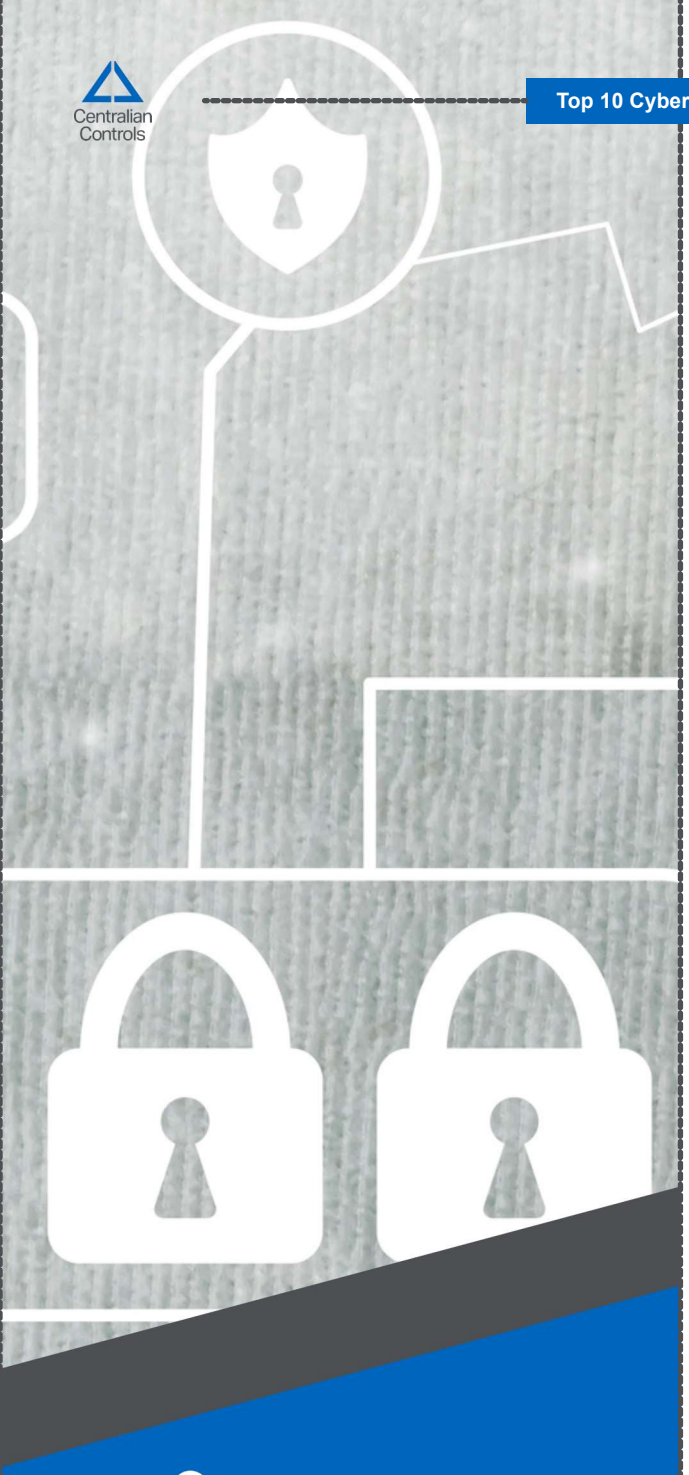
Centralian Controls

Top 10 Cyber Security Best Practices for SMEs

White Paper

Table of Contents



4.45 Million

This is the global average cost of a data breach in USD. That is equivalent to almost 7 million AUD. Is this something that you can afford to pay?

Source: Cost of a Data Breach Report 2023 (IBM)

Overview

As the digital landscape evolves, small and medium-sized enterprises (SMEs) in Australia are increasingly adopting technologies like artificial intelligence, cloud computing, and the Internet of Things (IoT). However, with these advancements come significant cyber security challenges. The ASD Cyber Threat Report 2022-2023 indicates a worrying trend: nearly 94,000 cybercrime reports were filed, marking a 23% increase, which equates to one report every six minutes. Furthermore, the 2023 Data Breach Investigations Report by Verizon reveals that SMEs and large corporations now share similar cyber security risks due to common technology use, yet SMEs often lack the extensive security resources of larger firms.

Considering the global average cost of a data breach is about 4.45 million USD (around 7 million AUD), the financial impact on SMEs can be devastating. It's imperative for these organisations to prioritise cyber security as a key aspect of their operational strategy.

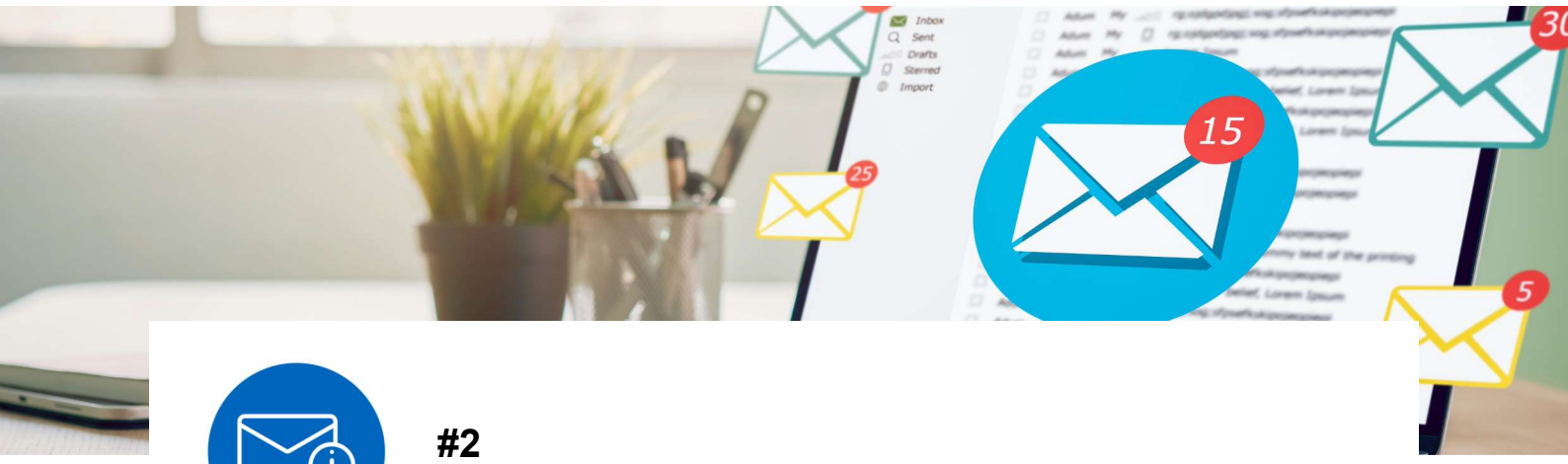
In line with this, the 2023-2030 Australian Cyber Security Strategy outlines specific plans to support SMEs in enhancing their cyber security. This white paper aligns with these national efforts, offering practical and effective best practices tailored for SMEs. These guidelines are designed to help small and medium businesses fortify their cyber defences, ensuring resilience and compliance in an increasingly complex cyber threat landscape.

#1 Security Awareness Training

The human element often represents the weakest link in an organisation's cyber security defence. In fact, a report says that around 74% of breaches were due to the human element. The Australian Signals Directorate (ASD) strongly recommends annual cyber security awareness training for all personnel. This is crucial because threat actors frequently exploit human vulnerabilities through social engineering tactics like phishing, which can lead to significant security breaches. Effective training equips employees with the knowledge to recognise and respond appropriately to these tactics, thereby reducing the risk of successful cyber attacks.

What SMEs Should Do:

- *Implement a cyber security awareness training program for all staff, focusing on current threats and recognising social engineering tactics.*
- *Integrate cyber security awareness into the induction process for new employees.*
- *Regularly test staff with mock phishing exercises to evaluate training effectiveness.*
- *Ensure training content is regularly revised to include the latest cyber security threats and practices.*
- *Promote a culture where staff are encouraged to report suspicious activities.*



#2
Email Security

Email remains a primary vector for cyber attacks, with a significant portion of breaches originating from malicious email activities. The convenience and widespread use of email make it a favoured target for attackers, often using tactics like phishing, spear-phishing, and malware distribution. Ensuring robust email security is crucial in safeguarding sensitive information and maintaining business integrity.

What SMEs Should Do:

- *Implement advanced email filtering solutions to block spam, phishing, and malicious attachments.*
- *Train employees to identify and report suspicious emails, especially those requesting sensitive information or containing unusual requests.*
- *Use email authentication methods like DMARC, SPF, and DKIM to prevent email spoofing and phishing.*
- *Regularly backup email data and ensure recovery processes are in place to mitigate the impact of email-based attacks.*
- *Encourage the use of secure email practices, such as avoiding the transmission of sensitive information via email whenever possible.*

#3
Access Control

Access control is a vital component of cyber security, especially considering that a significant portion of breaches involve compromised credentials. Reports like Verizon's Data Breach Investigations 2023 indicate that SMEs are particularly vulnerable, with credentials being compromised in a notable percentage of incidents. This is even more critical in SMEs than large corporations. Effective access control mechanisms are critical to thwart unauthorised access and safeguard business resources.

What SMEs Should Do:

- *Enforce strong password policies and change them regularly, especially post-incident*
- *Implement multi-factor authentication to add an extra security layer*
- *Conduct regular audits for all user accounts and access rights to prevent inappropriate permissions*
- *Educate staff on the importance of credential security and the risks of sharing login details*
- *Each employee should have their own unique login credentials and should never share them with anyone, not even colleagues or supervisors*
- *Regularly review user activity logs to identify any suspicious or unauthorised access*

#4
Network Security

Network security is the bedrock of protecting an SME’s digital assets and information flow. It involves deploying a combination of hardware and software tools to guard against intrusions and attacks. Segmentation, a key strategy in network security, divides the network into segments or subnets, limiting attackers' ability to move laterally within the system. This not only enhances security but also simplifies management and containment of potential breaches.

What SMEs Should Do:

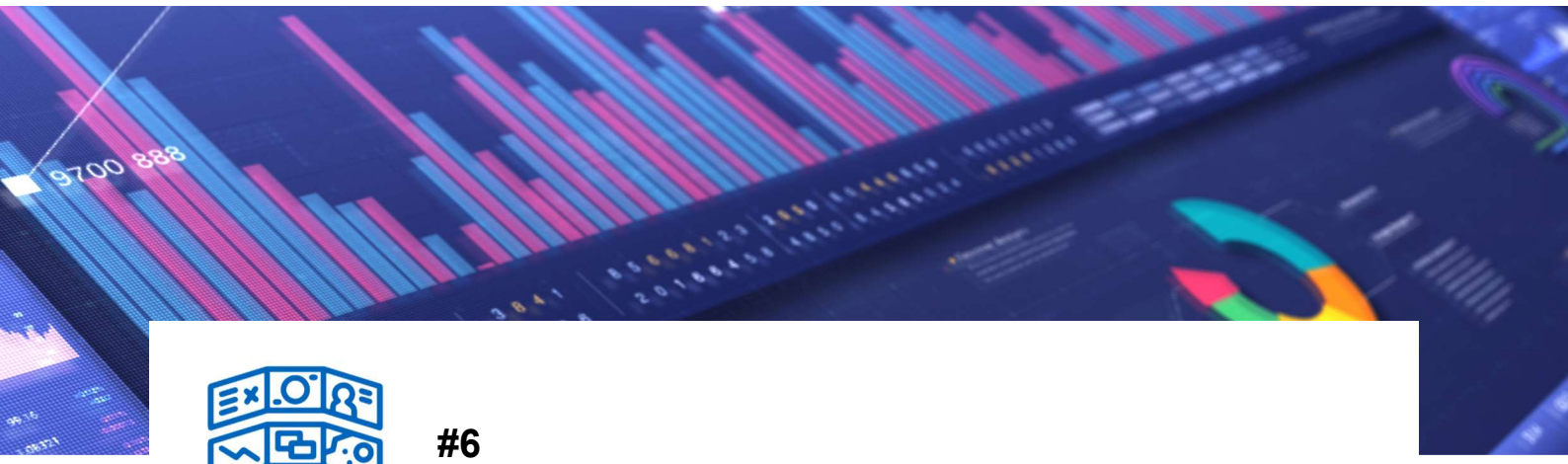
- *Deploy firewalls and intrusion detection systems to monitor and control incoming and outgoing network traffic*
- *Segment the network to create secure zones, especially for sensitive data, ensuring that a breach in one segment doesn't compromise the entire network*
- *Regularly update and patch network devices to protect against known vulnerabilities*
- *Implement strong encryption for data in transit across the network to prevent interception and unauthorised access*

#5
Endpoint Detection and Response

In the ever-evolving cyber threat landscape, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) have emerged as indispensable tools for SMEs. While EDR focuses on monitoring and responding to threats at the endpoint level, XDR takes a broader approach, integrating data from multiple sources across the IT infrastructure, including endpoints, networks, cloud environments, and user behavior. This holistic approach provides a more comprehensive understanding of security risks and enables more effective threat detection and response.

What SMEs Should Do:

- *Select an EDR solution tailored to the business's specific needs and risk profile.*
- *Train technical teams on the nuances of the EDR system to ensure they can manage and respond to alerts effectively.*
- *Incorporate EDR insights into the broader security strategy to inform policy updates and security improvements.*
- *Perform regular simulations and response drills to refine the EDR process and ensure readiness for various attack scenarios.*
- *For organisations with limited in-house security expertise, consided engaging an MSSP for EDR/XDR functionalities.*



#6
Log Management

Log Management is vital for maintaining visibility across an SME's network, providing insights into operational performance and security-related events. It serves as a foundational element for compliance with various industry regulations and frameworks, such as ISO/IEC 27001, which requires diligent record-keeping and analysis of log data for security monitoring. Integrating Security Information and Event Management (SIEM) systems enhances this process, enabling more efficient and intelligent analysis of log data.

What SMEs Should Do:

- *Set up systems to collect logs from all critical sources like servers, network devices, and applications, ensuring comprehensive log coverage.*
- *Consider implementing a SIEM system for advanced analysis and correlation of log data, particularly for identifying complex security threats.*
- *Develop a log retention policy that aligns with both operational needs and compliance requirements, ensuring essential logs are retained but not excessively.*
- *Utilise SIEM or other analysis tools to regularly review log data for indicators of security incidents or operational anomalies.*
- *Schedule periodic reviews of the log management process, including SIEM configurations, to adapt to new threats and evolving operational environments.*

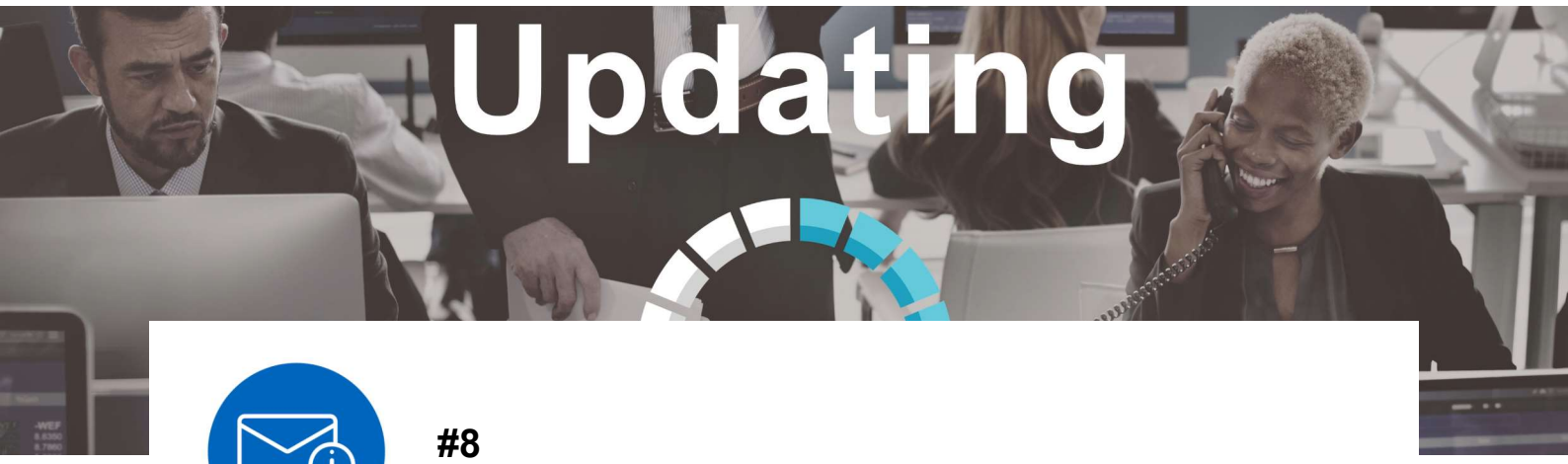
#7

Vulnerability Management

Vulnerability Management is a proactive approach to managing network security, involving regular scans to identify weaknesses before they can be exploited. It encompasses both Vulnerability Assessment, which systematically reviews security weaknesses, and Penetration Testing, where security professionals simulate cyber attacks to test defenses. It's a continuous cycle of assessment, identification, and remediation that's essential for maintaining strong cyber security posture.

What SMEs Should Do:

- *Perform Vulnerability Assessments semi-annually to identify and evaluate security weaknesses within their systems, considering their resources and risk exposure.*
- *Schedule external Penetration Testing at least once a year or more frequently if dealing with sensitive data or operating in a high-risk industry.*
- *Conduct internal Penetration Testing as resources allow, aiming for at least once a year to ensure robust internal security.*
- *Prioritise the remediation of identified vulnerabilities, focusing on the most critical risks first, and address less critical vulnerabilities in a timely manner.*
- *Establish a consistent patch management process, ensuring that patches for identified vulnerabilities are applied promptly and system maintenance schedules are adhered to.*



#8
Asset and Patch Management

Asset and Patch Management are crucial for maintaining the security and integrity of an SME's technology assets. Effective asset management ensures all assets are accounted for and assessed for risk, while patch management ensures that identified vulnerabilities within software are addressed through timely updates. Together, they form a critical barrier against many common cyber threats.

What SMEs Should Do:

- *Maintain an up-to-date inventory of all digital assets, including hardware, software, and relevant data.*
- *Implement a structured patch management process to apply critical updates and patches to software and systems as soon as they are released.*
- *Utilise automated tools to streamline the patch management process, reducing the window of opportunity for attackers.*
- *Perform regular audits to ensure the patch management process is effective and that no assets are overlooked.*

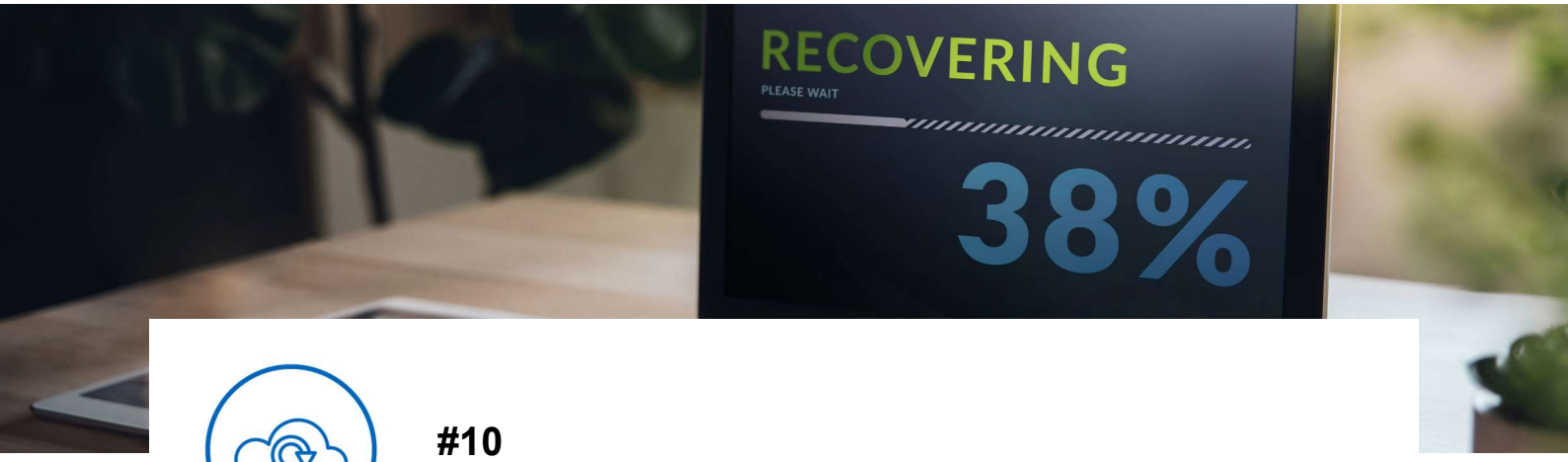
#9

Configuration and Change

Configuration and Change Management is a strategic process that involves setting and maintaining the desired state of system configurations and managing any changes to them. It's essential for ensuring that systems are hardened against attacks and that any modifications do not introduce new vulnerabilities. This process helps in maintaining the integrity and stability of IT environments.

What SMEs Should Do:

- *Implement baseline configurations to establish standard operating environments and ensure security uniformity across all systems.*
- *Develop change control procedures to manage system alterations, thereby reducing the risk of introducing exploitable vulnerabilities.*
- *Engage in regular system reviews to update and maintain configurations, keeping pace with evolving security practices and business requirements.*
- *Document all changes meticulously, including the justifications and impact assessments, to provide a clear and auditable change history.*
- *Employ automated compliance checking tools to consistently enforce adherence to established industry security standards.*



#10
Backup and Recovery

Backup and Recovery are essential practices that form the cornerstone of any SME's cyber resilience and business continuity strategy. They ensure critical data and systems can be quickly restored after disruptive events, protecting against data loss and maintaining operational integrity.

What SMEs Should Do:

- *Adhere to the 3-2-1 backup rule: keep at least three copies of data, on two different media, with one backup located offsite.*
- *Implement regular and systematic backup schedules to minimise data loss in case of an incident.*
- *Ensure backups are encrypted and secure to prevent unauthorised access or data breaches.*
- *Test backup restoration processes regularly to confirm that data can be effectively recovered when necessary.*
- *Develop a comprehensive Business Continuity Plan (BCP) that includes backup and recovery strategies tailored to the business's operational requirements.*
- *Train relevant staff on backup procedures and recovery protocols to ensure smooth execution during a crisis.*
- *Evaluate and update the backup and recovery strategies periodically to align with evolving business needs and emerging threats.*

Resource Links

Cost of a Data Breach Report 2023 (IBM): This annual report by IBM provides in-depth insights into the financial impacts and trends of data breaches globally.

ASD Cyber Threat Report 2022-2023: Developed by the Australian Signals Directorate, this report highlights the predominant cyber threats and security incidents impacting Australia in the past year.

2023 Data Breach Investigations Report: Verizon's comprehensive analysis offers a detailed overview of data breach patterns and cybersecurity challenges faced globally in 2023.

2023-2030 Australian Cyber Security Strategy: A strategic roadmap by Australia's Department of Home Affairs outlining the government's vision and plans to establish Australia as a global leader in cyber security by 2030.

Small Business Cyber Security Guide: Curated resources by the ASCS to provide guidance and support to small organisations.

Small and Medium Business Resources: A comprehensive collection of resources compiled by the the US' National Institute of Standards and Technology, or NIST, relevant to small and medium-sized businesses.

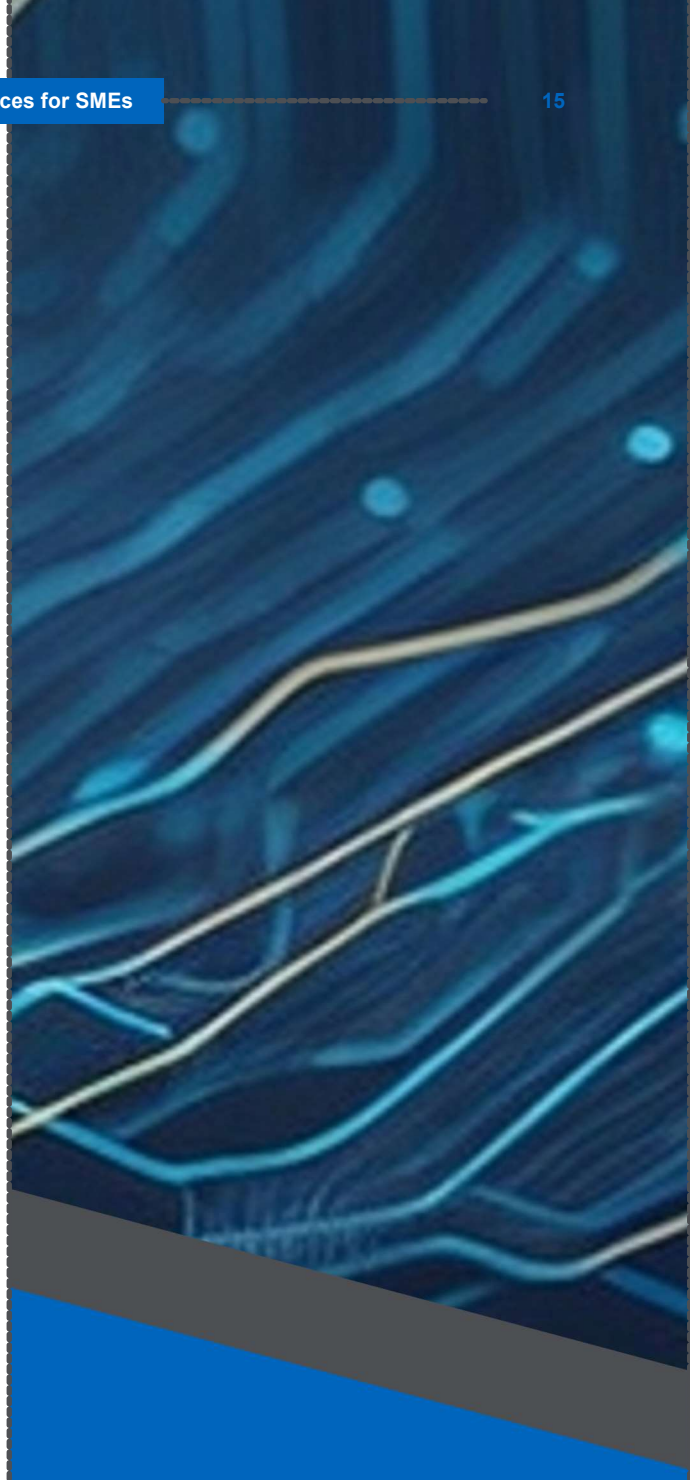
Centralian on Cyber: The cyber security services and products offered by Centralian Controls.

About Us

Centralian Controls, a stalwart in control and automation, has been advancing the sector since 1987. What began as a partnership with a single manufacturer has flourished into a comprehensive provision of control and automation product lines, sourced from a variety of esteemed local and international brands. Our South Australian roots have grown deep into a thriving enterprise that prides itself on offering state-of-the-art process control, industrial automation, and IoT solutions. With a dedicated facility for developing turn-key solutions, Centralian Controls is committed to innovation and excellence.

As we expand our horizons, embracing the challenges of cyber security, we bring the same dedication and expertise that have long been our hallmark. Our venture into cyber security is not a departure but an expansion, a natural progression of our commitment to technological excellence and customer service. We understand the intricacies of cyber threats parallel to the complexities of automation and control systems.

We offer a comprehensive suite of cyber security products and solutions designed to protect critical infrastructure and safeguard sensitive data. From proactive threat detection to robust defense mechanisms, our cyber security offerings are meticulously crafted to provide maximum protection. Our team, with its rich heritage of technical excellence, works tirelessly to ensure that every solution aligns with the highest standards of reliability and performance.



Centralian Controls

www.centralian.com.au

Visit our website to learn more about our solutions.

Centralian Controls

Better Controls

Better Business

centralian.com.au

webquery@centralian.com.au

+61 8 8300 3500

2 / 6-7 Schenker Dr.
Royal Park, SA 5014