Evaluation of Data Security Methods

Danny A. Mase

"If you can measure it, you can improve it" – Lord Kelvin

Abstract

We are living in an age of data where the information stored on computerized systems is our most valuable asset. This study emphasizes the importance of applicable regulations, standards, and frameworks that impact organizational security posture and related domains. It also provides a primer on basic data security themes to inform readers of the ever-changing IT threat landscape, the current state of security regarding data and technology, and the ongoing cybersecurity efforts in information security management.

In an effort to develop strong cyber resilience, the primary objective of this study is to identify and evaluate best practice for the security of data stored on information systems. The Evaluation of Data Security Methods project will identify the top three most effective threats and vulnerabilities to information systems and information systems security, to provide the building blocks required for a comprehensive, quantifiable assessment into increasing organizational security posture and reducing security risks.

Introduction

Cyber Receiver Inc. has selected Danny A. Mase as the Project Manager for the Evaluation of Data Security Methods (EDSM) project. At Cyber Receiver, we believe that cyberspace can be secure and resilient. This project will result in the development of a data security effort that supports Cyber Receiver's strategy of providing progressive cybersecurity to clients that will enhance the overall performance of information systems security. While a number of proposed risk frameworks are currently available, Cyber Receiver's dedicated project team can develop a solution far superior to the local technology currently available. Cybersecurity fundamentals deal with the protection of digital assets. The primary objective of this study is to identify and evaluate best practices for the security of digital information stored on information systems.

Tasks	Description
	Identify threat and vulnerability
Step 0:	Assess the Asset Value (AV).
Step 1:	Assess the Single Loss Expectancy (SLE) and Exposure Factor (EF)
	Formula: SLE = EF * AV
Step 2:	Assess the Annualized Loss Expectancy (ALE).
	Formula: ALE = SLE * ARO
Step 3:	Asses the Annulized Rate of Occurrence (ARO)
	Formula: ARO = 0.0822 (1 month) * 12 (1 year)
Step 4:	Strategy for risk responding.
Step 5:	Countermeasures (optional)

Research Design & Data Collection

For this experiment, a Quantitative Risk Assessment (QRA) is performed that should not be confused with quantitative risk analysis based primarily on numeric values. The QRA is conducted by assigning values to the company's most valuable assets. The development of the EDSM project risk register is part of the risk identification process. During the QRA process, the risks are documented with a unique identification number, timestamp, detailed description, probability of the risk occurring, impact to the project, and the criticality of the risk to the project if the risk occurs. Other elements to consider are preventive actions, contingency action, risk ownership, and the status of the risk. The goal of QRA is to be cost-effective. To answer the research question, the steps described in Figure 1 were conducted.

Results

The identified risks were quantified to enable the project to develop effective mitigation strategies for the risks, or to include appropriate contingencies in the project estimate. The results for the project QRA are presented in Table 1 below:

Table 1. Quantitative Risk Assessment (QRA)I.

Unique-ID	Risk	Asset	AV	EF	SLE	ALE	ARO	CIA Triad Affected
1-EDSM-CR-1	Outdated Servers	Data Breach, Critical Infrastructure, Valuable Information (PII, PHI), Military Secrets	$200,000	1	$200,000	$200,000	1	Confidentiality, Integrity, and Availability
1-EDSM-CR-2	Malware/Ransomware	Digital Information, Proprietary, Critical, Data Leakage	$100,000	0.5	$50,000	$600,000	12	Confidentiality, Integrity, and Availability
1-EDSM-CR-3	Internet of Things (IoT)	Critical Infrastructure, Data Breach, Digital Information Unavailable	$100,000	0.7	$70,000	$420,000	6	Confidentiality, Integrity, and Availability

Uniq-ID	Date	Desc.	Category	Probability	Impact	Criticality	Preventive Action	Contingent Actions	Owner	Status
1-EDSM-CR-1	10/2/2021	Outdated Servers	Equipment	VH	VH	VH	Replace everything	Contact manufacture	Stakeholder	Close
1-EDSM-CR-2	10/3/2021	Malware/Third-Party	Partnership	H	VH	H	Policy	Seek Legal	Organization	Close
1-EDSM-CR-3	10/5/2021	Internet of Things (IoT)	Organization	VH	VH	VH	Policy	Compliance	Organization	Close

Chart 1. *Akamai Live-Threat.*

Discussion

The data provided in "Figure 1: QRA Guide" acts as a guide for this assessment. The project team used NIST SP 800-30 as a basis for threat identification. Through cyber threat intelligence sources, location-specific threats are also identified. Next, the project team creates a list of known system vulnerabilities that could be exploited by potential threat vectors. The NIST SP 800-53, Security Baseline Worksheet documents and categorizes vulnerabilities collected from sources. The determination of risk for a particular threat was expressed as the likelihood of the probability that a potential vulnerability might be exploited. The next major step in measuring the level of risk was to determine the impact that would result from the successful exploitation of a vulnerability.

Conclusions

The primary objective of this study was to identify and evaluate best practices for the security of digital information stored on information systems. While it is difficult to quantify risk, it still needs to be assessed in an attempt to address risk.

Clearly, there are many ways to attack a target system, by DoS attacks, outdated Operating Systems (or supply chain attacks), Internet of Things (IoT) devices, malware and more. However, many if not most, attacks are preventable. In most cases, the best security practices includes, regular patching of the system, use of antivirus tools, avoid opening suspicious email attachments and links, and blocking of unneeded ports would prevent such attacks.

Tasks	Low (0.10)	Medium (0.35)	High (0.65)	Very High (0.90)
Cost	1-20% cost increase	20-50% cost increase	50-80% cost increase	80-100% cost increase
Time	1-10% time increase	10-30% time increase	30-60% time increase	60-100% time increase
Scope	A few minor areas affected	Sponsor approval necessary for reduction	Scope reduction unacceptable to the sponsore	The project is effectively useless
Quality	Only a few apps will be affected	Quality requires sponsor approval	Quality reduction unacceptable	The project is effectively useless

Contact

Danny A. Mase
University of Hawaii West Oahu
Email: Alaivaa@hawaii.edu
Website: https://www.cyberreceiver.com/
Phone: (785) 761-5174

References

1. Abombara, M., & Koien, G. M. (2015). Journal of Cybersecurity and Mobility. *Cybersecurity and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks.*
2. Aggarwai, C. C. (2015). SpringerLink. *Data Classification*, 285-344.
3. Akamai. (2021). *Web Application Attacks.* Retrieved from Akamai: https://globe.akamai.com/
4. Covington, M. J., & Carskadden, R. (2013). IEEE Xplore. *Threat implications of the Internet of Things.*
5. Datto. (2019). Ransomware Report. *Global State of the Channel Ransomware Report*, 26.
6. Harrington, D. (2021, July 6). Varonis. *Data Security: Importance, Types, and Solutions*, p. 1.
7. Hossain, M., Fotouhi, M., & Hasan, R. (2015). IEEE Xplore. *Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things.*
8. IBM. (2021). *Cost of a Data Breach Report 2021.* Retrieved from IBM: https://www.ibm.com/security/data-breach
9. IBM. (2021, September 17). *What is data security?* Retrieved from IBM: https://www.ibm.com/security/data-security
10. Russ, S. H., & Gatlin, J. (2020). IEEE Spectrum. *Three Ways To Hack A Printed Circuit Board*, 1.