International Journal of Research in Library Science (IJRLS)
ISSN: 2455-104X
DOI: 10.26761/IJRLS.6.2.2020.1352
Volume 6, Issue 2 (July-December) 2020, Page: 245-253, Paper ID: IJRLS-1352
Received: 2 Nov. 2020 ; Accepted: 23 Dec. 2020 ; Published: 29 Dec. 2020

Information Security Measures in Digital Publications

Dr. Rajashekhar Kumbar

Librarian, Government First Grade College, Kapu, District Udupi - 574106, Karnataka, India

raju_kims@yahoo.com

ABSTRACT

Electronic security does not involve protecting the hardware or physical environment. This is about protecting the information. Recent growth in the publication and use of e-resources has focused worldwide attention on the growing issues and challenges of privacy, security, and the potential for fraud and deception. A theoretical study was conducted to review the literature available on these issues and challenges. The risks inherent in e-publications can be harnessed only through appropriate security measures and legal procedures that ensure their integrity and reliability. It was found that there is a need to enforce a strong security policy, especially when a malicious attack occurs. A systematic procedure should be followed, such as authentication, ensuring confidentiality, and the use of cryptography for effective security while disseminating information over an open system.

KEYWORDS: Information Security, Copyright, Digital Information Resources, and ISO.

1. INTRODUCTION

The invasion of digital media has been one of the biggest technological events of the last two decades in the entire range of everyday life. The easy transmission and manipulation of electronic publications constitutes a real threat for information creators and publishers such as news agencies, museums, libraries, artists, scientists, and authors of multimedia documents. Information Security is a major concern in electronic research. Copyright owners want to be compensated every time their work is used. Furthermore, they want to be sure that their works are not used in an improper way, for example, modified or edited without permission. Topical problems of electronic publications are how to secure information resources from attacks and threats, how to decide which information is valuable, which one is useless, how to assess the quality of the usable information, and finally choose the right information from its abundance (Muneer, 2010).

Electronic publications refer to all forms of electronic information, its storage, and communication, including electronic storage media (such as disks, diskettes, CD-ROMs, DVD's, server shares, public folders, websites and news services, and computer screens), content (such as files and documents, database records, multimedia clips, web pages, e-mail, voice mail, chat room and forum discussions, and news items), and electronic communications media

(such as data lines, modem lines, local, wide area, and broadband networks, but do not include telephone conversations.

Handling complex and difficult privacy and information security issues has moved to the top of the list of electronic publications in the library. However, there are often gaps in communication and coordination between privacy and information security. These gaps create more complexity and greater challenges in handling information resources. Good information security means providing accessibility to information resources to appropriate users while simultaneously protecting the confidentiality of information resources and minimizing vulnerabilities to attacks and threats. Good security practices are driven by eight constructs. The eight constructs capture security practices that contribute to highly secure information. They are:

1. Vulnerability: Potential for data and networks to be tampered with, attacked, or destroyed
2. Accessibility: Availability of data and networks to appropriate users
3. Confidentiality: Protection of confidential corporate data and privacy of data about individuals
4. Information Technology (IT) Resources for Security: IT Resources for supporting data and network security practices
5. Financial Resources for Security: Financial Resources for supporting data and network security practices
6. Business Strategy for Security: Business Strategy for setting the direction and agenda for data and network security practices
7. Security Policy and Procedures: Stated data and network security rules and procedures
8. Security Culture: Supporting environment for implementing data and network security practices in the business process stage and at every level within the organization (Nagaraju & Narasimha, 2010).

2. NEED FOR INFORMATION SECURITY

Currently, in the digital arena, libraries are increasingly reliant on computer technology. There is a need to preserve and guard electronic publications and confidential user records, protect the electronic infrastructure from misuse, and guard the confidentiality of the users as much as possible. Therefore, librarians are under pressure to take computer security and electronic publication stewardship seriously. This has reverberations everywhere, from a small public or academic library. Apart from issues involving user privacy, there are also important concerns regarding the protection of valuable electronic publications, user authentication, and general information security issues that must be considered with any publicly available access point in the digital realm. Unfortunately, the issues of information security are perennial discussions that need to be addressed. In this paper, the available literature on the issues and challenges of electronic publications related to privacy, security, and the potential for fraud and deception are reviewed.

3. WHAT IS ISO 17799?

ISO 17799 is an internationally recognized Information Security Management Standard, first published by the International Organization for Standardization, or ISO (www.iso.ch), in December 2000. ISO 17799 is high-level, broad in scope, and conceptual in nature. This approach can be applied across multiple types of enterprises and applications. It has also made the standard controversial among those who believe that standards should be more

precise. In spite of this controversy, ISO 17799 is the only "standard" devoted to Information Security Management in a field generally governed by "Guidelines" and "Best Practices."

ISO 17799 defines information as an asset that may exist in many forms and has value for an organization. The goal of information security is to suitably protect this asset to ensure business continuity, minimize business damage, and maximize the return on investments. As defined by ISO 17799, information security is characterized by the preservation of information as:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: ensuring that authorized users have access to information and associated assets when required.
- As a primary conceptual standard, ISO 17799 is not
- A technical standard
- Product or technology driven
- An equipment evaluation methodology such as the Common Criteria/ISO 15408 (www.commoncriteria.org), which deals with functional and assurance requirements of specific equipment
- Related to the "Generally Accepted System Security Principles," or GASSP (http://web.mit.edu/security/www/gassp1.html), which is a collection of security best practices
- Related to the five-part "Guidelines for the Management of IT Security", or GMITS/ ISO
- 13335, which provides a conceptual framework for managing IT security, ISO 17799 covers only the selection and management of information security controls.
- Require utilization of a Common Criteria Equipment Assurance Level (EAL)
- Incorporate GASSP guidelines
- Implement GMITS concepts (Carlson, 2001)

4. IMPORTANT ISSUES AND CHALLENGES OF INFORMATION SECURITY

In recent years, information security has received considerable attention. Despite increasing concerns about the use of electronic information resources, there are numerous issues and challenges related to information security. Some of these issues and challenges are discussed below:

4.1 Copyright

Electronic media presents new challenges for copyright holders. Copyrighted material converted into digital form can be copied perfectly without any damage or diminution in the quality of the original (Cairncross, 1997). Electronic copyright is an uncertain area, but the establishment of an easily understood legal framework is needed in the interests of publishers, users, and libraries. Although the Dearing Report (NCIHE, 1997) on higher education recommended that copyright law be amended to give teachers and researchers easier access to digitized documents for research and study, the government has since indicated that it does not intend to change the law at present. However, if progress is to be made in building functioning electronic libraries, it is vital to remove the uncertainty over the use of digital material. Publishers are naturally concerned that unregulated access to and 'seepage' of their machine-readable data over the Internet might affect the level of return on their investment in publications. They fear that their business will be threatened if permission is given to users to copy and then widely distribute materials

that they have invested in to create. Therefore, they wish to regulate the use of their information by erecting barriers to its storage and access of their information, which contrasts with users who want to download material, annotate it, and forward it freely to others. Libraries are caught in the middle of all this activity and have the task of 'imposing rules set down by the law which may bear no resemblance to the realities of fulfilling demands from staff and students' (Oppenheim, 1998) Librarians are used to dealing with the regulation of print copyright and they can act as honest brokers in the electronic environment, if they can convince publishers that they can create a controlled environment within their institutions that provides protection for rights holders.

4.2 Licensing

The usage of electronic publications is usually regulated by licensing agreement, whereby the supplier leases the data to the library and its 'authorized users' make use of it, subject to a set of conditions. For example, CD-ROM databases can either be licensed for single use at stand-alone workstations or for multiple uses on a CD-ROM network, with a significant price difference between the two. Licensing conditions may also be so complex that there is a need for a library to consult an institution's legal advisers on the terms of a license before it is signed.

There are several ways in which a supplier can regulate access to an electronically networked product. It can be by individual or institutional password, password plus IP source address, institutional IP source address alone, or institutional subnets. In the latter example, access to electronic publications would be restricted to network calls originating only from within the subscribing site, and so a user might only be able to access the electronic publications if they are physically within the institution and so within its network 'domain'. As higher education institutions move towards off-campus learning, which may be promoted to potential students as providing the same learning experience as on-campus courses, students will then expect the same access to networked electronic publications from both on and off campus. The discussion needs therefore to center more on 'group' or 'community' licenses, rather than simply 'site' licenses, as the physical location of the user is often not the key membership criteria. In the above example, access can be addressed by ensuring that off-campus students access electronic publications by first connecting to the campus network and then to electronic publications. If this is required, the library will need to convince the computer centre of the importance of the issue and negotiate with them to ensure that they support the local and national dial-up facilities are in place (http://www.u-net.net/services/janet/). However, some electronic publication providers allow only password access to their information, regardless of the origin of the network call. Although this method is easier to manage, it requires the library to organize the issuing of passwords and for the user to remember yet another ID and password. All of these access restrictions, which will inevitably vary between electronic publications, will have to be managed and mediated to the user by the library, and this constitutes a considerable management overhead and possible bar to use. It is also possible that each electronic publication could have separate license terms, and one of the fears of librarians is that they will have to negotiate different license agreements with, for example, journal publishers.

When 'authorized users' is defined as the staff and registered students of the institution, it can mean that access cannot be provided to external or 'walk-in' users of the library, unless it is specifically negotiated with the data supplier. Many libraries have actively marketed their services to the local business community, or they may have a science or research park on campus, where access to the university library is promoted as one of the benefits of

locating on the park. Therefore, a significant move into electronic information services will represent a decline in the information resources available to external users. This contrasts with the ability of external users to make unrestricted use of printed materials in a library once they have been granted access. However, even if the site license can be extended to such users, there is the problem of how to gain access to the database, as this will, in most cases, be via the campus network, which is usually only available to staff and registered students.

4.3 Authentication and Authorization

By taking out a license for electronic publications, a library has also taken responsibility for ensuring that the terms of the license are adhered to and that only authorized users access the data. For network resources, this may involve authenticating the user prior to authorizing them to have access. Authentication can be defined as the process whereby a network user establishes the right to an identity (or possibly multiple identities) and authorization is the process of determining whether a particular identity is permitted to access a resource. Libraries have observed that one of the major deterrents to the rapid and pervasive take-up of electronic information resources has been the variety of authentication and authorization mechanisms in use, and therefore, the number of user ids and passwords that have to be learned and remembered. The new service, ATHENS, is intended to provide a single sign-on with the same username and password to major electronic publications and provide a transferable model. ATHENS has been designed to meet the needs of both users by providing easy access to electronic publications and to protect the needs of the resource supplier by providing strong safeguards on the security of the data.

4.4 Archiving and Preservation

One of the central issues related to the licensing of networked electronic publications is whether the institution will have continued access to the back files of the data after the license has expired. With a print resource, a library presently retains the books and journals that it has purchased, and users of the library can access the back files of a printed journal, even though a current subscription may not be held. This contrasts with most licensing models for electronic resources, where there is no guarantee of continuing access to back files once the subscription has lapsed.

As libraries build up local collections of digital resources, they will have to address the issues of archiving and preserving the data locally. Research libraries and archives have taken on the responsibility for archiving and preserving selected printed material as part of their collection policy, and scholars can reasonably expect to access preserved scholarly material that was published in printed texts over the past four to five centuries. Scholars also need to be confident that the digital material produced today will be accessible for future generations, and the academic library community has now begun to address this responsibility. However, it must be remembered that digital data are simply a sequence of bits, and retrieving a bit stream requires a hardware device, such as a disk drive, and technology for reading the physical representation of the bits from the medium. It also requires a software program and operating system software to interpret the bit stream, as most files contain information that is meaningful solely to the software to run these programs. Therefore, there is a need to save programs that generate digital documents, as well as the system software to run those programs35. The speed of technological change is so fast that the past few years have been littered with obsolete technology and with information resources that are unreadable.

Digital preservation is beyond the ability of most libraries or publishers to act individually, though libraries need to move 'higher up the food chain' to ensure that they have an input at the data creation stage into the implications for long-term preservation. The strategic, methodological, and practical issues involved in the long-term preservation of digital information resources provide guidance for libraries in best practice for digital preservation. The guidelines include:

- Developing digital collection management policies that may ensure the long-term viability of any digital resources included in a collection;
- The demonstrator tests and promotes the technical and organizational feasibility of the chosen strategy for digital preservation.
- Methodological guidelines developed by the demonstrator projects providing guidance on how to preserve different classes of digital resources, including detailed advice about appropriate storage media, back-up strategies, and data formats.
- Analysis of the cost implications of digital preservation.

4.5 Digital Obsolescence

One of the most important challenges is long-term access. Digital technology is developing rapidly, and retrieval and playback technology can become obsolete in several years. When faster, more capable, and cheaper storage and processing devices are developed, the older version is almost immediately replaced. When software or decoding technology is abandoned or a hardware device is no longer in production, records created under the environment of such technologies are at great risk of loss, simply because they are no longer tangible. This process is known as digital obsolescence'. This challenge is exacerbated by a lack of established standards, protocols, and proven methods for preserving electronic publications.

4.6 Standards and Protocol Issues

In the field of information security, standards and protocols are primarily concerned with encoding, data formats, and representation schemes. In the real world, there are a number of limitations to relying on standards alone as an information security strategy. There are many areas in which no technical standards exist. Commonly, new types of media, new forms of representation, and other innovations precede the development of open or proprietary standards. In the absence of open standards for many aspects of digital objects, proprietary standards have become the de facto standard. Even where open standards exist, they may not be effective because a proprietary standard is technically superior to an open standard or because few or no vendors produce products that conform to the open standard (Anand, Keshava, & Gowda, 2010).

4.7 Migration of Electronic Publications

Migration involves some transformation of the original bye stream into new media. During this process, the byte stream may be corrupted by software bugs, mishandling of data, or mechanical failure of the input or output devices. Changes to the original byte steam may involve loss of information, loss of functionality, introduction of errors into the target files, or changes in the way the information is rendered to users.

4.8 Intellectual Property Rights (IPR)

Information security is dependent on a range of strategies, which have implications for IPR in those resources. The IPR issues in electronic publications are arguably more complex and significant than those in traditional media and, if not addressed, can impede or even prevent preservation activities. Consideration may need to be given to not only the content, but also any associated software. Simply copying digital materials onto another medium, encapsulating content and software for emulation, or migrating content to new hardware and software all involve activities that can infringe IPR unless statutory exemptions exist or specific permissions have been obtained from rights holders.

As both migration and emulation involve manipulation and changing presentation and functionality to some degree, important issues of principle and practice arise in negotiations. It is important to establish a dialogue with rights holders so that they are fully aware of these issues and the actions and rights required to ensure the security of selected items (Jayaprakash, M, & Chidananda, 2010).

4.9 Privacy Issues

Replication and intellectual property risks exist owing to the relative ease with which digital data can be copied, modified, and disseminated. An important industry concern is that digital content emulates digital music and circulates freely over the internet. Technology companies are positioned to insert themselves into digital publishing as electronic wholesalers, taking the place of distributors of traditional books. They provide protection from copying, along with software and services to store and transmit digital books in exchange for a percentage of revenue. These systems typically require the following four elements.

1. Authentication of transmissions and messages to determine whether the originator is authentic or whether the recipient is eligible to receive information.
2. Data integrity checks determine whether the data are unchanged from their original sources.
3. Certification that the sender has delivered the data and that the receiver has received it, with evidence of the sender's identity.
4. Confidentiality to ensure that information can be read only by authorized entities. In the quest for security, publishers may restrict the growth of the new market. Let us consider printed books as an example. The purchaser reads a book and passes it on to another reader or sells it to a used-bookstore, which then sells it again. Although the publisher does not receive revenue from subsequent uses or sales, the reader may develop an affinity for the author or subject, which may stimulate future sales. Magazines are routinely passed. Publications are often copied for distribution purposes. In effect, we have had the "Napsterization" of the publishing market since printing was invented. However, this practice might not have been upset. Readers of electronic publications who wish to save issues for further reference may not be able to do so (the archives of The New York Times and The Washington Post, for example, charge for access) and may find that electronic book readers do not have external storage.

From the publishers' and authors' point of view, there is a cause for concern. Stephen King's Riding the Bullet was sold exclusively on the Internet. After 48 hours, Riding the Bullet sold more than 500000 downloadable copies worldwide, at a cost of $ 2.50 per copy. Although many initial orders were delivered through free promotions, the

financial implications of King's foray in electronic books are still staggering. It took less than two days to sell 500000 copies without printing, shipping, storage, wholesalers, distribution middlemen, or other traditional publishers' costs. However, within 48 h, pirated copies were present in the network.

Periodical publishers have an interesting problem with regard to digital rights management, and that is why they want to protect their content, but advertising rates in periodicals is in large part based on "pass along" copies. For example, most ad rates for large consumer publications are premised on the assumption that a single copy is passed on to five other people. If you secure a digital version of that publication, you will ensure that someone pays for it, but you will also prevent you from passing it along. How do you determine your advertising rate?

RECOMMENDATIONS FOR THE EFFECTIVE INFORMATION SECURITY

- Reliability: The system must routinely capture all electronic publications, which are part of it, and organize them in accordance with the nature of the requirements, protect them from unauthorized changes or disposition, and be a primary source of information about documented transactions. Electronic publications must be accessible and tied to metadata.
- Integrity: To ensure that electronic publications are not destroyed, altered, removed, or accessed by unauthorized party controls, such as access monitoring, user verification, authorized destruction, and security, must be implemented.
- Compliance: The system should be managed in accordance with the expectations of the organization and the users, which it is a part of, and comply with their needs and regulations.
- Comprehensive: The system should cover the entire organization that it serves.
- Systematic: Electronic publications should be created, maintained, and managed systematically. To do so, a documented policy is needed, spelling out methods and detailing who carries responsibility for different functions.

CONCLUSION

Information security is everybody's responsibility. Everyone must be aware of the potential risks involved in data and information security. However, security and privacy issues still tend to focus on risks from troubled users, theft, and censorship. When information security is addressed, it may be from the perspective of corporate information security management rather than the library environment. However, currently, information security is often underappreciated in libraries. Effective development and utilization of online learning content will require flexible and expressive information security solutions. The challenge, therefore, is to fund effective mechanisms for managing online learning content and foster the collaborative development of information security solutions for electronic publications. It is recommended that steps be taken in all libraries to assess and minimize information security risks.

REFERENCES

[1] Anand, D., Keshava, & Gowda, M. (2010). Digital Preservation: Issues and challenges. *KKBNET 2010* (pp. 80-84). Mangalore: National Institute of Technology Karnataka, Surthakal.

[2] Cairncross, F. (1997). *The death of distance: how the communications revolution will change our lives.* USA: Orion Business Books.

[3] Carlson, T. (2001). *Information Security Management: Understanding ISO 17799.* USA: Lucent Technologies Worldwide Services.

http://www.u-net.net/services/janet/ . (n.d.). Retrieved December 18, 2011, from Information Security: http://www.u-net.net/services/janet/

[4] Jayaprakash, M, B. M., & Chidananda, S. (2010). Preservation strategies in digital era. *KKBNET 2010* (pp. 395-397). Mangalore: National Institute of Technology Karnataka, Surathkal.

[5] Muneer, S. M. (2010). Security for digital resources. In S. S. Rao (Ed.), *Trends and challenges in management and corporate libraries in digital era* (pp. 392-395). Secunderabad: Allied Publishers Private Limited.

[6] Nagaraju, & Narasimha, C. (2010). Planning for security of information resources in digital era. In S. S. Rao (Ed.), *Trends and challenges in management and corporate libraries in digital era* (pp. 385-387). Secunderabad: Allied Publishers Private Ltd.

[7] NCIHE. (1997). *National Committee of Inquiry into Higher Education.* London: HMSO.

Oppenheim, C. (1998). *A balance in electronic copyright law.* London: The times higher.
