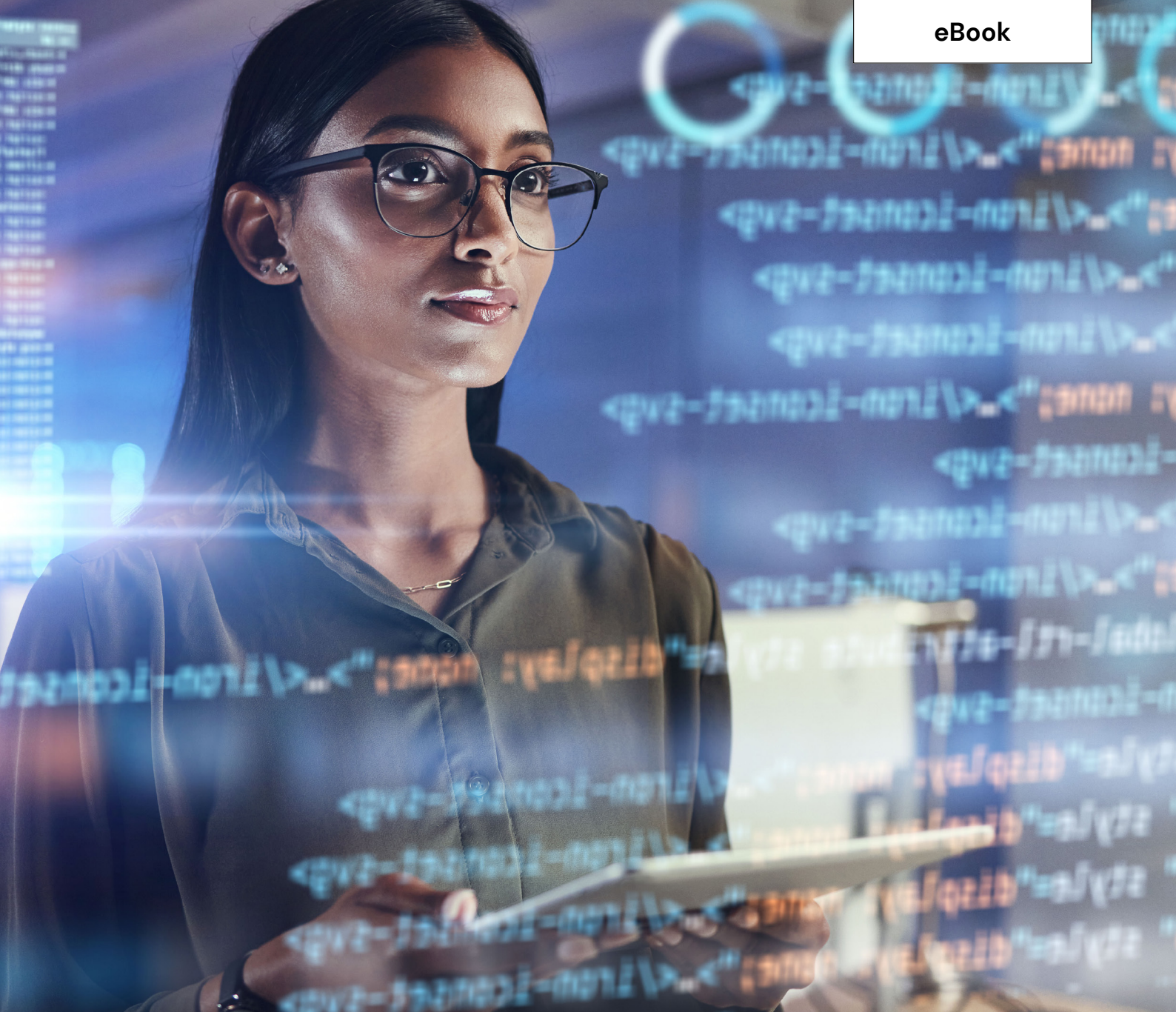
eBook



From data protection to cyber resilience

Proven practices for the public sector

Intermedium eBook Sponsored by Commvault

Intermedium

Commvault®

Introduction

Cyber resilience is critical in protecting agency operations and sustaining citizen trust. Data protection is vital but not enough.

Cyber-attacks orchestrated by criminal and state-sponsored adversaries are a persistent threat to Australian governments and a major risk concern for agency executives.

Adversaries seek to exploit weaknesses such as inadequate employee cyber hygiene and technology fragmentation, using various techniques and increasingly, artificial intelligence (AI) technologies.

Motivated by financial gain, espionage, or to cause embarrassment, the goals of government cyber adversaries include disrupting services by damaging or destroying technology infrastructure, and stealing and exposing citizen, agency, or commercial data.

Protecting agency business systems and data from cyber-attacks is becoming more challenging. Many agencies have mobile workforces and/or hybrid work arrangements coupled with ICT architectures that have a mix of contemporary cloud services and solutions on-premises.

Furthermore, Advanced Persistent Threats (APTs) – actors who are typically state-sponsored, well-resourced, and sophisticated – can go unnoticed for long periods.[1]

Data protection is not enough in this challenging cyber threat environment, as mobile work and cloud computing mean there is no longer a clear network perimeter to protect. Instead, agencies must manage cyber security risk by adopting an approach of cyber resilience that includes governance, protection, detection, response, and recovery measures.

"One thing is abundantly clear from what's happened to our cyber environment in the last five years: we simply can't continue as we are. We need to push harder, we need to get in front of this problem."[2]

Clare O'Neil
Minister for Home Affairs and Cyber Security

The complex risk environment faced by agency executives

- Rising frequency and sophistication of cyber-attacks[3]
- Expanding volumes of citizen and agency data[4]
- Cyber skills and resource shortages[5]
- Complex technology environments[6]
- Inadequate cyber awareness and maturity[7]
- Wide attack surface with fragmented endpoints[8]

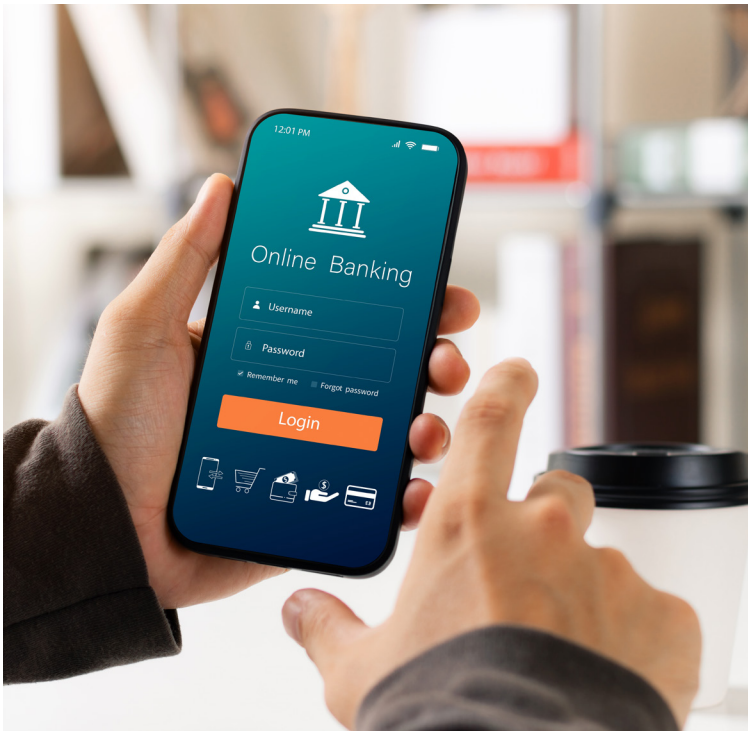
This eBook outlines how agencies can develop cyber resilience to help safeguard agency and citizen data and ensure business continuity in the face of rising threats.

"To uplift our collective cyber security, the Government must itself adopt cyber best practices..."

2023-2030 Australian Cyber Security Strategy[9]

This eBook includes proven practices from Australian information security risk reduction policies and guidance material, including the Australian Government's Essential Eight Strategies to Mitigate Cyber Security Incidents[10] and Information Security Manual (ISM).[11]

Many of this eBook's proven practices – particularly those enabling greater automation – also support agency efficiency. This is vital in the current budget context of competitive demands for limited resources.[12]



Impacts of cyber-attack and data breach

	Impact	Example
Citizen	Physical safety	Address exposure
	Financial security	Leaked credentials and payment information causes identity theft and scams
	Mental health	Leaked health records with sensitive personal data
	Customer experience	Updating details, passwords, etc. with government service providers
Agency	Reduced citizen confidence in online services	Fewer digital transactions, unwillingness to provide personal information
	Reputation	Agency peers reluctant to partner
	Commercial	Inability to negotiate future contracts/pricing effectively
	Costs	Data recovery, victim support

Proven practices to build cyber resilience

While safeguarding business systems and data is more difficult than ever for agencies, new cyber resilience tools and approaches are emerging, allowing agencies to reduce risk by following proven practices.

Establish clear responsibilities for cyber resilience

As the adage goes, 'cyber security is everyone's responsibility.' Notwithstanding this, and in addition to this, agencies are establishing clear roles and responsibilities for cyber security.

The ISM nominates two key roles for agencies to establish:

> **Chief Information Security Officer (CISO):** A CISO is responsible for leading security uplift across the agency, including instituting controls, training, reporting, incident response, continuity planning, and managing supplier relationships, resources, and personnel.[13]
>
> **System owner:** A system owner is responsible for an individual information technology system, including selecting, implementing, and assessing controls; and authorising and monitoring system security.[14]

Leverage the Whole-of-Government (WofG) cyber security unit

Agencies have specific spheres of responsibility, which can lead to a 'siloed' and potentially sub-optimal approach to cyber security. Most ANZ jurisdictions have created a WofG cyber security function (typically led by a CISO or equivalent) to share best practices, eliminate duplication of effort, and encourage collaboration.

WofG CISOs receive budget allocations to support or supplement agency capabilities, offering support for areas such as training and awareness, vulnerability management, intelligence and incident response, as well as policy, standards, and procedures implementation assistance.[15]

Establish a centralised view of risk

Agency technology environments now typically comprise multiple cloud and on-premises systems, creating a complex cyber environment to manage.[16]

Furthermore, remote work arrangements create a wide 'attack surface.' In the Australian Government, 55 per cent of employees work partially from home.[17] Remote workforces often have poor cyber hygiene due to ignorance or lack of cyber hygiene training.

To guard against 'shadow IT' and other vulnerabilities created by the increased complexity of the ICT environment, agencies can centralise and integrate security, governance, and visibility via cloud-based systems. This will reduce complexity and allow stakeholders to collaborate and address threats.

Security Orchestration, Automation, and Response (SOAR) platforms connect various systems via application programming interfaces (APIs) to identify risks, register attacks, and automate responses using designated scripts. Linked systems can include Security Information and Event Management platforms, threat feeds, data protection and recovery, intrusion detection and prevention, and endpoint protection.[18]

Data protection and recovery is a vital component of an enterprise cyber resilience approach. Leading cloud-based systems allow system administrators to manage the backup of agency data stored in the cloud and on-premises via a single interface. 'Regular backups' are one of the Essential Eight strategies, requiring agencies to ensure that backups are performed regularly according to agency business continuity requirements.[19]

Agencies can also centrally manage other Essential Eight security strategies, including user application hardening, restricting Microsoft Office macros,

and regular patching of applications and operating systems.[20]

Reducing the number of point solutions by adopting comprehensive data security offerings and integration also supports more efficient use of resources by avoiding duplication. More does not equal better when building resilience.

Deploy independently assessed solutions

Many suppliers understand Australian public sector regulatory requirements and participate in risk assessments such as the Infosec Registered Assessors Program (IRAP).

The IRAP assessment must be consistent with the process prescribed in the ISM and the Protective Security Policy Framework (PSPF).

Suppliers must evidence controls and governance arrangements, including cryptographic controls, incident response, and multi-tenancy mechanisms to stop unauthorised access. Suppliers should be IRAP assessed every 24 months, according to the ISM.[21]

However, procuring services from cloud service providers (CSPs) does not absolve agencies of security responsibilities. The 'shared responsibility model' typical of cloud contracts means that agencies retain responsibilities, including data management and identity and access management.

Apply zero-trust principles

"We will… [aim] to develop a whole-of-government zero trust culture."

2023-2030 Australian Cyber Security Strategy[22]

Zero-trust is widely considered a cyber security best practice. Insider threats and the rising use of valid credentials to access systems mean that agencies must act as if threat actors have already entered their enterprise environment.

Zero-trust involves restricting and monitoring access to systems and data. Access permissions should only be granted to employees or systems with a demonstrated need to access data or systems. This is often called the 'principle of least privilege.'[23] Under this principle, access must be revoked once the user no longer needs the system or data, and senior personnel should only be given access to the

systems and data required to perform their role. Only select backup administration accounts should be able to access, modify, and delete backups.[24]

Apply behavioural-based threat detection

Zero-trust identity and access management can be enhanced with 'behavioural-based security' features. This involves using AI and other automation technologies to detect and contain system users who are displaying variations from their normal behaviour, for example, logging in to agency systems from unusual locations, outside of working hours, or performing bulk downloads.

Behavioural-based security features can trigger Multi-Factor Authentication (MFA) to guard against adversaries using stolen credentials. Despite being one of the Essential Eight, a 2023 Victorian Government audit found that 94 per cent of government accounts did not use MFA.[25]

Stop data sprawl

Agencies can reduce data sprawl by prioritising information management. Data sprawl can occur when data is stored across various on-premises, cloud, and legacy solutions. It puts agencies at risk of data duplication, retention of unnecessary data, concerns over data integrity, and unnecessary data storage costs.

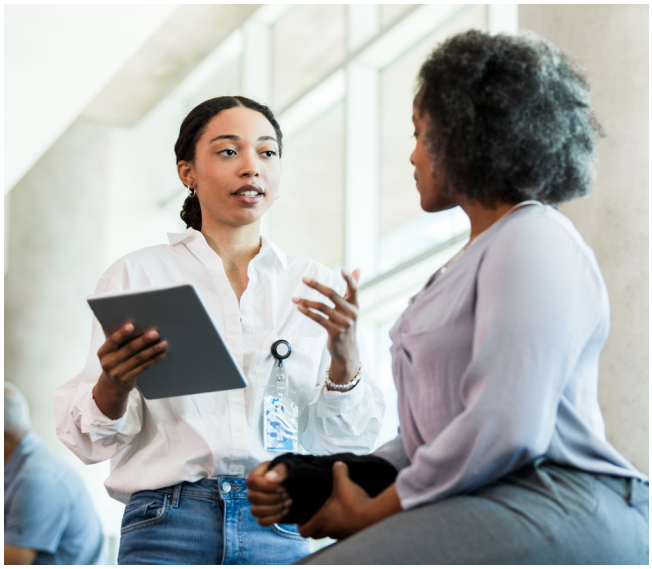
Unnecessary storage of personal and agency data increases the risk and damage of data breach, which is why jurisdictions are developing digital IDs where citizen data is stored on personal devices rather than in the systems of multiple service providers.

Data governance includes systems of rules, regulations, protocols, and accountabilities to safeguard data. Automated data management processes which align with governance requirements can support agencies to scan and categorise sensitive data to ensure that live and backed-up data are stored with appropriate security protections.

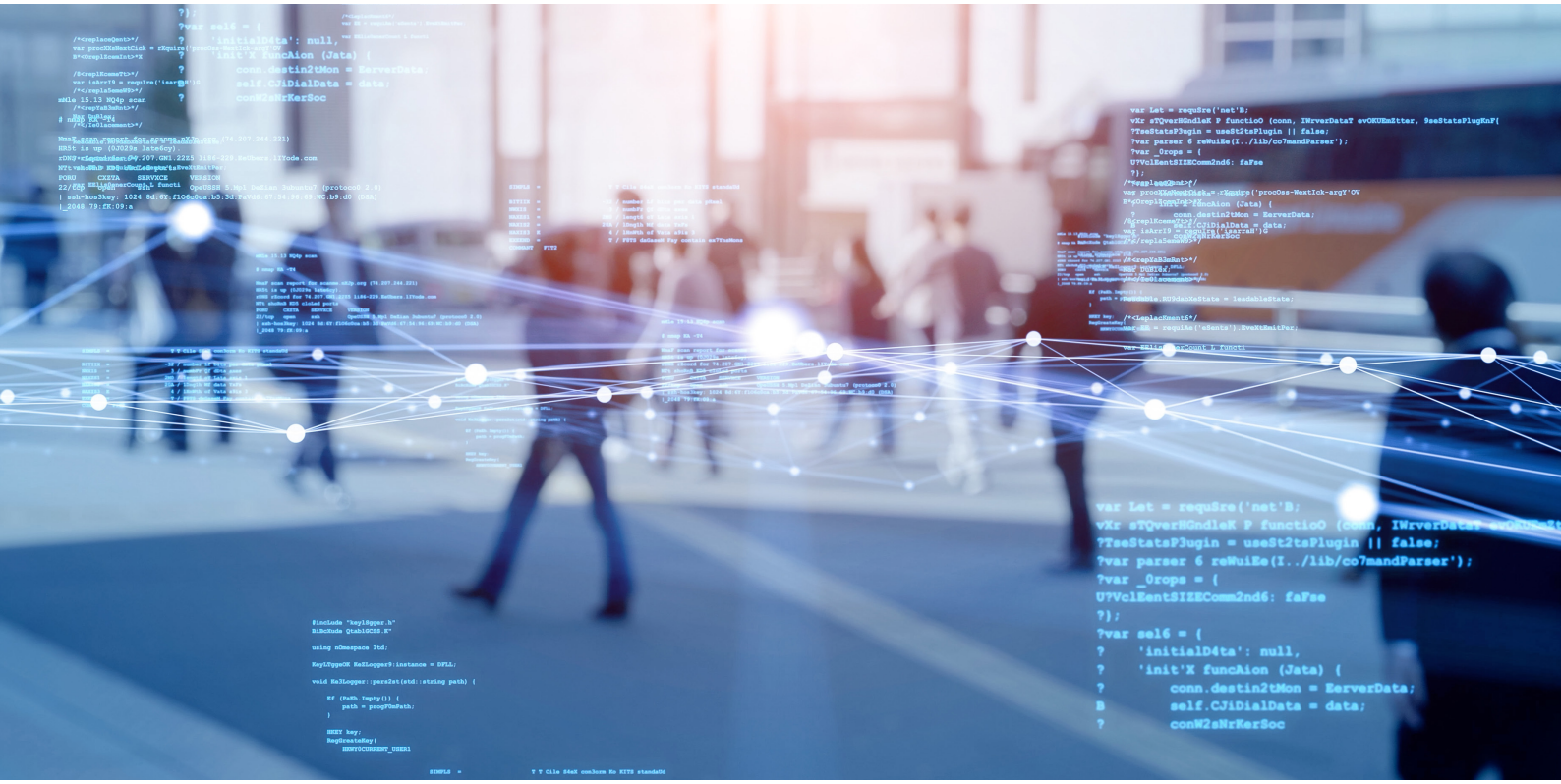
Automating classification reduces human error, particularly for straightforward cases, allowing humans to focus on more complex instances of data categorisation, including personally identifiable information.

The Australian Privacy Act 1988 identifies types of sensitive information, including information on an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record, health records, and biometrics.[26]

Business-critical and sensitive data – often referred to as the 'crown jewels' – may need extra protections like air gaps. Air gaps are when data is not physically or, in the case of virtual air gaps, logically connected to the outside network. The Australian Government is currently reviewing its sensitive and critical datasets to determine if its current storage and protections are risk-appropriate.[27]



Case Study:
NSW Government leaks sensitive location data



In 2021, NSW released a dataset of 'COVID-safe' businesses. The dataset contained the addresses of sensitive locations including domestic violence shelters, defence sites, and a missile maintenance unit. Anti-domestic violence advocates expressed shock, noting that identifying the location of shelters could have serious consequences. One advocate told the Sydney Morning Herald that the data leak "could be a matter of life and death."[28]

The government pulled down the dataset, acknowledged its error, and briefed the state Privacy Commissioner, who was satisfied "with the actions taken to contain, respond to, and remediate the incident."[29]

Nevertheless, the publication of the data should never have happened. Data governance tools can screen large volumes of data for sensitive information and ensure that data authorisation and other governance procedures are applied.

Detect threats through forensic analysis

Agencies must contend with rising volumes and varieties of data. Automation is essential to manage this data effectively, including identifying risks.

Agencies can access solutions from leading suppliers that incorporate AI and other automation technologies to assess data for malware or other risks. Files that can suggest compromise include those that may be new, renamed, modified, corrupted, or encrypted.

Leading solutions can analyse data to identify safe recovery points from backups before the compromise, so agencies can restore data and maintain business operations.

Minimise the damage of successful cyber-attacks

Cyber resilience is about safeguarding agency business continuity and protecting the social contract with citizens to use their data for their benefit.

Leading data protection solutions allow governments to restore data quickly to the required location, avoid operational disruption and minimise citizen impact. Systems supporting immutable backups allow executives to be confident in the restored data.

Agencies can regularly test their ability to perform fast ransomware-free recovery at scale of data across all systems. It is too late to discover that not all data has been backed up following an attack.

Encrypting sensitive data reduces the impact of a breach. The Australian Signals Directorate provides approved encryption algorithms for data classified as protected level and below.[30] Data encryption minimises the value of leaked data for adversaries without an encryption key.

Prioritise employee awareness and training

Repeated government audits point to agency difficulties in improving poor employee cyber hygiene.[31]

Therefore, employees need regular cyber resilience awareness training to understand the risks associated with shadow IT, unsecured networks, phishing/social engineering techniques, password practice, etc.

Training needs to be role-specific and informed by agency weaknesses. Agencies can perform penetration testing to identify vulnerabilities, which can then be featured in training programs.

Next steps

Step 1

Determine the extent to which your agency has implemented the ten proven practices.

1.	Establish well-defined roles and responsibilities
2.	Leverage the services of the WofG cyber security unit
3.	Establish a centralised view of risk across clouds and on-premises systems
4.	Deploy independently assessed solutions
5.	Apply zero-trust principles to identity and access management
6.	Adopt behavioural-based threat detection with AI and automation to detect and contain threat actors
7.	Automate information management to reduce data sprawl and safeguard the 'crown jewels'
8.	Detect threats through forensic analysis of data
9.	Minimise the impact of cyber-attacks with solutions enabling rapid ransomware-free data restoration at scale
10.	Prioritise role-specific employee cyber security awareness and training

Step 2

Consider implementing not-yet-instituted proven practices as per your agency's risk management framework. The following summary of the NIST *Risk Management Framework*[32] is a basic process agencies can implement for effective cyber resilience.

Implementing proven practices

Prepare	Categorise	Select	Implement	Assess	Authorise	Monitor
Identify agency roles, common controls, types of information stored in systems, risk tolerance, and risk management strategy.	Identify the 'crown jewels' and determine the business impact of a successful cyber-attack.	Choose appropriate controls based on agency characteristics and government policies and standards (e.g. Essential Eight).	Implement selected controls. Controls may be processes, procedures, products, services, etc.	Establish that the controls are correctly applied and effective.	Establish accountability by requiring an official to sign off that the risk is managed appropriately.	Continue to monitor that the risk is managed appropriately considering emerging threats, changing business processes etc.

Step 3

If your agency's current data management and cyber resilience practices do not align with the proven practices, consider procuring a solution that:

- Easily monitors and manages data stored in cloud and on-premises environments;
- Provides a consolidated user interface allowing for the implementation of controls, including automating the application of zero-trust controls to restrict and monitor system and data access;
- Has been assessed under the conditions of government risk assessment programs;
- Enables rapid ransomware-free data restoration;
- Automates information management to reduce data sprawl; and
- Pre-empts cyber-attacks and draws on AI and automation to identify and eliminate the risk presented by unexecuted malware.

The procurement process can evaluate the following:

Evaluation criteria	Sample evaluation questions
Fitness for purpose	Will the procurement... • Enable the implementation of proven practices? • Support compliance with WofG cyber security standards, controls, and guidance?
Alignment with broader government objectives	Will the procurement... • Support the WofG architecture (e.g. interoperability, cloud-first)? • Enable secure cross-agency or cross-jurisdictional information sharing? • Give greater confidence in data integrity allowing for data-led decision making? • Support fast, secure, and convenient access to digital services?
Total cost of ownership	What are the... • Total costs of acquisition, implementation, maintenance, support and transition off? • Possible costs of cyber-attacks if the procurement does not occur? • Expected cost savings to be realised in the agency (e.g. replacing point solutions, reduced manual workload)?
Risk	What are the... • Supplier risks (e.g. commercial, capability, supply chain)? • Procurement risks (e.g. probity, legal, financial)? • Risks of not progressing with the procurement (e.g. regulatory, reputational, commercial)?
Supplier capability	Does the supplier... • Participate in government risk management assessments? • Have proven expertise, experience, and capacity? • Conduct in lawful and ethical behaviour?

Agencies can enhance their cyber resilience with Commvault's solutions and more effectively predict, protect, and recover from cyber-attacks.

Commvault Cloud provides layered defence — minimising the impact of cyber-attacks with early warning and detection, while accelerating recovery with comprehensive threat scanning, remediation, intelligent quarantining, clean recovery validation, and unparalleled recovery speeds at the lowest TCO (total cost of ownership).

Learn more about public sector cyber resilience at: commvault.com/use-cases/public sector

References

1 US Government, accessed January 2024, **Nation-State Cyber Actors**

2 Australian Government, 2023, **2023-2030 Australian Cyber Security Strategy** [PDF]

3 Australian Government, 2024, **Notifiable data breaches report July to December 2023**

4 IDC, 2022, **High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises** [PDF]

5 ISC2, 2023, **ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce** [PDF]

6 Including on-premises, cloud and oftentimes legacy systems. See, for example, Victorian Government, accessed February 2024, **Risk scenario 2 – Legacy systems case study**

7 See, for example, Cameron Sinclair, Intermedium, November 2021, **Addressing NSW's cyber security failings – the state of play**

8 In the Australian Government, 55 per cent of employees work at least partially from home. See Australian Government, 2022, **State of the Service Report** [PDF]

9 Australian Government, **2023, 2023-2030 Australian Cyber Security Strategy** [PDF]

10 The Essential Eight are priority measures to protect against cyber threats. The eight measures are: Patch applications; Patch operating systems; Multi-factor authentication; Restrict administrative privileges; Application control; Restrict Microsoft Office macros; User application hardening; Regular backups. For more, see Australian Government, accessed February 2024, **Essential Eight Maturity Model**

11 Australian Government, accessed February 2024, **Information Security Manual (ISM)**

12 See, for example, Cameron Sinclair, Intermedium, 2024, **Victoria: Rising Debt Likely to Drive Down Digital Investment**

13 Australian Government, accessed February 2024, **Information Security Manual (ISM)**

14 Australian Government, accessed February 2024, **Information Security Manual (ISM)**

15 Intermedium, 2023, **Government Cyber Security Readiness Indicator 2022**

16 Australian Government, 2023, **Building trust in the public record**

17 Australian Government, 2022, **State of the Service Report 2021-22** [PDF]

18 Tech Target, accessed January 2024, **SOAR (security orchestration, automation and response)**

19 Australian Government, accessed February 2024, **Essential Eight Maturity Model**

20 Australian Government, accessed February 2024, **Essential Eight Maturity Model**

21 Australian Government, accessed February 2024, **Information Security Manual (ISM)**

22 Australian Government, 2023, **2023-2030 Australian Cyber Security Strategy** [PDF]

23 AWS, accessed February 2024, **Reaching Essential Eight maturity on AWS: AWS Prescriptive Guidance** [PDF]

24 Australian Government, accessed February 2024, **Cloud Computing Security for Tenants**

25 Victorian Government, 2023, **Cybersecurity: Cloud Computing Products**

26 Australian Government, accessed February 2024, **Federal Register of Legislation Privacy Act 1988**

27 Australian Government, 2023, **2023-2030 Australian Cyber Security Strategy** [PDF]

28 Jonathan Kearsley and Clair Weaver, 2022, Sydney Morning Herald, **Sensitive business addresses among 500,000 published in COVID data breach**

29 NSW Government, 2022, **Legislative Assembly Hansard – 17 February 2022**

30 Australian Government, accessed February 2024, **Guidelines for Cryptography**

31 See, for example, Cameron Sinclair, Intermedium, November 2021, **Addressing NSW's cyber security failings – the state of play**

32 US Government, accessed November 2023, **NIST Risk Management Framework**

About Intermedium

Intermedium researches the Australian and New Zealand public sector's use of information and communication technology and progress in digitising government services. Our independent and objective analysts utilise qualitative and quantitative data to analyse public sector trends in technology adoption, funding levels, and procurement. Almost 100 public and private sector clients utilise our syndicated content and online dashboards, consulting and research services.

Intermedium.com.au

About Commvault

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organisations to uncover, take action, and rapidly recover from cyber attacks – keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced AI-driven automation – at the lowest TCO.

www.commvault.com

Intermedium

Commvault®