CONTENT
RECORDS
MANAGEMENT

STANDARDS PROGRAM

2021

Reducing the potential impact of Ransomware affecting critical records

This article was developed by members of the WG2 – Trustworthy Content/Records Management standardization committee, which is part of the larger ECM Standardization Organization. The ECM industry standard setting organization has responsibility to develop relevant standards, best practices, and technical reports in the electronic content/records management industry, is sponsored by the PDF Association, and includes ANSI accredited experts representing the US to the international standardization efforts (ISO) within TC/171 SC2 and TC/46 SC11.

Reducing the potential impact of Ransomware affecting critical records

Over the past few years, and even as recent as last week, organizations have suffered from ransomware attacks and/or have been affected by data breaches. These attacks have become so frequent that they became a major topic of discussion at the recent G7 meetings, and the US has increased resources within the DHS CISA (Cybersecurity and Infrastructure Security Agency) department to help deal with the most serious of these attacks and breaches.

The volume of these attacks has been substantially increasing over the past several years, many that are successfully raising significant concerns at both the state and national level—especially for organizations such as government agencies, healthcare facilities and banks—about how to protect their critical records.

Critical Records are "records that are essential to an organization to function daily, ensure business continuity and accountability over time, and preserve information of public interest and permanent value" (Hart, 2021). The term encompasses data and information commonly referred to as mission critical, vital, essential, and/or official records. It includes records that have short-term or transitory value such as documentation of ongoing transactions or system documentation.

Critical records include information with a specific retention period, such as those needed to meet financial and legal requirements, as well as records that must be retained permanently. Many, if not most, of these records are commonly stored in email or in personal/department/division 'folders' within network drives and cloud storage. In addition, many users will store copies of attachments or files they created in departmental/organizational archives resulting in numerous copies of the same document/record. The overall number of copies typically increases when the electronic information is emailed to others, who then typically replicate the storage process to some degree).

An issue that almost every organization encounters is that the internal cybersecurity teams take the approach that firewalls and network access security is sufficient to protect data, which is correct for network protections and general data protections but is not the case for electronic records.

The level of network security for most organizations has become quite sophisticated and protects against most unauthorized access but unfortunately not against those attacks utilizing "phishing" or "spear-phishing," or where users' access credentials are compromised. Unfortunately, network security cannot protect against these types of breaches, except in extreme circumstances where multi-factor authentication is established for all connections to all applications being accessed, which quickly becomes burdensome for routine internal users.

Organizational data such as database or application related files stored on networks, whether located "in-house" or "hosted," have different security and management requirements than electronic records as noted above! This is a very important item that all organizations should consider when assessing how their electronic records and other electronic data are stored and protected.

Data created by applications such as databases and raw data used for other applications are also important but have different security requirements. This is due to the fact that electronic records (and physical records) of an organization that are identified in the records retention schedule/policy(ies) need to be maintained for a specific amount of time and in a controlled environment; disposition requirements are also included when appropriate. Almost all of these records are considered to be critical records and may be used on a daily basis to perform/complete required work for the organization or considered "official" or "permanent" records upon creation/approval.

To provide the necessary levels of protection and management control, tools established through the implementation of a trustworthy electronic content environment are needed for the storage and management of these electronic records. These environments integrate, policies, procedures, and records management utilizing secure and trustworthy storage technologies.

The content/records management industry standards programs (ANSI/ISO) have developed a family of standards and best practices related to identifying areas within the current record keeping environment that need to be modified to prevent, or at least minimize, the impact of a potential attack resulting in the loss, or access, to these critical records. These include ISO/TR 18829 Assessing ECM/EDRM implementations—Trustworthiness, ISO/TR 22957 Analysis, selection, and implementation of enterprise content management (ECM) systems, and ISO/DTS 18759 Trusted storage sub-system (TSS) functional and technical requirements.

The purpose of these standards and best practices is to assist organizations in evaluating their vulnerabilities, provide a methodology for addressing identified issues, and guidance in preventing or at least greatly reducing the potential of record loss due to data breaches and ransomware attacks.

The key to deciding if any of this is relevant to the organization, "C" level and other management level resources should consider the following. Almost every organization has some type of electronic storage in use today (in fact, it would be exceptionally rare to find any organization today not using electronic technology to create and store records), but most organizations still utilize network attached storage and server/windows-based security models relying on network/access level security models. We have found that this doesn't provide the necessary security and protections for electronic records as can be seen be the various and rapidly increasing number of data breaches and ransomware attacks we have all heard about over the past several weeks/months.

The good news is that preventing or at least greatly reducing the impact of data breaches / ransomware attacks can be achieved by:

1. assessing existing solutions and identifying gaps in the security models for the records (not data security models);
2. reviewing the integration between the electronic records, the retention schedules and the storage of the records;
3. determining if the records are being maintained in a secure trustworthy storage environment that cannot be 'hacked' through both physical and logical controls; and
4. ensuring the electronic records cannot be accessed directly but only through the electronic records management environment modules.

Additionally, the content stored on the trustworthy storage technologies create a secondary copy internally for safekeeping ensuring data integrity with hash-based verification, and each environment should have a disaster recovery site that would be a full replica of the primary site. These tools and methods have proven to be effective and prevent unauthorized access and more importantly prevents unauthorized deletions and modifications.

The first step in preventing these types of data breaches is to perform an assessment of the existing environment(s), reviewing established policies and procedures in place throughout the organization, identifying those that need to be developed, and examining the existing methodology of storing and protecting content and records. The assessment (in some areas this is also referred to as a Business Impact Analysis) should examine how information is ingested and protected, along with how the records are protected and controlled through the use of any existing records management solution in compliance with the policies and procedures throughout the organization.

As many organizations simply use an electronic storage solution with network storage, planning and working to implement the records management application is critical, as that component provides the necessary controls related to record disposition following the retention schedule and enabling litigation controls, PII security and creating consistency throughout the organization with appropriate policies and procedures.

As the organization begins to consider how to assess their current records environment, it is important to utilize vendor-neutral human resources who have 'hands-on" expertise performing these detailed standardized assessments/evaluations and who understand various content/records management technologies that potentially can be utilized, or may be required, to establish a trustworthy environment addressing identified issues.

The assessment process must be thorough and include an examination of how records are received, stored, and managed for each major process, a review of the extent of organizational policies and procedures that need to be developed, and an assessment of the ability of the organization to embrace necessary change management. Additional detailed information on what should be incorporated in these assessments and what should be provided in the assessment report is documented in detail in ISO/TR 18829.

The next step is to address the identified issues. During this process, the organization needs to select the appropriate storage technology and retention management software and begin restructuring the electronic content to come into compliance with the organizational policies and procedures and subsequently configured in the retention management software. At the beginning of the restructuring process the organization should develop a 'retention bridge' to document the relationship between the updated record taxonomy and the retention policy(ies) and ensure the selected records management solution provides the ability to function utilizing an ISO/DTS 18759 Trustworthy storage solution.

This should be performed in a consistent fashion for each organizational activity that creates/manages electronic content ensuring all electronic records, along with ensuring system and application logging and reports are stored and maintained as appropriate. The importance of including the system and application logging and reporting is to enable the system administrators to review this information on a routine basis ensuring that any errors or issues are addressed expeditiously and that a log of the health of the system is maintained. While many of these steps seem simple and straight forward, it is important to remember that change management and policy and procedure development is critical as many of the required updates and changes will require updates to business processes along with using trustworthy storage technologies in many cases.

The final aspect of these standardized assessments is to identify records related issues and develop/provide realistic 'road-maps' and actionable plans to enable the organization to address those identified issues and other areas that need to be addressed. Using ISO/TR 18829 – Accessing ECM/EDRM implementations—Trustworthiness is a key step to start the process of evaluating vulnerabilities to identify areas that need to be updated using the appropriate trustworthy records environment technologies components (this includes policies, procedures, storage solutions, and records management software). Conducting these standardized assessments will be of value to any organization and has been shown to greatly assist securing and protecting critical records.

This article was developed by members of the WG2 – Trustworthy Content/Records Management standardization committee, which is part of the larger ECM Standardization Organization. The authors are Robert M. Blatt, President and Principal Consultant with Electronic Image Designers (EID), Inc.; Dr. Patricia C. Franks, Professor Emerita, San José State University; and Amitabh Srivastav, VP, Compliance & Governance, HELUX.

The ECM industry standard setting organization has responsibility to develop relevant standards, best practices, and technical reports in the electronic content/records management industry, is sponsored by the PDF Association, and includes ANSI accredited experts representing the US to the international standardization efforts (ISO) within TC/171 SC2 and TC/46 SC11.

The ECM standards organization consists of 3 working groups: WG2-Trustworthy Content/Records Management, WG1-Trustworthy Storage Technologies, and WG3-Information Capture. For more information or assistance on these topics, please contact Betsy Fanning, Program Director, ECM Standards Program at betsy.fanning@pdfa.org or Robert Blatt, WG1/WG2 Committee Chair at blatt@eid-inc.com.

References

Hart, Susan. (In press). "Critical Records." In *The Handbook of Archival Practice*, edited by Patricia C. Franks, 37-38. New York: Rowman and Littlefield.

International Organization for Standardization (ISO). ISO/DTS 18759 Document management—Trusted storage sub-system (TSS) functional and technical requirements. https://www.iso.org/obp/ui/#iso:std:iso:18759:dis:ed-1:v1:en

International Organization for Standardization (ISO). *ISO 18829:2017 Document management—Accessing ECM/EDRM implementations—Trustworthiness.* https://www.iso.org/standard/63513.html

International Organization for Standardization (ISO). *ISO/TR 22957:2018 Document management—Analysis, selection, and implementation of enterprise content management (ECM) systems*. https://www.iso.org/standard/71605.html

About the Primary Author

Robert M. Blatt has more than 35+ years extensive technical experience working with various electronic content/Records management (ECM) technologies along with over 20 years providing eForensic expertise. This experience ranges from the technical development, analysis, design, project management & oversight roles through full solution implementation of these technologies. In addition, consulting activities have included providing Trustworthy content/record environment analysis, project management, vendor oversight and technical assistance & training to numerous clients either implementing or planning to implement or update existing environments to a Trustworthy electronic record environment.

Accredited as an AIIM-Master of Information Technology in 1997. Received the Laureate credentials and recognition in Content Management in 1998 and a second Laureate in Workflow technologies in 1998. In addition, Mr. Blatt achieved the CHPA-III eForensic Certification in 2015. Appointed to US TAG to ISO TC/171 in 1998 This committee represents US interests in the Content/Records Management industry establishing international standards, technical reports, and best practices for end-users and vendors.

Mr. Blatt is the chairperson of several national and international standard setting committees related to the content/record management industry and is a current member of the industry standards board. Mr. Blatt has developed and participated in the development of numerous Content/Records Management industry standards and best practices for over 30 years, plus he is an acknowledged national and international industry expert and analyst. Mr. Blatt is currently the chair of the Trustworthy Storage (WG1) and Trustworthy Content Management (WG2) standardization committees, and ISO convener for WG11 TC/171 SC2 – Trustworthy Record Storage.

Mr. Blatt has been President and Principal Consultant with Electronic Image Designers (EID), Inc. since 1994. EID is one of the industry's first vendor-neutral consulting organizations focusing on content/record management assessments, planning, design, and implementation oversight efforts. EID has provided these services at both the national and international levels bringing a level of expertise to the client who desires/requires direct knowledge related to industry standards and how these technologies actually function in the "real-world" environments.