Spring 5-21-2018

Rescuing Records: Safeguarding Vital Museum Records

Brianna LoSardo
brianna.losardo@shu.edu

Rescuing Records:

Safeguarding Vital Museum Records

Brianna LoSardo

Submitted in partial fulfillment for the degree

Master of Arts in Museum Professions

Seton Hall University

May 2018

Approved by: Jürgen Heinrichs

Juergen Heinrichs

Thesis Advisor

Abstract

Every activity undertaken by museums relies in some way on records and information. As technology becomes more and more integrated into museum operations, these records are increasingly being created, used, and stored in electronic format. The rapid proliferation of electronic records has left many institutions unprepared to safeguard electronic records that are vital to their operations from disaster, both natural and man-made. In addition, a historical focus on collection records has siloed records management concerns into registration and collections management departments, an approach that no longer suffices in today's museum. In this thesis, I argue that museums should empower staff to take proactive steps to manage vital electronic records. Through a national survey, I assess the current state of vital records management in museums and identify areas where improvements could have a major impact. Crucially, formalizing vital records management through the creation of policies and procedures as well as a basic level of records-handling training for all staff members who use electronic records could greatly increase the security and preservation of these records. Taking these steps now will ensure that records are adequately protected going forward so that vital records are not damaged or lost.

Table of Contents

Introduction

Accurate records have always been essential to carrying out the work of museums, but an increasing reliance on technology and electronic records has created new considerations and complications for safeguarding records. In 2017, credit-reporting agency Equifax received national attention when it was hacked, endangering the personal information of as many as 143 million people.[1] While Equifax was undoubtedly a high-profile target for hackers, museums are not immune to these kinds of attacks. In October 2017, the Denver Art Museum reached out to 800 donors, members, and employees to warn them of a data breach that included sensitive personal and financial information. That breach took place in June of 2017 and was the result of a phishing scam, which compromised some of the museum's e-mail inboxes.[2] The Ashmolean Museum at Oxford University was hacked in 2014, compromising information about approximately 8,000 visitors, including names, addresses, e-mail addresses, and telephone numbers.[3] While no financial information or especially sensitive data was exposed in this attack, the hack raised concerns that visitors' contact information might be used to try to trick visitors into donating to false organizations.[4] While they are on a much smaller scale than the Equifax data breach, these incidents demonstrate that museums are vulnerable to such kinds of attacks and need to take steps to mitigate these risks.

[1] Siegel Bernard, Tara, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *The New York Times*, September 7, 2017. Accessed October 1, 2017. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[2] Wenzel, John. "Denver Art Museum warns donors, members, employees after sensitive data breach." *The Denver Post*, October 30, 2017. Accessed December 12, 2017.

[3] "Ashmolean Museum Website Hackers Access Customer Details." BBC News. June 18, 2014. http://www.bbc.com/news/uk-england-oxfordshire-27909976.

[4] Rawlinson, Kevin. "Ashmolean Accused of Underplaying Risk after Visitors' Details Hacked." The Guardian. June 18, 2014. Accessed April 16, 2018. https://www.theguardian.com/culture/2014/jun/18/ashmolean-underplaying-risk-details-hacked.

In this rapidly changing landscape, many museums have adopted significant electronic records without establishing clear policies and procedures. Vital records, especially in electronic format, are not sufficiently controlled and their protection and preservation is often not accounted for in existing policies and emergency plans. Electronic records face unique threats and vulnerabilities that are not well-covered by procedures established for paper records. In addition, record-keeping in museums is often seen as exclusively the province of registrars and collections managers, and the majority of the literature that exists on museum records focuses solely on collection records without regard for the other types of records museums, which are vital to their operation. In this thesis, I argue that policies and procedures as well as staff training that extends to all areas of the museum can significantly mitigate the risks to electronic records and ensure that vital records are not compromised or lost through inaction, attack, or accidental causes.

The first chapter of this thesis focuses on the history of vital records programs in museums. This includes an explanation of what constitutes a vital record, the types of vital records museums commonly hold, and examines how museum practices compare to those used in the business and government sectors, with an emphasis on electronic records. In this section, I demonstrate how the role of records and information has expanded in museums and how influence from other fields can be an asset to shaping museum thinking about records and information. The second chapter discusses the types of threats and vulnerabilities that electronic records face and how they overlap with and differ from those that face paper records. The third chapter addresses the current practices that museums use to deal with their vital electronic records through a national survey with a focus on institutional policies and staff training. The fourth chapter determines some recommendations and best practices that museums can use to establish a vital records program that takes electronic records into account, emphasizing practical solutions for small institutions and the importance of educating staff at all levels about proper records handling and security.

Chapter I

Card Catalogs to Computers: Evolution of Museum Records Management Practices

In order to understand how to move forward in safeguarding museum records, it is necessary to understand what vital records are and how they have been dealt with by museums in the past. In this chapter, I clarify the terminology to be used throughout this paper, identify the types of vital records commonly held by museums, and explore how record-keeping practices developed in museums compared to those in other sectors. Finally, I will address the effect of electronic records on the established paper record-keeping systems in museums and the new challenges that they create.

It is important to clarify the terminology regarding records because there are a number of terms that are often used in a variety of contexts or that are understood differently across professions. We will begin with the basics of distinguishing *data, information, record,* and *vital record,* all of which are closely related terms with meanings that overlap but contain important distinctions. ARMA International (formerly the Association of Records Managers and Administrators), the major professional organization for records and information professionals, defines data as "Any symbols or characters that represent raw facts or figures and form the basis of information."[5] In turn, information is defined as "data that has been given value through analysis, interpretation, or compilation in a meaningful form."[6] In other words, data becomes information when it is given context that creates meaning. A list of temperature and humidity readings is a set of data. If that data is related to a set of dates and timestamps and labeled

[5] ARMA International, *Glossary of Records Management and Information Governance Terms*, 5th ed. (Overland Park, KS: ARMA International, 2016), 12.
[6] Ibid., 28.

"Environmental Conditions - Collections Storage," it becomes information about the environment of a collections storage room over a period of time, which is useful and meaningful to the user. Information is fundamental to the definition of record: "Any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business."[7] To put it another way, a record is information recorded in a fixed medium, regardless of the type of medium. (Paper, microfilm, electronic, etc.) If the above-mentioned information on environmental conditions is recorded in a handwritten log or saved as a spreadsheet on a museum's server, it becomes a record. Museums create and maintain a wide variety of records, but only some of them are vital records, which are defined as "A record that is fundamental to the functioning of an organization and necessary to the continuance of operations."[8] Without vital records, an organization cannot resume operations after a disaster.

Museums hold many different types of records that could be considered vital records, although an exact list will necessarily vary by institution. The most obvious example is the collection records containing information about the museum's holdings. Without these records, the museum would not be able to locate, identify, and use objects in its collection to fulfill key functions such as exhibitions, loans, and research. Much of the value of a collection of objects lies in the ability to place the objects in context using the information about them that is stored in records, and loss of this information could have just as great an impact on the museum's ability to carry out its mission as loss of the objects themselves. Furthermore, object records often contain deeds of gift or other documents that establish the museum's rightful ownership of an object, and lack of these could create legal issues or challenges to ownership.

[7] ARMA International, *Glossary*, 43.

[8] Ibid., 56.

However, while object records are the most obvious type of vital record held by museums, it is important to consider other categories of records that could be considered vital. A museum's foundational documents, such as its charter, articles of incorporation, and bylaws need to be preserved for legal reasons. We must also take into account the types of records that facilitate the day-to-day operation of the museum. Personnel and payroll records are necessary to maintain staffing of the museum, and may also be required to show compliance with legal and tax requirements. Other categories may include tax and financial records, grants records, donor records, and building plans. Ultimately, each museum must examine its records and operations to determine what its vital records are, where they are currently stored, and what plans are already in place to ensure they are preserved in the event of a disaster.

Looking at the history of museum record-keeping practices can give us insight into the basis for the current state of museum records. Throughout much of museum history in the United States, the focus has been primarily on collection records. In 1895, George Brown Goode, the Assistant Secretary of the Smithsonian Institution, wrote "The value of a collection depends in the highest degree upon the accuracy and fullness of the records of the history of the objects which it contains."[9] This strong emphasis on collection records continued throughout the expansion and professionalization of museums, especially through the development and increase in registrar positions with explicit documentation and record-keeping duties in the early 20th century.[10] In 1911, a paper read before the American Association of Museums in Boston urged museums to draw inspiration from the business world in tracking and documenting their collections: "Surely neither such red tape nor slipshod, unbusinesslike methods of administration

[9] George Brown Goode, *Principles of Museum Administration,* (York: Coultas & Volans, 1895), 54.
[10] Rebecca A. Buck and Jean Allman Gilmore, eds., *Museum Registration Methods,* 5th ed. (Washington, DC: The AAM Press, 2010), 3-4.

should be tolerated in a museum any more than in a factory, although this is a point which does not seem to have been considered worthy of much attention heretofore, if we judge by the literature on the subject."[11] The paper emphasized how the detailed record-keeping processes it outlined would keep museum objects safe in "a building of long distances where many employees and visitors are coming and going...thousands of objects are added in a year, and…hundreds of thousands of dollars are involved in these transactions."[12] However, it did not devote any attention to safeguarding the records themselves, and despite making connections to the business world, it focused only on collection records and did not make mention of any other types of records the museum needs in order to operate.

By the 1950s, it became apparent that museum records were becoming a significant challenge, as many museums found they were taking up an increasing amount of resources and space.[13] It became clear that more active management of records involving systematic procedures for retention, storage, and classification was necessary. The Cleveland Museum of Art was one of the first to create a list specifying which records were to be destroyed after a specified period of time and which were to be kept permanently—effectively creating a records retention schedule.[14] However, although the schedule was adopted by the museum's board in 1956, no one was designated as responsible for carrying out the schedule and it was largely ignored until the museum hired its first archivist/records manager in the 1980s.[15]

[11] "Business Methods in the Metropolitan Museum of Art: A Paper Read before the American Association of Museums in Boston, May 23, 1911." *The Metropolitan Museum of Art Bulletin* 6, no. 8 (1911): 169, accessed January 5, 2018, https://www.jstor.org/stable/3252513
[12] Ibid.
[13] Deborah Wythe, *Museum Archives: an Introduction*, (Chicago: Society of American Archivists, 2004), 4.
[14] Ibid.
[15] Ibid.

During this time, the field of records management was developing in the government and business sectors. The National Archives and Records Administration (NARA) was established in 1934 to assess federal recordkeeping practices and preserve historical records. The agency quickly found itself overwhelmed by the volume of records, especially as the government underwent the necessary expansion in paperwork from all of the emergency agencies operating during WWII.[16] In 1943, the Records Disposal Act was passed, which allowed the National Archives to work on developing records disposal schedules that would allow some records to be destroyed after a specified period of time.[17] In 1946, President Truman signed an executive order requiring federal agencies to adopt records management programs, causing an increase in records management activity that led to the creation of a Records Management Division within the National Archives.[18] By 1954, records management programs had spread through the government agencies to such a degree that the vast majority of records were covered by the schedules.[19]

Post-WWII also saw an increase in business and industry in the United States, which gave the newly formed discipline of records management an opportunity to demonstrate its utility to the business world. By 1965, records management was becoming more commonplace in private businesses, and business records management specialist F.L. Sward articulated the reasons why in a paper presented before the Society of American Archivists in October 1965:

> The records manager can show business how to reduce the costs of creating records by forms control, correspondence and reports control, and similar techniques. He can reduce costs by improving file systems, by moving records from expensive file equipment to an inexpensive storage center, and by scheduling records for early destruction instead of letting them pile up indefinitely. He can show management how to protect its vital

[16] Candy Schwartz and Peter Hernon, *Records Management and the Library: Issues and Practices*, (Norwood, NJ: Ablex, 1993), 26.
[17] Ibid.
[18] Ibid., 27.
[19] Ibid., 27.

> information from being lost through a disaster. Records managers are very familiar with these sales pitches, which have a strong appeal to management because they affect the profits of the enterprise by improving utilization of space, facilities, and manpower.[20]

This shows that, at the time, businesses were already beginning to consider vital records protection as part of their records management programs. Businesses generally see the value of records management programs in terms of the impact of records on efficiency and risk management, and records managers were able to effectively make the case for their discipline. The main driver of corporate adoption of records management was the cost savings realized by managing records well (not spending resources on maintaining records that were no longer needed), better compliance in case of lawsuits or regulatory issues, and less disruption of business after a disaster. Therefore, many businesses have adopted vital records programs to ensure that operations can resume as quickly as possible after a disaster.

With these developments taking place in the government and business sectors, where do museums fit in? In the United States, most museums are not government-run, and neither are they for-profit businesses. However, they experience elements of each, such as the obligation to the public that comes from operating as a non-profit, but maintaining the financial independence of a business. Instead of turning to either of those sectors, museums looked to libraries for guidance. Although many libraries are government-run they often operate fairly independently, and there has been a long history of collaboration and communication between libraries and museums. In 1923, John Cotton Dana, director of both the Newark Public Library and the Newark Museum, established an apprenticeship program that combined library and museum

[20] F. L. Sward, "Business Records Management," *The American Archivist* 29, no. 1 (1966): 70, accessed January 2, 2018, https://www.jstor.org/stable/40290566.

practices.[21] Two graduates of this program, Irma Bezold and Dorothy Dudley, went on to write the *Museum Registration Manual (MRM)* in 1954.[22] The *MRM* was very influential in documenting the practices of museum registrars, including record-keeping procedures. However, it did not address the overall records of a museum.

Despite the fact that records management has taken a different trajectory in museums than in other industries, the advent of electronic records has created new opportunities and challenges. Now, instead of card catalogs, vast amounts of collection information is stored in electronic databases. Administrative records may be created and stored electronically, in a variety of file formats and storage environments. The volume of records has increased as well—a museum's staff could easily generate thousands of e-mails relating to all aspects of the museum's operations. These changes lead to an increased pace of activity within the museum and greater interconnectedness, but they also create potential issues and new risks. It is clear that active management and planning is needed in order to ensure the safety of vital museum records held in electronic formats.

[21] Richard J. Urban, "Library Influence on Museum Information Work," *Library Trends* 62, no. 3 (2014): 606, accessed January 2, 2018, https://muse.jhu.edu/article/542832.
[22] Ibid., 607.

Chapter II

Hackers and Mishaps: Threats Facing Electronic Records

Although it is important to protect vital records in all formats from disaster, electronic records pose a unique set of risks and vulnerabilities. In the past, many paper records were preserved not by design, but by accident.[23] This is because even with little attention, paper records stored in a stable environment can last hundreds of years, so often records were preserved only because of lack of action to dispose of them, rather than proactive action to preserve them. This haphazard approach will not suffice for electronic records, which need much more active management in order to ensure preservation. Electronic records are also more susceptible to malicious attacks and data theft—securing a physical location is not enough to protect them. Crucially, the human element is a much greater factor in electronic records preservation vs. analog records—an untrained staff that does not understand proper electronic records handling procedures can damage records through mishandling or inadvertently expose the institution's records to attack. In this chapter, I examine in more detail the threats and vulnerabilities facing electronic records and how lack of staff training can play a role in those threats.

Like paper records, electronic records face the risk of accidental destruction. In a disaster that threatens the records facility, electronic records stored on physical media can easily be lost. Many such media, including hard drives, portable USB drives, and compact disks are very vulnerable to harm from water, fire, or physical damage.[24] Even electrical surges can damage

[23] David O. Stephens, *Records Management: Making the Transition from Paper to Electronic* (Lenexa, KS: ARMA International, 2010), 11.
[24] Ibid.

electronic storage media, while they would have little effect on paper records. These risks can be mitigated by the fact that electronic records are more portable and easier to duplicate than paper records, meaning that there are more options for protecting them from these types of physical threats.[25] However, these measures must be proactively put into place before a disaster occurs in order for them to be useful, and often require the regular, active involvement of staff to maintain. (Even automated backups must be set up and periodically monitored to ensure they are functioning correctly.) If a loss occurs, electronic records are often more difficult to restore—paper records can often be successfully restored, unless they have been destroyed by fire, whereas electronic records are much more difficult and, in many cases, impossible to restore once they have been lost.[26]

Failing to recognize and address the unique needs of electronic records early in their life cycle can put them at risk. Unlike paper records, which are immediately readable by humans, electronic records are only machine-readable, and often rely on specific hardware and proprietary software to display in a form that is understandable to humans. It may take only a few years for such records to no longer be supported by the underlying technology, and the longer action regarding these records is delayed, the more difficult it will be to recover their contents. For this reason, "long term preservation" for electronic records is generally considered to be any period longer than one generation of technology, about 5-7 years.[27] In contrast, long-term preservation for paper records is often considered to be 25 years or more.[28] Added to this difficulty is the fact that there is no "permanent" preservation media for electronic records—

[25] Robert F. Smallwood, *Managing Electronic Records: Methods, Best Practices, and Technologies* (Hoboken, NJ: Wiley, 2013), 143.
[26] Stephens, *Records Management*, 11.
[27] Kelvin Smith, *Planning and Implementing Electronic Records Management: A Practical Guide* (London: Facet, 2007), 130.
[28] Ibid.

disks, hard drives, and other physical media are fragile and prone to corruption and failure.[29] The media themselves are also not immune to the problem of obsolescence. For example, while 3 ½ inch floppy disks were ubiquitous in the 1990s, by 2007 98% of new computers sold lacked floppy disk drives entirely.[30] An even more recent example is the decline of optical drives used to read CDs and DVDs in computers. Once commonplace, optical drives are no longer included on most new computers due to the shift to distributing content on non-physical media and consumer desire for smaller, lighter mobile computers.[31] As these examples demonstrate, if care is not taken to periodically refresh storage media, records can easily be lost.

The human factor plays a significant role in the threats that electronic records face. Careless handling can cause permanent loss of electronic records more easily than with paper records. Especially for frequently referenced files, accidental erasure or overwriting of files can be a major concern.[32] Data entry and other errors can result in electronic records becoming invisible to indexing or other search systems, the equivalent of mis-filing a paper record.[33] Many organizations also fail to manage the volume of electronic records as efficiently as they manage paper records. Because digital storage space does not actually take up much physical space, there is a greater tendency to "keep everything—just in case", which can result in an excess of records being kept long after their lifecycle should be over, making it more difficult to manage the

[29] Smallwood, *Managing Electronic Records*, 287.

[30] David Derbyshire, "Floppy disks ejected as demand slumps," *The Daily Telegraph*, January 30, 2007, accessed January 12, 2018, https://www.telegraph.co.uk/news/uknews/1540984/Floppy-disks-ejected-as-demand-slumps.html.

[31] Mark Kyrnin, "The Death of the Computer Optical Drive: Why Do Most New PCs Not Come with DVD or Blu-ray Drives?" Lifewire, accessed April 07, 2018, https://www.lifewire.com/death-of-the-computer-optical-drive-832403.

[32] William Saffady, "Count the Cost: Quantifying Your Vital Records Risk," *The Information Management Journal* 49, no. 1 (January/February 2015): 28, accessed January 28, 2018, Academic Search Complete.

[33] Ibid.

electronic records that are truly vital.[34] Not only does this make it difficult to find and retrieve needed records, but it also results in the expenditure of more resources than necessary on maintaining unnecessary files. Without an effective records management program and systematic procedures for handling of electronic records, these and other errors of careless handling can pose a significant threat.

If all of these factors make it significantly more difficult to preserve electronic records, why not simply reformat them in paper or microfilm instead of going to great lengths to preserve them digitally? This would seem to be a simple solution, however in many cases, electronic records cannot simply be converted to paper without losing critical context, functionality, and information.[35] For example, the information in a museum's collection database contains text, images, and often multiple pages and levels of information that link to other records. These types of records cannot be represented with their full functionality in paper form, although often a report representing some of the information held there may be printed. However, many would argue that the functionality of the database system warrants the greater effort needed to ensure its preservation.

There are also some threats facing electronic records that do not necessarily result in the destruction of records, but nonetheless present serious risks to the organizations facing them. In particular, the improper disclosure of electronic records is becoming an ever more present threat.[36] There are many ways in which improper disclosure can occur. One of the most difficult

[34] D. R. Prescott, "Debunking the Myth of Electronic Records Retention". *Inform* 11 no.10 (November 1997): 32, accessed February 3, 2018, https://search.proquest.com/docview/217561177?accountid=13793.
[35] US Government Accounting Office, *Electronic Records: Management and Preservation Pose Challenges : Statement of Linda D. Koontz, Director, Information Management Issues*, GAO-03-936T, Washington, DC: GAO, July 8, 2003): 10, accessed February 1 2018, https://www.gao.gov/new.items/d03936t.pdf.
[36] Saffady, "Count the Cost", 29.

to defend against is an internal threat—a museum employee intentionally stealing information.[37] This situation is more common in the corporate world but cannot be discounted entirely with regard to museum records. This type of risk is also not necessarily limited to employees of the museum itself—if the museum is using a cloud storage vendor to store its electronic records, the employees of the vendor may contribute to this potential vulnerability.[38]

Malicious attacks by hackers attempting to steal information are another unfortunate reality in the modern records management environment. One common method of attack is through the use of malware, malicious software designed to infiltrate computer systems.[39] There are many types of malware, but the most common include viruses, worms, trojans, spyware, and ransomware. While these types of attacks may seem to be beyond the museum's control, hackers often rely on vulnerabilities created by users who lack training in recognizing and avoiding suspicious online activity.

Viruses are malicious code that attach themselves to computer files.[40] Like biological viruses, they reproduce themselves within the infected computer, and can then be transmitted to other computers via infected files.[41] However, viruses cannot spread to other computers on their own—they rely on users transmitting infected files to other users, such as by sending an infected e-mail attachment or transferring infected files on a portable data storage device.[42] Worms are similar to viruses, but instead of reproducing within individual infected computers, they use computer networks to replicate.[43] In addition to slowing down the network they are infecting,

[37] Smallwood, *Managing Electronic Records,* 199.
[38] Smallwood, *Managing Electronic Records,* 199.
[39] John R. Vacca, *Managing Information Security* (Waltham, MA: Syngress, 2014), 7.
[40] Mark D. Ciampa, *Security Awareness: Applying Practical Security in Your World*. (Boston: Cengage Learning, 2017), 78.
[41] Ibid.
[42] Ibid., 80.
[43] Ibid., 81.

worms can delete files from computers in the infected network or allow attackers to take remote control of the computer.[44] Because they are able to transmit themselves over networks, worms do not require user action to spread. Trojans are executable programs that appear to be benign. However, while outwardly performing a benign function, the trojan also secretly performs malicious actions as well.[45] Like viruses, their transmission depends on user action—installing and running infected programs. Spyware is another type of malware that is used to secretly collect information without the user's consent.[46] Spyware can be transmitted through different means, including as part of a virus or trojan.[47] Finally, Ransomware is a type of malware that has gained prominence since the invention of the electronic currency Bitcoin made it easier to conduct anonymous payment transactions online.[48] Ransomware locks the infected computer and encrypts its data, demanding a sum of money to be paid (usually in Bitcoin) in order to return control to the user.[49] Some types of ransomware attacks only lock the computer, allowing the data to be recovered if the malware is removed or the hard drive is moved to an uninfected computer.[50] However, the most malicious types encrypt the data so that even if the malware is removed, the data remains inaccessible.[51]

Another way in which hackers can gain unauthorized access to computers is through social engineering, which is a type of attack that uses deceit to trick users into compromising

[44] Ibid., 81.
[45] Ciampa, *Security Awareness*, 81.
[46] Ibid., 86.
[47] Michael Erbschloe, *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code* (Amsterdam: Elsevier Butterworth Heinemann, 2005), 26.
[48] Ronny Richardson and Max North. "Ransomware: Evolution, Mitigation and Prevention" *International Management Review* 13, no. 1 (January 2017): 10, accessed February 11, 2018, https://search.proquest.com/docview/1881414570?accountid=13793.
[49] Ibid.
[50] Ibid.
[51] Ibid.

their system.[52] For example, a common social engineering strategy is to trick users into opening an infected e-mail attachment by making it appear to have been sent by an acquaintance.[53] The user's initial suspicion towards opening an unfamiliar attachment is overcome by the fact that it seems to be coming from a source that they trust. Another common type of social engineering is phishing, in which the user is sent a "lure," usually in the form of an e-mail that appears to be from a legitimate business. The e-mail will then direct the user to a fraudulent website that has been made to look similar to the legitimate business' website, in order to trick the user into entering information such as passwords and personal information.[54] Social engineering and phishing attacks like this can slip past even very well-defended organizations, because they exploit human nature and require users to be vigilant about their activity. For instance, phishing was responsible for the recent data breach of donor records from the Denver Art Museum, which was the result of some of the museum employee's e-mail inboxes being compromised. [55] Providing training in how to recognize and avoid such attacks can help to prevent such data breaches.

It is clear that electronic records present some unique challenges, especially with regard to long-term preservation of vital electronic records and information security. These challenges are not insurmountable, but require proactive planning and attention to electronic records throughout their lifecycle. What many of these threats demonstrate is that there is a major human

[52] John R. Vacca, *Computer and Information Security Handbook* (Amsterdam: Morgan Kaufmann, 2013), 83.
[53] Ibid.
[54] Vacca, *Computer and Information Security Handbook*, 83.
[55] John Wenzel, "Denver Art Museum warns donors, members, employees after sensitive data breach," *The Denver Post*, October 30, 2017, accessed December 12, 2017, https://www.denverpost.com/2017/10/30/denver-art-museum-data-breach-800/.

component to protecting vital records, and all employees who work with records need to be educated on information security best practices and the proper handling of electronic records.

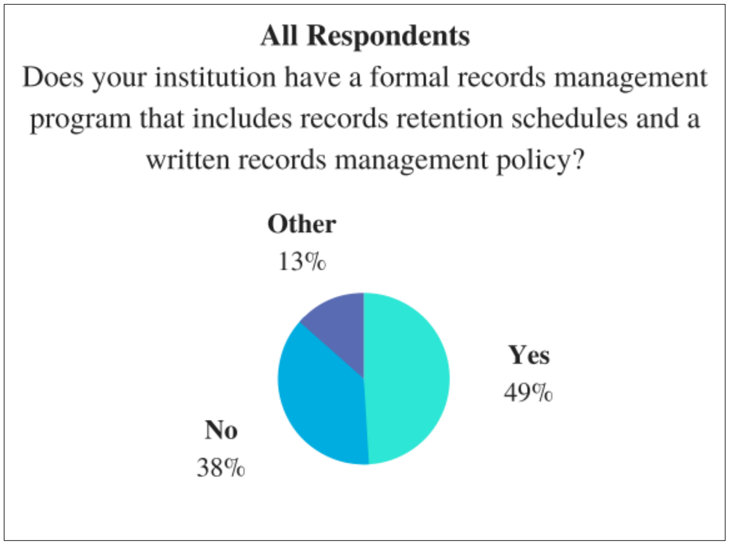
Chapter III

Secured or Ignored? The Current State of Museum Vital Records Practices

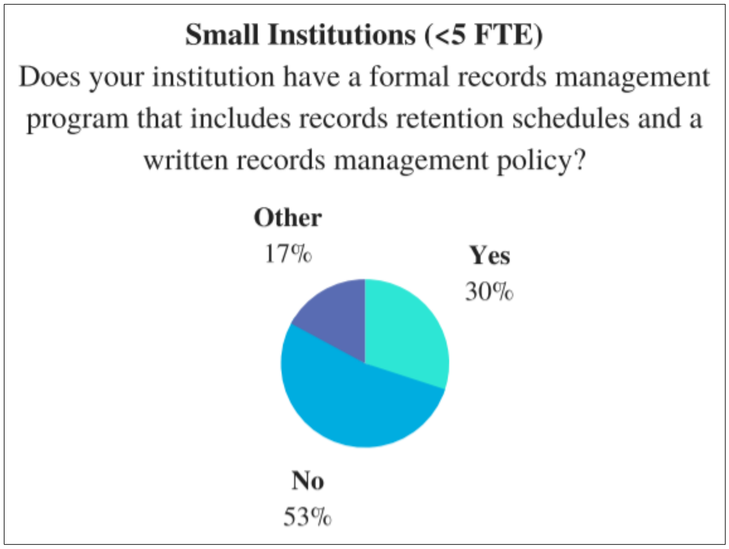
In order to assess the current state of museum practices regarding vital records, I conducted a national survey focused on institutional policies and staff training. The eight-question survey was sent out via the American Alliance of Museums Collections Services Professional Network (CS-AAM) listserv, the Society of American Archivists Museum Archives Section (SAAMUS) listserv, and the American Alliance of Museums Museum Junction Open Forum. I received 104 responses from a variety of institutions, ranging in size from organizations with 0 full-time equivalent (FTE) staff to those with more than 500. The major questions addressed by the survey were: do institutions have a formal records management program, are institutions including both electronic and physical records in their emergency plans, do institutions have a written information security policy, and which departments in an institution receive training on electronic records handling? Overall, the answers to these questions showed that museums would benefit from formalizing procedures and providing training to a broader group of employees.

Prevalence of Formal Records Management Programs in Museums

I first wanted to assess the level of overall records management in the institutions surveyed. 49% of the survey respondents indicated that their institution does have a formal records management program in place, including records retention schedules and a written policy. 38% indicated that their institution does not, and 13% answered “other.”



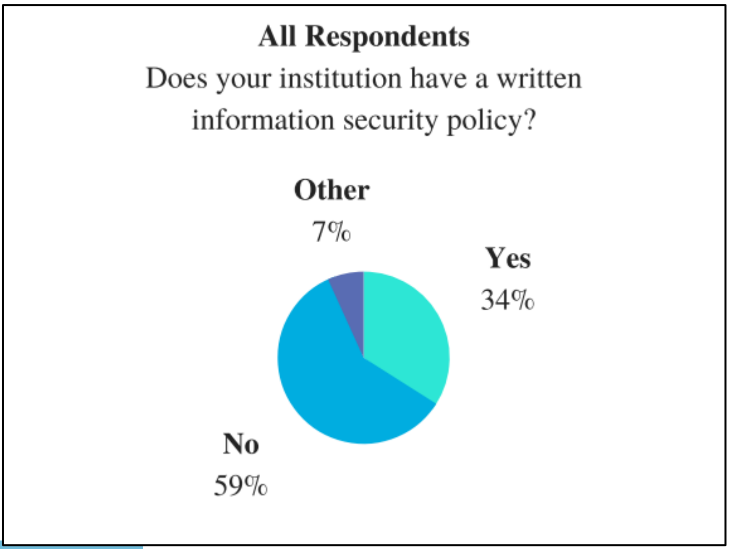
However, in small museums (those with fewer than 5 FTE staff) formal records management programs are less prevalent, with only 32% responding yes, 52% responding no and 17% responding "other." This is not surprising, as it stands to reason that organizations with less staff time and resources overall would be less likely to devote time to formalizing records management procedures. However, even developing basic records management programs in such areas could make a significant impact.



Across all of the responses, survey participants who selected "other" were able to write in their own open-ended response. For this question, most of these indicated having some parts of a records management program. For example, "we have a records management policy but no records retention schedules," or, "we have a formal policy for collections related records but not accounting." Others discussed having a policy in progress: "Our records management policy remains in draft form even after revising it four years ago. It includes a records retention schedule that has not been revised," and "beginning to develop." This is promising, as there is an opportunity to strengthen these procedures and build on what has already been done.

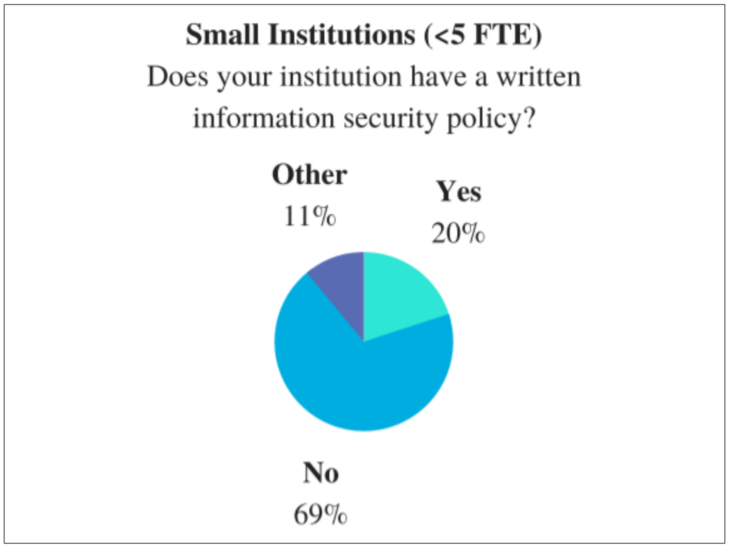
Prevalence of Information Security Policies

Only 34% of respondents indicated that their institution has a written information security policy. 59% said they did not, and 7% said "other." Unlike the previous question, most of the "other" responses for this question indicated uncertainty, such as: "I'm not sure. I've never looked for one," and "Probably, but I am not aware of it." This indicates a lack of training with



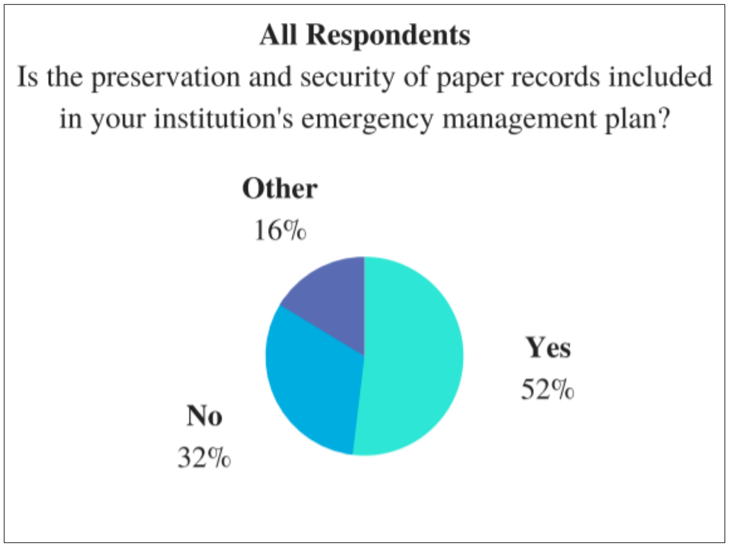
regard to information security. There is a clear need to establish more concrete policies and training surrounding the issue of information security.

Again, small institutions were less likely to have an information security policy. Only 20% of respondents who reported less than 5 FTE staff had a written information security policy. 69% reported “no” and 11% “other.” It may seem that small institutions are less attractive targets to potential hackers and therefore less in need of such a policy, but they still likely have electronic records that are vital to their operation and must be protected. Furthermore, in a small institution each staff member is likely to have access to a greater proportion of the organization’s information assets, which makes ensuring that they are informed about information security best practices especially important.

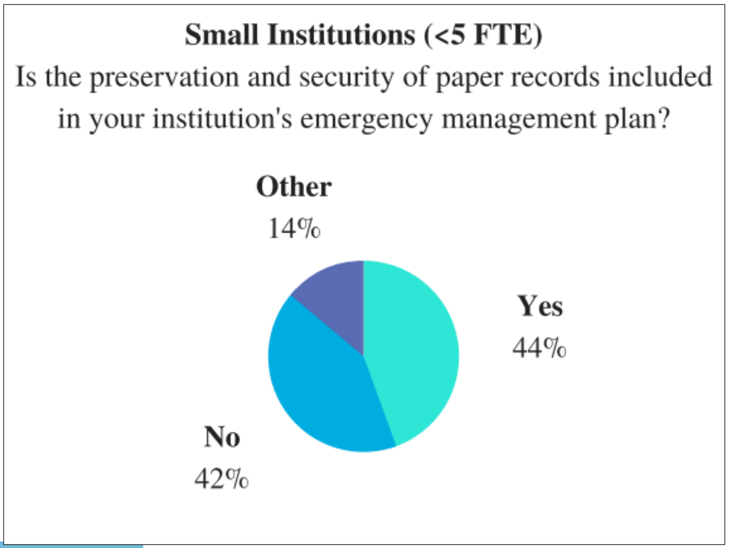


Are Paper Records Addressed in the Institution’s Emergency Plan?

In regard to paper records, 52% of respondents said they were included in the institution’s emergency plan. 32% said they were not included, and 16% answered “other.” Many of the “other” responses indicated that the respondent did not know, or that their institution does not currently have an emergency plan. One reiterated that collections records are treated



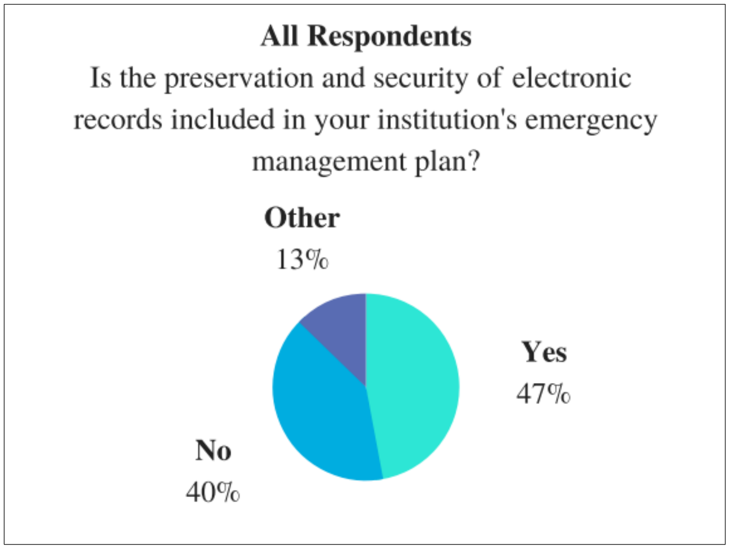
differently than the institution's other records: "Again yes for collections no for anything else." This response reflects the development of museums and the historical focus on collections records above others. However, while collection records are certainly vital to museums, neglecting to take into account other types of records that the museum needs in order to operate could leave the museum in an unfortunate position in a disaster. The "I don't know" responses reveal a lack of training—if staff do not know the contents of the emergency plan, they will be unable to quickly enact the plan if a disaster strikes.



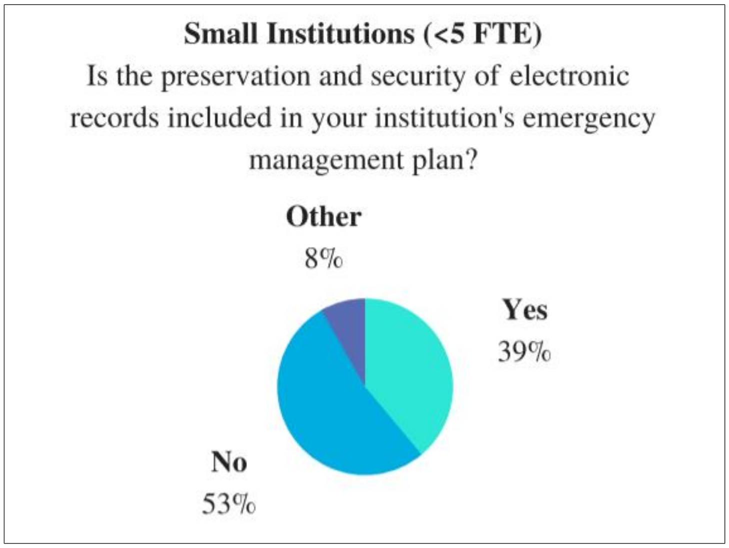
In small institutions, it was slightly less prevalent for paper records to be included in the emergency plan, with 44% answering yes and 42% answering no. Again, this likely reflects a tendency for procedures to be less formalized in small museums with fewer staff.

Are Electronic Records Addressed in the Institution's Emergency Plan?

The responses for whether electronic records are addressed in the institution's emergency plan were slightly lower than those for paper records, with 47% responding yes, 40% responding no, and 13% responding "other." Most of the "other" responses were based on not knowing the answer, and one respondent wrote: "Maybe. I'm not IT, so I can't answer." This indicates a lack of training, as well as the view that electronic records are solely the responsibility of IT, which discounts the fact that users managing electronic records well can make a significant difference.

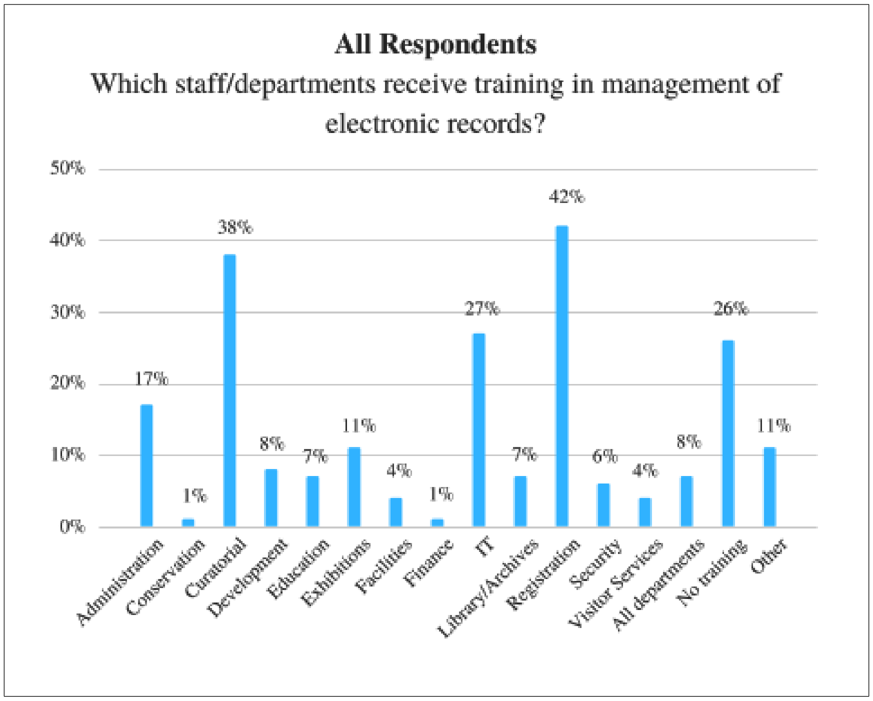


Small institutions were even less likely to have electronic records included in their emergency plan, with only 39% responding yes and 53% responding no.



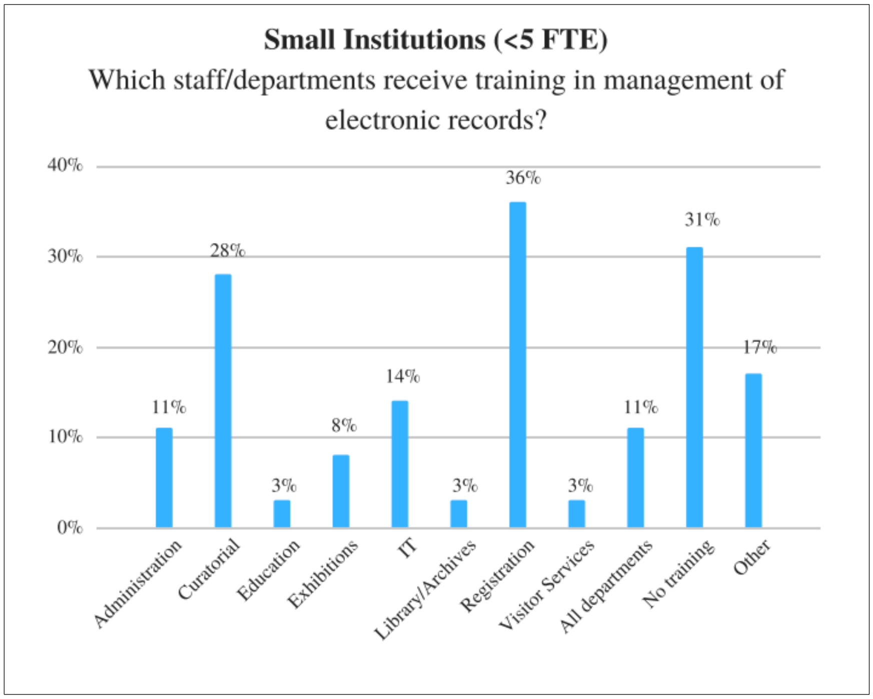
Who receives training on managing electronic records?

Finally, I was interested in which departments in an institution receive training on managing electronic records. 26% of respondents indicated that no training at all was given. Only 8% said that all departments received training.



Registration and curatorial (42% and 38% respectively) were the departments that were entered most frequently, followed by IT at 27% and administration at 17%. This shows that overall there is a lack of sufficient training in electronic records management in museums, and the training that exists focuses mostly on collections-related departments rather than including the organization as a whole.

Small museums followed much the same trends on this question, although they were both more likely to have no training given (31% vs. 26% in the overall group) and more likely to have training given to all departments (11% vs. 8% overall.) This is likely because a smaller staff tends to require individual staff members to wear many hats, so if training is offered it is more likely to be offered to all staff. Like in the overall group, registration and curatorial were the departments entered most frequently, again reflecting the strong focus on collection records.



The main takeaways from the survey are that museums are in need of more formalized policies and procedures with regard to records management, especially for the protection of vital records in both paper and electronic format. Information security needs to be addressed more thoroughly and training given to ensure that staff understand the impact they can have on maintaining information security. Finally, there is greater need to ensure that this type of training extends throughout the institution as a whole, rather than being overly focused on specific departments. While some departments may require more specialized or extensive training, a basic level of training throughout the organization can help to mitigate many of the issues discussed in chapter II.

Ultimately, these results show that many museums have significant gaps in the staff knowledge and institutional procedures required to manage electronic records well, which could result in vital records being lost. This likely stems from the rapid pace at which electronic records became widespread, and the fact that museums have historically focused their attention on collections records rather than the records of the institution as a whole. As records become more integrated in all aspects of museum operations, concentrating records management training and responsibilities primarily on the registration staff is no longer viable to ensure preservation of an institution's vital records. While this survey identified broad trends and areas where improvement is necessary, potential future studies might investigate in greater detail the extent to which the existing policies (in museums that already had them) address electronic records management issues. In addition, future researchers may be able to compare museums, which have established policies and training for all departments and those that do not, in order to assess outcomes.

Chapter IV

Best Practices: Protecting Vital Museum Records

It is clear that vital records in museums need to be secured and protected from disaster. Electronic records in particular face unique risks and vulnerabilities. However, they also offer additional options that can make disaster response and recovery easier as well. Electronic records have a significant advantage over paper records in the ease with which they can be copied and shared, which creates opportunities for more copies to be stored in more locations. However, as they are also vulnerable to different threats, they require electronic protective storage and an understanding of records-handling procedures on the part of staff. Clear policies and training of all staff who handle records are the key to protecting vital records in museums.

In order to protect vital records, museums must first identify what vital records they hold and where they are currently stored. It makes sense to integrate this into the emergency planning process. Ideally, this would be part of an overall records management program for the museum that establishes clear policies for records retention of all record types (not just vital records). However, completing a vital records survey as a separate process can still provide a way for small museums to make sure they are protecting their most important records even if there is not enough staff time or support for a broader records management program. A survey of vital records should gather information on what records series (groups or categories of records) the museum keeps, reference activity, location of records, existing methods of protection, software and version required to access electronic vital records, type of protection required, and anticipated cost of maintaining protection.[56] Once vital records have been identified, they can be

[56] ARMA International, *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records* (Overland Park, KS: ARMA International, 2010), 7.

assessed in order to set priorities for how soon they will need to be accessed after a disaster. Generally, three categories are used: vital records that are essential for emergency operations, vital records that are essential for the resumption and continuation of business after a disaster, and vital records that are essential for legal or audit purposes.[57] All of these categories need protection, but the method of protection can vary based on the needs for access, i. e. records that are needed for emergency operations must be accessible immediately, while those that are needed for legal or audit purposes do not need to be immediately accessible. Once the records have been identified and classified, a vital records schedule can be created listing each records series, where the records are located, and protection methods and instructions.[58] This should be made available to all staff with record-keeping responsibilities and reviewed periodically so that it is kept up to date. However, we must also recall the example of the Cleveland Art Museum's early records management program discussed in chapter I, which faltered because no one was designated as responsible for carrying it out. Even if the museum does not have a dedicated records manager, one member of the staff should be designated as responsible for the vital records program, so that other staff have a clear contact person if any questions or concerns arise.

The primary methods of vital records protection are dispersal and protective storage.[59] I would propose a combination of both to create an effective strategy for preserving museum vital records. Dispersal refers to the transfer of duplicate records to off-site locations.[60] Electronic records have an advantage in this regard as they are very easy and cost-effective to duplicate and disperse. In comparison, paper records are often transferred to another medium such as

[57] ARMA International, *Vital Records Programs,* 8.
[58] Ibid.
[59] Virginia A. Jones and Darlene Barber, *Emergency Management for Records and Information Programs* (Overland Park, KS: ARMA International, 2011), 42.
[60] Ibid.

microfilm or electronic media before dispersal in order to reduce their volume and limit the cost of storage at the dispersal location.[61] There are two types of dispersal: routine dispersal and designed dispersal. In routine dispersal "records are maintained in two or more locations—and possibly on more than one medium—as part of an existing business process."[62] While this type of dispersal is more easily applied in the private sector by larger companies with multiple offices, some museums with multiple locations may practice it as well. Smaller museums could establish partnerships with other institutions to house each other's duplicate records. However, both partners would need to be satisfied with the storage and security arrangements in each facility, and space is often at a premium in small museums. They would also need to invest time in upkeep—in order for routine dispersal to be sufficient for protecting vital records, care must be taken to keep the duplicate copies current and make sure they can be accessed when needed.[63]

The other method of dispersal, designed dispersal, is likely to be more appropriate for most museums. "Designed dispersal is a duplication procedure established as a routine business process in order to protect vital information."[64] Whereas routine dispersal relied on adapting existing business practices to protect vital information, designed dispersal involves establishing new practices specifically for that goal and therefore is likely to be more thorough and targeted at vital records. However, it also requires greater investment of staff time and resources, as it is not "piggy-backing" on processes that are already in place. The American Alliance of Museums recommends this type of dispersal in a reference guide on emergency planning: "As a risk management measure, it may be wise to make duplicates of important records and store them off

[61] ARMA International, *Vital Records Programs,* 15.
[62] Ibid., 14.
[63] Ibid., 14.
[64] Ibid., 14.

site."[65] Integrating this type of dispersal into the institution's emergency plan as suggested by AAM ensures that information about duplicate records is readily available in an emergency, and training about the vital records can be combined with training about emergency procedures.

Protective storage involves the use of storage methods to secure and protect records. Generally, this is through the use of fire-proof cabinets and other physical measures to protect records, and for the protection of vital records is often combined with similarly protected copies at an off-site location.[66] While these measures can protect physical media, there are also methods of electronic protective storage, such as electronic vaulting, data replication, mirroring, shadowing, migration, password protection and encryption.[67]

Mitigation of risks from disaster by incorporating vital records in the museum's emergency plan is a very important step to caring for vital records. However, that is only part of the puzzle. As we have seen, electronic records are subject to additional threats through malicious attacks. Therefore, information security must also be taken into account. Organizations should establish administrative, technical, and physical controls to protect information security.[68]

Administrative controls are the policies and guidelines that help ensure information is managed appropriately.[69] In particular, museums should establish information security policies that provide guidelines for how information security will be handled. "Policies will help to define and categorize information as an asset, inform the employees on their responsibilities to protect these important assets from unauthorized access, modification, disclosure, and

[65] American Alliance of Museums. *Alliance Reference Guide: Developing a Disaster Preparedness/Emergency Response Plan* (Washington, DC: American Alliance of Museums, 2012), accessed February 4, 2018, http://www.aam-us.org/docs/continuum/developing-a-disaster-plan-final.pdf.
[66] ARMA International, *Vital Records Programs*, 15
[67] Ibid.,16.
[68] Vacca, John R. *Managing Information Security*. (Waltham, MA: Syngress, 2014.), 11.
[69] Ibid, 11.

destruction, and how to respond and report to policy violations."[70] Policies can vary depending on the institutions' needs, but generally information security policies address IT access, passwords, e-mail usage, internet usage, and laptop usage.[71] As discussed in chapter III, many institutions lack a formal information security policy, or staff may not be aware of the policy. Establishing clear policies and training employees on how to carry out those policies is crucial to mitigating some of the human factor risks discussed in chapter II.

Technical controls are the hardware and software that control access to information systems, such as passwords, firewalls, and encryption.[72] These controls are important as they also help to mitigate human error and violations of the information policy and other administrative controls.[73] Technical controls are especially important as we become more interconnected and many files reside on networked computers, which opens up more opportunities for risk that technical controls try to address. Technical controls are associated with the "principle of least privilege" which "requires that an individual, program, or system process is not granted any more access privileges than are necessary to perform the task."[74] This is another way of mitigating risk by controlling access so that potential vulnerabilities are kept to a minimum. While responsibility for technical controls generally resides primarily with IT staff, it is important that the reasoning and importance behind these controls is communicated to all staff so that they understand the potential issues. For example, passwords are a type of technical

[70] Andress, Jason, and Mark Leary. *Building a Practical Information Security Program*. (Amsterdam [Netherlands]: Syngress, 2017), 63.
[71] Mooney, Tom. *Information Security A Practical Guide: Bridging the Gap Between IT and Management*. (Ely: IT Governance Publishing, 2015.), 108-110.
[72] Vacca, *Managing Information Security*, 12.
[73] Ibid.
[74] Ibid.

control, but it is important for staff to know how to create a strong password and how to properly handle passwords so they are not accidentally compromised.

Physical controls protect the physical environment in which the computer equipment is located, such as limiting access to server rooms to select staff.[75] They prevent theft or tampering with the physical media on which information is stored. Securing the area where computer equipment is stored is a key part of physical control, and may include using locks, guards, swipe cards or badges, video cameras, biometrics, and other measures.[76] Environmental concerns, such as maintaining stable power, protecting against extremes of temperature and humidity, and protecting against pests are also part of physical controls.[77] Fortunately, in the case of museums many physical controls are likely already in place for the purposes of securing collections storage areas and work areas where collections are used, but it is worth assessing whether that protection extends to records storage and IT infrastructure, and upgrading those areas if necessary.

Ultimately, each museum must tailor its strategies to its particular situation and records, but following these strategies can help ensure that vital records are protected from disasters, accidents, and malicious attacks. Integrating vital records into the emergency-planning process offers a natural opportunity to address these issues, especially if they have not previously been given much attention, particularly with regard to electronic records. While the specific technologies will continue to change and evolve, it is a clear trend that records and information are becoming more and more integral to every aspect of museum work. Therefore, it is important that records are seen as assets that are essential to carrying out the museum's mission, and that their protection merits serious consideration. The role of the museum's staff in protecting records

[75] Ibid.
[76] Jason Andress and Mark Leary, *Building a Practical Information Security Program* (Amsterdam: Syngress, 2017), 107-111.
[77] Ibid., 109-111

is the most important element in ensuring that the measures discussed in this chapter will have success. Implementing clear policies and providing adequate training to all staff who handle records is critical to this process.

Conclusion

Vital records are critical to the operations of a museum, and their preservation and security should be a high priority for any institution. In order to manage museum vital records effectively, proactive steps must be taken to ensure that policies and procedures are in place and all staff who handle records are properly trained. This is especially crucial for electronic records, which face unique threats and challenges and which must be actively managed at an early stage in their life cycle in order to ensure preservation.

Historically, museums have placed great emphasis on preserving collection records, while the institution’s other vital records often remained unaddressed. While collection records are undoubtedly among the most important records museums create, as technology becomes more integrated into all aspects of the museum, many other areas are now generating large amounts of electronic records, some of which are also vital to the museum’s operation. Going forward, museums are going to have to shift towards seeing vital records as an issue that affects the entire institution, and therefore ensuring that all staff have the knowledge and guidance to manage records effectively.

Bibliography

American Alliance of Museums. *Alliance Reference Guide: Developing a Disaster Preparedness/Emergency Response Plan*. Washington, DC: American Alliance of Museums, 2012. Accessed February 4, 2018. http://www.aam-us.org/docs/continuum/developing-a-disaster-plan-final.pdf.

ARMA International. *Glossary of Records Management and Information Governance Terms.* 5th ed. Overland Park, KS: ARMA International, 2016.

ARMA International. *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records.* Overland Park, KS: ARMA International, 2010.

British Broadcasting Corporation. "Ashmolean Museum Website Hackers Access Customer Details." BBC News. June 18, 2014. Accessed April 16, 2018. http://www.bbc.com/news/uk-england-oxfordshire-27909976.

Buck, Rebecca A., and Jean Allman Gilmore, ed. *Museum Registration Methods.* 5th ed. Washington, DC: The AAM Press, 2010.

"Business Methods in the Metropolitan Museum of Art: A Paper Read before the American Association of Museums in Boston, May 23, 1911." *The Metropolitan Museum of Art Bulletin* 6, no. 8 (1911): 169-70. Accessed January 5, 2018. https://www.jstor.org/stable/3252513.

Ciampa, Mark D. *Security Awareness: Applying Practical Security in Your World*. Boston: Cengage Learning, 2017.

Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Amsterdam: Elsevier Butterworth Heinemann, 2005.

Goode, George Brown. *Principles of Museum Administration.* Reprinted from the Annual Report of the Museums Association, 1895. York: Coultas & Volans, 1895.

Jones, Virginia A., and Darlene Barber. *Emergency Management for Records and Information Programs*. Overland Park, KS: ARMA International, 2011.

Kyrnin, Mark. "The Death of the Computer Optical Drive: Why Do Most New PCs Not Come with DVD or Blu-ray Drives?" Lifewire. Accessed April 07, 2018. https://www.lifewire.com/death-of-the-computer-optical-drive-832403.

Marty, Paul F., and Katherine Burton Jones, eds. *Museum Informatics: People, Information, and Technology in Museums*. New York: Taylor and Francis, 2012.

Mooney, Tom. *Information Security A Practical Guide: Bridging the Gap Between IT and Management*. Ely: IT Governance Publishing, 2015.

Prescott, D. R. 1997. "Debunking the Myth of Electronic Records Retention". *Inform* 11, no.10 (November 1997): 32-33. Accessed February 3, 2018. https://search.proquest.com/docview/217561177?accountid=13793.

Richardson, Ronny, and Max North. 2017. "Ransomware: Evolution, Mitigation and Prevention." *International Management Review* 13, no. 1 (January 2017): 10-21,101 Accessed February 11, 2018. https://search.proquest.com/docview/1881414570?accountid=13793.

Saffady, William. 2015. "Count the Cost: Quantifying Your Vital Records Risk". *The Information Management Journal.* 49, no. 1 (January/February 2015): 27-31. Accessed January 28, 2018. Academic Search Complete.

Schwartz, Candy, and Peter Hernon. *Records Management and the Library: Issues and Practices*. Norwood, NJ: Ablex, 1993.

Smallwood, Robert F. *Managing Electronic Records: Methods, Best Practices, and Technologies*. Hoboken, NJ: Wiley, 2013.

Smith, Kelvin. *Planning and Implementing Electronic Records Management: A Practical Guide*. London: Facet, 2007.

Stephens, David O. *Records Management: Making the Transition from Paper to Electronic*. Lenexa, KS: ARMA International, 2010.

Sward, F. L. “Business Records Management.” *The American Archivist* 29, no. 1 (1966): 69-74. Accessed January 2, 2018. https://www.jstor.org/stable/40290566.

US Government Accounting Office. *Electronic Records: Management and Preservation Pose Challenges: Statement of Linda D. Koontz, Director, Information Management Issues*. GAO-03-936T. Washington, DC: GAO, July 8, 2003. Accessed February 1 2018, https://www.gao.gov/new.items/d03936t.pdf.

Urban, Richard J. “Library Influence on Museum Information Work.” *Library Trends* 62, no. 3 (2014): 596-612. Accessed January 2, 2018. https://muse.jhu.edu/article/542832.

Vacca, John R. *Computer and Information Security Handbook*. Amsterdam: Morgan Kaufmann, 2013.

Vacca, John R. *Managing Information Security*. Waltham, MA: Syngress, 2014.

Wythe, Deborah. *Museum Archives: an Introduction*. Chicago: Society of American Archivists, 2004.