Are We Missing the Cybersecurity Factors in Recordkeeping?

Fariha Tasmin Jaigirdar[1(✉)], Ozhan Saglik[2], Carsten Rudolph[1], and Joanne Evans[1]

[1] Monash University, Melbourne, Australia
{fariha.jaigirdar,carsten.rudolph,joanne.evans}@monash.edu
[2] Bursa Uludag University, Bursa, Turkey
ozhan.saglik@uludag.edu.tr

Abstract. When creating, storing, and maintaining sensitive records, such as government data or records that reflect citizen rights or represent their health data, those records need to be trustworthy and secure. Since organizations are creating huge digital records, security in recordkeeping grows in complexity, and the relationship between the cybersecurity and recordkeeping domains is also expanding. While integrity and appraisal of records have always been considered important for records, existing standards and security discussions are missing some essential perspectives. Thus, research is needed to understand cybersecurity factors (different cybersecurity standards, techniques, protocols, etc.) for recordkeeping and the potential consequences of ignoring factors. With this goal, we explore two core standards, International Organization for Standardization ISO 15489 and ISO 27001, and selected relevant recent literature. This study makes a case for a universal standard for these cross-domain aspects of recordkeeping and cybersecurity by considering the existing standards and identifying the missing cybersecurity factors in recordkeeping. It also discusses relevant challenges and future research directions.

Keywords: Cybersecurity · Recordkeeping · Archives

1 Introduction

Security has always been considered important for records and archives. Researchers discuss confirming audit processes [29], information governance, policies and safety rules [4,11] approach achieving cybersecurity by imposing different standards [5] and suggest blockchain-based trusted systems [7,8]. Despite these various approaches, reports show different cybersecurity vulnerabilities and threats in record management [1], which urges the need for further study between these different domains [2].

I. Sserwanga et al. (Eds.): iConference 2023, LNCS 13971, pp. 3–13, 2023.
https://doi.org/10.1007/978-3-031-28035-1_1

Records have characteristic features like integrity, authenticity, reliability, and usability that are required for records to be regarded as trustworthy. Integrity is mainly related to the preservation of the records, meaning they are unaltered and not subject to unauthorized modifications. Authenticity is more focused on the records' provenance, i.e., that the record has been created from an authentic source, by an authentic person, or another authentic entity. The suitability of a person in the record to have the authenticity to sign the record and make transactions and relevant activities combined with trusting the systems involved, can be used to explain reliability [31]. A usable record is one that can be located, retrieved, presented, and interpreted by connecting it to the business process [13].

Records management can be defined as the efficient and systematic control of records [13]. It includes the processes for records to be the representatives of transactions so that records have an evidential and informational value [32]. Malicious activities can potentially threaten all phases of record management. Cybersecurity has the techniques and methods for preserving the integrity, authenticity, and usability of the records [14]. Although cybersecurity mechanisms analyze how the qualities of the data can be protected and offer solutions, it is argued that there is not enough attention [2,12] to maintain the security of complete digital record lifespan from creation to appraisal. Therefore, it is anticipated that cybersecurity approaches can be applied to create and maintain reliable records.

Interestingly, recent discussions on trusted recordkeeping mostly cover the area of blockchain and how blockchain technology can be used as a method for trusted repositories. It is particularly focused on *preserving* records and maintaining authenticity rather than protecting the complete process. It seems that large parts of recordkeeping and record management processes are not covered in the current discussion, and in particular, the relevance of cybersecurity for record authenticity is underrepresented. While blockchain technology can potentially support secure record management after the record has been created and added to the chain, we focus on investigating cybersecurity for the complete data chain leading to the creation and potential future adaption of the record. To explore this area and identify further research opportunities, in this paper, we address the following research question.

– **Research Question (RQ)**: Does the current approach to cybersecurity in recordkeeping consider all relevant factors?

This paper aims to demonstrate what we currently have in recordkeeping in terms of cybersecurity and to identify missing cybersecurity factors in the complete lifespan of record creation to record adoption. Additionally, it poses new research questions that both subject-matter specialists need to address.

2 Research Approach

To address the research question, we follow a two-way approach. First, identifying and analyzing the related standards, and second, investigating closely related literature in these two domains. The authors of this paper are well-balanced experts in these domains: two of them are cybersecurity experts, one is a recordkeeping expert, and the other one is a scholar in these two interdisciplinary areas.

This paper analyses standards and draws from recent academic research. For the first one, standards that are core have been selected: ISO 15489 [13] for recordkeeping and ISO 27001 [14] for cybersecurity. This study can potentially be extended in the future through covering other standards for recordkeeping such as ISO 22428 [23], 18829 [18], 15801 [16], 14641 [20], and 17068 [17] and cybersecurity such as ISO 27002 [24], 27003 [19], 27005 [21], 27035 [15], and 27050-1 [22]. However, none of these standards is focused on cybersecurity and recordkeeping. Therefore, for this first step in the research we analyse the core requirements provided in the two core standards. For the second segment, we search for closely relevant literature exclusively in this two domains by specific keywords: "cybersecurity AND recordkeeping (records management)" and "cybersecurity AND archives". From our search results, we explored news articles, research reports/articles, investigation reports, conceptual papers and identified the key approaches/ideas used, whether there were any comments for future research/challenges. Further, we discussed the suitability of the articles among the authors and identified ten articles from 2016 to 2022 that were closely related to the research scope.

3 Findings on Correlated Areas: Cybersecurity and Recordkeeping

Since organizations are adopting more and more digitized processes, they need to have a 'reliable' and 'trustworthy' recordkeeping system to demonstrate the records are produced following their business processes and are authentic. Thus, cybersecurity techniques and approaches are obvious for the success of reliable recordkeeping. In this section, we first discuss two core standards in two domains and then illustrate ten relevant articles. We discuss our findings that show the connections between these domains, pertinent challenges, and potential future research directions.

3.1 Core Standards for Recordkeeping and Information Cybersecurity

There are various ISO standards for cybersecurity and recordkeeping like 27002 [24], 18829 [18], 27035 [15] and 14641 [20]. However, given that the underlying concepts of these standards are applicable to cybersecurity and recordkeeping,

and taking into account the size of the study, we concentrate on two fundamental criteria: "ISO 15489: Records Management" and "ISO 27001: Information Security Management Systems". To explain their acceptability, "ISO 15489 establishes the core concepts and principles for the creation, capture, and management of records. It sits at the heart of a number of International Standards and Technical Reports that provide further guidance and instruction on the concepts, techniques, and practices for creating, capturing and managing records" [13]. For ISO 27001, "this standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system" [14].

While records management is about current records, archiving examines the non-current records. However, the qualifications of the records that will be archival material are determined in the process of records management. Principles regarding records management also apply to archiving. Thus, there is no self-contained standard for archive management as a part of ISO 15489. Since the cybersecurity process naturally does not distinguish between current and non-current records, records management and archiving are interpreted together in this study which examines the relationship between cybersecurity and record-keeping.

ISO 15489 defines records management as the "field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records" [13]. Therefore "records should possess the characteristics of authenticity, reliability, integrity, and usability to be considered authoritative evidence of business events or transactions" [13]. It is understood that authenticity, reliability, integrity, and usability are the key requirements of the records.

A similar approach has been seen in the ISO 27001 Information Security Management Systems. According to the standard, "the information security management system preserves the confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed" [14]. Therefore, it can be said that ISO 27001 and ISO 15489 cover overlapping security requirements for data but have a different focuses. We further analyze these two standards with ten common requirements: policy and procedures, integrity, authenticity, reliability, usability, classification, access control, security, documentation, and disposition. We cite the quotes in the standards, ISO 15489 and 27001, then discuss challenges or/and directions for future research in Table 1.

Table 1. Overlapping of ISO 15489 and ISO 27001 with comments

Require ments	ISO 15489	ISO 27001	Comments for future research/challenges
Policy and procedures	Policies on the management of records should be developed, documented, and implemented	Information security incidents shall be responded to in accordance with the documented procedures	Do the records management policies/procedures of organizations include documenting cybersecurity incidents?
Integrity	A record that has integrity is complete and unaltered	Records shall be protected from loss, destruction, falsification, unauthorized access, and release, following legislation, regulatory, contractual, and business requirements	Integrity is a rather weak requirement. ISO 27001 is more precise and requires protection from falsification. Semantic integrity and tamper evidence is needed to check if the context is preserved, which is not satisfied by using integrity measures, such as hash values and checksums
Authenti city	Records creators should be authorized and identified	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained	Standards state what should be done, but practitioners need how they should be carried out. Therefore the question of the organizations has a framework or concept about authenticity comes to mind
Relia bility	A reliable record is one whose contents can be trusted as a full and accurate representation of the activities	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed	Do the current logs enough to assess the reliability of the records? What additional cybersecurity factors would be helpful?
Usability	A usable record should be connected to the business process or transaction that produced it	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization	How are the records linked to the business processes to document cybersecurity requirements?
Classification	Development of business classification schemes that are applicable to records should be based on an analysis of functions, activities and work processes	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization	Do organizations identify cybersecurity risks and interrelate them to the business functions? How?
Access control	Access to records should be managed using authorized processes	An access control policy shall be established, documented and reviewed based on business and information security requirements	Do organisations' access control processes include cybersecurity requirements? If yes, are secure processes implemented and are events logged? What additional factors would be helpful?
Security	The measures should be put in place to ensure the following: routine protection and monitoring of physical and information security	Large segments of ISO 27001 are relevant for this requirement	Which security measures for digital records need to be applied to satisfy the ISO 15489 requirement? What is there and what is missing?
Documentation	Records requirements and decisions on how to fulfill them should be documented	Operating procedures shall be documented and made available to all users who need them	Can the requirements of ISO 27001 be adopted for the documentation of the complete lifespan of digital records?
Disposition	Disposition processes should be carried out in conformance with rules in authorized and current disposition authorities	Media shall be disposed of securely when no longer required, using formal procedures	How is the disposition of the digital records carried out by adopting cybersecurity requirements? Do the organizations fulfill General Data Protection Rules (GDPR) requirements?

The review of ISO 15489 and ISO 27001 shows how closely cybersecurity and recordkeeping are intertwined with each other. Organizations that want good records management should base their systems on good cybersecurity techniques. The guidelines for using these techniques need to be part of record management tenets. Otherwise, if the records management principles do not adopt cybersecurity for the provenance, appraisal, storage and maintenance of records, there is a substantial risk that the core requirements for recordkeeping cannot be achieved.

Considering all of these, we note several challenges. For example, various cybersecurity factors are missing for recordkeeping while describing policy and procedures, integrity, reliability, and access control policies in Table 1. Other open questions include whether organizations include cybersecurity techniques (different cybersecurity factors) in their records management policy, or are records management principles based on their cybersecurity procedures? What is missing in logs and audit trails from the cybersecurity and recordkeeping perspective? Do organizations assess the risks related to records by applying cybersecurity viewpoints? These aspects should support future research directions on cybersecurity and reliable records management systems.

3.2 Recordkeeping And/or Archival Studies and Cybersecurity

In this section, we discuss selected relevant literature to illustrate scholarly knowledge/understanding of the relation between cybersecurity and recordkeeping. Table 2 illustrates ten relevant research publications in this context along with key approaches used in these articles and comments for future research.

Table 2. Relevant literature in recordkeeping and cybersecurity with comments

Research area/content	Key approach/ideas	Comments for future research/challenges
Risk in trustworthy digital repository certification [10]	Discussion on risks involved in digital preservation from the social phenomenon, which authors organized into five categories: financial, legal, organizational governance, repository processes, and technical infrastructure	Future research should focus on the cybersecurity perspectives of the risks involved to handle real-life digital record vulnerabilities
Compliance with the NSW cyber security policy (CSP) [2]	Discussion on why CSP is not achieving the objectives of improved cyber governance controls and cultures	Recommendation on prioritizing improvements to cybersecurity resilience as a matter of urgency. The next challenges to be considered are: a) How to work on cybersecurity resilience? b) What should be the next step to include resilience in the record life span?

(*continued*)

Table 2. (*continued*)

Research area/content	Key approach/ideas	Comments for future research/challenges
Professional and ethical balance in digital record management [12]	Discussion on maintaining and promoting professional and ethical balance in the records management system and provide a theoretical framework	Further research strives to include cybersecurity factors with ethical discussion
Attacks in record handling in service NSW [1]	Discussion on phishing emails targeting service NSW employees from a spoofed domain. Call for multi-factor authentication to be added on email	Future research needs to add cybersecurity factors (for example, information on service providers, software version details, and protocol used)
Evaluation of email records management and cybersecurity issues [6]	Discussion on how archivists, record managers, and cyber security experts issued impossible-to-follow guidance for electronic records and emails	Motivation for further research in designing acceptable guidance for cross-domains
A meta-model for recordkeeping metadata [30]	Discussion on possibilities for participatory recordkeeping that embraces multiple participants, a diversity of perspectives, and inclusiveness of engagement. Access control is discussed in the paper with authentication, authorization, reproduction rights management, tracing, and audit	Further investigation is needed to explore the issues of trust and the role of authoritative sources in a semantic network. For example, how should end-users locate, identify and evaluate the veracity of sources of recordkeeping documentation?
Integrity in nation's records [26]	Discussion what integrity means for records and why it is important to maintain integrity	Further discussion is needed for born-digital and digitized records to maintain integrity.
Trust in digital record [9]	Discussion on the importance of transparency to achieve trust in records. Transparency, accountability, accessibility, choice, integrity, and preservation are discussed as issues that are critical to trust of online records	Cybersecurity in the cloud received little debate. But the cloud just tells a portion of the tale; what about a data record's entire lifespan?
Trust in records [27]	Discussion on trusted digital recordkeeping (focusing on long-term management and preservation of trusted digital records). Implications of relying on blockchain technology for the long-term management and preservation of trusted digital records	Discussion on several limitations and challenges in implying blockchain for record preservation. What can be done regarding authenticity, reliability, and risks in digital records? could be a future research focus
Contents of born-digital records [3]	Born digital records pose many challenges for government departments, including high volumes of records and a lack of structure. There are broader information management and security concerns for born-digital record collections.	Further research strives to design an acceptable model for cross-domains

While the literature clearly identifies a number of challenges, the analysis shown in Table 2 identifies several additional questions: For trusted records, is the overall lifespan of a record considered? Who needs to check whether the source of the record is secured? Do we have any list of cybersecurity requirements/factors that need to be checked for resilience? What are the missing cybersecurity factors? Who needs to check whether record processing steps are secured and how?

4 Discussion and Conclusion

This study explores evidence that shows the current understanding of cybersecurity factors in recordkeeping. The prominence of digital archives and record management increases the urgency of establishing trustworthy systems not only for archives or storage, but across the complete record management systems and including documenting security of the systems that generate data for record appraisal. One main problem is that cyber attacks can be stealthy, and any traces of the attack can be removed after records have been manipulated. Thus, data can potentially be corrupted, deleted, or additional data added via an attacked system without creating any evidence of the change. Furthermore, even strong security mechanisms, such as digital signatures, can be exploited to create a false sense of security if a malicious actor gets access to the private keys used to digitally sign. As a result, for reliable recordkeeping, cybersecurity measures and documenting cybersecurity-relevant aspects are essential.

This study makes the case for a universal standard for these cross-domain aspects of recordkeeping and cybersecurity by considering the existing standards and identifying the missing cybersecurity factors in recordkeeping. ISO 15489 and ISO 27001 are created by different technical committees. 27001 belongs to the committee of "Information security, cybersecurity and privacy protection", and 15489 is owned by the "Archives/records management" committee. Even though it is usual that standards take different approaches to trustworthiness, when discussing digital records, requirements for cybersecurity are similar to requirements identified in generic cybersecurity standards. These include authenticity, reliability, access control, and disposition. Therefore, it is important to consider cybersecurity and digital records management together. In this study, missing cybersecurity factors in recordkeeping are demonstrated. However, the inverse is needed to be researched as well. In particular, the question of recordkeeping principles are ignored in cybersecurity processes.

While existing standards provide generic guidance for metadata of records to show that actions taken on records are properly defined and managed, the metadata may not include cybersecurity factors like risk assessment, event history, or access trails which provides information on the risk of attacks to the systems involved or the communication links used to transfer data. Current provenance mechanisms in archival science and records management collect data history that provides evidence of the creator's and project data lineage by indicating the entities, activities (workflows), and users involved in producing data and data flows. This provenance information should be extended to enable users to achieve better situational awareness and to empower them to adequate risk assessment.

The trustworthiness of digital records and repositories in existing standards is not sufficient to derive information on records' cybersecurity properties across the complete lifespan. It is essential to associate cybersecurity techniques with organisational policies and procedures, information governance approaches, records metadata, and archival legislation for securing trustworthy records. Besides, records are composed of various data. This data should come

from a trusted source and should not been changed or manipulated between data processing and aggregation. Data provenance, for example, following the PROV standard by the W3C [28] defines what kind of information needs to be collected in a data flow to describe who is responsible for data creation or related activities and when. Also the effects to modern concepts of recordkeeping, for example following the records continuum perspectives [30], need to be investigated. Cybersecurity metadata is not part of existing standards, and fundamental cybersecurity issues remain to be resolved.

This study also discusses opportunities for future research by incorporating cybersecurity factors as security evidence in digital recordkeeping. Recent research [25] has shown that extending provenance by cybersecurity metadata can provide substantial insight into the risks of manipulations. Identifying potential sources of corruption, misuse, or manipulation of data and consequences of mined, mapped, compiled, implied or inferred records will become an essential task for record management systems to achieve high resilience against cybersecurity attacks. A transparent system with an indication of the risks involved also provides an opportunity for better decision-making. This is in principle applicable to all types of digital data with a risk of being manipulated. Examples include health records, where manipulations can have dramatic consequences, financial records, business analytics, stock markets, political records, or digital evidence. Thus, extending metadata in recordkeeping with cybersecurity evidence is highly significant for digital archives and records management. Further, it builds on current research on cybersecurity-aware provenance and provides innovative extensions to the developing field of continuous recordkeeping for digital data.

References

1. Attacks in record handling in service NSW. https://www.itnews.com.au/news/service-nsw-told-to-urgently-improve-data-handling-after-cyber-attack-559244
2. Compliance with the NSW cyber security policy (CSP). https://www.audit.nsw.gov.au/our-work/reports/compliance-with-the-nsw-cyber-security-policy
3. The application of technology-assisted review to born-digital records transfer, inquiries and beyond. Technical report, The National Archives UK (2016)
4. Allegrezza, S., et al.: Policies for recordkeeping and digital preservation. Recommendations for analysis and assessment services-code 04. Project report (2017)
5. Bak, G.: Trusted by whom? TDRs, standards culture and the nature of trust. Arch. Sci. **16**(4), 373–402 (2016)
6. Bearman, D.: Office of the secretary: evaluation of email records management and cybersecurity requirements, ESP-16-03. Am. Arch. **80**(2), 459–462 (2017)
7. Bralić, V., Stančić, H., Stengård, M.: A blockchain approach to digital archiving: digital signature certification chain preservation. Rec. Manag. J. **30**(3), 345–362 (2020)
8. Bui, T., et al.: Archangel: tamper-proofing video archives using temporal content hashes on the blockchain. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (2019)

9. Duranti, L., Rogers, C.: Trust in records and data online. In: Integrity in Government through Records Management, pp. 227–238. Routledge (2016)
10. Frank, R.D.: Risk in trustworthy digital repository audit and certification. Arch. Sci. **22**(1), 43–73 (2022)
11. Hofman, D., Lemieux, V.L., Joo, A., Batista, D.A.: The margin between the edge of the world and infinite possibility: blockchain, GDPR and information governance. Rec. Manag. J. **29**, 240–257 (2019)
12. Huda, M.: Empowering professional and ethical balance in digital record management. Organ. Cybersecur. J. Pract. Process People **2**(1), 60–73 (2021)
13. International Organization for Standardization (ISO): 15489 information and documentation - records management - Part 1: concepts and principles. Standard, ISO, Cenevre (2016)
14. ISO: 27001 information technology - security techniques - information security management systems - requirements. Standard, ISO, Cenevre (2013)
15. ISO: 27035 information technology - security techniques - information security incident management - Part 1: principles of incident management. Standard, ISO, Cenevre (2016)
16. ISO: 15801 document management - electronically stored information - recommendations for trustworthiness and reliability. Standard, ISO, Cenevre (2017)
17. ISO: 17068 information and documentation - trusted third party repository for digital records. Standard, ISO, Cenevre (2017)
18. ISO: 18829 document management - assessing ECM/EDRM implementations - trustworthiness. Standard, ISO, Cenevre (2017)
19. ISO: 27003 information technology - security techniques - information security management systems - guidance. Standard, ISO, Cenevre (2017)
20. ISO: 14641 electronic document management - design and operation of an information system for the preservation of electronic documents - specifications. Standard, ISO, Cenevre (2018)
21. ISO: 27005 information technology - security techniques - information security risk management. Standard, ISO, Cenevre (2018)
22. ISO: 27050-1 information technology - electronic discovery - Part 1: overview and concepts. Standard, ISO, Cenevre (2019)
23. ISO: 22428 managing records in cloud computing environments - Part 1: issues and concerns. Standard, ISO, Cenevre (2020)
24. ISO: 27002 information security, cybersecurity and privacy protection - information security controls. Standard, ISO, Cenevre (2022)
25. Jaigirdar, F.T., Rudolph, C., Bain, C.: Prov-IoT: a security-aware IoT provenance model. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1360–1367. IEEE (2020)
26. Larsen, D.: Integrity and keeping the nation's records. Public Sector **42**(2), 23–24 (2019)
27. Lemieux, V.L.: Trusting records: is blockchain technology the answer? Rec. Manag. J. (2016)
28. Moreau, L., et al.: The open provenance model core specification (v1.1). Future Gener. Comput. Syst. **27**(6), 743–756 (2011)
29. Mosweu, O., Ngoepe, M.: Trustworthiness of digital records in government accounting system to support the audit process in Botswana. Rec. Manag. J. **31**(1), 89–108 (2021)
30. Rolan, G.: Towards interoperable recordkeeping systems: a meta-model for recordkeeping metadata. Rec. Manag. J. **27**(2), 125–148 (2017)

31. SAĞLIK, Ö.: Arşivlenen elektronik belgelerin güvenilirliğini tehdit eden riskler: Teknolojik koşullar açısından bir inceleme. Bilgi Ve Belge Araştırmaları (16), 29–47
32. Yeo, G.: Records, information and data: exploring the role of record-keeping in an information culture. Facet Publishing London (2018)