**Cyber Resilience Survey**

|  |
| --- |
| This questionnaire is developed from the ASIC (Australian Securities and Investments Commission) Cyber Pulse Survey 2023[[1]](#footnote-1) and has been adapted for industry-wide SMEs. It has also been updated based on the latest NIST Cybersecurity Framework (CSF) 2.0[[2]](#footnote-2) released in February 2024. This questionnaire is designed for the purposes of academic assessment for Deakin University’s unit MIS761 Cyber Security Strategies[[3]](#footnote-3). |

# Organization Profile

|  |  |  |
| --- | --- | --- |
|  | | |
| **What function(s) best describe the role of the person or people that completed this survey?** | Owner/Founder  Manager  IT Specialist/Consultant  Employee  Volunteer (for NGO/NPO)  Other [Free text] | [Multiple Selection] |
| **Number of employees** | Micro (1-9 persons employed)  Small (10-25 persons employed)  Medium (26-199 persons employed)  Large (200 or more persons employed) | [Single Selection] |
| **What sector best describes your organization's activity?** | Accommodation and food  Automotive electrical services  Building and construction trade services  Education, training, recreation and support services  Health care and personal services  Manufacturing  Machinery and equipment repair and maintenance  Professional, scientific and technical services  Retail trade  Transport, postal and warehousing  NGO/NPO  Other [Free text] | [Single Selection] |
| **What is the most senior role accountable for overseeing the management of cybersecurity in your organization?** | Owner/Founder  Manager  IT Specialist/Consultant  External IT Service Provider  Volunteer (for NGO/NPO)  Unknown  Other [Free text] | [Single Selection] |
| **Which is the most senior role, group, or function responsible for the day-to-day management of cybersecurity in your organization?** | Owner/Founder Manager IT Specialist/Consultant External IT Service Provider Volunteer (for NGO/NPO) Unknown Other [Free text] | [Single Selection] |
| **Does your organization handle (e.g., store, use and/or transmit) confidential information?** | Yes No | [Single Selection] |
| **How many cybersecurity incidents did your organization experience, directly or indirectly, in the past two financial years?** | 10+ 5–10 2–5 Less than 2 Zero Unknown | [Single Selection] |
| **In the past 24 months, has your organization had difficulty recruiting and retaining staff (or external expertise) with sufficient cybersecurity expertise?** | Yes Partially No Have not recruited | [Single Selection] |
| **What does your organization consider are the top three cybersecurity threats (ranked in order) to the continued operation of your organization?** | Threats in the supply chain Threats to cloud Software threats Insider threats Weak passwords/credentials Phishing Social engineering Business email compromise Ransomware Other [Free text; <50 characters] | [Multiple Selection; mandatory selection of 3, ranked] |
| **List your organization's top three technology providers that support the organization’s critical business services, that could cause a major disruption if any are unable to render their services.** | [Free text; 3 fields] |  |
| **Which of the following frameworks does your organization implement or benchmark against?** | ACSC Essential Eight Maturity Model American Institute of Certified Public Accountants (SOC2) Australian Government Information Security Manual (ISM) Centre for Internet Security (CIS) Control Objectives for Information and Related Technologies (COBIT) Custom Organisational Internal Standards Cybersecurity Maturity Model Certification (CMMC) Federal Financial Institutions Examination Council (FFIEC) ISO/IEC 27001: Information security management MITRE Privacy Maturity Model National Institute of Standards and Technology (NIST) Cybersecurity Framework NIST SP 800-53: Security and Privacy Controls for IS and Organizations Unknown No standard Other [Free text] | [Multiple Selection |
| **What percentage of your organization's annual revenue is allocated to security and IT?** |  |  |
| **What percentage of your organization's annual revenue is considered an acceptable loss due to cybersecurity incidents?** |  |  |
|  | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| GOVERN (GV): **The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *How well does your organization understand the circumstances that impact its cybersecurity risk management decisions?* | The organization has minimal understanding of its mission, stakeholder expectations, dependencies, or legal and regulatory requirements. | The organization recognizes its mission and some stakeholder expectations but lacks a comprehensive understanding of dependencies and legal requirements. | The organization has documented its mission, stakeholder expectations, dependencies, and key legal and regulatory requirements. | **In addition to 2:** The organization regularly reviews and updates its understanding in response to changes in these areas. | **In addition to 3:** The organization proactively adapts its cybersecurity strategies based on an advanced understanding of its organizational context. |
| *How effectively does your organization establish and communicate its risk management objectives, appetite, and tolerance?* | The organization lacks clearly defined risk management objectives, risk appetite, and tolerance. | Risk management objectives and risk appetite are informally agreed upon and communicated only at higher levels of management. | Risk management objectives, appetite, and tolerance are formally established and communicated within the organization, but not regularly reviewed or updated. | **In addition to 2:** These elements are not only clearly established and communicated but are also maintained and integrated into the broader enterprise risk management processes. | **In addition to 3:** The organization continuously updates and communicates risk management strategies, ensuring alignment with changing business environments and objectives. Effective communication channels across the organization and with third parties are actively maintained. |
| *How effectively does your organization integrate and operationalize its cybersecurity risk management strategies into its overall business operations?* | Cybersecurity risk management is disconnected from overall enterprise risk management processes. | Basic methods for calculating and documenting risks are used, but they lack standardization or are not communicated effectively. | Standardized methods for risk calculation and documentation are established and communicated, but may not fully include or prioritize strategic opportunities. | **In addition to 2:** The organization actively characterizes and includes strategic opportunities in risk discussions, ensuring that risk management is adaptive and proactive. | **In addition to 3:** Comprehensive systems are in place to continuously evaluate, prioritize, and communicate both risks and opportunities, with robust mechanisms for adapting strategies in real-time based on evolving organizational and external conditions. |
| *Does the organisation have defined cyber security roles and responsibilities?* | Cyber security roles and responsibilities are generally not defined or documented. | Some cyber security roles and responsibilities are defined and documented. | Internal cyber security roles, including for the organisations’ leaders and IT function, are defined, documented, and communicated to all personnel. | **In addition to 2:**  External cyber security roles and responsibilities are defined, documented, and communicated to all personnel. | **In addition to 3:** Internal and external cyber security roles align with and support the organisations’ cyber security strategy. |
| *To what extent is your organization’s cybersecurity policy established, communicated, and enforced?* | The organization does not have an established cybersecurity policy. | There is a basic cybersecurity policy, but it is inconsistently communicated and rarely enforced. | The cybersecurity policy is formally written and communicated to relevant stakeholders. | **In addition to 2:** The cybersecurity policy is consistently enforced with regular updates and compliance checks. | **In addition to 3:** The policy is fully integrated into all business operations and evolves with changing cybersecurity landscapes. |
| *How effectively does your organization use the results of cybersecurity risk management activities to improve and adjust its strategies?* | The organization does not track or use results of cybersecurity activities to inform risk management. | There is limited use of cybersecurity activity results, focusing mainly on ad-hoc adjustments. | Results from cybersecurity activities are systematically collected and used to make informed decisions. | **In addition to 2:** There is a formal process for using cybersecurity results to drive continuous improvement. | **In addition to 3:** The organization has advanced mechanisms in place for real-time adjustments and predictive risk management based on cybersecurity activities. |
| *How effectively does your organization establish and manage cybersecurity supply chain risk management processes, including program development, roles, and responsibilities?* | There is no established cybersecurity supply chain risk management program or clear roles and responsibilities for managing these risks. | Basic cybersecurity supply chain risk management policies and processes are established but not fully integrated or communicated across the organization and with external parties. | Cybersecurity roles and responsibilities for managing supply chain risks are defined and communicated internally and to key external parties; however, integration into broader risk management processes is inconsistent. | **In addition to 2:** Comprehensive supply chain risk management is integrated into overall cybersecurity and enterprise risk management, with all roles and responsibilities clearly coordinated and prioritized. | **In addition to 3:** The organization has an advanced, continuously improved cybersecurity supply chain risk management program that is fully aligned with organizational risk strategies and communicated across all relevant stakeholders, ensuring active engagement and compliance. |
| *How effectively does your organization operationalize and monitor cybersecurity supply chain risk management, including supplier prioritization, incident management, and post-relationship activities?* | Suppliers and third parties are not systematically assessed or monitored for cybersecurity risks, and there is no planning for post-relationship risks. | Basic due diligence is performed before entering relationships with suppliers, but ongoing risk assessment and prioritization are limited. | Suppliers are prioritized by criticality, and cybersecurity requirements are integrated into contracts; however, comprehensive incident planning and recovery activities with suppliers are not fully established. | **In addition to 2:** There is robust risk management throughout the supplier relationship, including incident planning and response. Suppliers’ cybersecurity practices are actively monitored and assessed. | **In addition to 3:** The organization has a sophisticated, proactive approach to supply chain risk management, including advanced monitoring of supplier performance throughout the product and service lifecycle and detailed planning for post-contractual activities, ensuring minimized risks from end to end. |
| Govern | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IDENTIFY (ID): **The organization's current cybersecurity risks are understood** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *How effectively does your organization maintain and manage inventories of its assets?* | The organization lacks inventories of hardware, software, and data, and does not maintain representations of network data flows. | Basic inventories of hardware or software are maintained sporadically, with limited or no details on network data flows. | Comprehensive inventories of hardware, software, and services are maintained, along with basic representations of network communications. | **In addition to 2:** Detailed and updated representations of both internal and external network data flows are maintained. | **In addition to 3:** Inventories and network representations are fully integrated, continuously updated, and systematically verified for accuracy and completeness. |
| *How effectively does your organization prioritize and manage its assets throughout their lifecycle?* | There is no formal process for prioritizing assets or managing them through their lifecycle. | Some assets are prioritized based on criticality, but there is minimal lifecycle management. | Assets are prioritized based on classification, criticality, and impact, with basic lifecycle management practices in place. | **In addition to 2:** Comprehensive lifecycle management processes are established for all prioritized assets. | **In addition to 3:** Advanced techniques such as predictive analytics and automated tools are used to optimize lifecycle management and asset prioritization, ensuring alignment with organizational objectives and risk strategies. |
| *How effectively does your organization identify and assess vulnerabilities and threats affecting its assets?* | The organization does not systematically identify vulnerabilities or threats to its assets. | Key vulnerabilities are identified, but there is limited systematic threat intelligence gathering or assessment of threats. | The organization identifies and records vulnerabilities and receives cyber threat intelligence regularly. | **In addition to 2:** Comprehensive assessments of internal and external threats, and the potential impacts and likelihoods of these threats exploiting vulnerabilities are conducted and updated regularly. | **In addition to 3:** Advanced processes for continuous vulnerability validation, threat intelligence integration, and proactive management of potential impacts are fully operational and integrated into the organizational risk management practices. |
| *How effectively does your organization manage responses to cybersecurity risks and ensure the integrity of critical processes and suppliers?* | The organization lacks formal processes for managing risk responses, vulnerabilities, or the assessment of suppliers. | Basic processes are in place for managing risk responses and assessing critical suppliers, but they are not consistently applied or tracked. | Risk responses are chosen and prioritized with established processes for managing changes and exceptions; however, these are not fully integrated across the organization. | **In addition to 2:** Processes for vulnerability disclosures are well-established, and there is systematic tracking and communication of risk responses and exceptions. | **In addition to 3:** The organization has robust, dynamic systems for responding to vulnerabilities, managing supplier risks, and ensuring the authenticity and integrity of hardware and software, with full traceability and continuous improvement mechanisms. |
| *How effectively does your organization identify and implement improvements across all cybersecurity functions?* | Improvements to cybersecurity are rarely identified and implemented, with minimal use of evaluations, tests, or operational reviews. | Improvements are occasionally identified from basic evaluations or tests but lack systematic implementation across cybersecurity functions. | Improvements are routinely identified from evaluations, security tests, and operational process executions, with some coordination with third parties. | **In addition to 2:** The organization has structured processes to identify improvements from a wide range of activities, including incident response and security tests, with effective implementation plans that are communicated and maintained. | **In addition to 3:** The organization continuously and proactively identifies improvements across all cybersecurity functions through comprehensive evaluations, advanced testing regimes, and meticulous execution of operational processes, including third-party coordination. Incident response and other cybersecurity plans are not only maintained but also regularly enhanced to adapt to emerging threats and operational demands. |
| Identify | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PROTECT (PR): **Safeguards to manage the organization's cybersecurity risks are used** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *How effectively does your organization manage identities, credentials, and access permissions for users, services, and hardware, ensuring secure authentication and authorization practices?* | Identity and access management is either non-existent or poorly implemented, with frequent unauthorized access. | Basic identity and credential management is practiced, but without thorough verification, protection, or policy enforcement. | The organization manages and authenticates identities and credentials effectively, with policies that enforce least privilege and separation of duties, though reviews could be more consistent. | **In addition to 2:** Identity assertions and access permissions are systematically protected, verified, and reviewed; physical access controls are strictly enforced. | **In addition to 3:** The organization employs advanced identity and access management technologies and practices, continuously updating and auditing these systems to adapt to new threats. |
| *Does your organisation provide cyber security awareness training to personnel?* | The organisation does not generally provide cyber security awareness training to personnel. | Cyber security awareness training is provided to some personnel. | Mandatory cyber security awareness training is periodically provided to all personnel. | **In addition to 2:**  Tailored cyber security awareness training is provided to personnel relative to their seniority, role, privileges, and responsibilities.  The organisation evaluates personnel completion rates | **In addition to 3:**  Where applicable, the organisation seeks to enhance consumer cyber security awareness, updating the content regularly |
| *How does your organization protect the confidentiality, integrity, and availability of data at rest, in transit, and in use, including effective backup and recovery processes?* | Data protection measures are inadequate across all stages (at rest, in transit, and in use) | Basic protections are in place for data at rest and in transit, but data in use and backup processes are not comprehensively managed. | Data security is enforced across all data states with consistent application of protective measures and some testing of backup systems. | **In addition to 2:** Data security practices include advanced protections and regular testing of backups to ensure data integrity and availability in any situation. | **In addition to 3:** The organization employs state-of-the-art data protection technologies and methodologies, with continuous improvements based on the latest security trends and internal assessments. |
| *How does your organization manage the security of its software and hardware platforms, including secure development practices, configuration management, and unauthorized access prevention?* | Platform security is largely overlooked, with outdated software and hardware, and no controls against unauthorized installations. | Basic platform security measures like configuration management and software updates are inconsistently applied. | Software and hardware are maintained with risk-based security practices, including logging and monitoring for continuous oversight. | **In addition to 2:** Unauthorized software installation is effectively prevented, and secure development practices are integrated across the software lifecycle. | **In addition to 3:** The organization continuously optimizes platform security through cutting-edge technologies and best practices, ensuring robust protection and compliance with security standards. |
| *How effectively does your organization protect its technology infrastructure from unauthorized access, environmental threats, and ensure resilience and capacity in all operational conditions?* | Infrastructure security and resilience practices are either nonexistent or insufficient | Basic protection against unauthorized access and environmental threats is in place, but resilience planning is limited. | Protective measures for networks and environments are established, and the organization maintains adequate resources for normal operations. | **In addition to 2:** The organization implements advanced mechanisms to ensure resilience in adverse situations and continuously assesses capacity requirements. | **In addition to 3:** Comprehensive and predictive resilience strategies are employed, with the organization proactively adapting to emerging threats and scenarios to maintain continuous availability and security. |
| Protect | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DETECT (DE): **Possible cybersecurity attacks and compromises are found and analyzed** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *How comprehensively does your organization monitor networks, physical environments, personnel activities, external services, and computing systems to detect potentially adverse events?* | Monitoring of assets and activities across the organization is minimal or non-existent, leaving significant gaps in security detection. | Basic monitoring is implemented in key areas like networks and computing hardware, but it does not fully encompass physical environments, personnel activities, or external services. | Comprehensive monitoring systems cover networks, physical environments, personnel activities, and computing systems, with routine checks for adverse events. | **In addition to 2:** Advanced monitoring tools and processes are in place, including the monitoring of external service provider activities, enhancing the organization’s ability to detect a broad spectrum of adverse events. | **In addition to 3:** The organization employs state-of-the-art monitoring technologies across all domains, integrating real-time analytics and automated response systems to preemptively address potential security threats. |
| *How effectively does your organization analyze and respond to adverse events, integrating cyber threat intelligence and correlating information from multiple sources?* | Analysis of adverse events is rudimentary or overlooked, with little to no integration of external intelligence or correlation of data. | Adverse events are analyzed to a basic extent, focusing on immediate impacts without thorough correlation or integration of cyber threat intelligence. | Systematic analysis includes correlating information from multiple sources and understanding the scope and impact of adverse events, though integration of cyber threat intelligence could be improved. | **In addition to 2:** The organization integrates cyber threat intelligence and conducts in-depth analyses, providing comprehensive information to authorized personnel and tools for effective incident response. | **In addition to 3:** Advanced analytic capabilities are utilized, including AI and machine learning, to dynamically integrate threat intelligence and correlate data across multiple sources, ensuring proactive and precise incident declaration and management. |
| Detect | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RESPOND (RS): **Actions regarding a detected cybersecurity incident are taken** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *Does your organisation have a cyber security incident response plan?* | The organisation does not have a cyber security incident response plan. | The organisation has a cyber security incident response plan | The organisation has a documented cyber security incident response plan. | **In addition to 2:**  The cyber security incident response plan includes the requirement for the organisation to document incident investigation and mitigation activities. | **In addition to 3**:  The organisation has established criteria for escalating cyber security incidents to leadership. |
| *Does your organisation investigate cyber security events?* | The organisation does not generally investigate cyber security events. | The organisation occasionally investigates cyber security events. | Appropriately qualified personnel have the tools to investigate cyber security events.  The organisation has a documented process is in place for conducting incident triage or investigations | **In addition to 2:**  Cyber security events that are deemed to be cyber security incident are escalated in accordance with a documented process. | **In addition to 3:**  Cyber security events are analysed for broader behavioural patterns. |
| *How effectively does your organization coordinate response activities and communicate incident-related information with internal and external stakeholders?* | The organization has no formal process for incident response coordination or communication with stakeholders | Incident response communication is limited; only major incidents are reported to internal stakeholders, with minimal external communication. | The organization has defined procedures for notifying stakeholders about incidents, but these procedures are not consistently followed or fully compliant with all relevant laws and regulations. | **In addition to 2:** Response activities are well-coordinated, and stakeholders are consistently informed as required, with established processes ensuring compliance with laws and regulations. | **In addition to 3:** The organization employs advanced communication tools and protocols that ensure real-time, secure sharing of incident details with all designated stakeholders, enhancing the effectiveness of the response and adhering to compliance standards. |
| *Does your organisation ensure appropriate steps are taken to contain, remediate a cyber security incident?* | The organisation generally does not consider containment and remediation of cyber security incidents | The organisation does not have a formal plan for the containment and remediation of cyber security incidents. | The organisation has a documented plan that includes strategies to contain and mitigate various types of cyber security incidents (e.g., DDoS, malware, ransomware). | **In addition to 2:** Containment strategies include notifying impacted third parties, consumers, and relevant regulators.  Mitigation strategies are designed to minimise disruption to critical business services. | **In addition to 3:**  Cyber security incidents response testing includes testing of containment strategies, such as red and blue teaming |
| Respond | | | | | |
| RECOVER (RC): **Assets and operations affected by a cybersecurity incident are restored** | | | | | |
|  | 0 | 1 | 2 | 3 | 4 |
| *How effectively does your organization execute recovery plans following a cybersecurity incident to ensure the operational availability of systems and services?* | Recovery planning and execution are either non-existent or consistently ineffective, leading to prolonged system and service outages. | Basic recovery actions are performed, but they lack coordination and thorough verification of integrity before restoration. | The recovery plan is activated and executed with consideration of scoping and prioritizing recovery actions, yet verification of backups and restored assets is not systematically enforced. | **In addition to 2:** Integrity of backups is verified, critical functions are considered, and restoration activities are well-coordinated, ensuring a return to operational norms. | **In addition to 3:** The organization employs comprehensive and dynamic recovery processes that include thorough verification of asset integrity, detailed documentation of recovery actions, and a formal declaration of recovery completion, ensuring robust and resilient operational restoration. |
| *How effectively does your organization communicate recovery activities and progress during the restoration of operational capabilities to internal and external stakeholders?* | There is minimal or no communication about recovery activities, leaving stakeholders uninformed and potentially non-compliant with regulatory requirements. | Recovery communications are limited and often reactive, focusing only on internal updates without systematic external communication. | Designated stakeholders are informed about recovery activities and progress; however, public communications are not always managed through approved methods. | In addition to 2: Recovery activities are consistently communicated to all relevant internal and external stakeholders, including through public updates using approved messaging. | In addition to 3: The organization employs a strategic communication plan that ensures timely, secure, and clear updates during recovery, fostering transparency and trust with all stakeholders, and effectively managing public perception and stakeholder expectations. |
| *Recover* | | | | | |

1. <https://download.asic.gov.au/media/4c1jmiz1/cyber-pulse-survey-2023.pdf> [↑](#footnote-ref-1)
2. <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final> [↑](#footnote-ref-2)
3. <https://www.deakin.edu.au/courses-search/unit.php?unit=MIS761> [↑](#footnote-ref-3)