International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 20]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

A Review on Some Pertinent Software Security Risk Management Frameworks

Syed Anas Ansar[1] , Mohd Faizan[2] , Mohd. Waris Khan[3]

Research Scholar, Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India[1]

Research Scholar, Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India[2]

Assistant Professor, Department of Computer Application, Integral University, Lucknow, India[3]

ABSTRACT: Nowadays, the software makes our work more ingenious as well as more organizable for peoples and organizations. It has been seen tremendous growth in software deployment. It makes our functioning circumstances more convenient, but on the other hand, it has security issues, and it becomes a primary concern for security experts to deal with it systematically. Software security risks are the weakness in the software which accidentally permits hazardous manipulations. To give prime consideration to the security mechanism, the valuable assets must be protected. Hence, prompt detection and remediation of software security risks is a crucial issue in software security. Software security experts rely primarily on risk management, and on the other hand, they do not implement convenient risk management model. In this paper, the researchers have laid stress on incorporating security mechanisms at the initial stage of SDLC (Software Development Life Cycle).

KEYWORDS: Confidentiality, Integrity, Availability, Security, SDLC-Software Development Life Cycle, Risk Management.

I. INTRODUCTION

We are now in the age of digitalization, where software, hardware, and sensors are working together, and nearly all services are provided through computers [1]. The researchers have observed severe attacks in recent years, which exploits the vulnerabilities in IoT network devices. In addition, attackers may use vulnerability relationships to penetrate deep within the network [2]. An excessiveness of recent applications, which are launched every day in-app marketplaces to fulfil the stress of on-line booking, gaming, finance management, and different tasks that users will perform through one's mobile devices [3]. Growing adoption and deployment of software undermines user's security, safety, and privacy, while additionally facilitating "cybercrime at scale" and reducing the limitations to practical disbursed Denial of carrier (DDoS) attacks that threaten the integrity of the internet's infrastructure. Like other evolving socio-technical structures, causality, and effects inside the IoT are not continually trustworthy [4,5]. Nowadays, the software has emerged as the organization's "new-perimeter." Financial and customer assets, i.e., "information" have become an important entity, and applications must be secured sufficiently to guard them [6]. The urge to maintain security in this current scenario is a prime consideration. Risk management is a new discipline whose primary aim is to perceive, address, and remove software security risks. Risk is the possibility of an undesirable outcome or a loss.

Software security risk management comprises of methods which are used to access as well as control risk. Risk identification and prioritization and its analysis are the sub-steps of risk assessment, while risk monitoring, risk management, planning, and risk resolutions are the sub-step of risk control [7]. Risk management is an approach in which project members regularly laid down what could adversely impact the projects. The development of a risk management system is a significant task of the overall issue of maintaining security [8]. It gives disciplined surroundings for strategic decision-making to continuously access what can go incorrect and recognize the risks that are important to address and enforce actions to address them [6].

There is a lack of understanding of software security in the early phase of the Software Development Life Cycle (SDLC), which should be illuminated as well as handled. Researchers, therefore, failed to create a stable program when implementing best practice software engineering. Not just integrating security requirements right from the beginning of SDLC but also ensures secure software. Therefore, it is logical that we need a software security framework to facilitate the security requirements process [1]. A number of different methods, as well as procedures so far to measure software

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 20]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

security risks among them a few, are based on CVSS scores and selection benchmarks. C. Wang and W. A. Wulf, as well as R. Ortalo et al., have recommended a technique for the estimation of security risk on the basis of weakest-link principle [9, 10]. Some researchers have suggested that the security risks must be considered at each and every phase of SDLC and also mentioned that the idea of rectification of requirement as well as design process to bring focus at early phases of SDLC [11]. According to Baker et al., there is a sufficiency of security procedures that helps in the secure development of software, but appropriate security quantification tools are scarce [12]. Ansar et al. have highlighted some common software security risks at the design phase based on CWE (Common Weakness Enumeration) list [13]. This paper is closely-knitted as: Section 2 shows some pertinent software security frameworks. Section 3 discusses the major findings. Section 4 describes the conclusion as well as future work.

II. SOME PERTINENT SOFTWARE SECURITY RISK MANAGEMENT FRAMEWORKS

This section provides an overview of some pertinent software security framework:

Table 1: List of Frameworks

S. No.	Framework	Year	Author Name(s)	Description
1.	PRISM: a Strategic Decision Framework for Cyber security Risk Assessment.	2020	Goel, R. et al.	Based on the PRISM framework for risk assessment of cybersecurity.
2.	Classifying Software Vulnerabilities by Using the Bugs Framework	2020	Adhikari, T. M., and Yan Wu, Y.	Based on the bugs framework provided by NIST.
3.	Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)	2020	Dodson, D., et al.	SSDF framework applying in SDLC.
4.	A Framework for Risk Management in Scrum Development Process.	2019	Chaouch, S., et al.	Based on the integration of risk management in agile project development.
5.	Risk Management Framework for Distributed Software Team: A Case Study of Telecommunication Company	2019	Husin, W. S. W., et al.	New dimension, "**communication**" is added in the previous mechanism to mitigate risk in the team of Distributed software.
6.	Security Risk Mitigation Framework for Cyber-Physical Systems	2019	Zahid, M., et al.	Based on CIA and hybrid cryptosystem.
7.	Confidentiality, Integrity, and Availability-Finding a balanced IT Framework	2018	Aminzade, M.	Based on the hybrid framework.
8.	Information Security Risks Management Framework –A Step Towards Mitigating Security Risks in University Network	2017	Joshi, C., and Singh, U.	Based on the OCTAVE Risk framework.

A brief explanation of the above frameworks is given below:

1. The researchers have proposed a novel framework for risk assessment, i.e., PRISM "Prioritize Resource Implement Standardized Monitor" to support an institution at the strategic level. This framework suggests an appropriate method to address cybersecurity problems and risk management within the organization. This Framework provides a unique method of process-oriented, which must adopt a five-step approach in an organization. PRISM stems from the fundamental hypothesis that the lack of strategic emphasis on prioritizing

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 20]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

cyber activities represents a central gap in tailoring an effective risk management strategy. Identification of key risk drivers among these interdependencies is "**Prioritization**." The rest of the steps ensure that relevant and identified security controls are resourced and implemented in the enterprise systems and processes of the organization [14].

2. Particular types of bugs in software are software vulnerabilities that can exploit by the intruder to trigger drastic impacts, i.e., accessing or modifying unnecessary data. This framework describes vulnerabilities in software by using data-mining and classify them into specific groups using the NIST, i.e., National Institute of Standards and Technology. The researchers have suggested that this framework helps software engineers to avoid wastage of time and save energy to build secure software by avoiding vulnerabilities by taking proper precautions [15].

3. The researchers have suggested that for the development of secure software, the techniques of SSDF (Secure Software Development Framework) is needed. It is to be enforced in each and every phase of the SDLC model to ensure software security. This technique helps software developers to minimize the vulnerabilities in applications, and slacken down its impact.

4. In this paper, the researchers have suggested that risk management has a key contribution to a successful project, which is not used in agile project methodologies. Scrum does not provide clear procedures, so explicit integration is necessary for risk management. Researchers have recommended that applying a risk management approach to other agile approaches may improve the project's success rate by evaluating them in a scenario of real-life growth. This framework aims to strengthen the process of risk management and increasing the success rate in the Scrum project [17].

5. This framework is carried out in Malaysia at a telecommunication firm. This framework collected the data from a case study, which is obtained through questionnaires and literature review. The previous mechanism added the DSD (Distributed Software Development) risks with the list of known risks, and in the current framework, the new dimension **"Communication"** is added. The updated version of the current risk management system would fit for organizations with distributed existence, and future work is performed an in-depth survey to take steps to mitigate the risk. It is useful for project managers who supervised projects developed by the distributed team 18].

6. Researchers have proposed a framework for reducing the security risk. It mainly focused on CIA (Confidentiality, Integrity, Availability) constraints including non-repudiation, and freshness of data. This framework uses the hybrid cryptosystem (DES, i.e., Data Encryption Standard + Triple-DES + RSA) concept, by removing the key management process to reduce the complexity of time and efficient memory use [19].

7. In this paper, researchers have addressed that an organization must be aware of the risk and able to mitigate the impact of risk and its threat. Each employee needs to know their role in the process of keeping an organization safe. Evaluating the IT risks of an enterprise is not something that needs to be taken lightly. The probability of a ransomware attack or the same kind of attack may higher than ever before. Security is emphasized throughout the entire organization, from the top levels to down levels. In addition, researchers have suggested that optimum security levels can be achieved with the help of available security mechanisms. All organizations must find a hybrid solution for the migration of security risks, i.e., a hybrid framework was used for risk assessment to provide a better result. The first and only way to protect a company's security effectively is to review its function periodically [20].

8. The researchers have introduced a risk evaluation model for quantitative information security based on OCTAVE risk frameworks (OCTAVE model based on risk assessment), primarily developed for the computing environment of the university. This framework eliminates the likelihood of a security breach through three phases. The first phase; here, vulnerabilities and risks are addressed to determine the vulnerable ends in the academic institutions. The second phase; this phase focuses on the highest risk and develops a preventive plan. The final phase; it identifies the enforcement criteria of vulnerability management to enhance the security of the University. In addition, the researchers have suggested that the framework reduces security breaches and can be applied to any higher educational organizational [21].

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 20]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

III. MAJOR FINDINGS

Nowadays emergence of software creates a new way in an organization and makes work more straightforward, but as well as it has created a drastic problem, i.e., security risks. Security risks in software applications became a primary concern for organizations, researchers, and security experts all around the world. Some of the significant findings from the literature review are given below:

- It is clear from the literature survey we cannot avoid security risks altogether after taking all preventive measures.
- To mitigate risk, security effectiveness needs to be strengthened, and this needs to prior identification of threats and vulnerability assessment to determine significant risks for secured systems.
- Vulnerability, i.e., risks within the software, must be identified because it is a weakness within the system, and this can be exploited by attackers to disrupt the process.
- Assessment of the IT risk is not something that can be taken lightly. The assessment must be reviewing its function periodically to manage security.
- In the majority of software, security procedures are not taken from the initial phase of SDLC.
- For the development of an appropriate framework to reduce risk, researchers must integrate the lowest-cost strategy and introduce the most effective controls, with minimal effects on the resources of the organization.

IV. CONCLUSION AND FUTURE WORK

Recently, we have seen tremendous growth in the field of software. Nowadays, technology has made complicated work much more accessible and more straightforward, yet any untidiness in the development of software leads to a matter of life and death. The majority of security experts have mentioned that it is not possible to build a 100 percent secure system and suggested that a hybrid system can provide optimum protection. In addition, this optimum system enhances the security level by minimizing security risks. Researchers have suggested that if the security issues are taken into measure from the beginning of SDLC, then it will undoubtedly assist in the mitigation of security infringements. So, as a result, an appropriate approach for the development of secure software must be taken into account. As we know that secure software development is an arduous as well as an error-prone job, and when we are talking about software, then “data” is a valuable asset. So, it is very important to build a proper mechanism to protect these valuable assets. The security risks need to be assessed in a regular period and must be prior aware in the initial phase of software development. In addition, researchers have suggested that it should not be taken lightly by the security experts. It is clear from literature survey various software security framework have developed for risk assessment and risk management regularly, maximum among them is in vague condition, and a very few of them is tested on a large scale. So, there is an urgent need to develop a framework to reduce risk, which uses a low-cost strategy and introduces the most effective controls, with minimal effects, and should be tested on a large scale. In the future, researchers are planning to develop a framework to provide optimum security by minimizing the risk to provide an efficient, secure, and reliable mechanism.

REFERENCES

[1] Rehman, Shafiq Ur & Gruhn, Volker. (2018). An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. Technologies. DOI 10.3390/technologies6030065.

[2] G. George and S. M. Thampi, "A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations," in IEEE Access, vol. 6, pp. 43586-43601, 2018, DOI: 10.1109/ACCESS.2018.2863244.

[3] Liao, Zhung-Xun & Lei, Po-Ruey & Shen, Tsu-Jou & Li, Shou-Chung & Peng, Wen-Chih. (2012). Mining Temporal Profiles of Mobile Applications for Usage Prediction. Proceedings - 12th IEEE International Conference on Data Mining Workshops, ICDMW 2012. 890-893. 10.1109/ICDMW.2012.11.

[4] Brass, Irina & Sowell, Jesse. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance. 10.1111/rego.12343.

[5] Hezam, Akram & Nijdam, Niels & Collen, Anastasija & Konstantas, Dimitri. (2019). A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. Symmetry. 11. 774. 10.3390/sym11060774.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 20]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

[6] M. Chowdhury, A. Al, and S. Arefeen, ‘‘Software risk management: Importance and practices,’’ in Proc. IJCIT ISSN,2011, pp. 2078–5828.
[7] Madachy, R. (1994), “A Software Project Dynamics Model for Process Cost, Schedule and Risk Assessment,” Ph.D., Dissertation, University of Southern California. Semin, Valeriy & Shmakova,
[8] Elena & Los, Alexei. (2017). The information security risk management. 106-109.10.1109/ITMQIS.2017.8085774.
[9] C. Wang and W.A. Wulf, "Towards a framework for security measurement," in 20th National Information Systems Security Conference, Baltimore, MD, pp. 522-533, 1997
[10] R. Ortalo, Y. Deswarte and M. Kaâniche, "Experimenting with quantitative evaluation tools for monitoring Operational security," Software Engineering, IEEE Transactions On, vol. 25, pp. 633-650, 1999.
[11] P. T. Devanbu and S. Stubblebine, Software engineering for security: A roadmap, Proc. of the Conference on the Future of Software Engineering, Limerick, Ireland, pp.227-239, 2000.
[12] W. Baker, L. Rees and P. Tippett, Necessary measures: Metrics-driven information security risk assessment and decision making, Communications of the ACM, vol.50, no.10, pp.101-106, 2007.
[13] S. A. Ansar, J. Yadav, K. Jaiswal, A. Yadav and R. A. Khan. (2020) “Some Common Software Security Risks at Design Phase” ICCCIT 2020, pp: 47-51, ISBN 978-93-5407-928-3.
[14] Goel, Rajni & Kumar, Anupam & Haddow, James. (2020). PRISM: a strategic decision framework for Cybersecurity risk assessment. Information & Computer Security. ahead-of-print. 10.1108/ICS-11-2018-0131.
[15] T. M. Adhikari and Y. Wu, "Classifying Software Vulnerabilities by Using the Bugs Framework," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-6, DOI: 10.1109/ISDFS49300.2020.9116209.
[16] Dodson, Donna & Souppaya, Murugiah & Scarfone, Karen. (2020). Mitigating the Risk of Software Vulnerabilities By Adopting a Secure Software Development Framework (SSDF). https://doi.org/10.6028/NIST.CSWP.04232020.
[17] Chaouch, Syrine & MEJRI, Asma & Ghannouchi, Sonia. (2019). A framework for risk management in Scrum development process. Procedia Computer Science. 164. 187-192. 10.1016/j.procs.2019.12.171.
[18] Husin, Wan & Yahya, Y azriwati & Mohd Azmi, Nurulhuda & Sjarif, Nilam & Chuprat, Suriayati & Azmi, Azri.(2019). Risk Management Framework for Distributed Software Team: A Case Study of Telecommunication Company. Procedia Computer Science. 161. 178-186. 10.1016/j.procs.2019.11.113.
[19] Zahid, Maryam & Inayat, Irum & Daneva, Maya. (2019). Security Risk Mitigation Framework for Cyber-Physical Systems. Journal of Software: Evolution and Process. 10.1002/smr.2219.
[20] Aminzade, Michael. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. Network Security. 2018. 9-11. 10.1016/S1353-4858(18)30043-6.
[21] Joshi, Chanchala & Singh, Umesh. (2017). Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications. 128-137.10.1016/j.jisa.2017.06.006.