The Records Side of Cyber Security

BY XANDER HUNTER ARIM

Aligning records management and cyber security strategies improves their impact and reach across the organisation. Cyber security specialists understand how to protect systems and networks from potential threats, and the actions which need to be taken should a cyber-attack occur.

Records management specialists understand the records the systems contain, including their risk, value, why they are being captured and kept, and how long they need to be retained.

Exploring how the two professional disciplines of cyber security and records management complement each other provides a road map for discussion and increased engagement. This in turn improves practices, strengthens desired outcomes, and maximises use of available resources.

Measures taken as part of cyber security programs are related to the confidentiality, integrity, and availability of records, information, and data (hereafter referred to as records). These measures protect the records and associated systems from external or internal threat. Records are at the centre of cyber-attacks, regardless of whether the attack seeks to steal records, or target an organisation's infrastructure. Without records, the business of an organisation comes to a standstill. The organisation has no memory, cannot justify past actions or decisions made, and is severely limited in the business it can conduct.

INFORMATION SECURITY MANUAL ALIGNMENT

Preservation of confidentiality, integrity and availability of records aligns with cyber security in business continuity and/or disaster recovery plans. Records and cyber security programs need an understanding of the same space to do their work effectively, even though their area of focus and skill sets differ. It should come as no surprise then that recordkeeping practices align well with the four sets of principles under a key cyber security framework, the Information Security Manual (Australian Signals Directorate March 2024; hereafter referred to as ISM).

Some recordkeeping practices relate to having structures and processes in place that will aid a cyber security investigation, some diminish risk, some document the space to aid understanding, and some provide the means to commence recovery. For example, the set of principles under 'Govern' relate to identifying and managing security risk, and may include recordkeeping practices such as:

- Identifying and documenting high-value high-risk records.
- Knowing and applying Retention and Disposal Authority coverage across all systems.
- Identifying risk to records and planning mitigation strategies.
- Developing and applying longevity and preservation strategies as needed.
- Documenting systems, technologies, and applications (including artificial intelligence (AI) technologies) and their integration.

Preservation of confidentiality, integrity and availability of records aligns with cyber security in business continuity and/or disaster recovery plans.

The set of principles under 'Protect' relate to implementing controls to reduce security risks, and may include recordkeeping practices such as:

- Recordkeeping by design and across the lifecycle of both systems and records.
- Systems functionality and control configurations matching recordkeeping requirements.
- Using archival systems rather than backups for archiving records or offline storage options.
- Managing evidential integrity – (for example, through implementing a digital preservation scheme, such as the Victorian Electronic Records Strategy or VERS).
- Addressing ongoing business and stakeholder recordkeeping needs through relevant and current business continuity and disaster recovery plans.
- Implementing disposal programs in a timely fashion.

The set of principles under 'Detect' relate to detecting and understanding cyber security events to identify cyber security incidents. They may include recordkeeping practices such as:

- Developing and implementing relevant metadata schemes
- Documenting systems, technologies, and applications (including AI technologies) and their integration.

The set of principles under 'Respond' relate to responding to and recovering from cyber security incidents. They may include recordkeeping practices such as:

- Implementing disaster recovery plans for records.
- Implementing preservation strategies for records.
- Locating and recovering high-value high-risk records.

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Relating recordkeeping practices to confidentiality, integrity and availability provides us with a different perspective of where the two areas of professional discipline overlap.

Confidentiality of records relates to what the records are, why they are being captured and kept (including associated legislative and regulatory contexts), who they have value for and why, and the consequences of unauthorised people having access to them. Confidential records and the systems they are located in are likely to be flagged as high risk when documenting the value and risk of records.

Cyber security specialists armed with this information will be able to determine areas of vulnerability so that suitable protections can be put in place. This fits within the 'Govern' and 'Protect' sets of principles as specified in the ISM.

Integrity of records relates to their value as evidence and includes factors that can be used to demonstrate a record is what it purports to be. For example, metadata, audit trails, lineage mapping, formats, classification schemes, process mapping, and relation to other records; all of which

provide a record with meaning and context. Controls, such as levels of authorisation, audit trails, check-sum algorithms and other technical mechanisms can provide an indication that a record has been tampered with.

Cyber security specialists may use this information to determine and minimise the impact of a cyber-attack, and to put in places measures to prevent tampering. This fits within the 'Govern' and 'Protect' sets of principles as specified in the ISM. It is also required to achieve the 'Detect' set of principles.

Availability of records relates to whether records can be identified, located, retrieved, accessed, and used. It also relates to how long records are kept and their disposal sentence. Access policies for records need to balance being open and accessible so those who need it can locate, read, and use it, as well as being kept secure so those unauthorised to view or use it cannot do so. Locking down all records can result in people saving records outside of the systems, thereby placing the records at greater risk.

Cyber security specialists will need to understand how people access and use records in order to have protective measures in place and to plan for successful recovery from a cyber-attack. Different working environments, technologies, software, and business management systems will have different points of vulnerability and recovery. This fits within the 'Govern' and 'Protect' sets of principles as specified in the ISM. They also inform strategies needed to 'Respond'.

STORAGE LOCATION AND DISPOSAL PRACTICES

The location of records may differ, depending on whether they are required for ongoing business operations, needed for more specialised occasions, or not needed at all. Some records will be on current systems, which may or may not be interconnected with other systems or cloud storage. Some may be held in nearline or offline systems, or physical storage vaults. Some may have been exported and held in separate archives facilities, such as a State Archive.

Cyber security specialists will have different prevention and recovery methods for different kinds of storage locations and situations. Integrated and online storage can be more at risk than nearline or offline storage.

For example, transferring permanent value and long-term temporary records to a separate archive can minimise security risks, improve preservation risks, as well as reduce overheads. This fits within the 'Protect' set of principles as specified in the ISM.

Some records will have been destroyed in line with authorised and lawful disposal practices. An effective disposal program prevents records from being kept unnecessarily, meaning they are not at risk during cyber security incidents. This is important when personal or sensitive information is held. For example, some records may contain credit card numbers or personal identifiers. Disposing of this information in a timely fashion in accordance with a relevant disposal instrument (such as PROS 22/07 Retention and Disposal Authority for Records of the Identity Verification Function) ensures that the information is less likely to exist in order to be compromised.

Cyber security specialists value timely and relevant disposal actions for time-expired records, as it means they are not in systems to be stolen or compromised during a successful attack. This fits within the 'Govern' and 'Protect' principles specified in the ISM.

LONGEVITY, PRESERVATION, AND BUSINESS CONTINUITY

Business continuity and/or disaster recovery plans will include records and are likely to be based around longevity and preservation strategies. Cyber security programs will also form part of or align with business continuity and disaster recovery plans. All the ISM principles will relate in some way to business continuity and/or disaster recovery.

Longevity and preservation strategies ensure records are captured in a long-term sustainable format, that threats to the record (such as loss of the record) can be prepared for, and that systems have sufficient functionality to manage records. For example, maintaining relationships between records and their relevant contextual metadata in a manner that enables them to be migrated from one system to another. A successful cyber-attack would be one of the risk scenarios considered (along with other threats to the record) so that preservation and recovery can be planned for.

Longevity strategies focus on ensuring the record is robust from the outset. That records will remain readable, accessible, useable, and locatable from the point of their creation and capture throughout the duration of their retention periods.

Longevity strategies may focus on factors such as:

- What long-term sustainable formats are used and why?
- How to ensure that the software and hardware required to keep, manage, open, access, read and understand the record are maintained for the duration of the records' retention periods.
- Choosing storage options that don't diminish the longevity of records.

Preservation strategies often include longevity and focus on the identification and mitigation of risks to the records across their lifespan.

Business continuity plans should include longevity and preservation strategies, along with information about high-value high-risk records.

Preservation strategies may include:

- Migration strategies to enable records to be moved from one system to another, complete with their context, while remaining accessible and useable.
- Ongoing management of decommissioned and offline systems so that the records on them are not lost to degradation and remain accessible and useable.
- The limitations, structures, and other aspects of technologies used (hardware and software) that impact on being able to identify, locate, retrieve, access, open, read, understand, and use records.

Business continuity plans are strategies, plans, and processes, to enable ongoing business in times of disaster or disruption (including cyber-attacks). Business continuity plans should include longevity and preservation strategies, along with information about high-value high-risk records and what is needed in relation to them should disaster or disruption occur.

Preservation strategies and business continuity or disaster recovery plans should include:

- Where high-value high-risk records are located.
- How records may be recovered or restored under different disaster situations including cyber-attack.
- Whether there is sufficient provision for the recovery of records in budgets and resources.
- References to what records might be accessible and how they may be best obtained if the systems and infrastructure were suddenly unavailable (possibly due to cyber-attack, power outages, or internet being down). For example, what records are available offline and how are they accessed?
- A requirement to ensure that high-value high-risk records are created and maintained in long term sustainable formats where possible, and that they are part of actively managed digital preservation strategies.
- Transfer of permanent and long term temporary high value high risk records to a separate archive (such as a State Archive, for government records).

Reliance on backups to enable business to continue is not always possible. The backups held may also be compromised, and it may be difficult to detect or confirm that they have been compromised. Whether the backups are in the cloud or on tape may not make a difference if they contain undetected ransomware, or other malware.

CONCLUSION

Understanding where and how cyber security and records management overlap provides the common ground needed to build relationships, strengthen practices, and ensure that both areas are represented in relevant projects.

Cyber security programs can help maintain evidential integrity of records, while recordkeeping programs can enable cyber security efforts to focus on areas of high-value and high-risk. Recordkeeping and cyber security programs align well with each other and provide mutual support, especially regarding business continuity and disaster recovery. Perhaps this is why in Victoria we are seeing an increase in cyber security and recordkeeping specialists being part of the same work team.

References

- Cyber Security Topic Page (Public Record Office Victoria January 2024; https://prov.vic.gov.au/recordkeeping-government/a-z-topics/cybersecurity)
- Information Security Manual (Australian Signals Directorate March 2024; https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism)
- PROS 22/07 RDA for Identity Verification Function; https://prov.vic.gov.au/recordkeeping-government/document-library/pros-2207-identity-verification-function
- Victorian Electronic Records Strategy; https://prov.vic.gov.au/recordkeeping-government/vers

ABOUT THE AUTHOR

Xander Hunter, Standards and Policy, Public Record Office Victoria. Xander Hunter has worked in the records and information management profession for more than 20 years. Xander uses a multi-disciplined approach to developing policy and guidance across the Victorian public sector in their role as A/Manager, Standards and Policy at Public Record Office Victoria. Xander has a master's degree of Information Management and Systems from Monash University with streams in Knowledge Management and Records and Information Management. Xander is also a member of the Australian Anthropological Society with a BA Hons from La Trobe University majoring in Anthropology.