CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

MYEMPIRE
GROUP
Your cyber security partner

CSCRC Guidance Paper

Cyber Security Roadmap and Guidance for Cooperative Research Centres

January 2025

cybersecuritycrc.org.au

CONTENTS

CSCRC CEO MESSAGE

When I started in the role of CEO of the Cyber Security Cooperative Research Centre (CSCRC) there were many pressing priorities. From finding accommodation to working out how we would get paid seemed like the most important but also meeting so many new stakeholders and employing staff were of equal importance.

The CSCRC is now at the end of its term and I am surrounded by boxes and packing tape. Shelves have been emptied, documents stored online and laptops all wiped.

However, the moment that any CRC gets its first laptop or creates data, is the moment that you also need to have a cyber security strategy and approach in place.

Good cyber security practices have two critical components. The first one is that there is a strategy (or roadmap) of what technical and human controls you will have in place, that is, getting to an adequate steady state. The second component is of equal importance is maintenance of your steady state (which is also referred to often as good cyber hygiene).

Getting to good cyber hygiene takes time, budget and patience and in my experience is often not regarded as a priority but it must be. Data is the lifeblood of all organisations and a Cooperative Research Centre is no exception.

There are many excellent resources out there to assist you at every stage of your cyber security journey (along with this Guide). The Australian Cyber Security Centre aside from being one of our valued Participants has developed some excellent resources and our CSCRC partnered with the Australian Institute of Company Directors (AICD) on both editions of the Cyber Governance Principles (which has sections for SMEs and NFPs) as well as the Cyber Incident Management Guide with the AICD and Ashurst.[1]

I also want to acknowledge Alex Woerndle and his whole team at My Empire who have been our virtual Chief Information Security Officer for a few years now. They have been an invaluable source of guidance (and created this Guide) and been an integral part of our cyber security journey.

No organisation can ever completely eliminate cyber security risk but there are many steps you can take to effectively manage this risk.

I hope that you find this Guide useful for your CRC- good luck (and make this a budget priority)!

Best wishes,

Rachael Falk
Chief Executive Officer
Cyber Security Cooperative Research Centre

[1] For access to these and other CSCRC resources, refer to https://cybersecuritycrc.org.au/media-resources

PREFACE

The Cyber Security CRC Journey

Cyber Security Cooperative Research Centre (CSCRC) was established in 2018 with a focus on research projects to build Australia's cyber security capacity and capability and address both technology and policy related challenges.

As an advocate for robust cyber security, board and management were cognisant of the need to ensure CSCRC established its own effective security risk management program.

The purpose of this paper is to provide some guidance for other CRCs on the journey and learnings from CSCRC's investment in security.

Cyber security for CRCs requires continual focus throughout the funding term. The CSCRC's journey evolved since 2018 and progressively increased in effort and intensity. While the CSCRC had initially made significant investment in security tools to protect data, devices, intellectual property, and cloud services in use, management recognised the need to enhance its own practices to ensure a holistic risk-based approach.

Defining Business Requirements

Objectives

As a CRC focussed on addressing Australia's cyber security challenges and opportunities, it was natural for the Board and management to have a very low risk appetite in relation to cyber security and privacy risk.

All CRCs will manage conflicting objectives of protecting sensitive information and ownership of research data, with the fundamental principle of openness.

The CSCRC applied the following objectives when considering its own cyber security in line with the organisation's objectives and risk:

Visibility

- Having a clear understanding of what assets the CSCRC had. These assets included data, technology, and people. Of importance for each of the assets, was noting the business value of those assets (not monetary value but if they were to be stolen or lost, what risk did this pose to the research, their Participants and reputation), where they were, who had access to them and how they were protected.

Managing risk and compliance

- Understanding organisational risks and prioritising investment in controls that provided the greatest improvements to its cyber posture. Whilst compliance with obligations was critical, the Board's low risk tolerance meant a thorough understanding of 'what can go wrong' was the highest priority.
- CSCRC leveraged the ISO27001 and Essential 8 frameworks when considering appropriate governance and technical controls to manage its cyber security risk. Whilst there are numerous frameworks available, these were identified as appropriate for the organisation for the following reasons:
  - Essential 8 (maturity level 1) is recommended by the Australian Government as a baseline good practice

  - ISO27001 provided a risk-based approach that is recognised globally

Continuous monitoring and validation of controls

- Having the confidence in the controls deployed, and that CSCRC was well prepared to prevent significant incidents. The CSCRC established a program of continuous review and validation to ensure currency and effectiveness of controls, with regular reporting to the Board.

Structure and Ownership

- Ensuring senior management and key stakeholders understood their roles in protecting CSCRC assets and were actively engage in driving the security program. The CSCRC established a security steering committee comprising the executives and business managers/leaders to maintain focus on cyber risks and support decision-making on investment in security controls.

Incident preparedness

- Ensuring CSCRC was well equipped to quickly and effectively identify, contain, respond and recover from a cyber incident.

Constraints

Without proactive oversight, investment in cyber security can rapidly grow with the number of 'must have' tools to protect every facet of a CRC. Understanding assets, obligations, risks, and priorities were key to focussing investment on the right solutions at the right time.

Decisions to invest in services and technology were made considering the following constraints:

Budget

- CSCRC was no different to any CRC and had limited funding that required careful management. CSCRC focussed – via the security steering committee - on the balance between risk and return/reward when deciding to invest in services and solutions.

Resources

- The recruitment market for security professionals is difficult, and market rates are high. Additionally, the range of skills required to cover the core elements of a mature security function would have increased CSCRC's headcount almost 50%. To address this issue, a specialist firm providing a virtual security team (commonly referred to as a 'Virtual Chief Information Security Officer' or 'vCISO') with access to all the skills required, was engaged. This supported budget management with the vCISO providing the leadership and guidance on investment decisions and optimisation of security tools.

Balance between confidentiality and collaboration (of research)

- CRCs by their nature produce reports for a wide audience. However the inputs to this research can sometimes be confidential, so a balance is required between security and collaboration. Doing so requires setting organisational controls and technical controls to limit the risk of unauthorised access to information and systems without limiting collaboration.
- Organisational controls included agreements with third parties, defining baseline security expectations, and policies which governed the access and use of information and systems.
- Technical controls included implementing controls on user access (such as multi-factor authentication), solutions to protect devices from compromise, secure internet browsing, and ensuring limited sharing of information via only approved methods.

CSCRC Lessons learned

With the benefit of hindsight, there are some lessons to take from the CSCRC journey, to help other CRCs implement and maintain an effective cyber security posture, including:

Engage the right expertise early, and ongoing

- The CSCRC engaged several partners to support some of the technology utilised (e.g., office network, devices, and Salesforce), and relied on the guidance of the IT Managed Service Provider to guide cyber security. A vCISO was engaged in 2021 to take control of the program and guide structure and improvements. Engaging earlier would have resulted in lower risk exposure from the outset via investment in the right controls. A vCISO was preferred because they had a broader understanding of the threat environment, actively engaged with staff and were not just focused on technical solutions.

Establish governance, risk and compliance structures early

- The priority in the early days of CSCRC was to establish fundamental technical controls for specific systems. However, with hindsight, establishing governance risk and compliance structures earlier would have facilitated investment of resources across the broader business.

Establish consistency in technology upfront

- CSCRC identified that inconsistently implemented technologies lead to additional costs and inconsistency in security controls further down the track. Consideration should be given early in the lifecycle of the CRC to establish principles for technology that support business objectives and guide decisions in line with budgets, security risks and other constraints. Retrofitting security controls to a diverse ecosystem of hardware and software will take additional time and resources to implement and manage.

Establish data handling and protection early

- Personal Information (PI) was identified in many systems during the wind down. The largest PI set we held was collected through email and applications for scholarships. These needed to be carefully identified and destroyed. Establishing data handling and protection policies and practices upfront would have made this significantly easier during wind down.

Based on the CSCRC learnings, the below section provides a detailed series of recommended activities for all new and established CRCs.

ROADMAP

Recommended CRC Roadmap

Security priorities evolve throughout a funding term. Depending on a CRC's age and operational phase, the focus on security policies, tools, audit, and data protection requirements will shift.

The CSCRC's recommended focus areas are broken down assuming the below 4 phases of a funding term. Where a CRC is beyond the initial establishment phases in its funding term, but has yet to address the preliminary actions, it is highly recommended to consider commencing from the 'Setup' phase to ensure the fundamentals are in place.

Cooperative Research Centres follow a similar lifecycle through their funding terms, which can be summarised as:

Setup (month -6 to +6)

- Management and board are focussed on corporate setup, funding, board composition, operational team establishment, basic IT requirements and partnerships
- *Security focus:* The focus should be on identifying an IT Managed Services Provider (IT MSP) and core tech platforms, roles and responsibilities for IT management, and fundamental security requirements. Decisions on IT are important at this early stage, to establish consistency (e.g. Mac v Windows, etc). Establish and maintain a register to track hardware, software, cloud, IP and information assets.

Operational Establishment (month 6 to 12)

- Management is focussed on establishing partnerships, assessing project opportunities, establishing operational teams and internal processes
- *Security focus:* During this phase, establish security controls (awareness training, processes, and technical tools) and overall governance with a focus on risk management.

Research and commercialisation (from month 12 onwards)

- Management is focussed on the research program and outputs to achieve the CRC's vision and mission
- *Security focus:* With the fundamentals of risk management in place (steady state), focus turns to operational security management, with regular risk reviews, continual investment in controls to reduce areas of unacceptable risk, monitor and respond to breaches, and establish a program of audits to continually assess the effectiveness of security controls.

Wind down (final year of funding term)

- Board and management are navigating the commercialisation of research projects, potential transfer of IP to new commercial entities, research and industry partners, and the dissolution of the CRC.

- *Security focus:* Focus in the final year of operation will shift to retrieval of CRC data, destruction/transfer/retention of data based on the CRC's commercial agreements and obligations, the return of devices/assets, termination of legal agreements, and offboarding of staff to ensure security and privacy obligations are maintained post-termination.

Importantly, regardless of phase, the ability to continually identify cyber and data risks, and to pivot a CRC's focus to address new and evolving risks, is critical. As such a governance structure (bringing key CRC team members together regularly to consider cyber risks, control gaps, and mitigations), and access to appropriate external skilled advice is crucial throughout all 4 phases.

The following sections expand upon the security recommendations for each of the 4 phases.

Setup Phase

Security Objective during this phase: Establish a robust foundation for cyber security to support the CRC's mission.

The setup phase is crucial for laying the foundation of a CRC. During this phase, the focus is on establishing the organisational structure, identifying technology needs, and implementing basic cyber security measures. The rationale behind this focus is to ensure that the CRC starts with secure technology that can support its research activities.

Capacity and capability considerations are paramount at this phase, as the CRC must ensure it has the necessary skills and services to establish appropriate cyber security from the outset. Thus avoiding the difficulties of wedging security into established operations later. This includes appointing an IT Manager or outsourcing to an IT MSP and hiring a vCISO.

Establishing centralised management of devices from the outset, and basic cyber hygiene practices help in mitigating initial security risks and making future tasks of securing data and devices much easier to manage. Additionally, setting up onboarding and offboarding processes for employees is vital to protect sensitive information from the very beginning.

Setup Phase Activities

Recommended activities during the setup phase include:

- **Identify Business Requirements**
  - Consider objectives, priorities, constraints, obligations etc.
  - Consider technology requirements including devices, information storage and communications.
- **Define Expectations of Technology Partners**
  - Selection Criteria: Develop clear criteria for selecting technology partners, focusing on their ability to meet security standards, provide reliable support, and offer scalable solutions.
  - Roles and Responsibilities: Clearly define the roles and responsibilities of each technology partner in maintaining operational uptime, and cyber security.
- **Define Expectations of Research Providers**
  - Contracts: establish agreements with collaborators that details responsibilities with regards to access to and management of information and systems
  - Training: Provide training and or policies on use and protection of information and systems.
- **Appoint IT and Cyber Security Subject Matter Experts**
  - In-house vs. Outsourced: Evaluate the pros and cons of having an in-house IT Manager versus outsourcing to an IT MSP. Consider factors such as cost, expertise, and service level expectations (e.g., 24/7 support requirements).

  - Virtual CISO: Appoint a vCISO to oversee the cyber security strategy. The vCISO will be responsible for developing security policies, conducting risk assessments, monitoring the effectiveness of technical controls, identifying obligations (legal, regulatory, etc), and supporting compliance.

- **Decide on Core Technical Platforms**
  - Platform Selection: Choose secure and scalable platforms for research and collaboration. Ensure these platforms support the CRC's research activities and comply with industry standards and regulations. It is recommended to minimise the technology landscape over the course of the funding term to reduce data and cyber risks and simplify the wind down phase at the end of the term.
  - Platform Baselines: Where possible, decide on consistent hardware vendors and devices based on anticipated needs of staff. This will simplify security and device management whereas diverse platforms (e.g. Windows devices, Macbooks, etc.), will make management of policies and compliance more cumbersome.
  - Integration: Ensure integration of these platforms to facilitate efficient data sharing and collaboration. Ensuring compatibility of hardware, software and collaboration tools will simplify the technology landscape for easier management, and importantly, ensure security controls can be effectively deployed and managed.
  - Asset Tracking: Create an asset register to track all information and technology assets. Include details such as asset type, location, owner, data types stored/handled/processed by the asset, backup requirements, data retention requirements, and security controls.

- **Onboarding and Access of Employees**
  - Onboarding: Create procedures for onboarding new employees and partners. This includes setting up user accounts, securely sharing their initial login credentials and providing access to required systems.
  - Least Privilege Principle: Apply the principle of least privilege to minimise the risk of unauthorised access. Ensure that users have only the access necessary to perform their roles.
  - Passwords and Access Control: Consider utilising a secure password vault for all employees and establish training (aligned to the organisation's password policies) to ensure adoption.
  - Training: Establish cyber security and data privacy training for all staff. This includes phishing awareness, safe browsing habits, and secure data handling. At this early stage, establishing a solution to access training content and automate regular phishing testing is highly recommended to embed security awareness culture across the organisation from the start.

- **Technology Setup**
  - Multi-factor Authentication: Where possible, ensure multi-factor authentication is set up on all user accounts.
  - MDM Solutions: Use a Mobile Device Management (MDM) solution to enforce security policies, manage device configurations, and monitor device compliance for both company-issued devices and personal devices that may be permitted for accessing CRC applications and data.
  - Network Security: Set up firewalls, intrusion detection systems, and secure Virtual Private Networks (VPNs)s to protect the CRC's network. Ensure these systems are configured correctly and regularly updated. Where a hybrid working environment is anticipated, consider the use of a cloud-based Secure Access Service Edge ('SASE') solution for devices rather than just the traditional office-based VPN.

- Device Security: Acquire a reputable commercial Endpoint Detection and Response ('EDR') solution to protect devices from compromise.
- Domain and Website security: Establish your domain name(s) and setup auto-renewal. Undertake an assessment of your domain name and website security posture before the website goes live and develop a regular testing schedule.
- Patching: Regularly update and patch network infrastructure and your website to protect against known vulnerabilities. Implement a patch management process to ensure timely updates. Staff must also update devices such as phones (iOS updates).
- Encryption: Apply encryption to protect data at rest and in transit across all systems, where possible.

- **Office Setup and Physical Security Controls**
  - Office Layout: Design the office layout to support secure operations, including secure areas for sensitive research activities and meetings.
  - Access Controls: Implement physical access controls (such as keycard entry systems, biometric scanners, and security cameras) to monitor and restrict access to the office.
  - Environmental Controls: Ensure the office environment supports secure operations, including proper lighting, secure storage for sensitive documents, and fire suppression systems.

Operational Establishment Phase

Security Objective during this phase: Establish and refine cyber security controls as the CRC becomes fully operational.

The goal of this phase is to ensure the CRC has visibility of its systems, information and vulnerabilities and has the mechanisms in place to manage the associated risks.

During this phase, governance structures will become defined, and leadership will take an active role in driving security and privacy across all areas of the business.

Operational Establishment Phase Activities

Recommended activities during the operational establishment phase include:

- **Establish Governance Structures**
  - Governance Framework: Establish governance structures to ensure continual engagement with management, specialist providers and advisors. Define roles and responsibilities for overseeing cyber security.
  - Regular Meetings: Schedule regular meetings to review security policies, discuss emerging threats, and make strategic decisions.
  - Industry Frameworks and Certifications: Consider aligning to, or beginning the journey to certify against, privacy and security frameworks and certifications.
- **Maintain Asset Register**
  - Regular Updates: Regularly update the asset register to reflect changes in the CRC's information and technology landscape. Use the register to inform risk assessments and security planning.
- **Conduct Security Assessments**
  - Testing Schedule: Conduct a technical security assessment of the CRC's website, network and conduct security posture assessments of cloud environments (i.e., Microsoft 365, Google) to identify vulnerabilities in the CRC's systems and networks.

  - Remediation: Implement remediation measures based on the findings of security assessments.

- **Data Handling and Protection**
  - Data Classification: Implement data classification and protection measures to ensure sensitive data is handled appropriately. Noting that Personal Information (PI) requires special attention and that large PI data sets may exist and need to be handled appropriately in line with privacy laws.
  - Secure Storage: Ensure secure storage of sensitive research data. Use access controls to restrict data access to authorised personnel only.
  - Secure Transfer: Ensure transfer of information is protected to the extent required by each classification.
  - Data Retention Compliance Requirements: Identify and retain data or systems required for compliance with legal, regulatory, and contractual obligations. It is advisable at this stage to consider future requirements at wind down.
- **Risk Management**
  - Risk Management Framework: Develop a risk management framework to govern the ongoing management of risks to align with CRC objectives.
  - Risk Assessment: Conduct an assessment of enterprise risks which should include cyber risks alongside other business risk. Continued uplift and improvement will occur through mitigation plans and re-assessment.
- **Incident Response and Business Continuity Planning**
  - Incident Response: Develop an incident response plan that outlines the steps to be taken in the event of a cyber security incident. This includes identifying key personnel, communication protocols, and recovery procedures.
  - Business Continuity: Conduct a Business Impact Assessment (BIA) to understand key business processes and dependencies (people and technology), define recovery objectives, and document the CRC's Business Continuity Plans accordingly.
  - Testing: Conduct a test of the incident response and business continuity plans through simulations and drills with board and management. Ensure all staff are aware of their roles and responsibilities during an incident.

Research & Commercialisation Phase

Security Objective during this phase: Maintain and enhance cyber security to protect ongoing research activities.

The focus during this phase is on maintaining oversight of risks and monitoring for potential incidents. Subject to the fundamentals from the first 2 phases being established, this phase becomes more focussed on business-as-usual operations.

By conducting regular security audits, user access reviews, proactive monitoring of threats, routine risk assessments, and continual training for staff, leadership will have visibility of potential issues and the ability to effectively respond to incidents.

These activities are critical to ensuring the integrity and confidentiality of the CRC's research activities, enabling secure collaboration and innovation.

Research & Commercialisation Phase Activities

Recommended activities during the research and commercialisation phase include:

- **Security Audits**
  - Regular Audits: Conduct regular security audits to identify vulnerabilities and ensure compliance with security policies and frameworks (if applicable).
  - Finding Remediation: Document findings and implement corrective actions promptly.
  - Reporting: Ensure that audit reports and findings are presented to and assessed by senior management and the Board.
- **Proactive Monitoring of Threats and Security Alerts**
  - Threat Intelligence: Utilise threat intelligence services to stay informed about emerging threats.
  - Real-Time Monitoring: Implement pro-active monitoring to detect and respond to security alerts.
- **Routine Risk Assessments**
  - Risk Identification: Conduct routine risk assessments to identify potential threats and vulnerabilities. Evaluate the impact and likelihood of each risk.
  - Mitigation Strategies: Develop and implement mitigation strategies to address identified risks. Regularly review and update these strategies to adapt to the changing threat landscape.
- **Regular User Access Reviews**
  - Access Control: Perform regular reviews of user access to ensure that permissions are appropriate and up-to-date. Revoke access for users who no longer need it.
- **Continual Training and Awareness for Staff**
  - Training Programs: Deliver ongoing training programs to educate staff about cyber security best practices. Include topics such as phishing awareness, secure data handling, and incident reporting.
  - Phishing Simulations: Run regular phishing simulations to assess staff competency to detect and report suspicious emails.
- **Regular Testing of Business Continuity and Incident Response Plans**
  - Plan Testing: Regularly test business continuity and incident response plans through simulations and drills (at least annually). Ensure that all staff are familiar with their roles and responsibilities during an incident.
  - Plan Updates: Review and update plans based on test results and lessons learned. Ensure that plans remain relevant and effective in addressing current threats.

Wind Down Phase

Security Objective during this phase: Ensure effective management of system and data retention, destruction and transfer at wind up of the CRC, and meeting obligations into the future.

The wind down phase focuses on ensuring the secure closure of the CRC and proper handling of all data and assets. Implementing cyber security measures during the wind down phase of a CRC can be particularly challenging due to several factors, including:

Data Retention and Compliance

- Ensuring that all data required for compliance with legal, regulatory, and contractual obligations is retained securely can be complex (e.g. privacy laws). Identifying what data needs to be kept, how it should be stored, and for how long requires careful planning and execution. Understanding and documenting these requirements early in the CRC lifecycle and maintaining these records throughout the funding term will make the wind down process more efficient and minimise potential errors.

Secure Data Destruction

- Properly destroying or securely handing over IT assets and sensitive documents is critical to prevent data breaches. This involves ensuring that all data is irretrievably destroyed or securely transferred, which can be logistically challenging.

Managing User Access

- Conducting thorough user access reviews and system audits to ensure that no unauthorised access remains can be time-consuming. Ensuring that all access permissions are revoked and that no residual access is left open requires attention to detail.

Termination of Commercial Agreements

- Formally terminating commercial agreements with vendors, partners, and service providers involves ensuring that all contractual obligations are fulfilled and that all CRC data is removed from vendor systems. This process can be complicated by the need to coordinate with multiple external parties.

Capacity and Capability

- Ensuring that the CRC has the necessary skills and services to manage the wind down phase effectively can be challenging. This includes having the right personnel to oversee the secure destruction of data, conduct final audits, and manage the transition. Outsourcing certain tasks to specialists may be necessary, but finding and managing these external providers can add complexity.

Knowledge Transfer

- Transferring knowledge related to systems and research projects requires thorough documentation and effective communication, which can be difficult if key personnel have already left the organisation.

Wind Down Phase Activities

Recommended activities during the wind down phase include:

- **Obligations**
  - Identify and document post wind down obligations, such as ongoing compliance requirements. Ensuring that these obligations are met requires planning and monitoring, identification of custodians and establishing post-wind down service agreements for terms of up to 7 years.
  - Addressing these challenges requires careful planning, communication, and a focus on maintaining security standards until the very end of the CRC's lifecycle. This process should commence approximately 12 months prior to the term end.
- **Employee and Technology Offboarding**
  - Access Reviews: Conduct a final review of user access across all systems to ensure all access is revoked as employees end their employment with the CRC, and that no unauthorised access remains. Revoke access for all users who no longer need it before termination of employment, where appropriate.

- **Retention of Data or Systems Required for Compliance**
  - Data retention, destruction or transfer: Decide what information will be retained, destroyed or transferred at wind down and determine how this will be achieved.
  - Custodianship Considerations: Designate custodians for retained data and systems to ensure ongoing compliance and security, and support access requests beyond the wind down of the organisation.
- **Formal Termination of Commercial Agreements**
  - Contract Termination: Formally terminate all commercial agreements with vendors, partners, and service providers. Ensure that all contractual obligations are fulfilled and documented.
  - Data Removal: Ensure that all CRC data is removed from vendor systems and that vendors confirm the secure deletion of data.
- **Removal of CRC Data on Devices**
  - Data Wipe: Ensure that all CRC data is removed from personal devices used by employees and partners.
  - Secure destruction: Where required, engage a third party for the secure destruction of data and/or hardware on CRC-owned devices.

SUMMARY

The cyber security lifecycle of a CRC requires continued consideration alongside other elements of running a successful CRC. We hope that this guide has given you some insight into the requirements for managing your cyber security effectively.

Managing cyber security effectively does not need to be a costly exercise, there is ample support available in Australia for managing cyber security regardless of the budget available or the resources on hand.

To recap:

- Make time to understand what your obligations, objectives, and constraints are, and build from there
- Establish a governance structure, bringing management and board into the security conversation continually
- Understand and continually manage your risks
- Implement controls that directly address and minimise your risks
- Consider support available and engage external assistance where needed.