCE 1849

SOS CHILDREN'S
VILLAGES



ADAC

DeepL



DAIMLER
TRUCK

Huel®

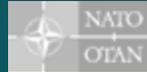


HITACHI valiant

MoëtHennessy

SCHÜCO

hagergroup



Miele

CANYON

WAGO

CLARK

STIHL®

s.Oliver

Serge Ferrari



GROUPE
LEDUFF

vodafone

BESTSECRET

Atos

NTT DATA

KNAUF

SAS

NHS

TUI Cruises

MUSTANG® Duvel

>500

diverse employees

>3.5M

users worldwide

>5,000

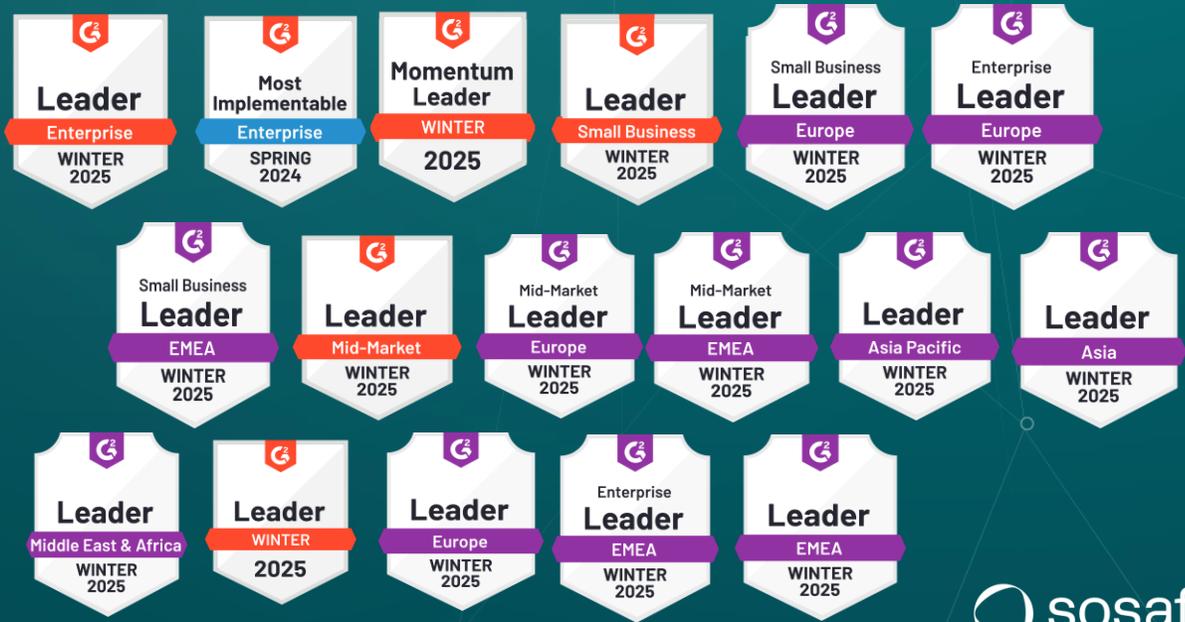
customers across all industries

Europe's largest Security Awareness & Human Risk Management player

...now in Australia!



Gartner Peer Insights: 4.3



PSYCHOLOGY

<Applied> behavioural science is our DNA

Founded by a trained psychologist

Employing 30+ experts with psychology and social science background

Our core tenets



Engage users

and empower them by leveraging psychology



Relieve security teams

in every phase of deploy, customise, manage, engage & support



Reduce friction

and unnecessary learning for end-users



Innovate & Adapt

To stay ahead of threats and adapt to your needs

Jacqueline Jayne (JJ)

Advocate for Human-Centric Security at SoSafe

Human Risk Management Expert

- SACP (Security Awareness Certified Professional)
- Security Influencer
- Online Safety Specialist



RSA
Conference

AISA

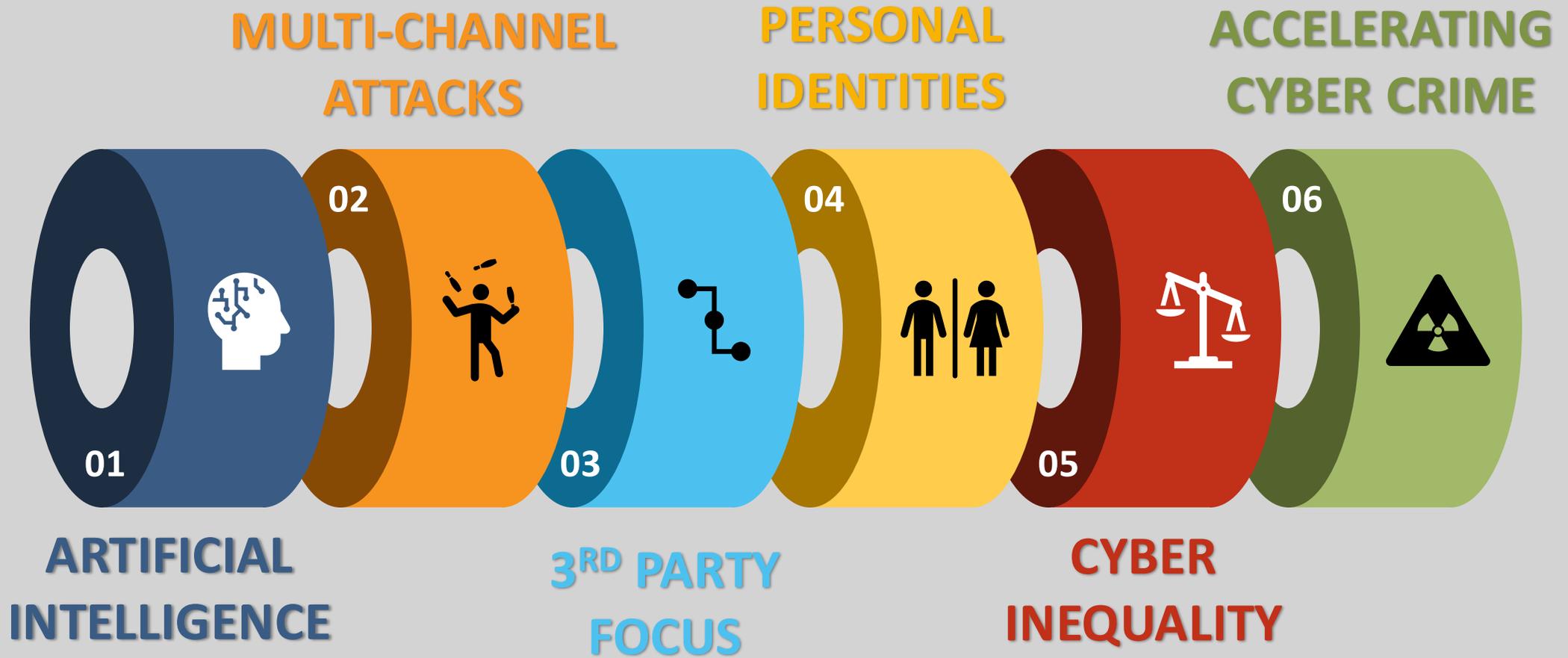
AUSTRALIAN
CYBER
CONFERENCE

blackhat
ASIA

sosafe

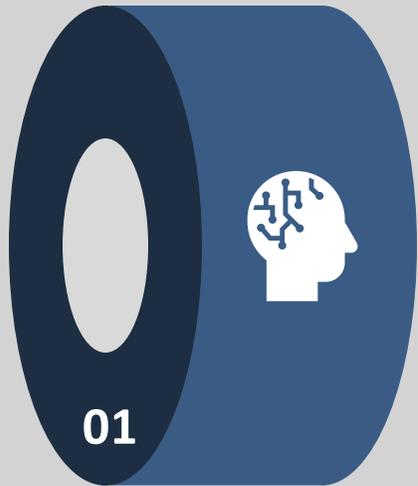
AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up



AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up

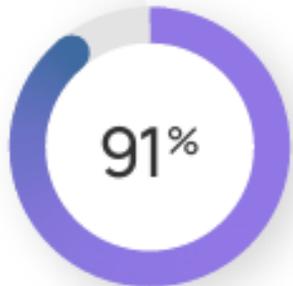


ARTIFICIAL INTELLIGENCE



AI IS EVOLVING TOO RAPIDLY

AI as a criminal accelerator



of worldwide security experts expect a **significant rise** in AI-driven threats over the next three years.

And even though **96%** of professionals **recognise the importance** of detecting AI-based attacks, ...



... only **26%** rate their ability to do so as "high".

AI isn't just a threat – it can also become a powerful ally

	All	UK	Australia	France	DACH	BENELUX
The difficulty in attributing attacks	50.8%	55%	52%	52%	54%	41%
The creation of entirely new attack methods	44.8%	45%	43%	56%	38%	42%
Realism of AI-generated content	41.6%	45%	44%	40%	36%	43%
Targeted precision	41.4%	46%	49%	33%	48%	31%
Lack of preparedness and detection tools for AI threats	38.8%	29%	48%	37%	41%	39%
Scale and speed of automated attacks	38%	38%	43%	38%	32%	39%



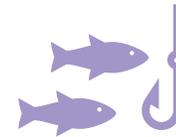
What aspect of AI-driven attacks concerns you most, if any?

AI IS EVOLVING TOO RAPIDLY

AI as a criminal accelerator



12% to 54%



Of employees click on AI driven phishing attacks

Source: HBR Nov 2024

88%



Of employees can be profiled using publicly available data to create unique spear phish

Source: HBR Nov 2024

100% to 2%



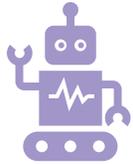
Reduction in attacker costs to spear-phish a target

Source: HBR Nov 2024

AI IS EVOLVING TOO RAPIDLY

AI-generated attacks are an increasing threat

91%



Expect the **threat** and **intensity** of AI-based cyberattacks to increase over the next 3 years.

Source: SoSafe Survey 2025



223% increase in the trade of deepfake-related tools on dark web forums in one year

74%



Lack confidence in their ability to detect AI based attacks

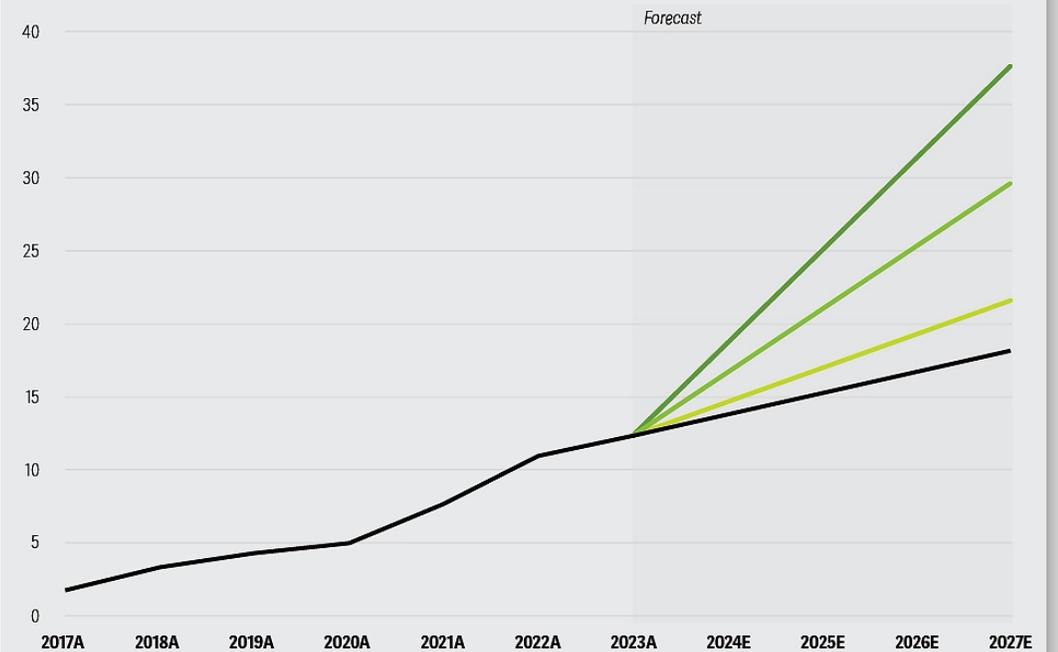
Source: SoSafe Survey 2025

Figure 1

Generative AI is expected to rapidly increase fraud losses in the years ahead

Fraud losses, actual and expected, 2017 to 2027 (\$US billion)

● No generative AI ● Conservative ● Base case ● Aggressive



Sources: The FBI's Internet Crime Complaint Center; Deloitte Center for Financial Services.

Deloitte Insights | deloitte.com/insights

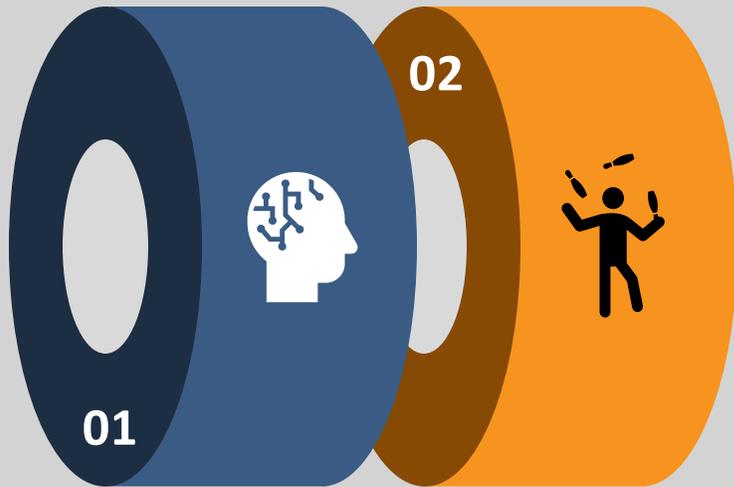


- **Educate and raise awareness:** Train staff on AI's capabilities and associated risks, including recognising AI-driven attacks like deepfakes.
- **Establish AI governance:** Create a governance committee and process to manage all AI solutions within your organisation. Maintain an inventory of AI tools, assign ownership, assess risks, and outline recovery paths for potential failures.
- **Avoid AI unification:** A single AI with access to all data may simplify user experience but introduces significant risks.
- **Cover security essentials:** Strengthen basics like least privilege access, segregation of duties, regular privilege reviews, MFA, and patching. Ensure a robust, well-rehearsed incident response plan is in place.
- **Align AI with regulations:** Treat AI outputs and decisions as subject to existing regulations. Ensure AI systems comply with regulations and other frameworks by maintaining auditable records and clear accountability for AI owners.

AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up

MULTI-CHANNEL ATTACKS

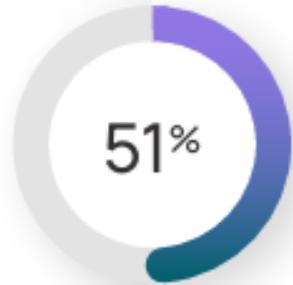


**ARTIFICIAL
INTELLIGENCE**



THE RISE OF MULTICHANNEL ATTACKS

Cybercriminals are combining channels in highly sophisticated 3D phishing attacks.



of global security professionals still report **email as a primary target**, but...

98%

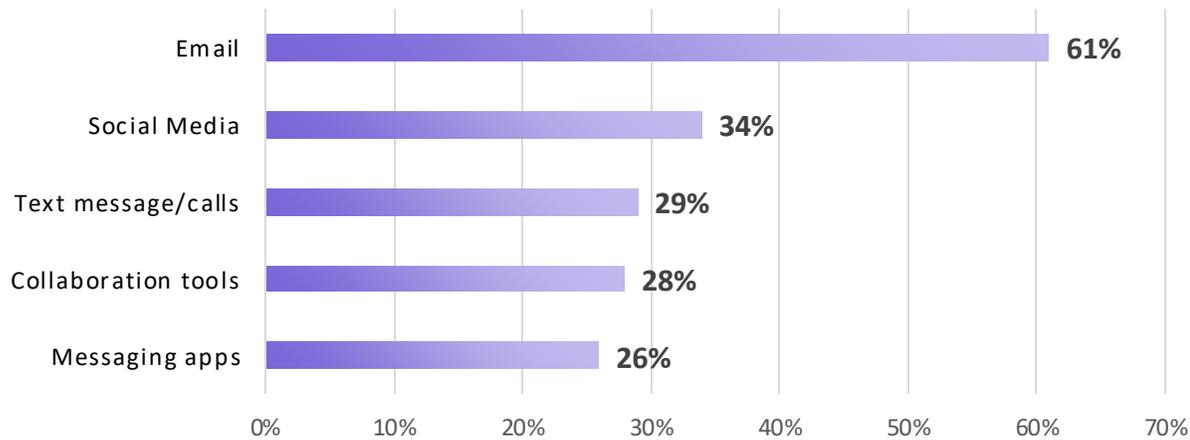
of Australian organisations report a rise in **multi-channel attacks** leveraging email, messaging apps, social media, and deepfake voice calls.



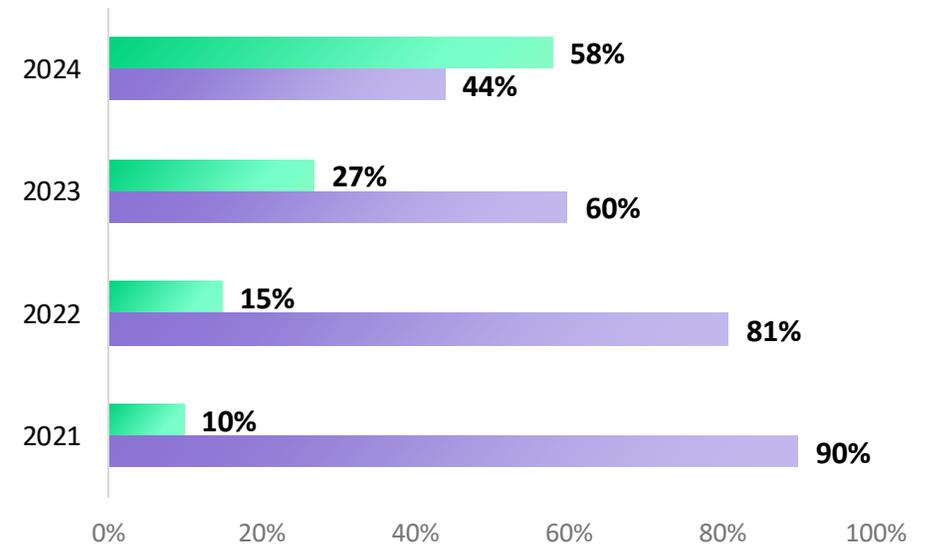
SOCIAL ENGINEERING IS BECOMING MORE COMPLEX

As we diversify our communications channels, so do cybercriminals

Top channels in which companies are targeted



Pretexting doubling & becoming #1 of Social Engineering action



Action varieties in Social Engineering incidents

■ Pretexting ■ Phishing



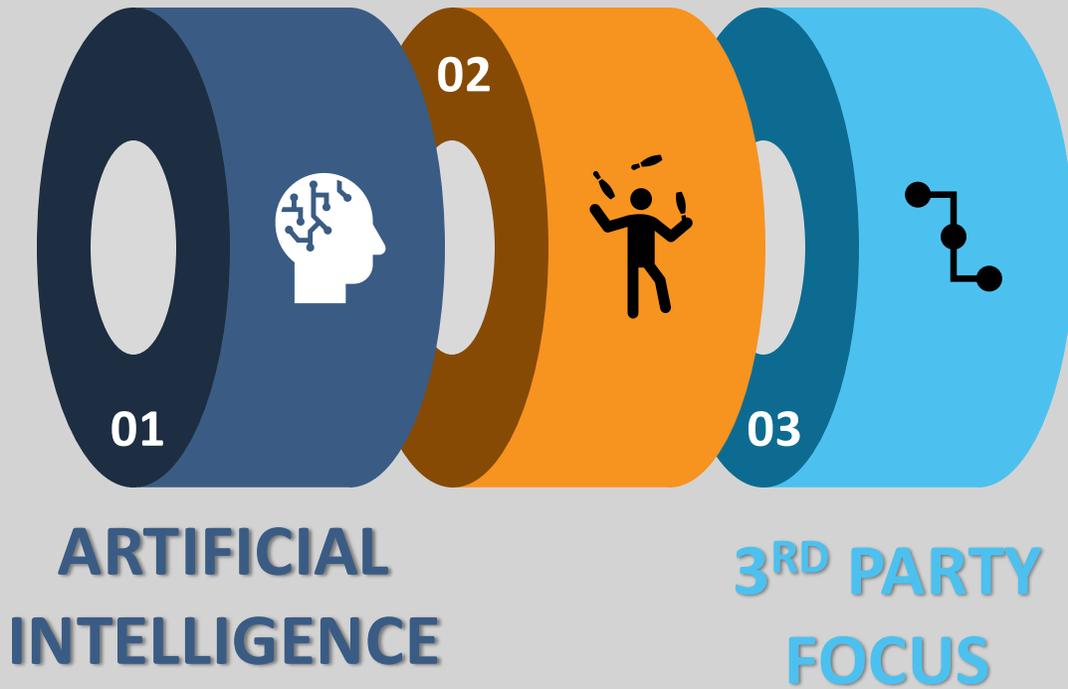
Practical Tips

- **Educate staff on attack methods:** Employees need to understand how attackers operate. Your awareness programme should highlight key techniques and channels to help staff stay vigilant.
- **Multichannel awareness training:** Move beyond email phishing simulations to include smishing and vishing to prepare your workers for diverse attack vectors.
- **Restrict corporate communication to secure tools:** Collaboration tools often allow external parties to connect, creating opportunities for attackers to exploit 'trusted' environments. Disable this feature unless absolutely necessary to reduce exposure to potential threats.
- **Reinforce core access controls:** Ensure that essential protocols like segregation of duties and least privilege are not only in place but also effectively implemented. Regularly review these controls to minimise the risk of unauthorised access.

AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up

MULTI-CHANNEL ATTACKS





Supply Chain Attacks - Third-party risks that escalate into massive breaches



84% of Companies had their operations disrupted by 3rd party risk incidents

66% Suffered adverse financial impact as a result

59% Suffered adverse reputational impact as a result

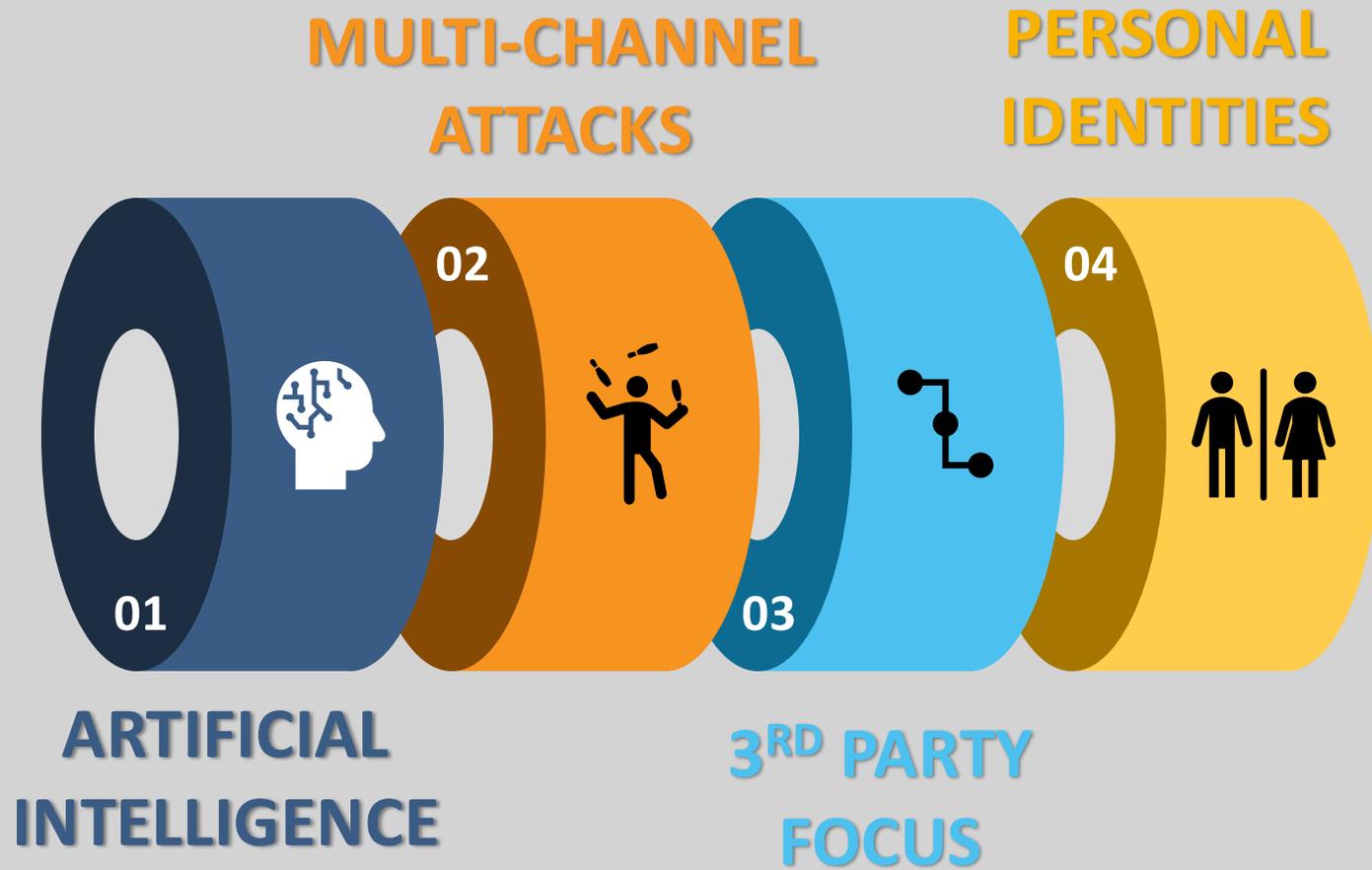


Practical Tips

- **Build and maintain a third-party inventory:** Many organisations lack full visibility into their supplier portfolios.
- **Classify third parties by risk level:** Develop a risk model to assess potential threats from each vendor. Tie scrutiny, contractual obligations, and controls to their risk levels, and ensure the supplier management team implements it.
- **Enhance risk assessments:** Supplement traditional questionnaires with on-site reviews, penetration tests, and perimeter scans to evaluate technical risks. *Don't overlook human factors like security awareness and culture within the vendor organisation.*
- **Segregate external collaboration zones:** Separate collaborative zones from critical systems to minimise the impact of a breach if a supplier is compromised.
- **Diversify your supply chain:** Avoid over-reliance on a single supplier. Ensure operational flexibility to pivot to alternatives if needed, reducing risks from attacks targeting key partners.

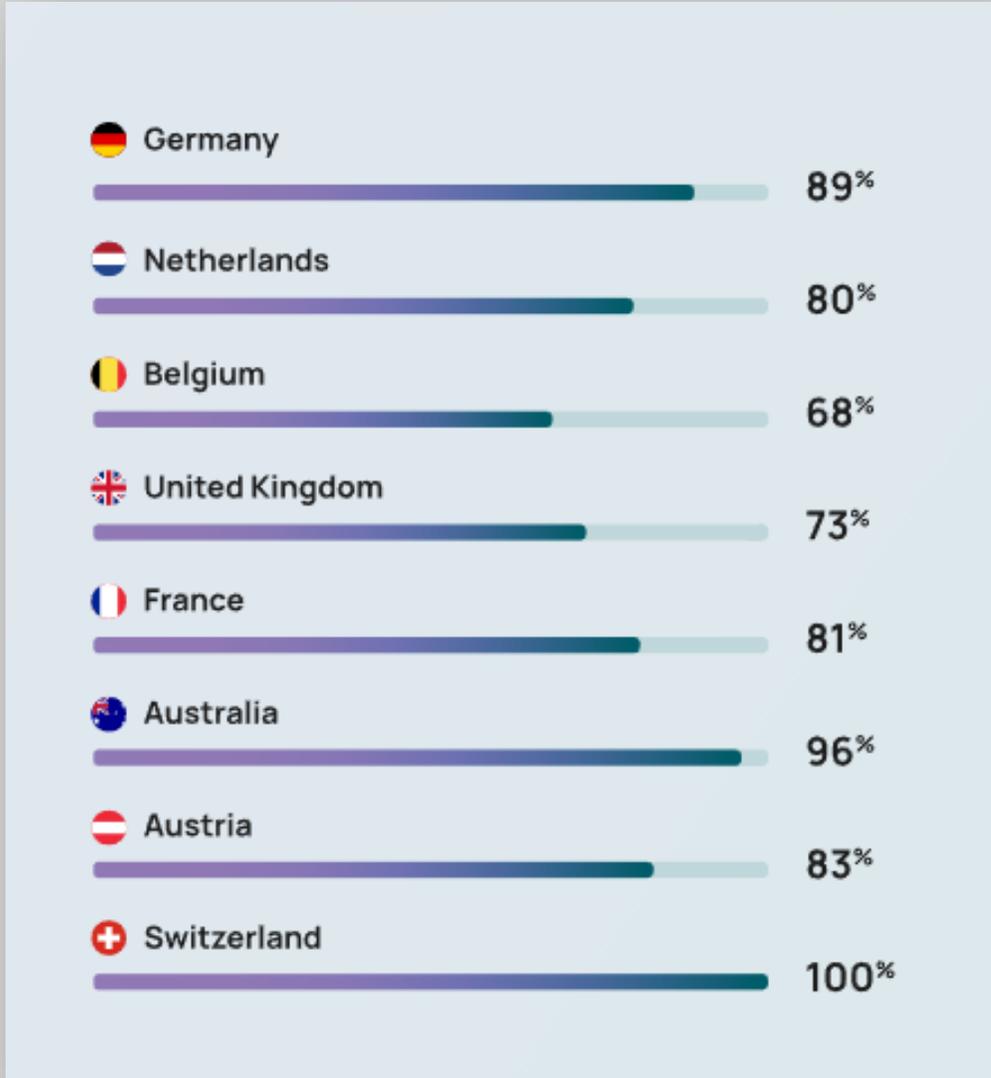
AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up



THE QUIET DOORWAY TO CORPORATE SYSTEMS

Hackers are turning personal devices into organisational threats





HYPER PERSONALISATION

Attacks move beyond the intended target

- The blurring of personal and professional boundaries tempt attackers to broaden their focus
- Your attack surface has never been better advertised
- Personal networks are less well protected than business ones



73%



Report a surge in consumer-focused threats in the past 12 months

Source: SoSafe Survey 2025



ATTACK OUTSIDE THE ORGANISATION

And no one is spared, not even your loved ones.

6 charged in 'grandparent scam,' more than \$250K stolen from victims: Investigators

By Jordan Bowen | Published June 24, 2024 9:29pm EDT | Florida | FOX 13 News | [↗](#)

US mother gets call from 'kidnapped daughter' - but it's really an AI scam

Jennifer DeStefano tells US Senate about dangers of artificial technology after receiving phone call from scammers sounding exactly like her daughter

70%

of people were not confident they tell the difference between a cloned voice and the real thing

3 secs

of audio is all that's required to create a voice clone

Calll. Dad someone has kidnapped brie

brie picked up and she's fine

she's calling you

she's fine for now at least idk what that ransom thing was about

Fri, Jan 20 at 7:22 PM





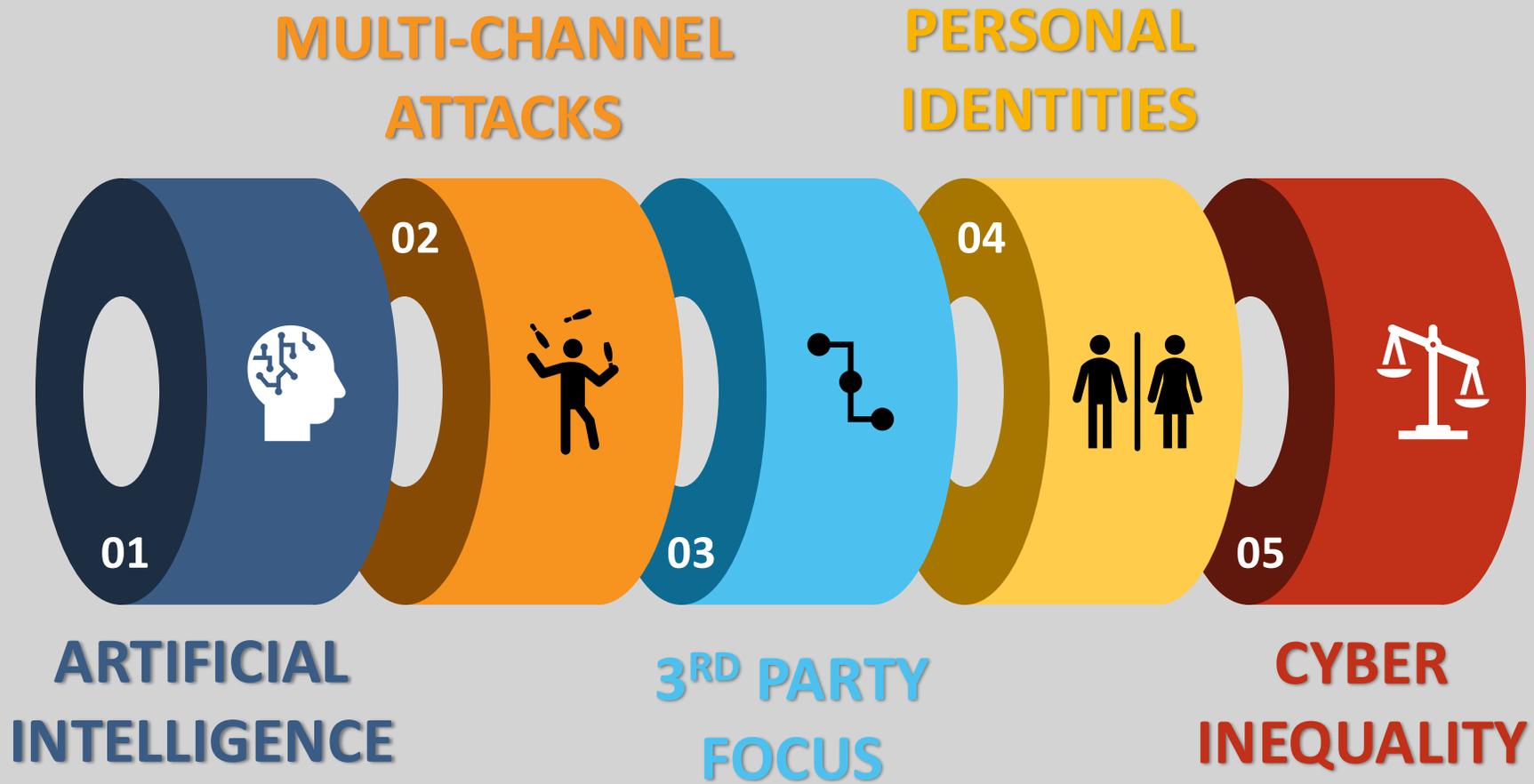
Practical Tips

- **Train on both personal and work identities:** Focus training on personal and work identities, highlighting attack tactics and consequences to help users understand their value to attackers in both roles.
- **Extend training to families:** Include families in training to protect their digital lives, as attackers may target relatives to access networks or extort employees.
- **Extend technical protection to home devices and non-corporate hardware:** Staff often use personal devices for work purposes, so consider partnerships with software vendors to achieve discounts on tools and controls that will enable them to be better protected, without increasing the burden on your security team to manage additional hardware.
- **Ensure secure remote connections:** Secure remote connections with MFA, VPNs, endpoint validation, and DLP to prevent accidental exposure of sensitive data outside corporate protection.
- **Strengthen access controls:** Operate under the expectation that breaches will happen and audit systems that safeguard sensitive data or operations. Maintain at least 12 months of logging and monitoring to trace employee activity if needed. Review and clean up password managers, eliminate shared accounts, and reinforce access protocols to minimise vulnerabilities



AGENDA

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up





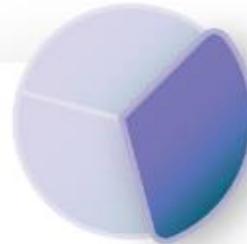
Cyber resilience inequality is putting essential services at risk



of respondents in Australia believe the **security gap is widening**,

leaving critical industries and small companies **unprepared** to fight against threats.

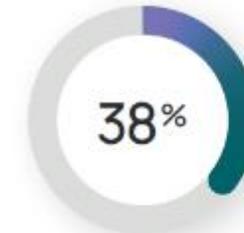
According to the World Economic Forum,



over 1/3

of global small organisations believe their cyber **resilience is inadequate**¹.

The **public sector** is also struggling...



of companies worldwide report **insufficient resilience**¹.

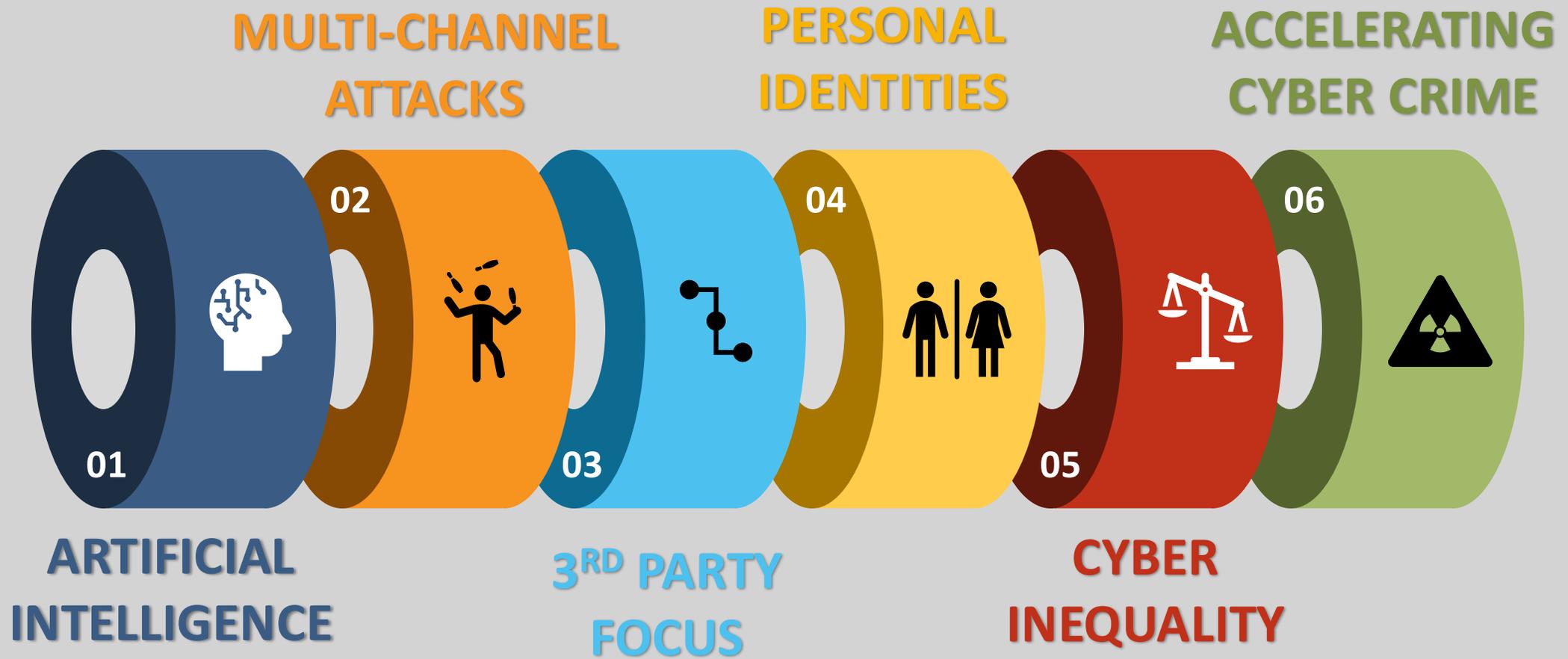


Practical Tips

- **Adopt recognised frameworks to stay ahead of threats:** Such as ISO 27001 and NIST CSF as your strategic foundation, regardless of regulatory requirements.
- **Collaborate with regulators:** Work proactively with your industry's regulators to develop practical guidelines that can benefit the wider industry and promote collective security.
- **Hold other departments accountable:** Security teams shouldn't bear the burden of inefficiencies in other functions. Ensure OS patching, code hardening, and legacy system deprecation are owned by the appropriate teams, with clear accountability for addressing the risks they create.
- **Learn from mature industries:** Network with organisations in highly regulated sectors to understand how they design resilient controls and adapt lower-cost alternatives that fit your industry's needs.
- **Build diverse talent pipelines:** Partner with universities and technical schools in underrepresented areas to create internships and apprenticeships that attract diverse cyber security talent.
- **Make strategies accessible to all teams:** CISOs in less regulated industries and smaller companies should ensure cyber security strategies are clear and actionable, enabling less technical teams – such as blue-collar workers – to actively contribute to defence efforts.

AGENDA

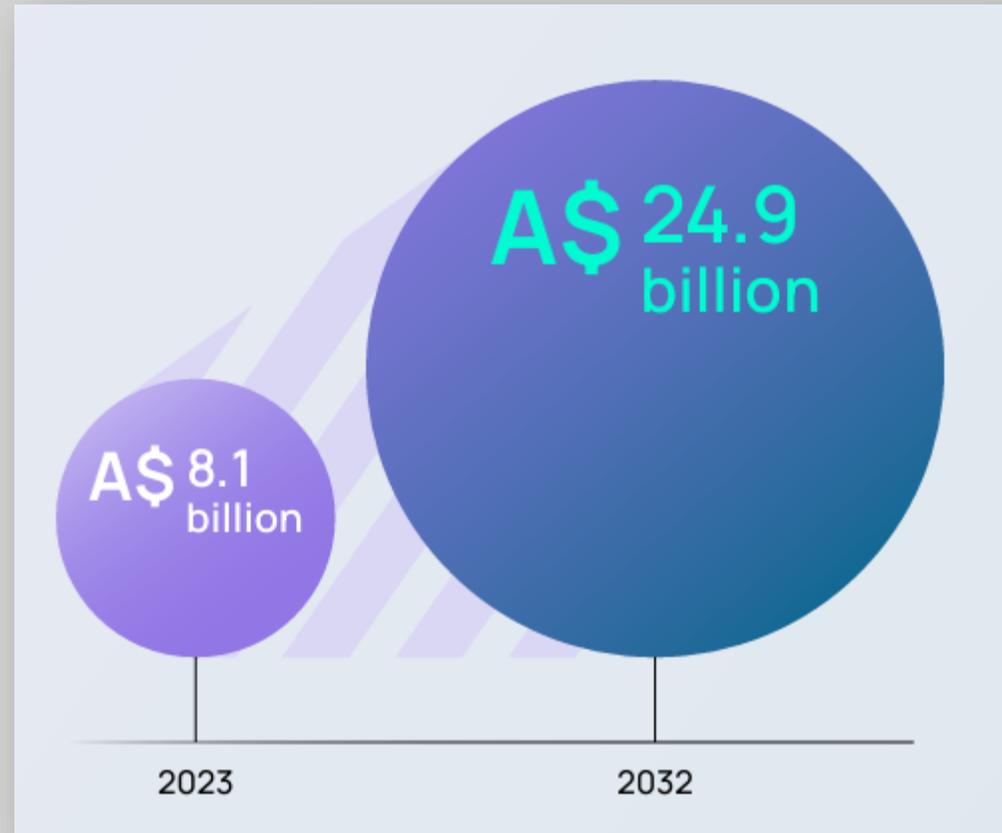
Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up





THE BOOM OF CYBERCRIME

Cybercrime has transformed into a highly organised, global industry.



Projected growth of Australia's national cyber security market



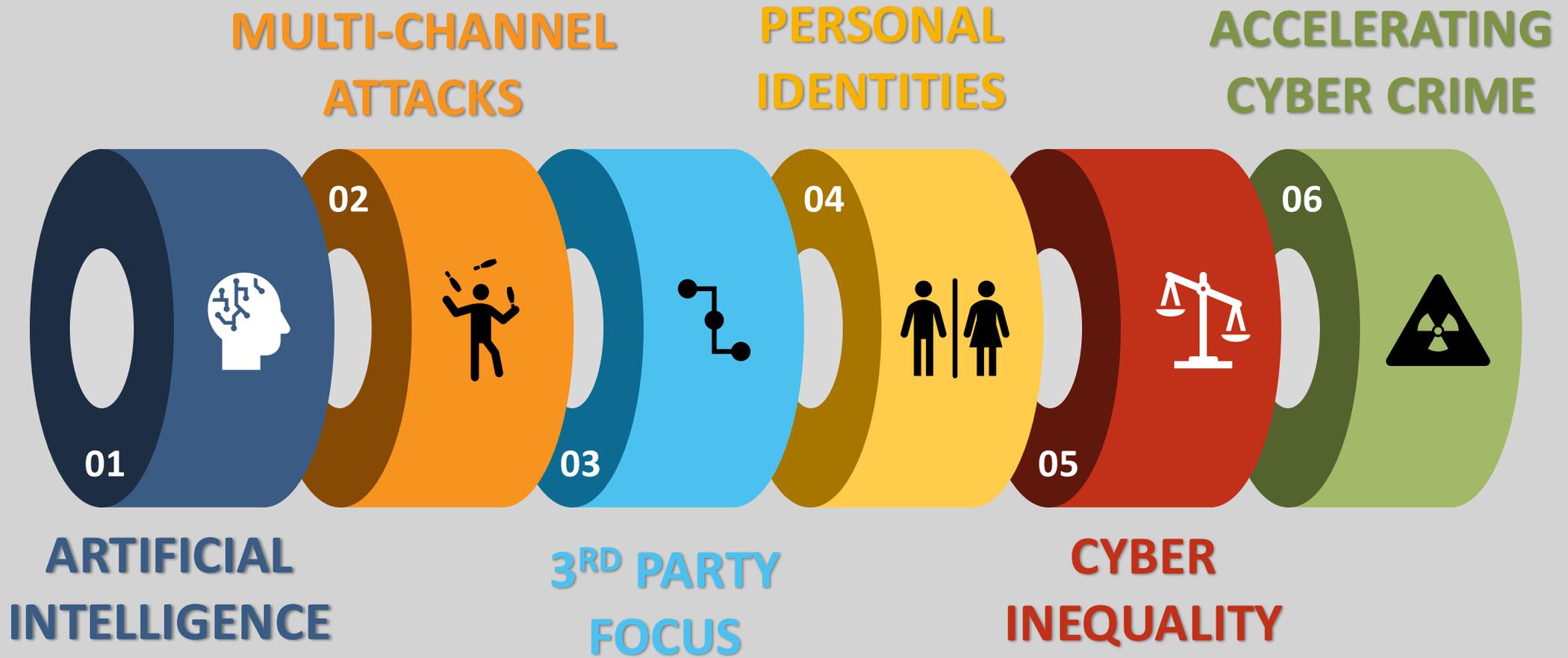


Practical Tips

- **Recognise and prioritise your expanding attack surface:** Understand which elements are under your control – and which aren't. Focus on technical, people, and third-party risks by applying the right scrutiny, due diligence, and resources based on your specific threat levels.
- **Simplify for agility and lower cost:** Each new layer, process, or system increases operational complexity and makes responding to threats more cumbersome. Consolidate vendors and systems where possible, and work with business units to ensure they maintain the same focus on streamlining.
- **Strengthen operational resilience:** Partner with business process owners to ensure they can continue critical tasks even in the face of a cyberattack – including offline methods like pen-and-paper workflows. This ensures your organisation can always deliver a minimum viable service or product.
- **Hold other departments accountable:** Security shouldn't carry the weight of poor quality control across the organisation. Escalate concerns so that the right teams own OS patching, code hardening, and legacy system deprecation, holding them accountable for addressing the risks they create.

RECAP

Cyber Crime Trends 2025 - Find Out About The Biggest Global Trends And How Australia Is Measuring Up



A clear benchmark to help you understand your organisation's level of preparedness against key cybercrime trends. It outlines the critical steps you need to move from a reactive security posture to a fully resilient one.

AI as an attack surface

Level 1 - Reactive

- > Basic 'don't use' or 'take care' policy regarding AI use.
- > Internal AI tools lack security controls.
- > AI-driven threats (deepfakes, phishing) are not monitored.

Level 2 - Proactive

- > AI governance committee in place; associated risks are documented and acknowledged.
- > AI risk managed through limiting AI data access; some prompt controls exist to remove obvious malicious intent.
- > AI-driven threats are monitored occasionally

Level 3 - Resilient

- > AI security is fully integrated into the development and maintenance lifecycle.
- > Strict data access controls; output monitoring and continuous AI threat surveillance.
- > AI-specific employee training and risk assessments.

CYBERCRIME TREND
Resilience Matrix

A clear benchmark to help you understand your organisation's level of preparedness against key cybercrime trends. It outlines the critical steps you need to move from a reactive security posture to a fully resilient one.

Level 1 - Reactive

Level 2 - Proactive

Level 3 - Resilient

AI as an attack surface

Multichannel Attacks

Supply Chain and third-party risk

Threats to personal identities

Cyber resilience inequality

The boom of cybercrime

Eager to know more?
Access the full report here:



“ Amateurs hack systems, professionals hack people.”

Bruce Schneier

Expert in Cryptography and Computer Security, Harvard University

Loved by customers



SoSafe SE

Sydney office: Hub Customs House

31 Alfred Street Sydney NSW 2000

sosafe-awareness.com/secure-australia/

info@sosafe.de