American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-13, Issue-9, pp-24-27
www.ajer.org
Research Paper Open Access

Assessment of the Practices of Cyber-Security in the Three Phases of Data in an Organization

Olasupo Olanrewaju Fatukasi[a] and Adegbenro Sunday Ajani[b]
[a]*United States Department of Agriculture*
[b]*Department of Physics and Materials Science, Faculty of Pure and Applied Science, Kwara State University, P.M.B 1530, Malete Ilorin, Nigeria*
[a]*supofat@yahoo.com*
[b]*adegbenro.ajani@kwasu.edu.ng*

Abstract
This article focuses on data transition, protection and stages involved in data movement for organizations. The continuous dependence on digital data has necessitated the importance of robust cyber-security measures within organizations. Virtually all sectors of life today are confronted with the threat of Cyber security, and the system architect must have the ability to integrate security features and functions as integral elements of a system. The assessment of procedures and practices for protecting data at rest, data in transit and data in use are discussed in this article. The investigation suggests that a dynamic approach, integrated policy, up-to-date technology, and staff training, are the essential measures for safeguarding organizational data throughout its life-cycle.

Date of Submission: 13-09-2024 Date of acceptance: 27-09-2024

I. Introduction

Data security is the procedure of protecting digital information all through its life-cycle to safeguard it from being corrupt, hacked, or from unapproved access. Data Security entails software, hardware storage devices, and user devices, administrative controls; and organizations' procedure and policies.

Data security utilizes technological tools that enhance visibility of a company's information and how it is being deployed. These tools can secure data by procedures such as data masking, encryption, and redaction of important information. The process also assists organizations slim-fit their auditing parameters and comply with increasingly sensitive data protection regulations. (Snyder *et al*, 2015)

A strong data security management and strategy procedure helps an organization to protect its sensitive information against cyber attacks. It drastically reduces the human error and threats within the insiders, that constitute the cause of data threats mostly. (Neuman *et al*, 2005).

Data Security also means the state of being free from information damage, threat or corruption. As a cyber-security analyst, the practices of safeguarding digital information from unwanted access, illegal entry, corruption or theft should not be trivialized, from the way data is being preserved and secured in an organization. Organizations are under obligation legally to protect customers and users information from being stolen or ending up in the wrong destination. (NIST, 2018).

II. Three Stages of Data Movement in an Organization

There are three (3) basic sections of data movement in an organization which are Data in motion, Data at rest and Data in use, and they all require protection as shown in figure 1.

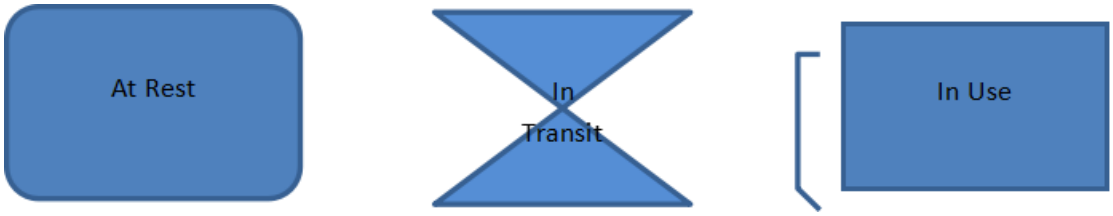

Figure 1: The Three Stages of Data

(i) Data in motion: This refers also to Data in Transit and it is the data that is actively traversing from one location to another. It can be moving across the internet or within a private network. It takes place each time an information is being uploaded within an organization or to a partner organization site, or when an information is being saved to a USB pen drive. (Hershey, 2012). There are various steps in which data in motion can be secured, which are;

· Identifying and classifying the data types: Numerous data types can be available within an organization such as personal identifiable data (PID), financial records as so on. The starting point to deploying data in motion security is to identify the form of data in existence within the organization's information reservoirs and consistently track all newly gathered data also.

· Define the strategies for data protection and conduction: after all the data is grouped, instructions handling have to be associated with each type of information with respect to the amount of required privacy.

· Impose stringent measures on data transfer: As a precaution control, it is imperative to permit data transfer out of the organization only when required. This is because some businesses' critical information cannot be transferred through work-stream collaboration platforms, public network and cloud storage service. Users mostly convey such information in a variety of peripheral devices. Therefore, organizations should enforce restrictions of device transfer based on file details and data size in motion so that only information necessary for the task at hand is extracted by secured users.

· Implement real time tracing of all data in motion: Whenever files are to be elicited from the organization vaults, all details concerning the operation should be documented for maximum visibility into how the information shall be used and for whatever purpose(s). These details should contain the real location of files, destination at which the data in motion will eventually be deposited, the user performing the transfer, the device used and the computer system involved.

· Security of data in motion also can be executed through device control plus.

(ii) Data at rest: To secure data at rest, the following procedures are required:

· Identify and locate data: To adequately secure data at rest, organization should know which data is highly sensitive such as business information, personal information and classified data.

· Classify data: Methods of data classification differ from one organization to another. It is quite necessary that diverse commercial sector leaders assist in ranking and assessing which data and applications are rated most crucial from market continuation prospect.

· Embrace data encryption: There are different ways of getting around performance matters such as the selective encryption of database fields, rows and columns versus encrypting all information whether highly sensitive or not.

· Train users: Employees who have access to business sensitive data must understand the gravity of protecting data at rest to prevent loss of information.

(iii) Data in use: These are data that are presently going through update, processed, erased, accessed or read by a computer. This kind of information is not being stored passively but is actively moving through parts of a network infrastructure. Examples are files stored in RAM database. Due to data in use being directly accessible by one or more users, data in this state is vulnerable to attack and it is important to secure data in use. Common practices for securing data in use involve:

· Reporting and tracking information access to detect malicious activity and potential attacks.

· Strict access control and endpoint security management with authentication control in place.

· Non-disclosure agreements (NDA) for stakeholders employees.

III. Methods of Data Movement Security

The following gradual procedures are employed for protecting the stages of data movement in an organization and they are described out in phases;

Phase I for Data at Rest

End-point Data Securing: This intends to limit the user's ability on only software installation and modify security settings.

Host Encryption: Thus ensures the hard disks are well encrypted on all the entire PCs, networks, servers, and computers.
Mobile Device Protection: It ensures all mobile devices are well pass-worded together with remote facilities.
Network Storage: It classifies information that are sensitive on a need to know basis.
Physical Media Access: This intends to Prevent copying of vital data to unapproved devices.
Safe Disposal: This deals with usage of data wiping software on old storage devices before safely disposing them.

Phase II for Data in Transit
Border Security: This security ensures unencrypted important data does not leave your covens.
Data Movement Monitor with Threats Identification: This monitors network traffic and flags unapproved data transfers.
Internet Access Control: IAC prevents users from opening unapproved websites to minimize the risks of data theft through social media.
Third Parties Exchange: It allows all third party exchanges to take place in a well secure premise on a case by case basis.
Instant Messaging (IM): It prevents file transfer of instant message applications.
Remote access: It allows remote access to the corporate network as the only secure conditions.
Phase III for Data in Use
User Monitoring: It monitors the activities of privileged users who have access to important information.
Usage Monitoring:This monitors the usage of important data to flag inappropriate usage.
Data Anonymizer: This anonymizes sensitive information when it is not in use.
Test Data: It gives anonymity of data before testing it, once it is not in required format.
Export Control: This controls the capabilities of the user to copy, paste or print critical information from unauthorized sections.

IV. Benefits of Data Movement Security

In a more simpler way, data movement security is more convenient to define by considering the advantages, which are here explained in details as follows:

Keeps your information safe from theft: Through adopting a mindset focused on data security and implementing the appropriate set of tools, one ensures important data does not enter or fall into the wrong hand. Sensitive information may include customer payment information, hospital records data, and identification information, to mention a few. With a data security agenda created to meet the specified requirements of the organization, this information stays protected and very secure.

Keeps your reputation clean: By the way transactions between people and your organization, they keep their sensitive information in your custody, and a data protection measure helps you to deploy the security they require. The reward of this will be an impressive reputation and integrity among partners, clients, and the business world in general.

Gives you a competitive edge: Among competitors in many industries, data breaches are common, once you can make a data secure, you set yourself apart from these numerous competitors, which may be competing to do the exact thing you do.

Saves on support and development costs: If you deploy a data protection mechanism early enough in the developmental process, you will minimize cost on resources for designing and deploying patches or fixing coding issues down the line.

V. Conclusion

The assessment of the practices of cyber-security in the three phases of data in an organization reveals that vulnerabilities are inherent at each stage. Organizations therefore must employ an holistic cyber-security strategy that addresses these vulnerabilities with appropriate policies, technologies, and staff development. By fostering a culture of security awareness and implementing robust security measures, organizations can better protect their data and mitigate the risks associated with cyber threats.

In conclusion, all the three stages of data movement in an organization require security. Organizations are legally obliged to secure customers' and users' information from being corrupt, stolen, lost or end up in the mischievous hands.

References

[1]. Verizon Enterprise Services (2017) Data Breach Investigations Report (DBIR). http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/. Accessed 30 May 2017
[2]. Veris Community (2014) VERIS framework. http://veriscommunity.net/veris-overview.html. Accessed 31 May 2017
[3]. Whitmore JJ. A method for designing secure solutions. IBM Syst J. 2001;40(3):747–768. doi: 10.1147/sj.403.0747. [CrossRef] [Google Scholar]
[4]. Hershey P, Silo C (2012) Procedure for detection of and response to distributed denial of service cyber attacks on complex enterprise systems. In Proceedings of 6th Annual International Systems Conference, Vancouver, 19–22 March 2012, p 85–90
[5]. NIST Computer Security Division (2006) Guide for developing security plans for federal information systems, NIST SP 800-18. rev 1. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf. Accessed 31 My 2017
[6]. NIST Computer Security Division (2006) Minimum security requirements for federal information and information systems, FIPS 200. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf. Accessed 31 May 2017
[7]. Snyder D, et al. Improving the cybersecurity of U.S. air force military systems throughout their life cycles. Santa Monica, CA: Rand Corporation Research Report; 2015. [Google Scholar]
[8]. SANS (2016) The CIS critical security controls for effective cyber defense ver 6.1. https://www.sans.org/critical-security-controls, http://www.tenable.com/solutions/council-on-cybersecurity-critical-security-controls. Accessed 30 May 2017
[9]. NIST Computer Security Division (2012) Guide for conducting risk assessments, SP 800-30. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Accessed 31 May 2017
[10]. Microsoft (2014) Threat modeling tool. https://www.microsoft.com/en-us/download/details.aspx?id=42518. Accessed 31 May 2017
[11]. MITRE Corp (2017) Common weakness enumeration. https://cwe.mitre.org. Accessed 31 May 2017
[12]. Chew E, et al. Performance measurement guide for information security, NIST SP 800-55. Gaithersburg: National Institute for Standards and Technology; 2008. [Google Scholar]
[13]. Bowen P, et al. Information security handbook: a guide for managers, NIST SP 800-100. Gaithersburg: National Institute for Standards and Technology; 2006. [Google Scholar]
[14]. Rozanski N, Woods E. Software systems architecture: working with stakeholders using viewpoints and perspectives. New York: Addison-Wesley; 2005. [Google Scholar]
[15]. Kindervag J. Market overview: network segmentation gateways, Q4 2013. Cambridge: Forrester Research; 2013. [Google Scholar]
[16]. Jones R, Horowitz B. A system-aware cyber security architecture. Syst Eng. 2012;15(2):225–240. doi: 10.1002/sys.21206. [CrossRef] [Google Scholar]
[17]. Trusted Computing Group (2014) TPM library specification. https://trustedcomputinggroup.org/tpm-library-specification/. Accessed 31 May 2017
[18]. Neuman C, et al. (2005) The Kerberos network authentication service (V5). https://tools.ietf.org/html/rfc4120. Accessed 31 May 2017
[19]. DISA . Determining the appropriate evaluation assurance level for COTS cybersecurity and cybersecurity-enable products (white paper) Ft Meade: Defense Information Systems Agency; 2004. [Google Scholar]
[20]. Yang K (2016) A ‘demonically clever’ backdoor. Michigan Engineer, Fall 2016
[21]. Cloud Security Alliance (2017) Cloud security research reports (multiple). https://cloudsecurityalliance.org/. Accessed 31 May 2017In conclusion, all the three stages of data movement in an organization require security. Organizations are legally obliged to secure customers’ and users’ information from being corrupt, stolen, lost or end up in the mischievous hands.
[22]. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
[23]. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
[24]. ISO/IEC 27001. (2013). Information Technology — Security Techniques — Information Security Management Systems — Requirements. International Organization for Standardization.