Data Governance for Public Sector Cyber Resilience

Intermedium Solution Brief Sponsored by Commvault

Intermedium

Commvault®

Cyber-attacks and data breaches are the #1 agency risk[1]

Agencies strive for high-quality data collection to improve policy development and service delivery, but without effective governance, these data assets become liabilities by introducing security and privacy risks.

Agencies need cyber resilience solutions that operationalise data governance and help ensure business continuity in the face of rising threats.

Cyber resilience requires effective data governance

Definition of Data Governance

The system of legislation, policies, regulations, processes and accountabilities for managing data to meet business requirements.[2] It establishes how data must be managed during its lifecycle[3] to handle security risks.

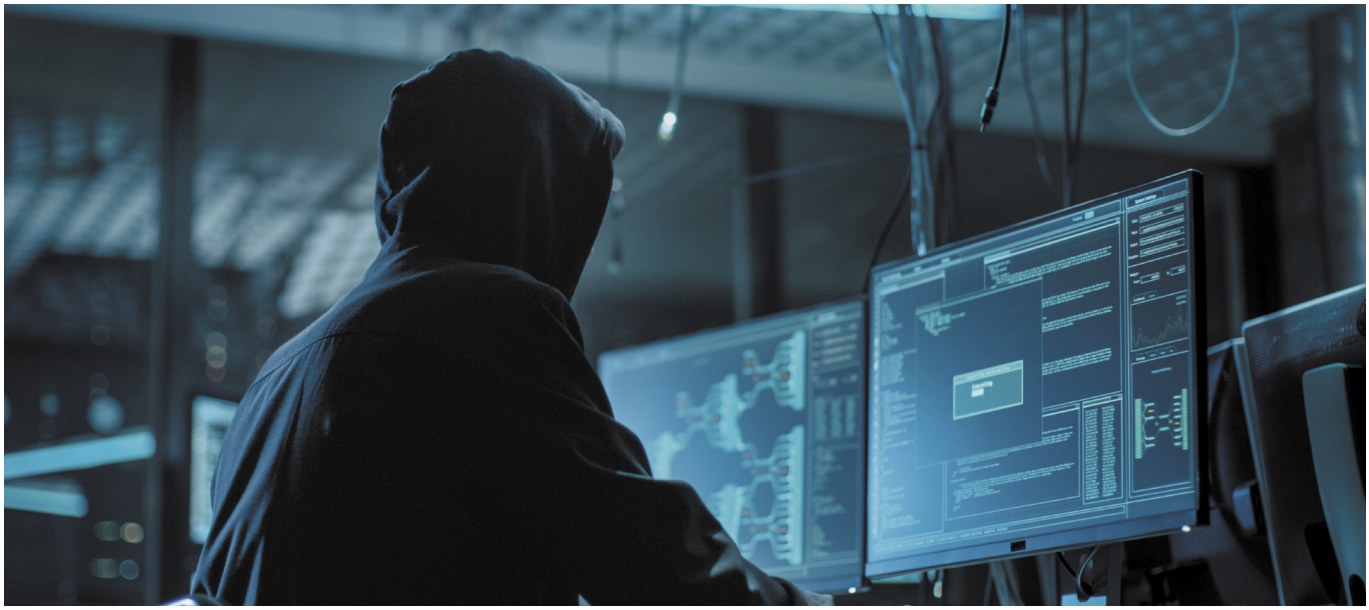
Effective data governance is vital for cyber resilience – i.e. the ability of an agency to continue to deliver its objectives regardless of cyber-attacks.

Compliance challenges

Australia's governments have developed frameworks for agencies to enhance data security, quality, integrity, discoverability, accessibility and useability.[4] However, complying with these obligations can be challenging for several reasons, including:

- **The existence of data silos and a lack of observability due to the operation of various on-premises and cloud systems**
- **The rising volume and variety of data to manage**[5]
- **Increasing frequency and sophistication of cyber-attacks**[6]

Cyber resilience solutions overcome these challenges and support agencies to operationalise their data governance requirements.



Operationalise data governance, develop cyber resilience

Moving data governance from legislation, policies, regulations and guides into operations is essential for building cyber resilience.

Risk, Readiness, Recovery = Resilience

- Identify and reduce unnecessary **risks**
- Establish **readiness** by instituting awareness and deploying controls, detection and response
- Support scalable **recovery** and **rebuilding**

Data governance guides each function.

'Data protection' alone is not enough to safeguard data integrity, privacy and accessibility.

Agencies must instead be clear on what is worth protecting and be 'recovery ready', as it is now a matter of 'when' not 'if' an adversary will breach agency defences.

19% **increase in data breach reports, January–June to July–December 2023**

Office of the Australian Information Commissioner [7]

This section draws from information security capabilities identified by the National Institute of Standards and Technology (NIST), Australian Cyber Security Centre's *Essential Strategies to Mitigate Cyber Security Incidents*[8] and *Information Security Manual*[9], and other materials used by Australian governments to describe how cyber resilience solutions enable agencies to operationalise data governance.

It is structured around NIST's Cybersecurity Framework's 'five functions' as it enhances the cyber resilience requirements of Australian jurisdictions.

Identify

Data governance establishes consistency and cooperation across agencies to help ensure that data is identified and protected with appropriate safeguards. The challenge for agencies is that historical practices often mean that data is spread across various legacy and contemporary technologies, on-premises and in the cloud.

Furthermore, agencies sometimes inherit data that nobody knows what to do with – what it is, why it was collected, or if it is even needed. This 'Dark Data' requires someone (or a digital tool) to 'shine a light' over it to identify any sensitive or Personally Identifiable Information (PII) data[10] before deciding whether it should be retained, sent to archive, or deleted.

How data discovery tools can support agencies

- Define the characteristics of sensitive and PII data
- Support sensitive and PII data identification using keyword proximity checks and Optical Character Recognition (OCR), including in live and backup data silos
- Identify suspicious or anomalous data

Identifying data is essential for compliance with jurisdictional security policies that require data and system inventories. Once agencies are aware of their data assets, they can institute risk-appropriate protections as described in the next section.

Case Study:
Location data leak risks citizens' safety

Establishing a comprehensive view of data not only reduces the risk of a damaging cyber-attack but can support agencies mitigate the risk of a data breach caused by human error.

The NSW Government made a major data release error when the addresses of more than 500,000 organisations were published on a website, including the locations of domestic violence shelters, defence sites, and even a missile maintenance unit.[11] The information was collected by the state's COVID-Safe QR code check-in app, but the data was not appropriately screened for sensitive information before it was published.

"The Department of Customer Service published in error addresses of businesses that were of a sensitive nature."

NSW Privacy Commissioner[12]

Domestic violence advocates expressed shock, noting that identifying the location of shelters could have serious consequences. Privacy advocates emphasised that failure to screen the locations would undermine public support for the check-in system.

While the NSW Department of Customer Service acknowledged the error and provided a briefing to the Privacy Commissioner, who was satisfied "with the actions taken to contain, respond to and remediate the incident"[13], it evidences how inadequate data governance processes can risk serious consequences for citizens.

Protect

Agencies implement strategies to protect data according to their data governance requirements. The following Essential Eight strategies are a foundational requirement of Australia's governments' (federal, state, territory, and local) approach.

1 Application control

Blocking unapproved applications to prevent unauthorised executions that put data at risk. Cyber resilience solutions can automate discovery to identify unapproved applications and trigger options for remediation processes.

2 Patch applications

Automated discovery of missing patches, testing and patch deployment.

3 Configure Microsoft Office macro settings

Blocking internet-sourced macros and stopping users trying to access non-vetted macros.

4 User application hardening

Removing risky components from common applications.

5 Restrict administrative privileges

Data governance establishes the rules for who can and cannot access systems and data, to help ensure that data is not tampered with, misplaced, stolen, released, altered or deleted.

Cyber resilience solutions should support the 'zero trust' security approach. In this approach, the only users permitted access to data and systems, including administration privileges, are those who can confirm they require access as part of their job requirement. This is called the 'principle of least privilege'.

6 Patch operating systems

Automated asset discovery identifying missing patches or updates for security vulnerabilities.

7 Multi-factor authentication (MFA)

Requires users to provide two or more verification factors before accessing data. Cyber resilience solutions should support MFA.

8 Regular backups

Backups are vital for establishing 'recovery readiness' to reduce the agency impact of a cyber incident.

Cyber resilience solutions allow authorised personnel to administer and monitor backups in the cloud to help ensure that data is backed up from across data silos.

Solutions must support a consistent backup and testing schedule and automated containment of anomalous behaviour. Sensitive data may require 'air gapping', where data is physically isolated from unsecured networks.

Detect

Agency executives realise that incursions can still occur regardless of protection efforts, and as such, place great emphasis on effective detection, response and recovery.

Solutions should provide real-time monitoring and early warnings to identify and neutralise threats.

This is done by scanning files across agency data environments (live and backups) looking for evidence of compromise. Evidence of possible compromise includes new, renamed, modified, corrupted, or encrypted files. Leading solutions use artificial intelligence to support this process.

Good data governance is essential because by ensuring that data is accurate, consistent, and accessible, agencies can better identify data for anomalies and potential threats, and determine who is responsible for the data and needs to be alerted of possible compromise.

Respond

Data governance determines the sensitivity of data held across the agency and therefore the incident response.

A breach of sensitive data, such as that containing PII, will require a different response compared to data that does not have a security classification. Australian jurisdictions differ in their classifications but tend to use variations on official/sensitive, protected, secret and top secret.

Cyber resilience solutions must enable decision-making between information technology, security and data owners during a cyber incident.

The response may include automated deleting, moving, or quarantining data that may have been compromised.

"Enabling automation is a critical component of every organization that wishes to address the speed and scale of modern cyber attack."

US Government Cybersecurity and Infrastructure Security Agency[14]

Cyber incidents affecting sensitive data may need specific compliance and reporting. For example, Australia's Notifiable Data Breach (NDB) Scheme requires entities (including agencies) to report breaches that are "likely to result in serious harm to any of the individuals to whom the information relates". [15]

Recover

Recovering from a cyber incident can take considerable time.[16] However, agencies that have instituted readiness measures like regular backups, establishing inventories, periodic test procedures, communication planning and training are well-placed to help ensure rapid recovery and minimal business impact.

Critical for recovery is analysing live and backed-up data to find safe recovery points before the compromise, so agencies can restore data and maintain business operations.[17]

Agencies can opt for backup tools that allow for regular testing of ransomware-free recovery, as it is too late to discover the agency has not effectively backed up data after the incursion.

Take the next step

Learn more about achieving cyber resilience in the face of advanced cyber threats.
Visit: commvault.com/use-cases/ransomware-and-cyber-defense

References

[1] AON, accessed June 2024, *Top Risks Facing Public Sector Organizations*

[2] NSW Government, accessed June 2024, *Data Policy*

[3] The Data Management Life Cycle includes: Creation, capture or collection; Organisation or storage; Use and analysis; Sharing; Reuse or maintenance; Archiving or destruction

[4] **The following table provides examples from Australian jurisdictions:**

Legislation	***Queensland Information Privacy Act 2009*** Governs agencies' management of personal information. Includes Information Privacy Principles for collection, storage, security and access.
Policies	***ACT Government Data Governance and Management Policy Framework*** Contains steps for improving data maturity, including that directorates develop an incident response plan.
Regulations	***Victorian Protective Data Security Standards*** Include the mandatory standard that agencies establish, implement and maintain an information security management framework relevant to its size, resources and risk.
Process Guides	***Australian Government Information Security Manual*** Directs agencies on protections for technology, applications and data, drawing from National Institute of Standards and Technology (NIST) materials.
Accountabilities	***NSW Government's Data Governance Toolkit*** Outlines responsibilities for Accountable Executives, Responsible Executives, Operational Data Managers, Data Creators, and Data Users.

[5] Dell Technologies, accessed June 2024, *Computational Storage in the Data Decade*

[6] Australian Government, 2024, *Notifiable data breaches report July to December 2023*

[7] Australian Government, 2024, *Notifiable data breaches report July to December 2023*

[8] Australian Government, accessed June 2024, *Strategies to Mitigate Cyber Security Incidents*

[9] Australian Government, 2024, *Information Security Manual* [PDF]

[10] Section 6 of the Australian Privacy Act 1988 includes a list defining forms of sensitive data, including information on an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record, health, credit, employee status, and Tax File Number.

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

[12] NSW Government, 2022, *Privacy Commissioner Statement on COVID-Safe business registration venues data set*

[13] NSW Government, 2022, *Privacy Commissioner Statement on COVID-Safe business registration venues data set*

[14] US Government, accessed June 2024, *State, Local, Tribal & Territorial Cyber Information Sharing Program*

[15] Australian Government, accessed June 2024, *Notifiable Data Breach (NDB) Scheme*

[16] US Government, 2024, *NIST Special Publication 800 Incident Response Recommendations and Considerations for Cybersecurity Risk Management* [PDF]

[17] US Government, 2016, *NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery* [PDF]

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®