Cyber Risk Assessment Principles for Modern Digital Museums

Todor Todorov[1, 2][0000-0002-2443-4618], Shpend Lutfiu[2][0000-0002-2745-6484]

[1] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
[2] St. Cyril and St. Methodius University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria
t.todorov@ts.uni-vt.bg, shpendlutfiu@gmail.com

Abstract. Modern museums as well as other sectors that have their activity exposed to the internet process digital data. The digitalization of museums and other institutions that promote cultural heritage has gained momentum in recent years, especially during the COVID-19 pandemic, when their activities were completely closed to the public. Cybersecurity is based on preventive methods applied to maintain the confidentiality, integrity and availability of digital data and services provided. In the paper is presented an analysis of the principles and standards for the risk management of modern digital museums. The paper analyses the principles risk management and compliance requirements needed to assess the risk of modern digital museums, based on which institutions dealing with cultural heritage will be able to decide on the investments necessary for protection of their technologies and services they provide.

Keywords: Digital Data, Cyber Security, Risk Assessment, Modern Museums.

1 Introduction

Modern digital museums and cultural heritage institutions in general are increasingly orienting their activities towards the use of information technology in the working process (Beagrie, Charlesworth, & Mill, 2014), (White paper UK Museum Sector, n.d.), (Paneva-Marinova, Stoikov, Pavlova, & Luchev, 2019). This was accelerated especially during the COVID-19 pandemic period becoming more necessary than ever before (Noehrer, Gilmore, Jay, & Yehudi , 2021), (Digital Skills, 2020), (Donaldson & Bell, 2019). Information and communication technology teams responsible for digital services in the modern digital museum sector must seriously address vulnerabilities, critical data and assets, engaging in the establishment of risk assessment and management procedures. These procedures are based on the key concepts of data security known as a CIA triad (shown on Figure 1) and constitute the basic standard for assessing and managing the security in any organization. Assets, digital data, technologies, and online activities performed by modern digital museums are almost similar to most organisations and sectors, and the aim of this paper is to addresses issues related to procedures for analysing the risks that may be encountered in cyberspace.

Digital Presentation and Preservation of Cultural and Scientific Heritage. Conference Proceedings. Vol. 12, Sofia, Bulgaria: Institute of Mathematics and Informatics – BAS, 2022. ISSN: 1314-4006, eISSN: 2535-0366

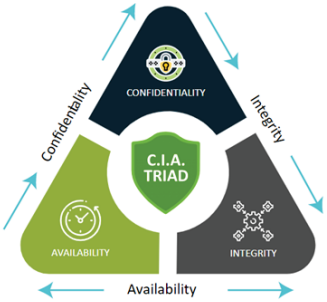

Fig. 1. CIA Triad (CIA TRIAD, 2021)

2 Cyber Risk Assessment Principles

The main purpose of risk assessment and management is to help strategic planning in responsible and ethical manner. On Figure 2 is presented the risk management cycle.

Fig. 2. Risk management cycle (Risk assessment, n.d.)

Organizations should develop the plan according to the steps of the risk management cycle. In Table 1 are summarized the general steps for developing risk management plan based on well-known standards and frameworks.

Table 1. Cybersecurity risk management plan (Tunggal, 2022).

Step	Description
Identify the most critical assets	Determining which assets are critical and most likely to be target by cyber criminals. This may include computers, networks, computer systems, application's, protocols, and digital data.
Assess Cybersecurity Risks	Steps to be taken in this phase starts with naming all assets and prioritizing their importance, identifying all threats and vulnerabilities, determining the like hood of the threat event occurring and analysing impact of the potential threats consequences

Cybersecurity Risk Mitigation Measures	Technological risk mitigation measures include encryption, firewalls, threat hunting software, and engaging automation for increased system efficiency.
Ongoing Monitoring	Ongoing monitoring of regular changes in IT systems and regulations, vendor risks, and internal users habits.

3 Risk Assessment Approaches

Cybersecurity risk management approaches should be based on one of the two most popular techniques known as bottom-up and top-down approaches.

Bottom-up approach typically describes cyber risk in terms of individual components, assessing the threat's that components face, vulnerabilities and consequences that may occur if the component is compromised. The top-down approach in other hand is focused on the whole system, rather than individual components of the system. Table 2 gives an example of the risk assessment. The basic risk assessment involves three factors described in the formula (1):

$$Risk = Asset * Threat * Vulnerability \quad (1)$$

Table 2. Risk assessment.

Assets	**Vulnerability**	**Threat**	**Severity**	**Solution**
Servers unavailable 3 hours (website, email etc.)	Air conditioning system is old	Overheating in the servers room	High	Buy new air conditioner (cost)
Web site unavailable	Firewall has proper configuration with a good DDoS mitigation	Web site will be unavailable	Medium	Monitor firewall
Natural disaster – flooding	Server room in high flour	All services unavailable	Low	No action needed
All files on the file share servers unavailable	Permissions are configured properly. Backups are taken regularly	Critical data will be lost, but could be restored from backups	Low	Continuously monitoring permeations changes, user privileges and backups

3.1 Bottom-Up Approach

This approach of risk assessment is focused on system components.

Elements of risk. These elements are described as: impact, vulnerability and threat. Impact is consequence of risk being occurred and usually the common way to assess is

in terms of confidentiality, integrity and availability. Vulnerability is weakness in the component being assessed that would enable an impact to be realized. While threat is individual or group of circumstances which cause the given impact.

Prioritizing risk. After the individual components where assessed, combined and the risk list was created, risks can be prioritized based one the concerns they may cause. Some standards communicate risk prioritization on the quantitative labels for description the impact level as *"likelihood"*, *"low", "medium"* and *"high"*.

3.2 Top-Down Approach

This approach for cybersecurity risk analysis is based on identifying risk which occurs from the interaction of all system components. On Table 3 are presented some related methods and frameworks.

Table 3. Top-down approach risk management methods and frameworks.

Method/Framework	Description
STAMP (Systems-Theoretic Accident Model and Process) (Leveson, 2020)	STAMP collection of techniques can be used for modelling the causes of cyber security incidents.
TOGAF (The Open Group Architectural Framework) (TOGAF Standard, n.d.)	This framework is based on an iterative process model at various levels across the organization's. Supports both risk assessment approaches.
(SABSA, n.d.)	This framework focuses on how organization generate value for stakeholders and goes down through number of business architectures levels

4 Risk Assessment Approaches

Cyber risk assessment is recommended to cover the whole IT infrastructure used by cultural heritage organizations. Applies to all hardware devices, system software and applications that are within the scope of assessment and meet the following criteria:

- Can accept connections from external untrusted hosts
- Can initiate communication with external untrusted hosts
- Can control the data flow for incoming and outgoing internet traffic

Requirements are specified under the five technical control objectives, as well as measures to be taken in order to follow essential standards specification, described in Table 4.

Table 4. Technical control objectives and essential security measures.

Technical control	Objective	Essential security measures
Firewall devices and applications	Only safe and important network services have access to the Internet	• block unauthenticated inbound connections • inbound firewall rules are approved and documented • remove or disable unnecessary firewall rules when they are no longer needed • use a software firewall on devices which are used on untrusted networks
Equipment, systems and applications configuration	Ensure that equipment's, systems and applications are configured properly in order to reduce the vulnerabilities and provide only necessary services	• remove and disable unnecessary user accounts, change default/week passwords • remove unnecessary software • disable any attempt which allows file execution without user authorization • authentication of users before allowing access to organizational data or services • ensure appropriate device locking controls
Access control	Ensure user accounts are as-signed to authorized individuals only, provide access to only those applications, computers and networks actually required for the user to perform their role	• user account creation and approval process • authenticate users before granting access to applications or devices • disable user accounts when no longer required • implement MFA, where available • use separate accounts to perform administrative activities only • remove or disable special access privileges when no longer required
Malware Protection	Restrict execution of known malware and untrusted software, to prevent harmful code execution	• Antivirus software must be kept up to date, with • signature files updated at least daily • scan files automatically • scan web pages automatically when they are accessed through a web browser • scan web pages automatically when they are accessed through a web browser • Application allow listing (only approved applications allowed to be executed on the devices) • code of unknown origin must be evaluated within a sandbox first

Security updates	Devices and software are not vulnerable to known security issues	• Ensure that all software's are licensed and supported from vendor • remove software when they become unsupported from vendor • enable automatic update

5 Conclusions

In the paper are introduced techniques for cybersecurity risk management. All the techniques are advised to be used when performing the risk assessment. When doing the assessment, the focus should be on people (board, staff, users, visitors, volunteers and patrons), assets (actual property, buildings, artefacts, library and archival materials and equipment), income (revenue sources from a variety of sources), and community perception (officials, relevant associations, other cultural organizations, and the general public). The paper analyses the need for any organization, including modern digital museums, to assess the risk that can come from cyberspace. Some principles related to risk assessment and management are presented.

References

Beagrie, N., Charlesworth, A., & Mill, P. (2014). *Cloud Storage*. Retrieved June 11, 2022, from Cloud Storage and Digital Preservation: https://cdn.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf

Bogdanova, G., Sabev, N., Tomov, Z., & Ekmekci, M. (2021). Physical and Digital Accessibility in Museums in the New Reality. *ISMSIT*, (pp. 404-408).

CIA TRIAD. (2021). Retrieved June 11, 2022, from https://websitesecuritystore.com/blog/what-is-the-cia-triad/

Digital Skills. (2020). Retrieved June 11, 2022, from Digital Skills for Heritage: Online Privacy and Security: https://www.heritagefund.org.uk/sites/default/files/media/attachments/Online%20privacy%20and%20security.pd

Donaldson, D., & Bell, L. (2019). Security, Archivists, and Digital Collections. *Journal of Archival Organization, 15*, 1-19. doi:10.1080/15332748.2019.1609311

Leveson, N. (2020). Safety and Security Are Two Sides of the Same Coin. In *SpringerBriefs in Applied Sciences and Technology*. Springer, Cham. doi:10.1007/978-3-030-47229-0_3

Noehrer, L., Gilmore, A., Jay, C., & Yehudi , Y. (2021). The impact of COVID-19 on digital data practices in museums and art galleries in the UK and the US. *Humanit Soc Sci Commun, 8*.

Paneva-Marinova, D., Stoikov, J., Pavlova, L., Luchev, D. (2019). System Architecture and Intelligent Data Curation of Virtual Museum for Ancient History. *SPIIRAS Proceedings, 18(2)* , 444-470. doi:10.15622/sp.18.2.444-470

Risk assessment. (n.d.). Retrieved June 11, 2022, from https://fim.edu.rs/en/the-act-on-risk-assessment-is-a-legal-obligation-of-companies/
SABSA. (n.d.). Retrieved June 11, 2022, from https://sabsa.org/
TOGAF Standard. (n.d.). Retrieved June 11, 2022, from https://www.opengroup.org/togaf
Tunggal, A. (2022). *Cybersecurity Risk Assessment*. Retrieved June 11, 2022, from https://www.upguard.com/blog/cyber-security-risk-assessment
White paper UK Museum Sector. (n.d.). Retrieved June 11, 2022, from https://www.cisco.com/c/dam/global/en_uk/solutions/digital-transformation/museums-culture/pdfs/Cisco-white-paper-UK-Museum-Sector-Embracing-Digitisation.pdf

Received: June 12, 2022
Reviewed: July 01, 2022
Finally Accepted: July 13, 2022