White Paper: The 100 Point Cyber Check

Summary

- Measuring cyber maturity should be the cornerstone of any cyber program
- Frameworks are often abstract and not easy to derive meaningful metrics from
- The 100 Point Cyber Check is freely shared under Creative Commons BY-NC-ND.

The Importance of Cyber Risk Assessment

In today's digitally driven world, the reliance on technology for business operations is greater than ever before. This interconnectedness has brought about numerous efficiencies and opportunities, but it has also introduced a complex array of cyber threats. Cybercriminals are constantly evolving their tactics, exploiting vulnerabilities in systems, networks, and even human behaviour to gain unauthorised access to sensitive information.

The 100 Point Cyber Check is one tool that organisations can use to measure and monitor their progress towards cyber maturity. It is presented in a simple questionnaire style that management teams can answer, and is straightforward to score and monitor.

Key Reasons Why Cyber Risk Assessment is Essential

- Protecting Data Integrity: Organisations handle vast amounts of data, including personal, financial, and proprietary information. A breach can lead to data corruption or loss, compromising the integrity and reliability of critical information.
- Ensuring Operational Continuity: Cyberattacks such as ransomware can halt operations by locking users out of systems. Assessing risks helps in implementing safeguards to maintain business continuity even during an incident.
- Maintaining Customer Trust: Customers entrust organisations with their personal information. A cyber incident can erode this trust, leading to reputational damage and loss of business.
- Complying with Regulations: Laws like SOCI, SLACIP, the Privacy Act, and others mandate stringent data protection measures. Risk assessments help ensure compliance, avoiding legal penalties and fines.
- Financial Impact Mitigation: Cyber incidents can result in significant financial losses due to downtime, remediation costs, and legal liabilities. Proactive risk assessment reduces these potential financial impacts.

Role of the 100 Point Cyber Check:

- Framework for Understanding Security Posture: It provides a structured approach to evaluate where an organisation stands in terms of cybersecurity maturity.

- Identifying Vulnerabilities: Highlights both technical gaps (like outdated software) and organisational weaknesses (such as lack of employee training).
- Guiding Enhancements: Offers insights into critical areas that require immediate attention and improvement.

By regularly conducting cyber risk assessments, organisations can stay ahead of threats, adapt to the changing cyber landscape, and implement strategies that safeguard their assets and stakeholders.

The Need for Quantitative and Objective Cyber Risk Assessments

Creating an effective cybersecurity strategy requires more than just awareness of potential threats; it necessitates a precise understanding of the organisation's vulnerabilities and the effectiveness of existing controls. Quantitative and objective assessments provide measurable data that is critical for informed decision-making.

Benefits of Quantitative Assessments

- Objectivity: Removes subjective bias, allowing for clear, data-driven insights into cybersecurity performance.
- Measurable Outcomes: Facilitates tracking progress over time, enabling organisations to see the tangible impact of their cybersecurity initiatives.
- Benchmarking: Allows organisations to compare their cybersecurity maturity against industry standards or competitors.
- Resource Allocation: Helps in prioritising investments by identifying the most critical vulnerabilities that need addressing.

Implementing SMART Goals in Cybersecurity

- Specific: Clearly define what needs to be achieved (e.g., reduce phishing incidents by 30% within six months).
- Measurable: Establish metrics to assess progress (e.g., number of incidents reported, time to detect breaches).
- Achievable: Set realistic targets considering available resources and constraints.
- Relevant: Align cybersecurity goals with overall business objectives and risk appetite.
- Time-Bound: Set deadlines to ensure timely implementation and accountability.

Aligning Investments with Strategic Goals

- Cost-Benefit Analysis: Quantitative assessments enable organisations to evaluate the return on investment (ROI) of cybersecurity measures.
- Strategic Alignment: Ensures that cybersecurity efforts support business objectives, such as expanding into new markets or adopting new technologies.

- Continuous Improvement: Regular assessments help in adapting strategies in response to emerging threats and technological advancements.

By grounding cybersecurity strategies in quantitative data, organisations can make more informed decisions, demonstrate the value of cybersecurity investments to stakeholders, and continually enhance their security posture.

Leveraging Quantitative Measures for Cyber Maturity, ROI, and Success Metrics

A structured, quantitative approach to cybersecurity allows organisations to not only understand their current state but also to plan and measure improvements effectively.

Evaluating Cyber Maturity with the 100 Point Cyber Check

The 100 Point Cyber Check is a comprehensive cybersecurity assessment tool designed to evaluate an organisation's security posture across key domains. It consists of 100 individual checkpoints, each representing a critical aspect of cybersecurity, including governance, risk management, data protection, and incident response. The assessment aims to identify strengths and weaknesses in the organisation's security framework, providing a detailed view of where improvements are needed.

Theoretical Justification for the 80% Maturity Target

Achieving an overall maturity level of 80% (or 20/25 in each section) is considered optimal for several theoretical reasons:

1. Pareto Principle (80/20 Rule):
    - Concept: Suggests that roughly 80% of effects come from 20% of causes.
    - Application in Cybersecurity: By reaching 80% maturity, organisations address the most critical and impactful 20% of cybersecurity controls and practices, mitigating the most significant risks.
    - Benefit: Ensures that the most significant vulnerabilities are addressed, recognising that further investments may result in diminishing returns.
2. Law of Diminishing Returns:
    - Concept: As investment in a particular area increases, the incremental benefit from each additional unit of investment decreases.
    - Application in Cybersecurity: Beyond 80% maturity, the effort and resources required to achieve additional improvements increase significantly, while the incremental benefits decrease.
    - Benefit: Optimises the balance between cost, effort, and benefit, avoiding excessive expenditure for minimal gain.
3. Balanced Approach:
    - Concept: Emphasises the importance of maintaining equilibrium across all areas.

    - Application in Cybersecurity: Achieving 80% maturity ensures that all critical domains are adequately addressed without overemphasising one area at the expense of others.
    - Benefit: Promotes a comprehensive and holistic cybersecurity strategy, enhancing overall resilience.

Measuring ROI

- Investment Tracking: By correlating improvements in maturity scores with investments made, organisations can assess the effectiveness of their cybersecurity spending.
- Demonstrating Value: Quantifiable improvements provide evidence to stakeholders that cybersecurity investments are yielding tangible benefits.
- Budget Justification: Clear ROI metrics support requests for future funding by showcasing past successes and ongoing needs.

Providing a Single Success Metric

- Simplified Reporting: A unified cyber maturity score allows for straightforward communication with non-technical stakeholders, such as board members or executives.
- Strategic Alignment: The single metric can be integrated into overall business performance dashboards, ensuring cybersecurity is considered alongside other critical business functions.
- Goal Setting: Establishing clear targets based on the success metric enables focused efforts and motivates teams towards achieving common objectives.

By leveraging quantitative measures and understanding the theoretical underpinnings of the 80% maturity target, organisations can make informed decisions, optimise resource allocation, and build a strong cybersecurity foundation.

The Importance of Both Technical and Non-Technical Controls

Cybersecurity is multifaceted, requiring a combination of technological solutions and human-centric approaches to effectively protect organisational assets.

Technical Controls

- Network Security Devices: Tools like firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways act as the first line of defence against external threats.
- Endpoint Protection: Antivirus software, anti-malware solutions, and endpoint detection and response (EDR) tools safeguard individual devices.
- Data Encryption: Encrypting data at rest and in transit prevents unauthorised access to sensitive information even if it is intercepted or stolen.

- Identity and Access Management (IAM): Systems that enforce strong authentication methods and manage user privileges reduce the risk of unauthorised access.

Non-Technical Controls

- Policies and Procedures: Clearly defined policies outline acceptable use, security protocols, and consequences for non-compliance.
- Security Awareness Training: Regular training programs educate employees about recognising phishing attempts, social engineering tactics, and best practices for data handling.
- Incident Response Planning: Establishing procedures for responding to security incidents ensures a swift and effective reaction, minimising impact.
- Vendor Management: Assessing and managing the security practices of third-party vendors prevent supply chain vulnerabilities.

Integrating Both Controls

- Holistic Security Posture: Combining technical defences with robust policies and an informed workforce creates a comprehensive security strategy.
- Reducing Insider Threats: Non-technical controls address risks posed by employees, whether due to negligence or malicious intent.
- Adapting to Evolving Threats: As cyber threats evolve, organisations need both technological upgrades and continuous education to stay protected.

Evaluating Through the 100 Point Cyber Check

- Balanced Assessment: The check evaluates both control types, ensuring that no aspect of cybersecurity is overlooked.
- Customised Recommendations: Based on the assessment, organisations receive tailored guidance on strengthening both technical systems and organisational practices.

By recognising the importance of both technical and non-technical controls, organisations can build a resilient cybersecurity framework that protects against a wide spectrum of threats.

Calculating Maturity Scores with the 100 Point Cyber Check

The maturity scoring system provides a clear roadmap for organisations to understand and improve their cybersecurity efforts.

Measuring Cyber Maturity with the 100 Point Cyber Check

The 100 Point Cyber Check evaluates an organisation's security posture across key domains, consisting of 100 individual checkpoints representing critical aspects of cybersecurity. These include:

- Governance
- Risk Management
- Data Protection
- Incident Response

The assessment identifies strengths and weaknesses, offering a detailed view of areas needing improvement.

Maturity Levels and Rubric with Qualitative Descriptors

To provide a more granular assessment, the following maturity levels and corresponding qualitative descriptors are typically used:

1. 0-20: Initial/Ad-Hoc
    - Description: Cybersecurity practices are largely reactive and uncoordinated. There may be some basic controls in place, but they are implemented inconsistently. The organisation lacks formal policies and procedures, with little to no strategic direction for cybersecurity, leading to significant vulnerabilities and high risk exposure.
    - Key Characteristics:
        - No formal cybersecurity framework.
        - Inconsistent or undocumented policies.
        - Cybersecurity incidents are managed on an as-needed basis with minimal planning.
        - Significant gaps in risk management and control implementation.
2. 21-40: Managed
    - Description: The organisation recognises the importance of cybersecurity and has implemented some key controls. Formal policies and procedures exist but may not be comprehensive or consistently applied. Cybersecurity efforts are more structured, with some degree of risk management, though gaps still exist.
    - Key Characteristics:
        - Basic policies and procedures established.
        - Some level of staff awareness and training.
        - Incident response processes are in place but may be underdeveloped.
        - Initial steps toward risk assessment and management.
3. 41-60: Defined
    - Description: Cybersecurity practices are well-defined and documented, guided by a clear framework. Controls are implemented more consistently, and the organisation is proactive in identifying and addressing cybersecurity risks. There is moderate integration across departments, with regular training and awareness programs.
    - Key Characteristics:
        - Formal cybersecurity framework actively managed.

  - Regularly updated policies and procedures.
  - Proactive risk management and incident response.
  - Cross-departmental collaboration in cybersecurity efforts.

4. 61-80: Optimising

- Description: The organisation has a mature cybersecurity program with optimising processes and controls. Cybersecurity is embedded in the organisational culture, with high employee awareness. Continuous improvement processes are in place, actively seeking to stay ahead of emerging threats. Emphasis on automation and efficiency in managing cybersecurity tasks.
- Key Characteristics:
  - Cybersecurity is a strategic priority.
  - High levels of automation in monitoring and response.
  - Continuous improvement and regular review of controls.
  - Strong alignment of cybersecurity with business objectives.

5. 81-100: Exemplary

- Description: Cybersecurity practices are exemplary, serving as a benchmark for the industry. The organisation is highly resilient to cyber threats, with advanced controls and continuously refined processes. Emphasis on innovation and leadership, often participating in industry-wide initiatives and sharing best practices.
- Key Characteristics:
  - Leadership in cybersecurity innovation and practices.
  - Advanced and highly automated cybersecurity solutions.
  - Regular contributions to industry standards and best practices.
  - High agility in responding to new and emerging threats.

Aggregating Scores Across Domains

- Balanced Approach: Achieving 20/25 in each section ensures a balanced cybersecurity posture, preventing overemphasis on one area at the expense of others.
- Actionable Insights: Scores highlight areas of strength and weakness, guiding targeted improvements.

Aim for 80% Maturity

- Optimised Balance: Reaching 80% maturity reflects a strong security posture while balancing cost and effort.
- Risk Management: At this level, organisations effectively manage most risks and are better prepared for emerging threats.
- Theoretical Justification: The Pareto Principle, Law of Diminishing Returns, and Balanced Approach all support the 80% target as an optimal point of maturity.

By utilising the maturity scoring system and understanding the qualitative descriptors, organisations can take a systematic approach to enhancing their cybersecurity, ensuring efforts are targeted and effective.

Comprehensive Mapping of the 100 Point Cyber Check to Key Cybersecurity Frameworks

Aligning the 100 Point Cyber Check with established cybersecurity frameworks ensures that organisations are meeting recognised standards and benefiting from best practices.

ISO 27001 Mapping Summary

- Alignment with ISMS Requirements:
  - Risk Assessment and Treatment: The check covers identification, analysis, and evaluation of risks, as required by ISO 27001.
  - Security Policy: Ensures that a comprehensive information security policy is in place and communicated.
  - Asset Management: Includes inventory and classification of information assets.
  - Access Control: Evaluates the effectiveness of user access policies and procedures.
  - Physical and Environmental Security: Assesses controls to prevent unauthorised physical access, damage, or interference.
- Benefits of Alignment:
  - International Recognition: ISO 27001 is globally recognised, enhancing credibility with customers and partners.
  - Structured Approach: Provides a systematic methodology for managing sensitive information.
  - Continuous Improvement: Encourages regular reviews and updates to the ISMS.

Essential Eight Mapping Summary

- Addressing Key Mitigation Strategies:
  - Application Whitelisting: Ensures only approved software can execute on systems.
  - Patching Applications and OS: Regular updates to fix security vulnerabilities.
  - Configuring Microsoft Office Macro Settings: Prevents malicious code execution.
  - User Application Hardening: Disables unnecessary features that can be exploited.
  - Restricting Administrative Privileges: Limits access to those who need it, reducing the risk of privilege misuse.
  - Multi-Factor Authentication: Adds layers of security for user verification.
  - Regular Backups: Ensures data can be restored in the event of loss or corruption.

- Benefits of Alignment:
    - Practical Focus: Emphasises actionable steps that can significantly reduce cybersecurity risks.
    - Government Endorsement: Recognised by Australian government agencies, enhancing compliance with local standards.
    - Cost-Effectiveness: Prioritises strategies that provide significant security benefits relative to their cost.

CIS Controls Mapping Summary

- Incorporation of CIS Top 20 Controls:
    - Inventory and Control of Hardware Assets: Identifying all devices connected to the network.
    - Inventory and Control of Software Assets: Keeping track of all software to manage vulnerabilities.
    - Continuous Vulnerability Management: Regular scanning and remediation of vulnerabilities.
    - Controlled Use of Administrative Privileges: Monitoring and managing user accounts and privileges.
    - Secure Configuration for Hardware and Software: Standardising configurations to minimise vulnerabilities.
- Benefits of Alignment:
    - Prioritised Actions: Focuses on controls that address the most common and damaging attacks.
    - Community Consensus: Developed by a global community of cybersecurity experts.
    - Adaptability: Applicable to organisations of all sises and industries.

Unified Assessment Approach

- Comprehensive Coverage: By mapping to multiple frameworks, the 100 Point Cyber Check ensures all critical areas are assessed.
- Simplified Compliance Management: Organisations can address multiple regulatory and best practice requirements through a single assessment process.
- Strategic Alignment: Aligning with these frameworks helps integrate cybersecurity into the organisation's overall strategic planning.

Implementation Considerations

- Customisation: The 100 Point Cyber Check can be tailored to focus on the frameworks most relevant to the organisation's industry and geographic location.
- Resource Allocation: Understanding the overlap between frameworks helps in optimising resource use, avoiding duplication of efforts.
- Continuous Monitoring: Regular assessments ensure ongoing compliance and adaptation to changes in regulations and threat landscapes.

By comprehensively mapping the 100 Point Cyber Check to key frameworks, organisations can streamline their cybersecurity efforts, ensuring they are effective, efficient, and aligned with recognised standards.

Results from Initial Implementation of the 100 Point Cyber Check

With the release of Australia's Cyber Security Strategy 2020, there is a clear emphasis on protecting small and medium-sized enterprises (SMEs). The 100 Point Cyber Check was designed to measure cyber risk for SMEs in Australia using a simple, straightforward instrument. Given the strategy's focus, it is instructive to examine the initial results from organisations that have utilised the check.

Overview of Initial Findings (2021)

- Average Score: The average score for the past year was 56.9%, indicating that SMEs are slightly above the halfway mark in cybersecurity maturity but still have significant room for improvement.
- Completion Time: On average, it took 26 minutes and 53 seconds to complete the check, demonstrating the tool's efficiency and accessibility for busy professionals.

Specific Criteria and Observations

- Cybersecurity Budgets:
    - 21% of organisations had a cyber budget of less than $1,000.
    - 50% had budgets ranging from $1,000 to $10,000.
    - 14% reported budgets of $1,000,000 and above.
    - Observation: There is a wide range in cybersecurity investment among SMEs, with a significant portion operating on minimal budgets.
- Presence of a Chief Information Security Officer (CISO):
    - 43% had a CISO, indicating a commitment to dedicated cybersecurity leadership.
    - 57% had no designated individual responsible for cybersecurity, highlighting a potential area of concern.
- Test Scores:
    - Lowest Score: 31%, reflecting a high level of vulnerability and inadequate cybersecurity measures.
    - Highest Score: 79%, demonstrating that some SMEs are approaching the optimal maturity level.
    - Budget Correlation: The best score was achieved by an organisation with a budget between $1,000 and $10,000, suggesting that effective cybersecurity does not necessarily require the largest budgets. Conversely, the worst score was associated with a budget between $100 and $1,000.
- Industry Sectors Represented:
    - Information Technology (IT): 50%

  - Health Care: 14%
  - Financials: 14%
  - Consumer Staples: 21%
  - Industrials: 7%
  - Observation: A diverse range of industries participated, with IT being the most represented sector.

Implications and Insights

- Average Maturity Level: An average score of 56.9% places SMEs in the Defined maturity level (41-60), indicating that while cybersecurity practices are documented and some proactive measures are in place, there is substantial progress to be made.
- Resource Allocation: The variation in budgets and the correlation with scores suggest that strategic allocation of resources is crucial. Organisations with moderate budgets can achieve high maturity levels through effective use of funds.
- Need for Leadership: The absence of a CISO or equivalent role in over half of the organisations points to a leadership gap in cybersecurity. Appointing dedicated personnel could significantly enhance an organisation's security posture.
- Call to Action: As SMEs are vital to the national economy, improving cybersecurity maturity across this sector is imperative. The results indicate that there is much work to be done to reach the optimal maturity target of 80%.

In summary, the initial implementation of the 100 Point Cyber Check reveals that the average SME is scoring just above 50% in cybersecurity maturity. This is a modest starting point, but there is considerable potential for improvement. By leveraging tools like the 100 Point Cyber Check, SMEs can identify gaps, allocate resources effectively, and enhance their cybersecurity resilience, contributing to a stronger national security posture.

Conclusion

The 100 Point Cyber Check serves as a vital tool for organisations aiming to protect their assets, reputation, and ensure long-term success. By adopting this comprehensive assessment, organisations can:

- Proactively Manage Cyber Risks: Identify and address vulnerabilities before they can be exploited.
- Optimise Resource Allocation: Focus on the most impactful controls, balancing cost and benefit.
- Enhance Cybersecurity Maturity: Progress through maturity levels by implementing best practices and continuous improvement.
- Demonstrate Compliance and Leadership: Align with key frameworks, showcasing commitment to cybersecurity to customers, partners, and regulators.
- Build Trust with Stakeholders: Strengthen relationships with customers and partners through demonstrated security resilience.

Given the findings from the initial implementation, there is a clear need for SMEs to elevate their cybersecurity efforts. Organisations are encouraged to utilise the 100 Point Cyber Check to assess their current posture, identify areas for improvement, and work towards achieving the optimal maturity level of 80%. Collective action in this regard will not only benefit individual organisations but also enhance national cybersecurity resilience.