Victorian
Chamber of Commerce
and Industry

Cyber Security and Scams Policy Position

Protecting small, medium and family businesses

victorianchamber.com.au

Table of contents

Loading... Business cyber security update in progress.

Cyberattacks and online scams are a growing threat to Australian business. In 2022, the average cost of cybercrimes to businesses jumped 14 per cent from the year prior.[i] Each cybercrime is now reported to cost over $39,000 for small business, $88,000 for medium business, and $62,000 for large business.[ii]

Despite the continued growth in incidents, many businesses believe they are adequately equipped to fend off cyber criminals. In a recent Victorian Chamber of Commerce and Industry study, 74 per cent of businesses surveyed were confident their cyber defences would prevent a notifiable data breach or ransom attack. Businesses are unaware of the high probability that they will, at some point, suffer a cyberattack.

If businesses are not protected, workers and clients are not protected. Livelihoods are at risk. Governments must prepare the entire business community to tackle the constant influx of bad actors. Inaction, or inappropriate action, will stunt productivity and economic growth.

As the war in Ukraine has demonstrated, modern warfare is the synchronisation of both physical attacks and cyberattacks. Australia's REDSPICE program aims to boost the nation's current cyber capability threefold and double our persistent cyber-hunt activities.[iii] But will this be enough?

Government funding in cyber security research has decreased from $9.8 million in 2019 to $7.5 million in 2022, and yet the number of cyberattacks in Australia is projected to double in the next five years.[iv] It is important Australia's expenditure on uplifting sovereign capability is in line with global best practice.

i ACSC (2022). *ACSC Annual Cyber Threat Report, July 2021 to June 2022.* https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

ii Ibid.

iii Australia Signals Directorate (2023). *REDSPICE.* https://www.asd.gov.au/about/redspice

iv AustCyber (2022), *Australian cyber security sector competitiveness plan 2022.* https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2022

The expansion of the Security of Critical Infrastructure Act 2018[v] (the SOCI Act) to 11 sectors was necessary to manage national security risks of sabotage, espionage and coercion. Through this, Australia is strengthening the security and resilience of critical infrastructure.

Small, medium and family enterprises (SMFEs), which are not directly captured by the SOCI Act, lack the incentive to uplift their cyber security. When surveyed, 73 per cent of businesses would be more inclined to strengthen their data security with government support. To ensure all Australians are protected, the forthcoming 2023-2030 Australian Cyber Security Strategy must focus on uplifting the cyber maturity of SMFEs.

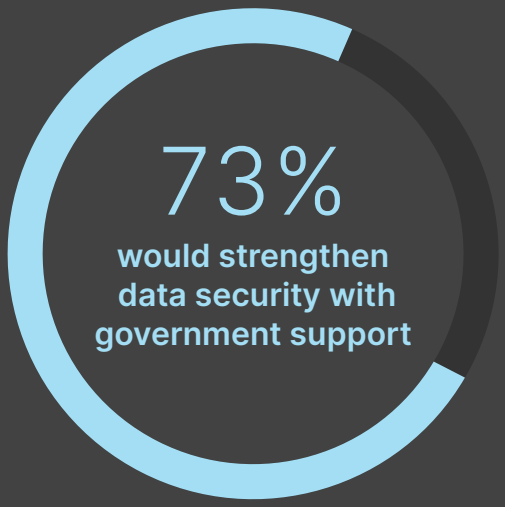
The best way to uplift cyber capability across the business community is through competition. In the fast-moving landscape of cyber security, legislation will date quickly. Instead, rewarding best practice will boost competition and drive Australia's resilience.

In this policy paper, the Victorian Chamber outlines the current cyber environment for business, steps to become the most cyber secure nation by 2030, leaders to deliver the Cyber Security Strategy, and Australia's desired cyber-safe end state. We have developed our 24 game-changers (recommendations) through extensive consultation with SMFEs, telcos, tech giants, social media platforms, health providers, education institutions, banks, and other critical infrastructure.

v Federal Register of Legislation (2018). *Security of Critical Infrastructure Act 2018*. https://www.legislation.gov.au/Details/C2021C00570

Survey results

- 74% of businesses surveyed are confident in their cyber defences



- 73% of businesses surveyed would be more inclined to strengthen their data security with government support

Top three game-changers:

1

Cyber Health Clinics

Establish industry-led Cyber Health Clinics to provide local, face-to-face solutions to uplift business cyber security with trust.

2

Cyber Safe Score

Establish a Cyber Safe Score that rates the level of cyber security maturity of businesses and any of their commercial products and services to boost competitiveness and secure supply chains.

3

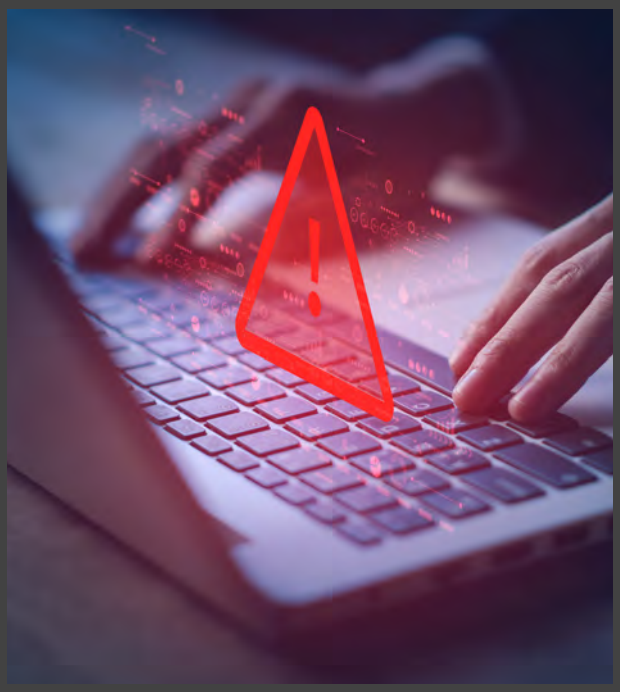
Apprenticeship training model

Adopt a cyber security apprenticeship training model to give students the practical work experience they need to directly enter the workforce.

2023 – Businesses are reactive to cyber threats

Our means of communication are under threat. One commonality between all businesses is the Internet. They communicate via email and send money to clients and employees through online bank transfers. The Internet is the playground of cyber criminals. Lurking in the background, bad actors try to hack devices, steal information and extort money.

Business email compromises are the new norm. Scammers send fake invoices that businesses pay. They change bank account details and impersonate both employees and employers alike. Spoofing occurs regularly, often in the form of false tender packages sent via email pretending to be a legitimate business.



Small and medium businesses are under assault daily. Research conducted in 2022 revealed that 49 per cent of Australian small and medium-sized enterprises have experienced a cyberattack in the last 12 months.[vi] Criminals catch SMFEs whose systems are weak due to their use of outdated computer software or by tricking employees into clicking on malicious phishing links in emails.

Ransoms are also common. Some small businesses are faced with the difficult decision of paying cyber gangs thousands to regain access to their data and systems or losing everything, including their reputation. Their livelihoods are in jeopardy. When businesses are in danger of going under, employees are at risk as well. Jobs will be lost when businesses are forced to fold following a ransom attack.

Banks are frequently blamed. Yet it is investment scams that they spend the majority of their time trying to resolve. Mum and dad businesses mistake scam ads on Google and Facebook as legitimate and succumb to the temptation of doubling their money. Financial losses are caused by active individual misguidance. Under these circumstances, banks are not responsible for losses. Reimbursements only occur when bank accounts have been hacked.

vi Inside small business (2022). *Research reveals extent of SMEs' vulnerability to cyberattacks.* https://insidesmallbusiness.com.au/technology/cyber-security/research-reveals-extent-of-smes-vulnerability-to-cyberattacks

THE INTERNET

is the playground of cyber criminals.

So, who do businesses turn to for help?

In the SMFE business community, there is limited understanding of cyber security and a lot of confusion around the complex, jargon-heavy terminology. Some family businesses self-train in cyber security, while other medium-sized companies afford to outsource their information technology (IT) to third-party service providers.

No matter the situation, the solution is local. SMFEs turn to the 'local IT guy' who is 'just down the road'. These technicians provide face-to-face solutions to fix cyber problems. Businesses talk to real people who they trust. However, these businesses put their trust in local technicians who, although well-meaning, have limited ability to prove their base-level certification and capability.

Currently, the onus is on businesses to maintain their education and keep up to date with the latest cyber scams. Trying to stay abreast of the ever-evolving changes in the cyber landscape is impossible. An effective way to transfer knowledge and updates on cyber security is through storytelling. This is what motivates businesses to proactively improve their cyber defences.

The Australian Cyber Security Centre[vii] (ACSC) outlines some effective cyber security mitigation strategies for businesses to adopt, known as the Essential Eight.[viii] Feedback from industry indicates there needs to be a more basic level, than Maturity Level One, for SMFEs to implement. The content on the Essential Eight webpage is complex and in written format, which is challenging to digest. The business community seeks face-to-face solutions to uplift their cyber capabilities.

For larger organisations, additional levels of the Essential Eight could be established and include internationally recognised standards like NIST zero trust[ix], ACSC Information Security Manual (ISM), and ISO.

Similarly, the CyberWardens[x] program aims to make non-technical employees cyber 'experts', instead of investing in training cyber security professionals. It is similar to training employees in First Aid, instead of investing in more qualified paramedics. Australia needs highly skilled cyber security professionals with extensive practical experience to combat online threats with confidence.

Currently, cyber security graduates struggle to find meaningful work. This is because they have insufficient work experience to meet the technical skills industry requires or they lack the permanent residency and citizenship industry expects. We need to rethink our approach to cyber security. To make Australia the most cyber secure nation by 2030, governments and businesses must get proactive.

vii Australian Cyber Security Centre (2023). https://www.cyber.gov.au/

viii ACSC (2023). *Essential Eight*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

ix NIST (2020). *Zero Trust Architecture*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

x CyberWardens (2023). https://cyberwardens.com.au/

How will Australia become the most cyber secure nation by 2030?

No matter the situation, the solution is local.

01

Governments need to implement bold cyber policies

The business community seeks trusted support to deal with cyber issues. You can't fix a virtual problem virtually. Physical **Cyber Health Clinics**, much like Apple Stores, would provide a practical resolution. Partnering with the private sector to deliver local, face-to-face solutions will work best.

There is no need to reinvent the wheel. The Federal Government should leverage pre-existing infrastructure and services by partnering with local trusted institutions (e.g., telcos, banks and certified IT stores) to deliver co-funded Cyber Health Clinics. They should focus on prevention with general check-ups for setup of multi-factor authentication (MFA), software updates, back-ups, etc.

Also, they should provide in-person assistance to recover data if employers or employees fall victim to scams.

Cyber Health Clinics would service vulnerable communities including small, medium and family businesses, remote workers, young entrepreneurs on social media, culturally and linguistically diverse (CALD) communities, First Nations people, and senior citizens.

In remote areas, such as many indigenous communities, the 'IT guy' is often hundreds of kilometres away. These communities would benefit from a scheduled **flying cyber doctor service**, much like the Royal Flying Doctor Service, whereby Cyber Health Clinics deliver cyber assistance to rural and remote areas.

At present, cyber security specialists are all self-proclaimed 'experts' because there are no industry standards in place. The establishment of a professional body for cyber security professionals, similar to the UK Cyber Security Council,[xi] would provide the industry with professional standards and ethics, careers advice, and learning opportunities.

It is crucial that Australia sets up an **Australian Cyber Security Council**. The Council could provide aspiring cyber professionals with guidance on the hundreds of different cyber security certifications on the market,[xii] all relating to different elements of the industry.

Competition is a powerful tool to influence action in cyberspace. A **Cyber Safe Score** for all businesses that rates their adherence to industry best practices would leverage competition to encourage enhanced cyber security. Similar to the UV protection ratings of sunscreen, Cyber Safe Scores would enable businesses and consumers to make informed decisions based on security levels, driving competition in supply chains.

The Score's parameters would be set by the Australian Cyber Security Council and peak industry bodies. The Federal Government should set the base standards across industries (e.g., MFA, auto-patching, secure by default) and peak business bodies would be responsible for setting industry-specific standards (e.g., PayID and name verification tools in the banking industry). To kick start uptake, governments should implement these standards in procurement processes.

Businesses would receive a score from zero to 100 on the cyber security level of their business and any of their commercial products and services connected to the Internet.

Self-assessments would be available, but to demonstrate mastery, a score of more than 50 would require an external independent cyber security audit. Businesses could promote their scores via digital badges, propelling competition across markets.

Cyber Safe Scores could be accessed through QR codes displayed on business products, platforms and websites. This would enable consumers to easily scan the QR codes to receive live status updates on business Cyber Safe Scores.

The Cyber Safe Score reduces the amount of vendor risk assessments, would feed competition in cyber security, and encourage businesses to increase investment in resources to secure their systems. The Score would empower the SMFE business community and consumers to instantly be able to compare products and services.

xi UK Cyber Security Council (2023). https://www.ukcybersecuritycouncil.org.uk/

xii Paul Jerimy (2023). *Security Certification Roadmap*. https://pauljerimy.com/security-certification-roadmap/

Non-technical elements could be included in the Cyber Safe Score to uplift whole-of-Australia resilience. Businesses over a certain threshold (e.g., large organisations) could be required to take on **cyber security interns** to train the next generation of professionals and provide them with practical work experience in industry during their studies. By doing this, large companies would gain extra points towards their Cyber Safe Score.

Further, businesses are overwhelmed with the amount of cyber information available and do not know which sources to trust. Industry associations can leverage their trusted reputation to run cyber security **education and training programs** for business. Training is essential to ensure cyber security is front of mind for both employees and employers. All staff should participate in regular cyber security trainings (e.g., short three-minute awareness videos) to keep up to date with the latest threat trends.

The Federal Government should also partner with industry associations to run **organic social media campaigns** on the latest scams and cyber security prevention measures. These campaigns would target vulnerable communities including small, medium and family businesses, and employees working from home.

The large social media followings of opinion leaders (e.g., industry associations, community groups, influencers, sports stars, celebrities, and other public figures) should be leveraged to influence the adoption of more cyber secure practices and technologies. The aim is to reach all diverse and vulnerable segments of society by making cyber security a trending topic, increasing awareness as well as the uptake of cyber hygiene best practices.

The cost of doing business is rising. In Victoria, it is particularly high.[xiii] With appropriate **incentives**, SMFEs would be able to uplift their cyber defences. Allowing write-offs for software as well as hardware would incentivise businesses to regularly update digital assets with the latest and safest technology.

Subsidies for operational cyber activities (e.g., Security Operations Centres (SOCs)) would mean businesses can afford to constantly monitor, prevent, detect, investigate, and respond to cyber incidents. With sufficient government support, businesses would invest in prevention measures such as security assessments (Penetration Tests), where cyber professionals to try to ethically hack company systems to reveal security vulnerabilities.

Australia needs to define what cyber success looks like. The Federal Government should set **cyber security key performance indicators (KPIs)** for businesses to strive to achieve by 2030. The KPIs could include targets for the number of new cyber graduates and professionals hired, average Cyber Security Score, level of cyber security maturity in industry, and reduction in the number of successful cyberattacks.

Tokenisation is an effective solution to avoid the collection and storage of identity documents. Australia's identity documents should be tokenised and stored federally. In such a system, businesses would access tokens as required. This system would prevent data breaches, information theft and extortion.

xiii VCCI (2022). *Cost and ease of doing business in Victoria*. https://www.victorianchamber.com.au/policy-and-advocacy/taskforces/cost-and-ease-of-doing-business-in-victoria-taskforce

Australia needs to define what cyber success looks like.

Stolen identities are often the pathway for money out of accounts. **Facial ID** applications (e.g., ConnectID[xiv]) avoid collection and storage of personal data such as driver's licences and passports. This deters the occurrence of cyberattacks like the Medibank and Optus breaches. Facial ID checks provide banking institutions with a more holistic view of account owners. Putting in place stricter measures to prove people's identity would make monetary theft more difficult.

Sovereign capability must also be a centrepiece of Australia's Cyber Security Strategy. To achieve this, collaboration between the states and territories is required. Harmonising **information security frameworks** across the country would facilitate cooperation.

Strong cyber security foundations will be key to uplifting businesses. One example is Internet Protocol version 6 (IPv6), which is considered an evolution towards a more secure version of the Internet.

The US Federal Government has mandated that all agencies and departments transition from IPv4 to the more secure version IPv6.[xv] China has also made IPv6 mandatory across industries by 2030.[xvi] Australia must ensure **best-practice technologies** are implemented to keep the nation safe. The adoption of such technologies could be reflected in Cyber Safe Scores.

Cyber insurance is an increasingly important issue for businesses as well. Australia should explore options to facilitate the uptake of cyber insurance in small and medium companies. Insurance may not make businesses more vigilant, but it will likely keep their doors open following a serious and costly ransom attack.

In Victoria, the appointment of a **Cyber Security Minister** and creation of a dedicated portfolio that manages all cyber-related issues would ensure appropriate action is being taken at a state level.

xiv ConnectID (2023). https://connectid.com.au/

xv Defensescoop (2023). *NSA issues security guidance for DOD's IPv6 transition*. https://defensescoop.com/2023/01/24/nsa-issues-security-guidance-for-dods-ipv6-transition/

xvi The Register (2021). *China sets goal of running single-stack IPv6 network by 2030, orders upgrade blitz*. https://www.theregister.com/2021/07/26/china_single_stack_ipv6_notice/

Game-changers:

01	**Cyber Health Clinics** Establish industry-led Cyber Health Clinics to provide local, face-to-face solutions to uplift business cyber security with trust.
02	**Australian Cyber Security Council** Establish an Australian Cyber Security Council to set professional standards and ethics in the cyber industry.
03	**Cyber Safe Score** Establish a Cyber Safe Score that rates the level of cyber security maturity of businesses and any of their commercial products and services to boost competitiveness and secure supply chains.
04	**Partnerships with industry associations** Partner with industry associations to run organic social media campaigns on the latest scams and cyber security prevention measures for business.
05	**Monthly cyber security training** Fund industry-led educational trainings on cyber security to uplift business cyber maturity.
06	**Incentives for business** Incentivise businesses (e.g., through tax rebates, grant programs) to improve their cyber security defences and uphold employee and employer livelihoods.
07	**Cyber KPIs** Set clear cyber security KPIs so that businesses know what targets to strive to reach by 2030.
08	**Tokenisation** Tokenise personal data to prevent businesses from collecting personal information and limit the opportunity for information theft and extortion.
09	**Information security frameworks** Harmonise information security frameworks across all states and territories in Australia so that businesses only have to abide by one standard process.
10	**Best-practice technology** Adopt best-practice technology (e.g., IPv6) to ensure Australia has strong technical foundations to continually uplift business cyber security.
11	**State Cyber Security Minister** Appoint a Cyber Security Minister to the Victorian Government to ensure there is a dedicated focus on uplifting cyber security at a state level.

Cyber security graduates need to be adequately trained and employable.

02

Cyber security tertiary courses require extensive practical work experience

Practical work experience in industry, through placements and internships, is essential to ensuring the next generation of cyber security graduates are adequately trained and employable. Businesses only hire IT and cyber professionals that have practical work experience.

At present, IT and cyber security students have limited exposure to real cyber threats. It is important to note that micro-credentials do not provide the breadth of knowledge required to create cyber security experts. To meet industry's needs, cyber security tertiary courses must be delivered through a paid **apprenticeship training model.**

The UK has several levels of cyber security apprenticeships ranging from advanced, higher and degree apprenticeships.[xvii] Tertiary education providers in Australia are supportive of this model, however one problem it has is business participation. In the UK, government is the main employer of cyber trainees. The key to success is providing appropriate **incentives for businesses to take on apprentices.**

The Israeli model for cyber security training is also worth consideration. Israel's cyber security talent pool comes from within its defence force. **Cyber soldiers** are trained during the country's mandatory military service post-secondary school. Universities, government and defence join forces to train cyber professionals, proving the country with a pipeline of talent.

Israel is also actively encouraging more young **women** to enter the cyber industry. Their Mamriot[xviii] (Rising Up) cyber education program, in partnership with the Israeli National Cyber Directorate, delivers specialised cyber and technology training to Israeli high school girls. Through this program, young women develop the relevant cyber security skills to serve in the Israel Defence Force.[xix]

xvii UK Cyber Security Council (2023). ENTRY ROUTES - REGULATED QUALIFICATIONS. https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/entry-routes-regulated-qualifications/

xviii Rashi Foundation (2023). *Mamriot.* https://rashi.org.il/en/programs/mamriot/

xix Jain (2022). *Israel focuses on training next-gen to drive its cyber systems.* https://timesofindia.indiatimes.com/world/middle-east/israel-focuses-on-training-next-gen-to-drive-its-cyber-systems/articleshow/92610619.cms

In Victoria, women represent only 22 per cent of the cyber workforce, which is lower than the national average of 26 per cent.[xx] Initiatives such as the Australian Women in Security Network (AWSN) address the gender imbalance. However, this needs to be scaled up and expanded to wider demographics (e.g., mid-career workers, mature cohorts, First Nations, people with disability, and CALD communities) to properly resolve the talent shortage and promote diversity in the cyber industry.

Cyber security education should start in **school** when students are required to use digital devices in the classroom. Our next generation of digital natives need complementary education on cyber hygiene best practices. This will uplift their own skills and give them the knowledge to provide base-level cyber advice to their parents, many of whom are small business owners.

Across the board, countries and industries struggle to retain cyber professionals. The more experienced professionals become, the more probable their poaching. Some businesses claim they would be lucky to retain a cyber professional for two years. Australia must implement **effective recruitment strategies** and seek diversity in the future cohorts of cyber trainees.

An Australian Cyber Security Council would be responsible for establishing a **base-level cyber security certification** for cyber professionals, developing industry standards around concepts like the Cyber Safe Score, and managing a **registry of qualified cyber professionals.**

Yearly registrations should apply to cyber professionals, as they do for lawyers, accountants, doctors and nurses. Industry associations can deliver yearly professional development courses for cyber professionals to keep them up to date with the latest technological advancements. This would help build trust in cyber professionals.

xx AustCyber (2022). *Cyber security sector competitiveness plan*. https://www.austcyber.com/resources/scp-2022/appendix-a1

Game-changers:

12	**Apprenticeship training model** Adopt a cyber security apprenticeship training model to give the next generation of cyber security professionals the practical work experience they need to directly enter the workforce.
13	**Incentives for employment of apprentices** Incentivise businesses to take on cyber apprentices to provide the next generation of cyber security professionals with the skills to uphold industry's cyber defences.
14	**Cyber security education in schools** Incorporate cyber security education into school curriculum to uplift students' cyber hygiene best practices, enabling them to provide cyber assistance to their parents who are often small business owners.
15	**Base-level cyber security certification** Establish a base-level certification for cyber professionals to ensure minimum knowledge and experience across the industry.
16	**Cyber professional registry** Establish a registry of qualified and certified cyber professionals so businesses know who to trust when they harden their defences or have a cyber incident.

03

Financial institutions must invest in more secure technologies

Banks are a critical component of the cyber challenge. They are responsible for granting access to transactions. There are multiple measures that banks can implement to better protect businesses and consumers from fraud and scams. Security features increasingly drive competition between financial institutions. The Federal Government should encourage all financial institutions to take up stronger fraud protection measures.

Setting minimum security standards applicable to all financial institutions is the pathway froward. An example is **MFA** that should be turned on by default and linked to a Cyber Safe Score. Establishing this as the standard across the industry would eradicate competition concerns where no financial institution wants to lose customers due to transaction friction.

Australia should adopt a similar stance to MFA as the European Union (EU), which requires the technology for online payments of more than €50.[xxi] Stronger authentication measures would make online payments more secure and help fight fraud.

To ensure a high level of cyber security across the banking sector, the entire financial industry must be able to come together as a united front to fend off scammers.

Communication and **information sharing between banks** needs to be permitted under certain circumstances. Current competition laws prevent meaningful engagement and the transfer of knowledge between banks to combat scams.

Innovations in the banking industry should be shared among financial institutions to improve fraud protection across the board. Noval technologies similar to the **name verification tool** NameCheck,[xxii] which verifies account names match account numbers, are great initiatives safeguarding businesses and consumers. However, the technology is based on historical data and therefore only works for existing payees.

Banks need to have a secure mechanism where they can verify account details between each other so that all transactions, whether to new or existing payees, can be checked. This would avoid billing scams and mistaken payments.

There needs to be further investment into banking innovations that ensure people know who they are paying. **PayID**[xxiii] is a great example of this. However, the technology is limited, only allowing one PayID (e.g., phone number, ABN, email address) to be linked to one bank account at a time.

xxi Onelogin (2021). *EU Now Requires Multi-Factor Authentication for Online Payments.* https://www.onelogin.com/blog/eu-mfa-online-payments

xxii CommBank (2023). *NameCheck.* https://www.commbank.com.au/support/security/namecheck.html

xxiii PayID (2023). https://payid.com.au/

This is problematic for businesses that frequently have several banks accounts. Governments should take the lead with PayID and set it as the default payment method for invoices and payment from government services (e.g., tax returns). To increase uptake in industry of PayID, further iterations that allow multiple bank accounts to be linked to the one PayID are required.

Banking institutions should also make PayID opt-out, instead of the current opt-in model. Further, partnerships with industry associations to boost wide uptake of PayID among the business community should be explored. There needs to be a strategic campaign explaining that PayID can be linked to ABNs.

New developments in the way banks communicate with customers, such as the removal of unsolicited links in text messages,[xxiv] are welcomed. Measures like this help to differentiate authentic customer communications from malicious scams. In addition to this, banks should block high-risk crypto payments and reimburse stolen funds caused by account hackings.

Dynamic CVCs (digital cards' three-digit security number that changes every 24 hours and is accessible in online banking apps) are an important fraud prevention measure for online purchases. Westpac Bank reports it has seen an 80 per cent reduction in card fraud for customers that use dynamic CVCs, instead of static CVCs on the back of physical bank cards.[xxv] Dynamic CVCs should be rolled out across the banking industry to shield businesses and consumers from online fraud. The adoption of dynamic CVCs could be incorporated into the Cyber Safe Score to encourage wider uptake.

xxiv itnews (2023). NAB removes links from text messages. https://www.itnews.com.au/news/nab-removes-links-from-text-messages-597719

xxv Westpac (2022). *TECH IN 10: 'Dynamic CVC' sees big dip in fraud.* https://www.westpac.com.au/news/making-news/2022/06/tech-in-10-dynamic-cvc-sees-big-dip-in-fraud/

In the unfortunate circumstance of a cyber breach, Australia must reduce the **complexity of notification of a cyberattack**. At present, banks need to notify dozens of different government agencies, all with a variety of reporting timelines and acts to adhere to. Harmonising and simplifying the notification process to government of a cyber breach should be a priority. The reporting process should be centralised into one federal agency. This would enable the bright minds of cyber professionals to remain defending businesses during cyberattacks – not briefing government.

Game-changers:

17	**Multi-factor authentication (MFA)** Make MFA mandatory across the banking industry for large transactions to reduce fraud and protect businesses.
18	**Anti-competitive legislation** Relax anti-competitive and privacy legislation, in certain instances, to allow the banking industry to collaborate to detect, prevent and destruct scams and other fraudulent activity.
19	**Innovative technologies** Encourage banks to implement the latest cyber security technologies (e.g., PayID, facial ID) to keep businesses and consumers secure.
20	**Scam prevention standards** Through a Cyber Security Score, encourage minimum scam prevention standards across the banking industry (e.g., dynamic CVCs, no unsolicited links in text messages) to stop scammers from imitating banks and other businesses.
21	**Complexity of notification** Simplify the notification process to government of a cyber security breach and streamline the reporting process into one central agency.

SECURE BY DEFAULT

04

Digital devices and software must be secure by default

In a world increasingly under threat by cyber criminals, social media platforms, software and digital devices require security settings that are enabled by default. Computers should come with anti-viruses already installed. Digital platforms and apps should have the highest security settings activated from purchase.

Secure by Default as the standard across all industries (e.g., telcos, social media platforms, tech giants and banks) would provide businesses and consumers with that extra layer of protection on their digital devices. It is vital that Australia sets minimum standards such as MFA and self-updating (auto-patching) software and hardware that fixes vulnerabilities.

Major software vendors do not enable security features by default due to the friction they cause customers when adopting their platforms. Therefore, businesses endure the complex task of opting-in to higher security settings upon installation. It is important that vendors like Microsoft, Google, Amazon and Meta sell their products and services for business with the strongest security settings already in place.

Increasing **vendor liability** would also help to keep businesses safe. Large multinational corporations, such as Google and Meta, need to be held accountable for scam ads on their platforms.

Inspiration can be taken from Brazil's Bill 2630[xxvi] and the EU's Digital Services Act[xxvii] when applying penalties to tech companies for promoting illegal material.

Social media platforms should be held liable for disseminating fraudulent ads, particularly paid ads, on their platforms. While social media platforms take bulk action by banning accounts undertaking phishing and multi-level marketing (known as pyramid schemes), these are reactive measures that frequently rely on individual users reporting illicit activity. The Federal Government should implement strong regulation against fraudulent advertising.

xxvi Aljazeera (2023). *Brazil's 'fake news' bill sparks outcry from tech giants.* https://www.aljazeera.com/news/2023/5/2/brazil-fake-news-bill-sparks-outcry-from-tech-giants

xxvii Aljazeera (2022). European Parliament adopts landmark laws for internet platforms. https://www.aljazeera.com/news/2022/7/5/eu-parliament-adopts-historic-new-rules-for-internet-platforms

SMS registries, such as that in Singapore[xxviii], are an effective means of combatting scammers. The announcement of the Australian Communications and Media Authority's (ACMA) Sender ID Registry, which will block incoming illegitimate messages impersonating consumers and businesses alike, is welcomed. However, more can be done.

Restricting the number of SIM cards individuals can purchase would help to stop bad actors from bulk buying SIMs to send trojan scam texts. Government should also encourage all telcos to implement advanced scam prevention measures, such as Telstra's Cleaner Pipes initiative,[xxix] to block scam text messages.

Game-changers:

22	**Secure by Default** Make Secure by Default the industry standard for all digital devices, software and apps so that businesses have to opt-out of the highest-level security settings instead of opt-in.
23	**Vendor liability** Hold vendors accountable for scam ads on their platforms and apply penalties if they allow fraudulent material to circulate online.
24	**SMS registry** Limit how many SIM cards individuals can buy to prevent bad actors from sending illegitimate messages imitating sender IDs

xxviii Infocomm Media Development Authority (2023). *Anti-Scam Measures*. https://www.imda.gov.sg/how-we-can-help/anti-scam-measures

xxix Telstra (2023). *Snitch a scammer: our new reporting number to help customers fight SMS and MMS scams.* https://www.telstra.com.au/exchange/were-now-blocking-around-1-5-million-scam-calls-a-week

Who is best placed to deliver Australia's Cyber Security Strategy?

Industry associations, community groups and other opinion leaders are credible voices that influence behavioural change in Australian society. Businesses actively seek out industry associations' advice and guidance, especially for complex issues such as cyber security. They are trusted information sources that government should leverage to uplift the business community's cyber maturity.

ACSC has some great educational material about cyber security. However, its messages are not reaching businesses or employees. On social media, ACSC is only active on LinkedIn, Facebook, X (formerly Twitter), and YouTube. Its messages do not target Millennials and Gen Zs, who predominantly use Instagram, Tik Tok and Snapchat. A large portion of the most vulnerable workforce is neglected in the outreach of the nation's top cyber security centre.

Today, young people do not watch the nightly news on TV. They consume news via social media by following influencers, news channels or satirical news sites such as *The Betoota Advocate*,[xxx] which puts a comical spin on current news and societal trends. A recent study has shown an increase in popularity of news consumption via TikTok and Instagram in Australia.[xxxi]

The Federal Government should seek to partner with opinion leaders in society, such as industry associations and influencers, to run strategic cyber security campaigns on social media.

The idea is to leverage the online networks of these opinion leaders to influence the actions of Australians and create a society that has enhanced cyber awareness and resilience.

To be effective, cyber campaigns on social media would benefit from mixing fear and humour tactics to engage audiences and guarantee their awareness of the cyber security landscape. These campaigns need to be in the form of short, catchy videos that get people's attention in the first two seconds. Content should be organic and contain real people doing everyday activities. To connect with target audiences, the people in the videos should be relatable to ensure that audiences easily identify with the messages being put forward.

Advances in telecommunications and Internet banking were developed to make people's lives easier and more efficient. Adding arduous steps to securely use digital devices and platforms can be a chore. Australia needs to make cyber security the norm, not the exception. Business and community leaders can help achieve this goal.

---

xxx The Betoota Advocate (2023). https://www.betootaadvocate.com/

xxxi University of Canberra (2023). *Digital News Report Australia 2023: TikTok and Instagram increase in popularity for news consumption, but Australians don't trust algorithms.* https://www.canberra.edu.au/about-uc/media/newsroom/2023/june/digital-news-report-australia-2023-tiktok-and-instagram-increase-in-popularity-for-news-consumption,-but-australians-dont-trust-algorithms

The Federal Government should partner with industry associations and influencers to run strategic cyber security campaigns.

Efficiency in IT systems and digital devices is no longer paramount, security is.

The ideal future in 2030 – Businesses proactively fend off cyber criminals

Australia takes a whole-of-ecosystem approach to protect the business community from cyber threats. Governments implement proactive cyber policies. Banks are incentivised to reduce fraudulent money transactions. Telcos are accountable for illicit text messages and calls. Tech giants and social media platforms are liable for scam ads. And businesses securely manage their data, assets and funds to uplift their Cyber Safe Scores. This entire ecosystem works in unison to continuously advance cyber security across all sectors of society.

Rapid detection and response to cyber incidents are the norm. Businesses know instantly when their systems are compromised. SOCs monitor digital assets to prevent, detect, investigate, and respond to cyberattacks. Proactively monitoring all network activity and digital communication empowers businesses with the knowledge to efficiently respond to cyber threats.

The game-changer has been improving cyber security maturity of small and medium businesses. Businesses are aware they need to layer their cyber defences to prevent an attack. They refer to the Swiss Cheese Model: all holes will line up one day and cyber criminals will get through. The business community understands cyber criminals run professional organisations that even have HR departments. They know that it's a matter of 'when' not 'if' they will endure a cyberattack.

Efficiency in IT systems and digital devices is no longer paramount, security is. Individuals accept that extra precautions must be taken to remain safe in the digital era.

Cyber security training is tailored to the SMFE audience in plain and simple English. The Federal Government engages industry associations, community groups and other opinion leaders to raise awareness and educate employers and employees on the latest scams and best-practice prevention measures.

Face-to-face support is available to businesses on demand. Local Cyber Health Clinics, equipped with experienced cyber professionals, deliver solutions with expert intelligence and trust.

Businesses and consumers alike continue to seek secure platforms where security settings are turned on by default. Secure by Default is the industry standard, where advancing the security settings breeds competition among vendors to attract customers, while simultaneously enhancing cyber defences across the board.

An apprenticeship-style training model for the next generation of cyber security professionals provides students with practical work experience in industry while they study. Upon completion of their studies, students are well-equipped to directly enter the workforce and service industry's cyber defence systems.

Diminishing the return on investment for cyber criminals is an ongoing challenge. Australia continues to implement appropriate measures to uphold strong cyber resilience.

Business update complete. Reboot all systems for advanced cyber security.

Combatting cyber criminals requires a whole-of-ecosystem approach. To achieve this, cyber security messages must be disseminated across all sectors of society: business, education, family, media, arts, law, and politics. The Victorian Chamber urges the Federal and State Governments to implement our 24 pragmatic game-changers and empower small, medium, and family businesses to proactively fend off any cyber threat.

GLOSSARY

Cyber defences

Cyber defences are measures that protect information, systems and networks from a cyberattack including backups, updates, multi-factor authentication, anti-virus software, and firewalls.

Business email compromise (BEC)

BEC is an attack on a business email where a criminal attempts to trick an employer or employee into transferring funds (e.g., fake invoices).

Spoofing

Spoofing is imitating a business or individual by faking their identity.

Phishing

Phishing is a type of social engineering whereby attackers send fraudulent communications, via email, text message or phone calls, that appear to come from a trusted source. The attacker's goal is to convince victims to divulge sensitive data (e.g., login credentials, credit card numbers) or install malware.

Ransoms

Ransoms are the extraction of sensitive data from a business by cyber criminals, who extort businesses to pay a ransom fee or threaten to publicly release the data online if payments are not made.

Investment scams

Investment scams are fraudulent investment opportunities frequently published on social media and search engines.

Victorian
Chamber of Commerce
and Industry

#vcci

The Victorian Chamber of Commerce and Industry,
150 Collins Street, Melbourne, Victoria 3000
Phone: (03) 8662 5333 victorianchamber.com.au August 2023

victorianchamber.com.au