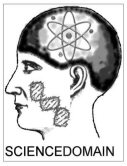
British Journal of Mathematics & Computer Science
11(6): 1-10, 2015, Article no.BJMCS.19872
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org



Revisiting Software Security Risks

Rajeev Kumar[1*], Suhel Ahmad Khan[2] and Raees Ahmad Khan[1]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India.
[2]Department of Computer Application, Integral University, Lucknow, India.

Article Information

DOI: 10.9734/BJMCS/2015/19872
Editor(s):
(1) Dariusz Jacek Jakóbczak, Chair of Computer Science and Management in this Department, Technical University of Koszalin, Poland.
Reviewers:
(1) Anonymous, MSA University, Egypt.
(2) James A. Rodger, University of Pennsylvania, USA.
(3) Anonymous, Federal University of Minas Gerais, Brazil.
(4) M. Bhanu Sridhar, Gvp College of Engg. for Women, Vizag, India.
Complete Peer review History: http://sciencedomain.org/review-history/11392

Original Research Article

Received: 01 July 2015
Accepted: 25 August 2015
Published: 15 September 2015

Abstract

Robustness of secure software is directly associated with better market and refining relations between customers and software vendors. Nowadays robustness of secure software is an assessment tool to find healthier market room by way of developing highly integrated quotient between customers and vendors. Software security risk management is a very highly appealing phenomenon to control security through establishing expensive countermeasures of security hazards and by controlling them. Existing approaches for security risk management are merely available which are having direct or indirect impact with the simple implementations through planning, development of established security requirements for modifications and execution of security design policies. This paper examines the associated security risks of software through different inputs of security risk management procedure. This review may be helpful to discover the new pitches of risk management techniques of software security controls at design level for high quality secure product. A contribution is made after reviewing views of authors in this paper in the form of a checklist for security risk evaluation and management at software design phase.

Keywords: Software risks; software security; security risks; software design; risk management.

1 Introduction

Software designers are facing new problems to improve security. Academicians and industry peoples are searching a flexible process for securing software products. In this situation, researchers, designers and corporations need to modify their plan to make security of software a flexible process. Risk is a problem that

**Corresponding authors: E-mail: rs0414@gmail.com[1], ahmadsuhel28@gmail.com[2], khanraees@yahoo.com[3];*

can create interruptions in the techniques which are well-defined and have definite objectives [1-3]. Risk management is a degree that is used for classification and evaluation of a specific security risks. Risk management is not just used to lessen the probability of occurrence of threats but it also enhances the chances of good performance by securing software [4]. Risk management has developed its great significance in the economy during development of software design. Security risk controlling and managing risks at the business platform is a key for numerous security risks which have to be improved.

Security risk management plan is a conceptual structure that monitors the improvement of a security program for security risk management and design safety innovations [5-6]. Security risk monitoring, controlling and managing are interrelated to the processes that are integrated into the security design. Security risk management has been identified with numerous traditional fields such as commercial, industrial and of course information technology [7-10]. The risk management technique has an inclusive process definition that supports risk management activities throughout the process of software development. The desired security risk management process is similar to many other risk management processes metaphors with some special characteristics.

Considerable study has been shown in the security risk management pitch in earlier periods. This study has followed in a quantity of structures and virtual reality types, plans, development prototypes, and numerous effective risk management procedures [11-14]. Hence, it is essential that aspect of effective security risks should incorporate these procedures with other aspects. In revisiting security risks, this review article constructs the whole study in two fold manner. The first one is reassessment and revisit of the literature including security risks and thier management process of software security. The second one is an advanced checklist which is prepared through re-evaluation mechanism for software security risk analysis at design phase.

2 Descriptions and Background

Software security risk analysis becomes an increasingly essential component of each organizational security development program [15]. Security risk estimation methodology provides the results in qualitative or quantitative manner depending upon the various factors. Such type of estimation mechanism having several advantages including early identification of threats and vulnerabilities with their specific impact on entire design of risk management [16-18]. Organizations have a huge reliance on information systems which plays supportive tools to control and manage risks. Nowadays, risk related to information security creates a major challenge for many projects, including project accountability, undesired outcomes, commercial damage and loss of trustworthiness [19-22]. It highlights the recent development and also adds some unidentified risk factors which are important to build a strong foundation. Some pertinent works related to this area are as follows.

A research on risk management perspective has been done by Wu Yanyan targeting the realm of e-commerce security challenges [23]. This paper discusses the three dimensional control which are measure, threat agent, and techniques for advance description of security. Ming-Chang Lee presented risk analysis methods and research trends like AHP and fuzzy comprehensive method for information security risk assessment and management [24]. An empirical study of rationality-based beliefs and information security awareness was presented by Burcu Bulgurcu for information security policy compliance [25]. This research clarified the facts of employee compliance with the policy of an organization about information security. A conceptual report on software risk given by Forrester Consulting discusses exploitable flaws of software risks. These exploitable flaws in open source can carry a stiff price in terms of high price of product; rely of customers, and irreparable damage to product [26].

Shruti patil presented secured cloud support for global software requirement risk management [27]. This approach provided ready to deliver strategies for software industry and less loss for project failures. This approach focussed on the fact to think over security problem mitigation techniques prior to face problems in software engineering. Don Gotterbarn and Simon Rogerson in his research work entitled: "Creating the

Software Development Impact Statement" presented responsible risk analysis for software development. This paper focuses on risk analysis of quantifiable security factors. It uses a fine understanding of the scope of a software project which contributes to significant software failures [28].

Jakub Miler presented a research paper which identifies software project risks with the process model. The approach involves unambiguous modelling of software processes and identifying risk by two dedicated techniques [29]. It introduces a meta-model that allows expressing the process risk. There are two systematic risk identification techniques which are proposed and presented in the form of detailed procedures. Both techniques refer to the process model to focus the analyst's attention in the investigation of the process risks. Janaa Nyfjord presented a research article which targets towards integrating agile development and risk management. In this paper researcher discusses about controlling risks, improves essential software development features such as product quality, planning precision and cost-efficiency [30].

Hooman Hoodat offered a research technique for classification and analysis of risks in software engineering. It contains the management of all issues involved in the development of software project namely scope and objective identification, evaluation, methods, effort and cost estimation [31]. Gary McGraw approached a framework of risk management. It introduced the definition of a full life-cycle activity of risk management. The main purposes of this description, consider risk management a high-level approach to iterative security risk analysis that is deeply integrated throughout the software development life cycle [32].

3 Earlier Development of Security Risk Management Process

Security risk management is applied all over the development lifecycle process to recognize and mitigate risks associated with achieved objectives targeting to requirements. Security risk management process in accordance with strategy and supervision has different focuses [33]. For example, the impact of the parameters including cost and schedule are not associated directly with security assessment, but they are integral parts of security risk management. The previous standards were focused on analyzing discrete alterations [34] which were not enough for addressing all hazards identified as a consequence of designed interactions and interconnectivity.

In fact, the functionalities for managing security risk would not only overlap but may create manufacturing risk [35]. This perspective was not considered in the past, but will be important to apply the concept of integrated security in present. Risk analysis and security management procedures represent a stronger and integrated technique to evaluate performance of security. Integrated risk management uses obtainable security policies and methodologies. Security risk assessment is consuming incorporated security management values in three direction or views including vertical, temporal and horizontal.

A risk is an exposure to loss or injury or a factor, thing, or element that involves uncertain danger. This uncertainty gives birth to less secure software. Hence given approach is focused on analysis and assessment which supports software security risk management process. This critical analysis discusses the compendious activities of security risk management process described in Table 1 [36]. Software security risk management is extra challenging noteworthy environmental, traditional and commercial variation. Normal approaches of risk control are relatively protected. Here a checklist is provided in which different scholars and their methodologies are studied. After deep study a checklist is given which recognizes if the project fulfills the need given in security risk management questionnaire.

This security risks review considers the authentic activities of software security risk management. Software security risk management has become a critical task. This study provides a checklist for improving the security risks management processes under software development process [37]. The reason behind this review was to contribute independence to declare responses in their own contexts. Such classification of questions has a confident influence while enquiring with the customer. Individual may draw out information about the planned realm. This segment presents the security risk management process status within the reviews different scholar's projects studied.

A checklist is provided here after doing analysis of different scholars approach to security risk. After doing this review of scholars, different views on risk has been concluded [38]. Important points that were left by these scholars while researches are considered in the questionnaire provided in appendix. This given questionnaire is fully hypothetical and is being prepared on the base of this review. Researchers will discuss in detail about this questionnaire in future research works. Here is presented review of scholars only.

Table 1. Assessment of security risks management activities

Phases/ Activities	Security risk management procedure	Ahem D., Clouse A., Tumer R., [3]	Boehm B., [35]	Charette R., [8]	Mattsson M. K., Nyfjord J., [36]	Verdon D., McGraw G., [2]
1.	**Security risk identification**					
A1.1	Classify significant earlier security risk information	X	X		X	
A1.2	Identify business taxonomy of risk types of security	X	X	X		
A1.3	Classify other relevant information of security risk if needed		X		X	
A1.4	Identify security risk exposure fields					X
A1.5	Identify the possible risk for each security risk	X	X	X		X
A1.6	Identify security risk consequences and effects		X		X	
A1.7	Identify the security risk foundations at the design phase		X			
A1.8	Analyze root-cause of security risks	X			X	X
A1.9	Define security risk classifications classes				X	
A1.10	Describe and record each identified security risk		X	X		X
A1.11	Create security risk list when development of secure design	X		X	X	
A1.12	Circulate security risk list		X			X
A1.13	Update security risk list consequently	X			X	
A1.14	Confirm security risk list		X			
2.	**Security risk analysis**					
A2.1	Analyze each security risks independently	X	X			X
A2.2	Assess security risk probability at design phase	X	X	X	X	
A2.3	Assess security risk impaction	X		X	X	
A2.4	Calculate security risk disclosure				X	
A2.5	Specify and analyze information with appropriate techniques		X	X		X
A2.6	Assign priority to the security risk	X		X	X	
A2.7	Document the assumptions of security risk if any made		X			X
A2.8	Specify and analyze the security risk in a group	X			X	
A2.9	Create a list of security risk re-concerning further attention		X			
A2.10	Suggest a preliminary plan for managing the security risks				X	
A2.11	Calculate security risk list and plan among stakeholders	X	X			X

Phases/ Activities	**Security risk management procedure**	**Ahem D., Clouse A., Tumer R., [3]**	**Boehm B., [35]**	**Charette R., [8]**	**Mattsson M. K., Nyfjord J., [36]**	**Verdon D., McGraw G., [2]**
A2.12	Updated security risk list, if needed	X	X	X	X	
A2.13	Confirm the security risk list with the preliminary preparation of security design	X		X	X	
3.	**Security risk management planning**					
A3.1	Revise the security risk list, analyze the plan	X	X	X	X	X
A3.2	Determine strategic procedure for managing the security risk		X	X		X
A3.3	Verify approval approach of security risk	X		X	X	
A3.4	Determine values that may trigger possibility procedures		X			X
A3.5	Develop a security risk management plan and implementing strategies	X			X	
A3.6	Characterize pertinent metrics for monitoring and controlling of the security risk		X	X	X	X
A3.7	Determine performance indicators for measuring action effectiveness				X	
A3.8	Define relevant measures for treating the security risk	X	X			X
A3.9	Develop a feedback action plan of security risks if needed	X	X	X	X	X
A3.10	Document the control, monitoring and action plan	X		X	X	
A3.11	Define relevant possibility actions for management of security risk	X		X		
A3.12	Document the possibility plan		X			
A3.13	Make a schedule for implementing plans	X		X	X	
A3.14	Categorize restriction of security risk management		X		X	
A3.15	Estimate efforts and resources	X		X		X
A3.16	Assign budget and roles responsible for managing it	X	X			
A3.17	Analyze and joining the security risk management plan steps	X		X	X	X
A3.18	Circulate the security risk management plan to the stakeholders troubled		X		X	
A3.19	Confirmation and documentation of security risk management plan and updated if needed					X
4.	**Security risk monitoring and control**		X		X	
A4.1	Ensure there are procedures to monitor security risk			X		
A4.2	Monitor and control the changes in the security risk status	X	X		X	
A4.3	Record status, if needed	X		X		X
A4.4	Implement the security risk action and contingency plan if needed		X		X	

Phases/ Activities	Security risk management procedure	Ahem D., Clouse A., Tumer R., [3]	Boehm B., [35]	Charette R., [8]	Mattsson M. K., Nyfjord J., [36]	Verdon D., McGraw G., [2]
A4.5	Monitor result to determine the effectiveness of planned action	X			X	
A4.6	Seek out and identify residual security risks	X		X		X
A4.7	Record and update security risk status and list	X	X	X	X	
A4.8	Approve by formal sign-off				X	X
A4.9	Security risk management status modernized	X	X	X	X	
A4.10	Identify deficiencies and failures of the process	X			X	X
A4.11	Record all outcomes and re-analyze		X		X	

4 Discussion

All of us are known to the fact that risk has different types. But with the concern of security, we have focused especially on security risk. In relation to the traditional risk management policy, it is considered that a company entire security risk collection in an integrated and holistic approach which helps to evaluate security risk as discrete direction is not enough. The overall assessment of organizational security risk in a single expression covering all aspects of security attributes is also the limitation of such system. Here we described security risk management requirements; further a questionnaire is given in appendix focusing on security risk management planning. This questionnaire can serve as a base for further research.

Prioritizing risks may reveal new threats and bugs in security. Risk management team identifies risks with its two factors that are external and internal. A relevant external factor includes globalization, industry consolidation and deregulation as well as regular pressure. In general, the internal factors can be reduced to the objective of security risk management, which is to enhance the company product value and quality [22-25]. Security risk management is also driven by methodological and technological growth together with advanced methods of security risk quantification and assessment. In this paper, we examine the security risk management process and its assessment with software development. This examines the effects which are pinched for preparation and future research in the area of security risk management of the software. The following are the objectives leading for the improvement of security risk.

- To identify the risks challenged by the security in developing software design.
- To suggest a plan for the development of security risk management.
- To investigate the approaches accepted by engineers for security risk management.
- To detect the forthcoming process of the security risk management.
- To fix the essential concepts and codes recycled in the existing security risk background.
- To find out the rank of security risk management process which is helpful for managing risk nowadays.
- To find out the problems that influence support in improving the security development process with the help of reviews.
- To find out the differences between previous and improved methodologies.
- To provide a checklist to developers for better implementation of security risk management plan.
- To enhance the process of security risk management by defining and improving methodologies.

5 Conclusions

Security risk management gives a structured mechanism to provide visibility into threat mitigation for success of project. The review Table 1 given in this paper provides a theoretical validation. This validation is prepared after taking reviews from different scholars which will help software developers to reduce security risk in development of product. While studying about this area, an analysis about security risk management is prepared in the form of questionnaire which is provided in appendix. This analysis will help to improve security risk management process by developers. By considering the potential impact of each risk item, one can make sure to control the most rigorous risk first. Without a formal approach, one cannot ensure that these risk management actions are being done in right manner. Security risk management has been recognized as a best practice in the software industry. As the security risk method has been expansively presented in other publications here we present only the checklists and main principles of the method.

Acknowledgements

The authors are grateful for the valuable comments and suggestion from respected reviewers. Their valuable comments and suggestions have enhanced the strength and significance of this paper. This work is sponsored by UGC-MRP, New Delhi, India under F. No. 43-391/2014 (SR).

Competing Interests

Authors have declared that no competing interests exist.

References

[1] De Marco T. Risk management for software projects. The Atlantic Systems Guild, Camden; 2004.

[2] Verdon D, McGraw G. Risk analysis in software design. IEEE; 2004.

[3] Ahern D, Clouse A, Turner R. CMMI distilled second ed. Addison-Wesley, Boston; 2005.

[4] Risk Management Framework (RMF) for DoD Information Technology.
Available: http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf last visit Dec 14 2014

[5] Boehm B. Software risk management: Principles and practices. IEEE Software. 1991;8(1):32-41.

[6] Kajko-Mattsson M, Nyfjord N. State of software risk management practice; 2008.

[7] Gatzert N, Martin M. Determinants and value of enterprise risk management. Empirical Evidence from the Literature Working Paper; 2013.

[8] Charette R. Software engineering risk analysis and management. McGraw Hill, New York, NY; 1989.

[9] Eclipse Process Framework (EPF).
Available: http://www.eclipse.org/epf/. Last visit Dec 14 2015

[10] European Cooperation for Space Standardization (ECSS).
Available: http://www.ecss.nl/. Last visit Nov 2014

[11] How Much Is Enough? A risk-management approach to computer security.
Available: http://iis db.stanford.edu/pubs/11900/soohoo.pdf last visit Jan 16 2015

[12] Technical white paper on reducing security risks from open source software. Available: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA0-8061ENW.pdf last visit Jan 14 2015

[13] Khan SA, Khan RA. Securing object oriented design: A complexity perspective. International Journal of Computer Applications. 2010;8:13.

[14] Chaudhary P, Hyde M, Rodger JA. Attributes for executing change in an agile information system. International Journal of Technology Diffusion (IJTD). 2015;6:2.

[15] Goral J. Risk management in the conceptual design phase of building projects, Master's Thesis in the International Masters Programme Structural Engineering Chalmers University of Technology Göteborg, Sweden; 2007.

[16] How good is your risk management? Available: http://www.ioshroutefinder.co.uk/PDF/How%20good%20is%20your%20RM.pdf Fab 02 2015

[17] UKTFA risk assessment checklist. Available:http://www.ebselk.co.uk/wp-content/uploads/2013/02/UKTFA-Risk-Assessment-Checklist-APPROVED.pdf Jan 30 2015

[18] Chakrawarthy B, Nielsen J. Design risk management. Aricus Consulting; 2012.

[19] Hoodat H, Rashidi H. Classification and analysis of risks in software engineering. World Academy of Science, Engineering & Technology. 2009;56446-452.

[20] Boban M, Pozgaj Z, Sertic H. Strategies for successful software development risk management. Management. 2003;8:2.

[21] Sahu K, Shree R. Risk management perspective in SDLC. International Journal of Advanced Research in Computer Science and Software Engineering. 2014;4(3):1247-1251.

[22] Zubcsek P, Chowdhury I, Katona Z. Information communities: The network structure of communication. Social Networks 38, ©Elsevier B.V. 2014;50-62.

[23] Yanyan W. Research on e-commerce Security based on risk management. International Journal of Security and Its Applications. 2014;8:3.

[24] Lee M. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. IJCSIT. 2014;6:1.

[25] Du S, Lu T, Zhao L, Xu B, Guo X, Yang H. Towards an analysis of software supply chain risk management. Proceedings of the World Congress on Engineering and Computer Science; 2013.

[26] Moores TT, Champion REM. A methodology for measuring the risk associated with a software requirement specification. AJIS. 1996;4(1):55-63.

[27] A Forrester Consulting Coverity. The software security risk report the road to application security begins in development September 2012. Available: http://www.coverity.com/library/pdf/the-software-security-risk-report.pdf last visit Jan 10 2015

[28] Patil S, Ade R. Secured cloud support for global software requirement risk management. IJSEA. 2014;5:6.

[29] Gotterbarn D, Clear T, Kwan C. Managing software requirements risks with software development impact statements. Citrenz; 2005.

[30] Miler J, Górski J. Identifying software project risks with the process model. Proc. of 17th International Conference Software & Systems Engineering and their Applications Nov 30 - Dec 2, Paris, France; 2004.

[31] Grabski SV, Leech SA, Lu B. Risks and controls in the implementation of ERP systems. The International Journal of Digital Accounting Research. 2001;1(1):47-68.

[32] SANS Institute InfoSec Reading Room. A Perspective on Threats in the Risk Analysis Process; 2002.

[33] Venkatesh J, Aarthy C. Threats in implementation of ERP applications. International Journal of Marketing, Financial Services & Management Research. 2012;1:7.

[34] Bulgurcu B, Cavusoglu H, Benbasat I, Information security policy compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness; 2010.

[35] Storch T. Toward a trusted supply chain. A Risk Based Approach to Managing Software Integrity Trustworthy Computing Microsoft Corporation; 2011.

[36] Nyfjord J. Towards integrating agile development and risk management. Universitetsservice US-AB, Kista; 2008.

[37] Hoodat H, Rashidi H. Classification and analysis of risks in software engineering. World Academy of Science, Engineering and Technology. 2009;3.

[38] McGraw G. Risk management framework. Cigital, Inc; 2005.

Appendix

Table 2. Sampling a questionnaire to be asked during security risk management process

S. no	Security risk management	Yes	No	Action by management
1.	Does your organization identify security risks when developed security of software at design phase?			
2.	Do you identify and manage many types of security risks?			
3.	Do you have a universal process for managing security risk?			
4.	Could you briefly described your security risk management process at design phase and its phases (e.g. security risk identification, security risk analysis, and monitoring and control security risk so on)?			
5.	Did you compare the differences and similarities between your and common existing security risk management process?			
6.	Is your specified list of activities are for each phase and carried out in your organization?			
7.	Does the figure below missed anything that you do for security risk management in your organization?			
8.	Are business roles involved in security risk management?			
9.	Do you have models specialized to each security risk type?			
10.	Do you use your general security risk design model?			
11.	Do you follow any standard when establishing your security risk management process at design phase?			
12.	Do you record security risk and security risk management activates?			
13.	Is there exact security risk information is recorded?			
14.	Does the recording of security risk varies between stages of the software design?			
15.	Do you use any other ways to communicate security risks in your software development?			
16.	Are there any problems with current security risk management process?			
17.	Do you think that security risk management is essential?			
	Design and security risk management process integration			
18.	Does your organization have the same stages concerning the business and engineering?			
19.	Do you conduct security risk management on business planning stage?			
20.	Do you conduct security risk management on the engineering stage?			
21.	Do you conduct security risk management in the implementation level?			
22.	Do you consider security risks within testing?			
23.	Are you describing the types of security risk within testing?			
24.	Is your S-RM process integrated with the development design?			
25.	Do you use new criteria for integrating the S-RM process?			
26.	Did you achieved maximal results when integrating security risk management with development design?			
27.	Are there any problems with how security risk management is integrated in development design currently?			
28.	Could you provide an example of a security design where S-RM was failure and success?			
29.	Did the S-RM standards present in agile environments?			
30.	Is there any difference in conducted security risk management and traditional process?			

© 2015 Kumar et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/11392