CRCYBER eBook

CRCYBER

ACSC Essential 8 Maturity Level 0 (ML0) Assessment for Small & Medium Businesses (SMBs)

Your essential guide to understanding, assessing, and improving cyber security at Maturity Level 0 using the ACSC Essential Eight framework.

ACSC Essential 8 ML0 Assessment for SMB’s

Cyber security is essential for businesses of all sizes, but Small and Medium Businesses (SMBs) often face unique challenges due to limited resources and expertise.

This eBook provides SMBs with a concise guide to understanding and assessing Maturity Level 0 (ML0) within the ACSC Essential Eight framework. It aims to help organisations identify critical vulnerabilities in their current cyber security posture, conduct effective assessments, and lay the groundwork for advancing to higher maturity levels.

The Importance of Cyber Security for SMBs

Why SMBs Are Targets

- **Limited security resources:** SMBs often lack dedicated IT security teams and the budget for comprehensive protection, making them attractive targets for cybercriminals.
- **Valuable data assets:** Despite their size, SMBs store sensitive data such as customer information, financial records, and proprietary business data, all of which are valuable to attackers.
- **Increasing reliance on digital platforms:** The shift towards online services, cloud computing, and remote work expands the attack surface, increasing the risk of cyber incidents.

Consequences of Poor Cyber Security

- **Financial losses:** Cyberattacks can result in direct financial theft, ransom payments, and the cost of remediation.
- **Reputational damage:** A data breach can erode customer trust and lead to a loss of business.
- **Legal and regulatory penalties:** Non-compliance with data protection laws and industry regulations can result in significant fines and legal actions.

Understanding the ACSC Essential Eight

What is the ACSC Essential Eight?

The Australian Cyber Security Centre (ACSC) developed the Essential Eight (E8) as a set of baseline mitigation strategies to help organisations protect their systems against a range of cyber threats.
These strategies are recognised as essential in minimising the risk of cyberattacks and improving an organisation's overall cyber resilience.

Overview of the ACSC Essential Eight

1. **Application Control:** Prevents unapproved applications from executing to reduce malware risks.
2. **Patch Applications:** Regularly updating applications to fix vulnerabilities that attackers can exploit.
3. **Configure Microsoft Office Macro Settings:** Restricting the use of macros to prevent malicious code execution.
4. **User Application Hardening:** Strengthening application settings to limit exploitable features.
5. **Restrict Administrative Privileges:** Limiting admin rights to reduce the risk of system-wide breaches.
6. **Patch Operating Systems:** Keeping operating systems up to date to close security gaps.
7. **Multi-Factor Authentication (MFA):** Adding an extra layer of verification to protect user accounts.
8. **Regular Backups:** Ensuring data can be recovered in case of an attack or system failure.

Maturity Level 0 (ML0) Explained

Understanding Maturity Level 0

Maturity Level 0 (ML0) represents the starting point on the ACSC Essential Eight Maturity Model. At this level, organisations typically have minimal or no implementation of the Essential Eight strategies. There is a heightened risk of cyber incidents due to insufficient protection against common attack vectors.

Common Characteristics

- **No formal cyber security policies:** Lack of documented policies leaves staff without clear security guidelines.
- **Lack of regular patching or updates:** Unpatched software and systems remain vulnerable to known exploits.
- **Weak password practices:** Use of simple, easily guessable passwords increases the risk of unauthorised access.
- **Absence of multi-factor authentication:** Reliance on single-factor authentication makes systems easier to compromise.
- **Infrequent or non-existent data backups:** Without regular backups, data recovery after an incident becomes difficult or impossible.

Conducting an ML0 Assessment

Assessing Your Current Position

- **Conducting initial risk assessments:** Evaluate existing systems, processes, and potential threats.
- **Identifying existing security gaps:** Highlight areas where current defences fall short of best practices.

Step-by-Step Guide

1. **Establish an Assessment Team:** Assemble a group responsible for evaluating security practices.
2. **Review Current IT Infrastructure:** Conduct a thorough review of hardware, software, and network configurations.
3. **Utilise ACSC Assessment Tools:** Leverage official checklists and frameworks to guide the assessment.
4. **Document Findings:** Maintain detailed records of vulnerabilities and areas requiring improvement.

Tools and Resources

- **ACSC Essential Eight Maturity Model:** A comprehensive guide outlining the different maturity levels and strategies for implementation.
- **Self-assessment checklists:** Structured checklists provided by ACSC to help organisations evaluate their adherence to each of the Essential Eight strategies.
- **Risk assessment templates:** Standardised templates that assist in documenting risks, vulnerabilities, and mitigation strategies, streamlining the assessment process.

Addressing Common ML0 Vulnerabilities

Application Control

- **Risks of untrusted applications:** Malware and unauthorised software can compromise systems.
- **Steps to implement basic controls:** Use application whitelisting to allow only approved software to run.

Patch Management

- **Importance of timely updates:** Unpatched systems are a leading cause of security breaches.
- **Setting up patching schedules:** Regularly schedule updates and monitor for new patches.

Macro Security

- **Dangers of malicious macros:** Macros can be used to execute harmful code.
- **Disabling unnecessary macros:** Restrict macros to only trusted documents and users.

User Application Hardening

- **Strengthening browser and application settings:** Disable unnecessary features that can be exploited.
- **Disabling unnecessary features:** Turn off scripts, plugins, and features that are not in use.

Administrative Privileges

- **Minimising admin accounts:** Limit admin access to essential personnel.
- **Implementing least privilege principles:** Ensure users have the minimum access necessary to perform their jobs.

Operating System Patching

- **Regular updates and security patches:** Keep operating systems current to mitigate known vulnerabilities.
- **Automating patch management:** Use tools to ensure consistent and timely updates.

Multi-Factor Authentication

- **Benefits of MFA:** Adds a critical layer of security beyond passwords.
- **Implementing MFA for critical systems:** Apply MFA to sensitive accounts and systems first.

Data Backups

- **Regular backup schedules:** Create and follow a routine for backing up critical data.
- **Testing backup integrity:** Regularly test backups to ensure they can be successfully restored.

Creating a Roadmap to Maturity Level 1

Setting Priorities

- **Addressing high-risk areas first:** Focus on vulnerabilities that pose the greatest threats.
- **Developing a phased implementation plan:** Break down improvements into manageable steps.

Building a Cyber Security Culture

- **Employee awareness and training:** Educate staff on best practices and security protocols.
- **Establishing security policies and procedures:** Develop formal guidelines to standardise security efforts.

Leveraging External Support

- **Engaging managed service providers (MSPs):** Consider outsourcing to experts for specialised tasks.
- **Utilising ACSC and industry resources:** Make use of freely available guides, tools, and advice.

Conclusion

Achieving cyber resilience starts with understanding where your organisation currently stands. By conducting a thorough ML0 assessment, SMBs can identify vulnerabilities, mitigate risks, and begin the journey towards stronger cyber security practices. While the path to higher maturity levels may require time and resources, the long-term benefits in protecting your business far outweigh the initial investment.

Want to safeguard your business? Contact us today for expert cybersecurity support.

CRCYBER

At CRCYBER we specialise in enhancing cybersecurity maturity through Tier 1 managed services with a strong security focus. Our expertise includes professional IT infrastructure services and seamless hardware procurement solutions.

“GOOD PEOPLE,

GOOD SERVICE,

GOOD OUTCOMES.”

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

Authored By Eryn Norie
February 2025