CRCYBER eBook

CRCYBER

Cyber Security Risk Reviews for Small and Medium Businesses (SMBs)

Understand cyber security risk reviews and learn how to protect your SMB from evolving threats.

Cyber Security Risk Reviews

In today's digital landscape, small and medium businesses (SMBs) are increasingly targeted by cyber threats. Despite common misconceptions, cybercriminals often view SMBs as easier targets due to limited security resources. Conducting regular cyber security risk reviews is essential to safeguard your business, protect sensitive data, and ensure compliance with industry regulations.

This eBook will guide SMBs through the process of conducting effective cyber security risk reviews, outlining practical steps and best practices tailored to your specific needs.

Understanding Cyber Security Risks

Definition of Cyber Security Risks: Cyber security risks refer to potential threats and vulnerabilities that can compromise the confidentiality, integrity, or availability of your business's information systems.

Common Cyber Threats Facing SMBs

- **Phishing attacks:** Deceptive emails designed to trick employees into revealing sensitive information.
- **Ransomware:** Malicious software that encrypts data and demands payment for its release.
- **Malware:** Software intended to damage or disable systems.
- **Insider threats:** Risks from employees or contractors who may intentionally or unintentionally compromise security.
- **Weak passwords:** Easily guessable and reused passwords that open doors to unauthorised access.
- **Social engineering:** Manipulating individuals into divulging confidential information.

The Importance of Cyber Security Risk Reviews
Regular risk reviews help identify vulnerabilities, assess potential impacts, and implement controls to mitigate threats. Understanding the specific risks to your business can prevent costly breaches and operational downtime.

The Risk Review Process

- **1. *Establish Objectives and Scope:*** Define the goals of the risk review, focusing on critical assets and systems. Consider relevant obligations and frameworks such as the Australian Privacy Act, Notifiable Data Breaches scheme, APRA CPS 234 where applicable, PCI DSS, ISO 27001, and the ACSC Essential Eight.

- 2. ***Identify Assets and Data:*** List all hardware, software, networks, and data that need protection. Use asset inventory tools to streamline this process. Pay special attention to sensitive information such as customer data, intellectual property, and financial records.

- 3. ***Identify Threats and Vulnerabilities:*** Conduct a thorough assessment using vulnerability scanners and penetration testing. Identify potential threats, such as cyber attacks, accidental data loss, supplier outages, and natural disasters, as well as vulnerabilities such as outdated software, weak passwords, and misconfigured systems.

- 4. ***Assess Risks:*** Evaluate the likelihood and potential impact of identified threats exploiting vulnerabilities. Use risk assessment matrices (RAM) and frameworks like FAIR (Factor Analysis of Information Risk) to prioritise risks. For example, an administrator account without MFA may be considered high risk because it is both likely to be targeted and could have a serious business impact if compromised.

- 5. **Develop Mitigation Strategies:** Implement controls to reduce risks. This can include:

    - *Technical solutions:* Firewalls, antivirus software, and multi-factor authentication.

    - *Policies:* Password management, access controls, and acceptable use policies.

    - *Training:* Regular employee awareness programs covering phishing, data handling, and reporting suspicious activities.

- 6. **Document and Report Findings:** Create a detailed report outlining identified risks, mitigation strategies, and recommendations. Include risk scores, prioritised action items, and clear timelines. Ensure that the report is accessible to both technical and non-technical stakeholders.

- 7. **Review and Update Regularly:** Cyber threats evolve constantly. Schedule regular risk reviews (at least annually) and update strategies to address new vulnerabilities. Incorporate lessons learned from security incidents, changes in business operations, new technologies, regulatory updates, and emerging cyber threats.

What should be reviewed?

A practical cyber security risk review should assess:

- Microsoft 365 security settings
- User accounts and administrator access
- Multi-factor authentication coverage
- Endpoint protection and device management
- Backup and recovery processes
- Email security and phishing exposure
- Password and access control practices
- Third-party applications and cloud services
- Staff awareness and incident response readiness
- Gaps against recognised frameworks such as the ACSC Essential Eight

Best Practices for SMBs

- **Employee Training:** Educate staff about phishing, social engineering, and secure password practices.
- **Regular Updates and Patching:** Keep software and systems up to date to address known vulnerabilities.
- **Access Controls:** Implement role-based access controls to limit data exposure.
- **Data Backup:** Regularly back up critical data and test recovery procedures.
- **Incident Response Plan:** Develop a plan outlining steps to take in the event of a security breach.
- **Align with the ACSC Essential Eight:** Use the Essential Eight as a practical baseline to improve cyber resilience, including patching, multi-factor authentication, application control, restricted admin privileges, regular backups, and Microsoft Office macro controls.

Building a Culture of Security

- **Leadership Involvement:** Ensure top management prioritises cyber security.
- **Continuous Improvement:** Foster a mindset of ongoing security enhancement.
- **Collaboration:** Encourage communication between departments to identify and mitigate risks.

Conclusion

Cyber security risk reviews help SMBs understand where they are exposed, what needs to be fixed first, and how to improve security in a practical and cost-effective way.

For many businesses, the biggest challenge is not knowing where to start. A structured risk review gives you a clear roadmap, helping reduce uncertainty, prioritise investment, and build long-term resilience.

CRCYBER helps Australian SMBs identify cyber risks, strengthen Microsoft 365 and endpoint security, improve governance, and build practical security roadmaps aligned to business needs.

CRCYBER

At CRCYBER, we help organisations improve their cyber security maturity through security-first managed IT, cyber risk reviews, Microsoft 365 security uplift, endpoint protection, and practical infrastructure support.

Smarter Cybersecurity, Made Simple.

Enquire Today
contact@crcyber.com
www.CRCYBER.com

Published
JUNE 2026