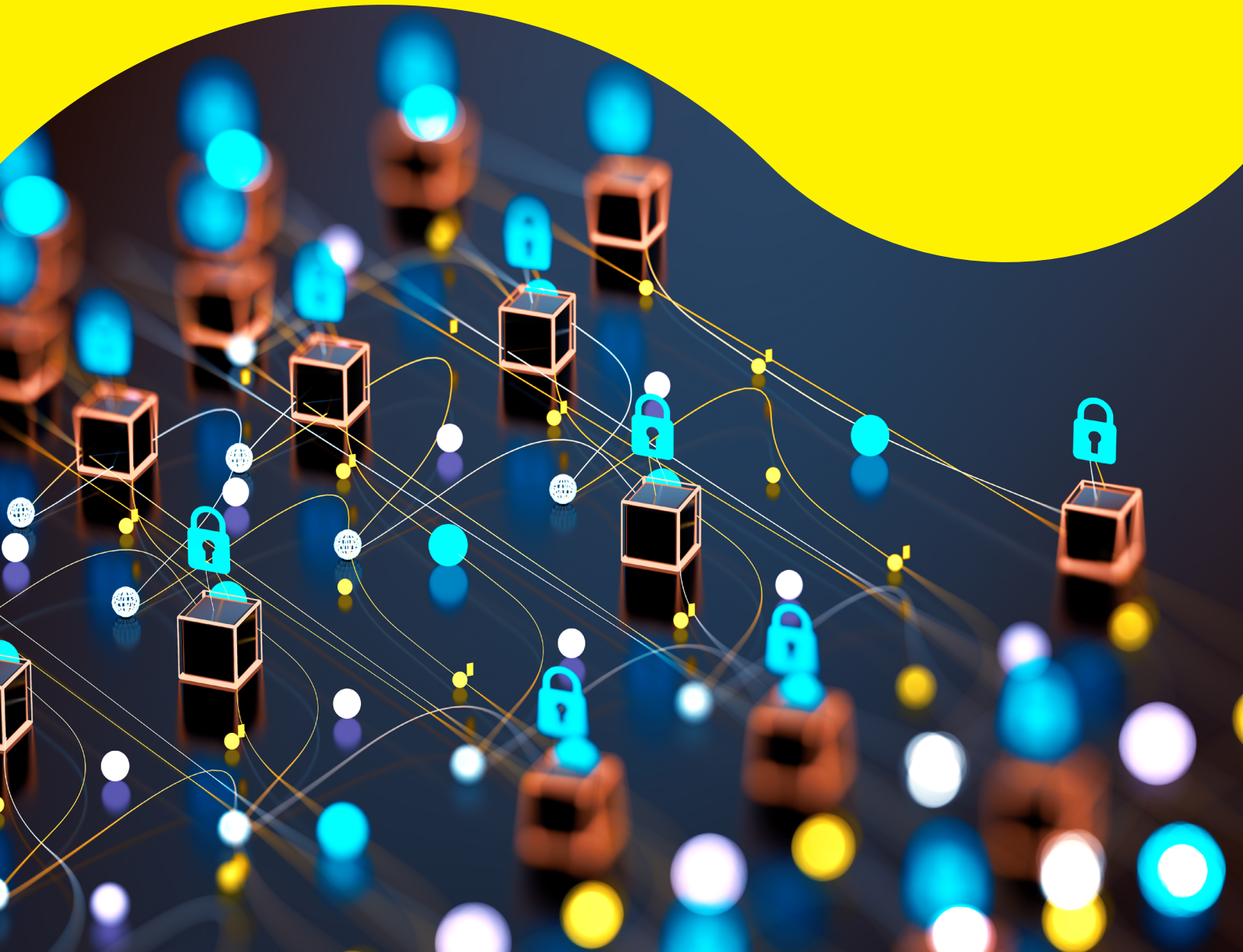
STANDARDS Australia

POSITION PAPER

Cyber Security Standards

January 2025



Contents

ABOUT STANDARDS AUSTRALIA

Standards Australia is Australia's peak non-government, not-for-profit standards organisation. We work with Australian industry, government, academia, consumer groups, and the community to help address the challenges and opportunities facing the nation. Standards Australia represents Australia at the ISO and the International Electrotechnical Commission (IEC) and specialises in the development and adoption of internationally aligned standards.

Standards Australia's vision is to be a global leader in trusted solutions that improve life – today and tomorrow. This vision has taken on renewed importance as we grapple with emerging technologies that are transformative and developing at a rate that outpaces regulation and legislation. We work with a diverse group of stakeholders nationally and internationally to act on the opportunities and challenges posed by these technologies including quantum computing, smart cities, digital twin, the metaverse, and artificial intelligence (AI).

Acronyms and Definitions

AI	Artificial Intelligence
CER	Consumer Energy Resources
IEC	International Electrotechnical Commission - Standards development organisation
ICT	Information and Communications Technology
IoT	Internet of Things
ISO	International Organization for Standardization - Standards development organisation
SA	Standards Australia - Standards development organisation
SME	Small-to-Medium Enterprise
SOC 2	System and Organisation Controls Type 2

Executive Summary

The consequences of cyber security attacks are far reaching, with the potential to impact Australian citizens and businesses around the country. In recent years cybercrime has been on the rise: According to the latest data, approximately every six minutes a new cybercrime incident is reported to the Australian Signals Directorate.[1] As the world becomes increasingly interconnected, the need to implement safe cyber security practices and mechanisms will be paramount.

The Australian Government's 2023-2030 Cyber Security Strategy outlines the Government's plan to establish Australia as a world leader in cyber security by 2030. The strategy incorporates six shields to mitigate cyber threats and build Australia's cyber resilience, including through cyber awareness campaigns, enhancing critical infrastructure security, and expanding the nation's cyber workforce. As Australia strives to become a global leader in cyber security, implementing relevant standards can be vital in protecting businesses, citizens and national sovereignty.

Standards foster global harmonisation and industry alignment, and aim to strengthen cyber security practices in key areas such as risk management, data protection and network security. Embracing and advancing standards will support national cyber efforts and enhance Australia's position as a world leader in cyber security.

This position paper has been developed by Standards Australia in consultation with experts from Australia's national standards technical committee for information security, cyber security and privacy protection (IT-012). It seeks to achieve the following objectives:

- Outline key cyber security standards and regulatory frameworks in Australia and internationally
- Demonstrate how Standards Australia, and standards more broadly, support Australian cyber security priorities
- Provide standards-related recommendations to enhance Australia's cyber posture

In this paper, Standards Australia presents four recommendations to encourage the uptake and implementation of standards to support a cyber secure nation.These recommendations include initiating the adoption of relevant international standards for digital technologies, supporting industry engagement in standards development, and enhancing awareness of cyber security standards among businesses.

1 2022–23 ASD Cyber Threat Report, Australian Signals Directorate (2023)

Recommendations Summary

Below is a summary of the recommendations. Recommendations are provided in full on page 15 of the report.

Recommendation 1: Adopt relevant international standards for emerging technologies

Recommendation 2: Raise industry awareness and understanding of cyber security standards

Recommendation 3: Support industry participation in Australian cyber security standards development

Recommendation 4: Implement Australian Cyber Security Strategy recommendations to increase security of consumer-grade smart devices

Introduction

The current domestic cyber security landscape is characterised by a complex interplay of evolving threats, increasing digital reliance, and government initiatives. Cyber threats are intensifying at an unprecedented pace, with malicious cyber actors increasingly targeting individuals, businesses, government systems and critical infrastructure. Between mid-2022 and mid-2023, the average cost of cybercrime for Australian businesses rose by 14%.[2] Given that cybercrime is expected to rise, establishing strong national cyber defences will be crucial.

Under the 2023-2030 Australian Cyber Security Strategy, the Australian Government seeks to make Australia a world leader in cyber security by prioritising six cyber shields (Figure 1). These shields provide a holistic approach to building national cyber capabilities, ensuring the protection of businesses, citizens and critical infrastructure against cyber threats. Leveraging Australia's robust regulatory frameworks, trusted partnerships, and internationally aligned standards can support the success of the cyber shields success of the cyber shields.

Standards play an important role in the cyber security ecosystem, establishing best practices that aim to promote data security, global interoperability and the safety of digital products. Additionally, standards promote consistency across industry and can enhance consumer trust consumer trust.

Figure 1: Six cyber shields.
Source: 2023–2030 Australian Cyber Security Strategy, Department of Home Affairs (2023)
Reproduced from 2023-2030 Australian Cyber Security Strategy published by the Australian Government at https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf, licensed under CC BY 4.0 licence.

2 ASD Cyber Threat Report 2022-2023, Australian Signals Directorate (2023)

Current cyber security standards and regulatory landscape

Significant progress has been made in the development of cyber security standards at both the national and international level. As Australia looks to future cyber security needs, the adoption of relevant international standards should be prioritised to support transparency, market enablement and digital trade. Meanwhile, understanding the existing standards landscape will enable the identification of potential gaps and opportunities for further standards adoption and development. This section provides a high-level overview of key standards and regulations for cyber security in Australia and internationally (as of November 2024).

Australian landscape

Australia has a robust cyber security standards landscape and strong policy frameworks that support national cyber priorities. The adoption of key international cyber security standards aims to contribute to a trusted digital trade environment and the protection of critical assets (Table 1). For example, AS/NZS ISO/IEC 27001:2023, *Information security, cybersecurity and privacy protection-Information security management systems-Requirements,* is a flagship cyber security standard that provides guidance for companies seeking to establish, implement, maintain and improve an information security management system. The standard provides information to support with the development of risk mitigation strategies, incident response plans, and security procedures to ensure businesses are equipped to manage cyber incidents.

Australia has also published AS 27701:2022 - *Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines*. This standard provides guidance on implementing a privacy information management system, modifying two of the most widely adopted international cyber security standards to accommodate existing Australian policies and regulations.

The rising use of smart devices, such as home security systems and electric vehicle smart chargers, introduces new vulnerabilities that could have widespread consequences. To help mitigate large-scale attacks on smart devices, Australia has adopted AS ETSI EN 303 645:2023, *Cyber security for consumer Internet of Things: Baseline requirements*. The standard specifies high-level security and data protection provisions for consumer Internet of Things (IoT) devices that are connected to network infrastructure, such as the Internet or home network, and their interactions with associated services.[3]

Cyber security challenges are also emerging in the area of consumer energy resources (CER). These challenges are rising due to the interconnected, interoperable and remote-control capabilities of CER devices including solar panels, electric vehicles and home energy storage systems. AS IEC 62443.3.2:2024, *Security for industrial automation and control systems, Part 3.2: Security risk assessment for system design*, offers potential mitigation strategies for CER cyber-attacks by providing a risk assessment methodology for the cyber security of industrial control systems. Nonetheless, the CER ecosystem is complex, and existing standards may need continuous refinement to meet emerging requirements.

Alongside standards, policy and regulatory frameworks play a fundamental role in protecting critical assets and government systems from cyber attacks (Table 2). For example, the Security of Critical Infrastructure Act 2018 outlines the protection of critical infrastructure in sectors including energy, defence, health and transport. It ensures that sectors covered by the Act have appropriate risk management plans in place and are equipped to respond to cyber incidents. At a state and territory level, information security requirements introduced by Australian state and territory governments should seek to align with existing regulations to ensure harmonisation across states and territories and help reduce regulatory burdens.

3 Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI (2020)

Recognising the need for strong cyber security measures at the organisational level, the Australian Signals Directorate has developed the Essential Eight to help organisations protect their IT networks from common cyber threats. The Essential Eight is a set of eight mitigation strategies that include patch applications, multi-factor authentication, admin privilege restriction and application control. Implementing the Essential Eight can help businesses assess their defence capabilities, reduce cyber risks, and improve their cyber posture in a cost-effective manner.

Key Australian Standards
AS/NZS ISO/IEC 27001:2023, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*
AS 27701:2022, *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*
AS/NZS ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls*
AS ISO/IEC 27003:2017, *Information technology - Security techniques - nformation security management systems - Guidance*
AS ISO/IEC 27004:2018, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*
AS/NZS ISO/IEC 27005:2012, *Information technology - Security techniques - Information security risk management*
AS ISO/IEC 23894:2023, *Information technology - Artificial intelligence - Guidance on risk management*
AS IEC 62443:2024, *Series Security for industrial automation and control systems*
AS ETSI EN 303 645:2023, *Cyber security for consumer Internet of Things: Baseline requirements*

Table 1: Key Australian Standards relating to cyber security

Key Australian Policy and Regulatory Frameworks
Security of Critical Infrastructure Act 2018 (Cth)
Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth)
Protective Security Policy Framework
Information Security Manual
Essential Eight
Telecommunications Act 1997 (Cth)

Table 2: Key Australian policy and regulatory frameworks relating to cyber security

International landscape

The international cyber security landscape has matured in recent years with the proliferation of international standards and frameworks aimed at enhancing global digital security. There is ongoing work at the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) to ensure international standards can meet the security demands of emerging technologies such as artificial intelligence (AI) (Table 3). Adopting and implementing relevant international standards for critical and emerging technologies may help Australia embrace these new technologies while striving for global compatibility and interoperability.

In the field of AI, ISO/IEC 42001:2023, *Information technology — Artificial intelligence — Management system* is a broad ranging standard that provides guidance on establishing, implementing, maintaining, and continually improving an AI management system. To help organisations understand and apply this critical AI standard, Standards Australia has partnered with the Australian National University to develop an online learning module, which provides an in-depth overview of the standard and its role in AI governance.

Guidance on security threats and failures in AI systems is currently being developed through the international standard DR ISO/IEC 27090, *Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems*. The draft standard aims to assist organisations in understanding the consequences of security threats to AI systems and provide information on how to detect and mitigate these threats. The emergence of AI presents new risks, and Standards Australia will be closely monitoring international developments in AI cyber security standards. See Recommendation 1.

Acknowledging the importance of consumer trust in IoT products, the ISO and IEC are currently drafting DR ISO/IEC 27404.2, *Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT*. This draft standard defines a Universal Cybersecurity Labelling Framework for the development and implementation of cybersecurity labelling programs for consumer IoT products. It includes guidance on risks, roles and responsibilities, conformity assessment, and mutual recognition considerations. The Framework seeks to facilitate market access and reduce compliance costs for IoT manufacturers by supporting the mutual recognition of labelling schemes across jurisdictions. Standards Australia encourages the consideration of international labelling frameworks such as those developed by the ISO and IEC in the development of an Australian labelling scheme for IoT. See Recommendation 4.

At a regional level, regulatory frameworks have been implemented to keep pace with increased digitalisation and an evolving cyber security threat landscape (Table 4). In the European Union, the NIS2 Directive provides a common framework for cyber security across the EU, with a focus on cyber preparedness, cooperation, and protection of critical sectors. The Directive mandates EU organisations to implement robust cybersecurity measures and establish effective incident response plans to enable a rapid response to cyber incidents when they arise.

To help service organisations protect customer data in the US, the American Institute of Certified Public Accountants developed the System and Organisation Controls Type 2 framework (commonly known as SOC 2). The voluntary framework specifies how organisations should protect customer data from unauthorised access, security incidents, and malicious activity. In order to obtain SOC 2 compliance, organisations must demonstrate adherence to the five trust principles outlined in SOC 2: security, confidentiality, availability, privacy, and processing integrity. Achieving compliance can build customer trust, reduce the risk of data breaches, and improve business reputation.

Key International Standards and Publications
ISO/IEC 19772:2020, *Information security — Authenticated encryption*
ISO/IEC 27014:2020, *Information security, cybersecurity and privacy protection — Governance of information security*
IEC TS 62443-1-1:2009, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*
ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
ISO/IEC 27032:2023, *Cybersecurity — Guidelines for Internet security*
ISO/IEC TR 6114:2023, *Cybersecurity — Security considerations throughout the product life cycle*
ISO/IEC 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security Part 1: Introduction and general model*
ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication Part 1: General*
ISO/IEC 42001:2023, *Information technology — Artificial intelligence — Management system*
DR ISO/IEC 27404.2, *Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT*
DR ISO/IEC 27091.2, *Cybersecurity and Privacy — Artificial Intelligence — Privacy protection*
DR ISO/IEC 27090, *Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems*
DR ISO/IEC 27019, *Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry*

Table 3: Key international standards and publications relating to cyber security, DR = Draft

Key Policy and Regulatory Frameworks by Region
Europe
European Union Cyber Resilience Act
NIS2 Directive
General Data Protection Regulation
European Union Cybersecurity Act
USA
NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
System and Organization Controls Type 2
US Cybersecurity Information Sharing Act
Health Insurance Portability and Accountability Act 1996
UK
UK General Data Protection Regulation
Data Protection Act 2018
Network and Information Systems Regulations 2018
Product Security and Telecommunications Infrastructure Act 2022

Table 4: Key regional policy and regulatory frameworks relating to cyber security

Australia's involvement in cyber security standards

Australia has been for many years and remains a key contributor to the development of international cyber security standards, providing expertise across a range of areas. Participation in the development of international standards allows Australian experts to shape the future of cyber security and advance the interests of Australian consumers, industry and government at the international level. In addition, standardisation efforts can open new markets for emerging technologies, ensuring interoperability and facilitating international trade while managing associated security risks.

National involvement

Standards Australia has been a major driver in developing standards that help to ensure the security, reliability, and accessibility of Australia's digital economy. At a national level, the IT-012 technical committee is responsible for the development of cyber security standards that aim to protect Australian businesses and communities.

This joint Australian and New Zealand standards committee is made up of members from a broad range of organisations including consumer groups, government, technical associations, academic organisations, and certification bodies. The committee's scope of work covers the development and adoption of standards in areas including:

- Management of information and ICT security
- Management of personal information
- Conformance assessment, accreditation and auditing requirements for information security management systems
- Cryptographic and other security mechanisms
- Techniques for managing the identity of people, organisations, and items of equipment and software
- Security management support documentation
- Security evaluation criteria and methodology

IT-012, *Information security, cyber security and privacy protection*, was created to mirror the ISO/IEC JTC-1 /SC 27 international committee of the same name. To date, the committee has adopted eighteen international standards for cyber security and information technology.

International involvement

As Australia's peak national standards body, Standards Australia is responsible for participating in the development and adoption of international standards through ISO and IEC. The organisation works with industry, government, and the community to facilitate Australian participation in the development and adoption of relevant standards.

International standards developed by ISO and IEC can be important conduits of trade facilitation and interoperability across geographic borders. They create cyber security guardrails that aim to protect societies around the world. Adopting and aligning with international standards can help ensure Australia's cyber security frameworks are compatible with international best practice and the global market, supporting innovation in a constantly changing digital environment. See Recommendation 1.

Experts from the relevant national technical committee represent Australia's interests on several international standards development committees including ISO/IEC JTC 1/SC 27, the committee responsible for information security, cybersecurity and privacy protection standards. This representation is important in ensuring that Australian interests are reflected in the development of global cyber security standards. Active participation also enables Australia to expedite the adoption of relevant standards, which in turn can foster a robust and secure digital environment in line with national cyber objectives and international frameworks. See Recommendation 3.

Role of cyber security standards in protecting businesses

The far-reaching consequences of cyber-attacks highlight the need for clear guidance and standards to help businesses develop robust cyber defence capabilities, regardless of whether they are a small company or a large corporation. Providing education and guidance to support businesses with the implementation of cyber security standards can help protect critical assets and mitigate exposure to cyber incidents. This section outlines how standards can protect Australian businesses across key aspects of cyber security. See Recommendation 2.

Stronger authentication

Strict identity verification and authentication is often a first line of cyber defence, functioning as a rigorous identity verification process. By meticulously verifying user identities, it aims to ensure that only authorised individuals and devices have access to designated resources. Implementing strong authentication standards can be an important means for organisations to mitigate cyber security risks such as unauthorised access and data theft. ISO/IEC 9798-1:2010 - *Information technology - Security techniques - Entity authentication*, provides a structured approach to authentication by outlining protocols and methods to help ensure authorised parties can access sensitive information. By implementing this standard, organisations can make it harder for attackers to impersonate authorised users.

Standard	Title	Description
ISO/IEC 9798-1:2010	Information technology - Security techniques - Entity authentication	Specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques.
AS/NZS ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection - Information security controls	Provides a code of practice for information security controls, offering guidance on selecting controls to implement an information security management system based on ISO/IEC 27001.

Table 5: Key standards for cyber authentication

Patch management

Patch management involves the systematic process of identifying, acquiring, and deploying software updates, known as 'patches', that address known vulnerabilities in operating systems and applications. These vulnerabilities are weaknesses in software code that could be exploited by individuals wanting to gain unauthorised access to systems and data.

Standards can support effective patch management by providing a clear framework for organisations to follow. For example, AS/NZS ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls,* offers best practices and control objectives related to key cyber security aspects. Organisations around the world have implemented international cyber security standards such as ISO/IEC 27002:2022 to guide best practice and manage risks (see Case Study 1).

Standard	Title	Description
ISO/IEC 15408-1:2022	Information security, cybersecurity and privacy protection - Evaluation criteria for IT security	General concepts and principles of IT security evaluation.
ISO/IEC TR 20004:2015	Information technology - Security techniques - Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	Specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.
AS/NZS ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection - Information security controls	Provides guidance for organisations looking to establish, implement, and improve an Information Security Management System focused on cyber security.

Table 6: Key standards for patch management

Case Study 1 - Strengthening cyber security through standards at the Commonwealth Bank of Australia

Banks are constantly under attack from a range of cyber actors. To strengthen their cyber security posture, the Commonwealth Bank of Australia has implemented an array of security controls aligned with international standards such as ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, and ISO 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls*. This proactive approach to cyber security and alignment with international best practice has helped maintain the security of systems and processes at the bank, and mitigate major cyber incidents.

Source:
Commonwealth Bank of Australia 2023 Annual Review

Case Study 1: Cyber security standards at the Commonwealth Bank of Australia

Protection of personal information

Personal information is a valuable asset to organisations, but its inherent value also makes it a prime target for cyber criminals. Large scale data breaches have had significant consequences including identity theft, financial loss, and reputational damage (see Case Study 2). Standards can play a role in supporting strong information security practices and safeguarding valuable data held by businesses. For example, AS/NZS ISO/IEC 27559:2024, *Information security, cybersecurity and privacy protection - Privacy enhancing data de-identification framework*, provides a framework for the de-identification and protection of personal data.

It sets ground rules for businesses to disclose information without compromising the privacy of individuals.

Standard	Title	Description
IEC TS 62351-1:2007	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	Information security for power system control operations.
AS/NZS ISO/IEC 27559:2024	Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework	Provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.
ISO/IEC 30111:2019	Information technology - Security techniques - Vulnerability handling processes	Provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service.

Table 7: Key standards for data security

Case Study 2 – Optus Cyber Vulnerabilities Exposed

In September 2022, Australian telecommunications provider Optus experienced a major data breach that compromised the personal information of millions of customers. Information compromised in the breach included names, dates of birth, driver's license details and passport numbers. Following the breach, the Australian Government amended the Telecommunications Regulations 2021 (Cth) to better protect Australians from data breaches, while the Department of Home Affairs established the Commonwealth Credential Protection Register to prevent the fraudulent use of compromised identity documents. This large-scale attack underscores the importance of robust cyber security frameworks and standards in a continually evolving threat environment.

Sources:
Optus media centre, 22 September 2022
Australian Communications and Media Authority, 8 January 2024

Case Study 2: Optus data breach

Recommendations

This section details four recommendations to enhance the national cyber standards landscape and position Australia as a global leader in the digital security ecosystem. Additionally, these recommendations seek to uplift cyber capabilities among businesses and instil consumer confidence in digital products while promoting market access and innovation.

Recommendation 1: Adopt relevant international standards for emerging technologies

Critical and emerging technologies provide an opportunity to transform the national economy and drive innovation. However, they may also be used by malicious actors to target Australian networks and systems in new and sophisticated ways. Standards Australia, the Australian Government and stakeholders should work together to propose the adoption of relevant international standards that support the cyber security of emerging technologies such as AI and consumer energy resources (CER). International standards can present an agile solution to shape the responsible design, deployment and evaluation of emerging technologies in the digital economy. Adopting relevant international standards can help Australia accelerate the secure deployment of new technologies by promoting trust, security and confidence that these technologies are fit for purpose.

Artificial intelligence:

Artificial intelligence has the potential to deliver new capabilities and benefits to the Australian economy and community. However, as with any new technology, these capabilities can challenge public perception and trust if not governed appropriately. International standards such as SATR ISO/IEC 24028:2024, *Information technology - Artificial intelligence - Overview of trustworthiness*, can support the safe use of AI by providing a common base for the responsible and trustworthy use of AI across sectors and jurisdictions. Adopting relevant international standards can help ensure AI systems are fit for purpose and deliver their intended benefits to the Australian society. These standards may also support interoperability and regulatory compatibility with AI systems in other jurisdictions, such as those being developed by the EU and the US, thereby reducing barriers to trade.

Consumer energy resources:

The rise in consumer energy resources, for example electric vehicles and rooftop solar panels, emphasises the growing importance of energy security. Standards Australia has conducted extensive research on cyber security standards for consumer energy resources as part of the Roadmap for CER Cybersecurity. The report identifies key international standards that Australia should adopt to mitigate CER-related cyber risks. These include standards for smart grid cyber security, industrial automation security, and the protection of power utility systems. The adoption and implementation of relevant international cyber security standards can help ensure that CER devices are secured from the outset, potentially reducing risks associated with their deployment and positioning Australia as a global innovator in energy security.

Recommendation 2: Greater education and support for industry on cyber security standards

A cyber resilient nation relies on digitally secure organisations. Standards can offer clear guidance for businesses in an ever-evolving technology landscape by setting common frameworks and ensuring consistency across borders. In collaboration with the Australian Government and industry, Standards Australia sees an opportunity to raise awareness of cyber security standards among industry and provide guidance for businesses seeking to implement these standards.

Foremost, greater education is needed to raise industry awareness on the benefits of cyber security standards, where they can be applied, and how they can be implemented. This education should involve training on how to implement key standards, such as AS/NZS ISO/IEC 27001:2023, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, to strengthen organisational cyber capabilities. Sector specific guidance should also be provided to address the unique cyber security challenges faced by different industries. For example, guidance tailored to the type of data businesses handle and the technologies they use. Ensuring businesses have the resources to implement appropriate standards can ensure they are equipped to respond to cyber attacks when they may occur.

Small-to-medium enterprises (SMEs) make up over 97% of all Australian businesses, yet they are often challenged by the time, resources and expertise required to implement cyber secure practices. Standards can be a particularly useful solution for time-poor organisations with minimal resources and knowledge of cyber safe practices. The ISO/IEC 27001:2022 handbook can be a valuable resource designed to simplify the process of implementing ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. The handbook provides useful information and practical guidance for smaller organisations seeking to implement an effective information security management system. Tailored to the unique needs of SMEs, the handbook includes actionable steps, case studies, and cost-effective strategies for implementing the standard, enabling SMEs to identify cyber risks and improve their cyber posture without placing a burden on their limited resources.

Recommendation 3: Support industry participation in Australian cyber security standards development

Cyber security standards are continually being developed and revised to respond to the rapidly evolving threat landscape. Industry has a crucial role to play in ensuring these standards meet the diverse cyber security needs across all sectors of the economy. Contributions from industry are essential to the development of robust, well-rounded, consensus-based documents. In recent years, relevant national standards committees have published several key cyber standards that help to keep businesses safe and provided valuable guidance to a complex field. Without continued input from industry, there is a risk that cyber security standards may not fulfil their intended purpose as market enablers. Standards Australia is committed to ensuring Australian Standards reflect the needs of businesses through ongoing industry engagement and outreach activities. In collaboration with relevant national standards committees and cyber security experts, Standards Australia will focus on uplifting cyber resilience across sectors by working with stakeholders to build industry engagement and participation in standards development projects.

Recommendation 4: Implement Australian Cyber Security Strategy recommendations to increase security of consumer-grade smart devices

Standards Australia supports the Australian Government's plan to develop a mandatory standard for IoT devices and an associated voluntary labelling scheme for consumer-grade smart devices. These initiatives will help provide consumers with confidence in the cyber security claims of the devices and solutions they are purchasing, while maintaining adaptability for manufacturers to implement security measures in accordance with need.

To support international trade and minimise implementation costs, the Australian Government should consider adopting and leveraging recognised international standards for IoT devices. Internationally aligned standards should also be considered in the establishment of minimum baseline requirements for cybersecurity to ensure consistency with guidance outlined in the Australian Government's voluntary Code of Practice for IoT devices. Standards Australia's understanding and participation in the international standards landscape would strongly support the Australian Government's standardisation objectives, helping to ensure regulatory compatibility and interoperability with other jurisdictions.

With over a century of standards development expertise and an extensive network of relevant stakeholders, Standards Australia is well placed to support the development of a mandatory standard for IoT devices and a voluntary labelling scheme for consumer-grade smart devices. These schemes are vital to the cyber security of IoT, and are a sensible pathway towards protecting governments, businesses and consumers from cyber, privacy and online safety threats.

Conclusion

The rising frequency and sophistication of cyber-attacks holds significant implications for individuals, businesses, and national sovereignty. While cyber security is essential for mitigating risks, it also presents an opportunity for Australia to expand its cyber industry, boost productivity and accelerate the digital economy.

Building cyber capabilities will require significant investment from both private and public sectors. The recommendations provided in this report call on Standards Australia, the Australian Government and industry to work together to enhance national cyber security and drive greater cyber resilience across the economy.

Standards provide a foundation to enhance interoperability, data protection and incident recovery. Globally aligned systems and processes can help safeguard sensitive information, protect critical infrastructure and instil trust in emerging technologies. A strong cyber security framework, underpinned by robust standards and regulations, can support increased resilience and stability, helping to create a secure and prosperous region where everyone benefits from the global digital economy.

As part of ISO and IEC processes, Standards Australia continues to facilitate Australian participation in the development and harmonisation of international standards. This is only possible with the contributions of Australian experts and supporting nominating organisations who participate in Australia's national mirror committees and their international counterparts to help draft and adopt cyber security standards and progress the future work program. Standards Australia welcomes the involvement of new expert contributors. For those interested in actively participating in cyber security standards as they continue to evolve, please contact SEM@standards.org.au. Additional resources on Standards Australia's initiatives for critical and emerging technologies can also be accessed on Critical and Emerging Technologies page on our website.