New Information Security Risk Management Framework as an Integral Part of Project Life Cycle

Mahmoud Alshawabkeh[1,a], Xichun Li[2,b] ,and Mohamed Sullabi[3,c]

[1]Universiti Pertahanan Nasiona Malaysia, Kem, Sungai Besi, 57000 Kuala Lumpur, Malaysia

[2]Guangxi Normal University for Nationalities, Jiangzhou Qu, Chongzuo Shi, Guangxi, China

[3]Libyan Academy, Musrata, Libya

[a]mahmoud.alshawabkeh@gmail.com, [b]291495244@qq.com, [c]sullabi@yahoo.com

*Mahmoud Alshawabkeh

Keywords: Cyber Security, Project Management, Leadership.

Abstract. One of the critical success factors in managing any information system project is the information security risk management. When taken seriously and implemented correctly according to best practice of project management process, information security risk management helps to deliver the project on the exact predefined time, on budget and with a high quality as requested by the project stakeholders. This paper explains a good practice of security risk management process and propose a new information security risk management framework to be applied into project life cycle.

1. Introduction

One of the critical success factors in managing any project is the information security risk management. The PMBOK® guide defines risk as the occurs of condition or event uncertain that has a specific effect on objectives of any project [1]. When taken seriously and implemented correctly according to best practice of project management process, security risk management helps to deliver the project on the exact predefined time, on budget, and with a high quality as requested by the project owners [2], [3]. This paper is about understanding information risk management and applying this to Qatar FIFA world cup finals in year 2022. Several researches demonstrate the need for managing security risk when doing any project [4]–[6]. This paper research gap can be presented in the problem statement, "*What is the effect of project security risk management on success of big projects as Qatar FIFA world cup 2022?*". Objectives of this research are, to explore project management life cycle and the security risk management; to identify top three information security risks of Qatar FIFA world cup; to classify risk probability of occurrence and risk potential impact (low or medium or high); to evaluate mitigation strategies; and to propose and measure solutions for the top three risks.

2. Literature Review

2.1. Qatar FIFA World Cup Finals 2022

Qatar will host the 2022 FIFA world cup finals beating Australia, Japan, South Korea and the United States. Qatar have hosted several large events specially the 2006 Asian Games and the AFC Asian Cup in 1988 and 2011. It has also hosted the Gulf Cup three times, winning the cup several time [7]. During 2022 finals, Qatar expected 1.2 million visitors and have constructed several major projects including the new Lusail iconic stadium shown in Fig. 1. with the 80,000-seater in the newly built Doha district of Lusail the venue for the final on 18 December. However, experts have pointed to the need for large event projects to provide security and reduce physical and information security risk [8].

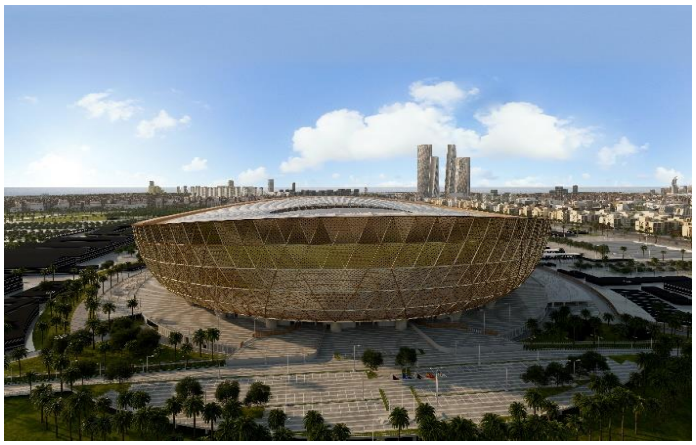

Figure 1. Lusail Iconic Stadium

2.2. Digital Forensics

In computer security, forensic investigation, also called first incident response is the first step in identifying, understanding, and mitigating security breaches. Digital forensics defined as a scientifically derived and proven method towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal: or helping to anticipate unauthorized actions shown to be disruptive to planned operations, for the purpose of presentation in a court of law [9]. Typically, digital forensics involves the recovery of data from digital storage media that may have been lost, hidden, or otherwise concealed or after an incident that has affected the operation of an information processing system. This could be an accidental or deliberate act, carried out by an employee or outsider, or after a malware attack of any type [10].

2.3. Information Security Management System (ISMS)

The information security management system ISO/IEC 27001:2013 is a standard that provides all the requirements for establish, implement, maintain, and improve the organization's information security management system [11]. ISMS can be used to assess the organization's ability to manage information security requirements. The main objective of information security management system as defined in ISO/IEC 27002 is to minimize the risks and impacts to business whilst maximizing business opportunities and investments and to ensure business continuity [12]. Organizations in deeply needed to establish and implement ISO/IEC 27001:2013 ISMS standard to manage risks and have full confidence that risks adequately managed. The ISMS standard require organization to develop and maintain a customer information security program. The security program must be a written plan that identifies risks and controls.

3. Proposed Information Security Risk Management Framework

In simple words, project risk management is about increasing the positive event probability and minimizing the negative event probabilities as well as their impact on the overall project. How successful is the project risk management in increasing the positive events probability and decreasing the negative events probability depends on the process and risk management steps that taken [1], [13]–[15]. Therefore, the to make FIFA world cup 2022 successful, project managers should consider using a good practice of security risk management process that involves the steps in project life cycle as shown in the proposed model in Fig 2.

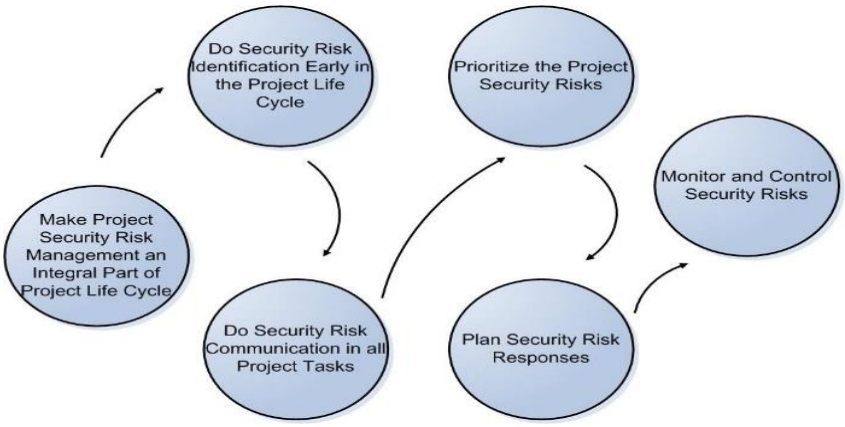

Figure 2. Proposed Security Risk Management Framework

3.1. Make Security Risk Management an Integral Part of Project Life Cycle

This is the most crucial step in the project security risk management process. To minimize the likelihood of negative events and their impact on the project, security risk management should be embedded in the project from the early beginning. Many projects are carried out with no solid security risk management process implemented, others are carried out with no security risk management at all because the project managers are ignorant, and they feel confident that no risks will occur in their project, and that is exactly where things go wrong. To make project a success, security risk management should be a part implemented early in the life of the project. It should also be a part of everyday activities. It should be discussed in every meeting and staff should be trained on security risk management. The nature of the Qatar FIFA world cup makes it very critical to have a security risk management implemented since the early stages of the project. Be it the nature of Qatar, which poses many risks in terms of political stability in the middle east region, or the nature of the football game stadiums, which easily can have terrorist threats on electronic doors and system databases. All this makes it important to have a security risk management since the early stages of the project.

3.2. Do Security Risk Identification Early in the Project Life Cycle

The second step to do is to identify the security risks that are present in project. To do so, project manager need to look at two main sources the previous projects, and the people. Previous projects do have many reports which highlights the risks encountered in these projects. These risks may not be very clear, but a careful look back at these reports and evaluating what went wrong will help a lot in identifying potential risks in projects. The second source of information is people. Project team and those who worked in similar projects are a great asset when it comes to identifying potential risks. Different people have different experiences and knowledge. Their past experiences in similar projects will add a lot of value to risks identification. They can reveal many types of risks that project may encounter and provide with ways to avoid these risks which may not have crossed mind. People will never be able to identify all the potential risks in project, however, with all team members' experiences and information they could provide on potential risks, they will be able to deal with the majority of risks and have enough time to deal with unexpected problems. In Qatar FIFA world cup, there are many possible risks that should be taken into consideration. Below are few examples of these risks: 1) Security attack to delay of finalizing the stadium designs, the games logo and other project specifications. 2) Cyberwarfare and cyberterrorism. 3) Security and terrorist attacks.

3.3. Do Security Risk Communication in all Project Tasks

The importance of this step boils down to the fact that many projects fail due to the fact that someone in the organization did see the signs of the risk but failed to communicate with the team about it. The best way to avoid this problem is to frequently carry out risk communication. A good approach to do that is by making risk communication part of every task performed. In every

meeting, risks should be discussed. It should be in the top priority of the meeting so that the team members realize that risks are important to the management. Team members should have a time to participate in this risk evaluation so that they have a chance to communicate the risks to their managers. In order to make sure that any sign of risk that is present in the project is reported to the management, risk communication should be implemented. The project team will have to report any type of risks which may arise throughout the project life in order for the management to take action faster and prevent the risk from happening or minimize its impact.

3.4. Prioritize the Project Security Risks

Risks are not the same. Some risks have higher negative impact than others, and therefore should not be treated equally. For a project to be successful, it is critical that the project manager prioritizes the risks. Risks that can cause a huge damage and big losses are the ones that should be dealt with first. There is no standardized way on how to prioritize risks. Risks can be prioritized based on gut feeling, however the best way is to prioritize risks is to have an objective way to do it which depends on a set of criteria. The two most important criteria are the effects of risk and the likelihood of that risk to happen. Project manager may add other criteria depending on the type and project objectives. For Qatar FIFA world cup a few risks can be classified as high priority risks which require a fast reaction and more attention than others. Based on the nature of the Qatar FIFA world cup, some risks have been identified as high priority risks. These risks are shown in Fig3. Identified risks are 1) Information security attack to delay in finalizing stadium designs, games logo and other project specifications. 2) Cyberwarfare and cyberterrorism. 3) Security and terrorist attacks.

	High (0.3 to 1)			3
Probability	**Medium (0.1 to 0.3)**	2		
	Low (0 to 0.1)		1	
		Low	**Medium**	**High**
		Impact		

Figure 3. Risk Map for Qatar FIFA World Cup.

3.4.1. Information security attack to delay in finalizing stadium designs, games logo and other project specifications (Low probability with medium impact). The probability of delay in designs of building stadiums and facilities centers is low likely to occur due to the organizing country has the capabilities of providing enough fund and resources to protect and finish all designs needed for building the stadiums before time. Furthermore, the country already has a good infrastructure of many building requirements as good quality airports, transportation, and hotels. By today, maybe half of the building requirements already exist. Unfortunately, the risk still exists that attacks on designs databases could make the organizing country fail to provide some stadiums and facilities needed before games starts on year 2022. Furthermore, the country has historical political problems with the neighboring countries. If any of these identified risks happen the risk impact is medium at border of high since the country already have some good stadiums because there were several major sport events organized.

3.4.2. Cyberwarfare and cyberterrorism (Medium probability with low impact). The probability of cyberterrorism to occur is high due to availability of internet connection and the creativity of hackers to cross the security barriers. Qatar would be an easy target specially to hackers from outside the country. But the impact is law due to easily recovery and backup systems that can restore all the damages within hours.

3.4.3. Security and terrorist attacks (High probability with high impact). The probabilities of terrorist attack during Qatar FIFA world cup is high due to games have players from all countries from the world. Some of the countries are in war with others. the organized international terrorism will find the time to attack. This impact is also high because the attackers are easy to get to the targets. Suicide attack require easy to find resources, but the results sometimes is up to killing more than 40 people.

3.5. Risk Analysis

Once the possible risks to project have identified and prioritized, the next step is to perform a risk analysis. The success of response to the risk project is facing depends entirely on how well the risk understood. Therefore, it is important to spend enough time in order to completely understand the nature of risks, their effects, and what could cause them. Project team have to name the risk and describe it. Furthermore, to be precise on what are referring to. Then start with the effects that the risk can cause. What could possibly happen. Describe the risks that can take place after the risk occurs. Describe what these effects can cost project in terms of time, budget and quality. Describe what could be the secondary effects of the primary effects of the risks and how far the impact can go. The other part of the risk analysis is to look at the causes of the risks. Nothing happens without causes. The best way to prevent risks from taking place is to look at the causes of these risks. Project team must list all the possible causes of the risk according to their percentage of contribution in causing the risk. Gather as much information as can in this stage as the information here will provide a valuable insight and will be useful when preparing the risk response. To do risk analysis:

3.5.1. Security attack to delay in finalizing stadium designs, games logo and other project specifications. Causes: 1) Controversy over the cost and design of the stadiums; 2) Designs are not according to requirements. Impact: 1) Delay in constructing the stadiums. 2) Delay in finishing the project on the right time. 3) Increase in budget required to finish a lot of tasks in short time. 4) Limited time to finish the tasks could compromise the quality of the final products.

3.5.2. Cyberwarfare and cyberterrorism. Causes: 1) Less experience at countering potential cyberwarfare and cyberterrorism. 2) Security practices are generally poor. 3) Fast growing threats of cyberwarfare and cyberterrorism. Impact: 1) Causing failure to the whole project. 2) Could hurt the reputation of Qatar.

3.5.3. Security and Terrorist Attacks. Causes: 1) Growing terrorist activities especially in global events like Olympics and games. 2) Weak crime prevention systems in Qatar. 3) No previous experience with terrorist attacks. Impact: 1) It could cause many casualties as a result of any terrorist activity during the event. 2) It could lead to the failure of the event.

3.6. Plan Risk Responses

All the previous steps of project risk management process were about collecting information about the risks, but this step is completely different. It is the step that really adds value to project risk management and planning. When planning risk responses, there are four strategies that can help mitigate the risks.

3.6.1. Avoidance of risk. The Avoidance of risk. This strategy involves organizing project in such a way to avoid the occurrence of the risk. This could be done by changing project plan, adapting new technologies and methods of doing the tasks. This strategy is about finding other ways to do the same task while avoiding potential risks.

3.6.2. Accept the risk. Sometimes there is no solution to the risk and the only option left is to accept the risk and try to find a way to minimize its negative impact on the overall project.

3.6.3. Minimize the risk. This strategy is based on the fact that not all risks can be avoided. Some risks are meant to happen; therefore, it is important to know how to successfully minimize the effects of such risks.

3.6.4. Transfer the risk. A better way to mitigate the risk when project team cannot deal with it is to transfer the risk to a third party that has the experience and can help you minimize the impact of the risks.

3.7. Monitor and Control Security Risks

In order to monitor and control the risks, a proper tracking system must be put in place. This step is about creating a risk log book in which is used to track all risks and associated tasks. Risks details and descriptions, risk responses and the tasks associated with it must be kept in this log. The risk log book should be updated in a regular basis preferably every week.

4. Conclusions

One of the critical success factors in managing any project is the security risk management. This paper starts by defining the research gap, problem statement, and objectives. Therefore, there is a need to integrate information risk management when implementing the Qatar FIFA world cup. Good practice project risk management process involves several important steps presented in the information security management system ISO/IEC 27001:2013, which is a standard that provides all the requirements for establish, implement, maintain, and improve the organization's information security management system [11], [12]. Security risk management process were to be applied to the Qatar FIFA world cup are introducing risk management, risk identification and mapping, risk communication, prioritize the risks, and finally do the risk analysis. By implementing the proposed solution as a model for information security management system for the FIFA world cup 2022, it can be audited and certified by wide range of standards.

References

[1] Project Management Institute, *A guide to the project management body of knowledge (PMBOK® Guide)*, 6th ed. Newtown Square, PA: Project Management Institute, Inc., 2017.

[2] C. Champman and S. Edition, *Project risk management, process, techniques and insights*. The Atrium, Southern Gate, Chichester: John Wiley & Sons Ltd, 2003.

[3] R. K. Wysocki, *Effective complex project management: An adaptive agile framework for delivering business value*. Ross, J. Publishing, Incorporated, 2014.

[4] S. Seyedhoseini, S. Noori, and M. Hatefi, "A gap analysis on the project risk management process," *Kuwait J. Sci. Eng.*, vol. 35, no. 1B, pp. 217–234, 2008.

[5] L. Birmingham and D. McNeill, *Strong in the rain: surviving Japan's earthquake, tsunami, and Fukushima nuclear disaster*, 1st ed. New York: Palgrave Macmillan, 2012.

[6] X. Li, M. Alshawabkeh, and Z. Li, "Security risk management approach for improving information security return of investment," in *Recent Developments in Data Science and Business Analytics. Springer Proceedings in Business and Economics*, 2018, pp. 209–216.

[7] G. Cup, "List of Champions Gulf Cup." [Online]. Available: www.gulfcup.sa/en/archives.php?id=2. [Accessed: 19-Dec-2018].

[8] M. M.-J. Chan, "Tokyo's Challenges in Hosting the 2020 Olympics," *Econ. Cult. Hist. Japan Spotlight Bimon.*, vol. 34, no. 3, pp. 34–37, 2015.

[9] DFRWS, "A Road Map for Digital Forensic Research," in *The Digital Forensic Research Conference*, 2001.

[10] D. L. Watson and A. Jones, *Digital Forensics Processing and Procedures*. Syngress Print, 2013.

[11] ISO/IEC27001, "Information technology -- Security techniques -- Information security

management systems -- Requirements," *ISO/IEC 27001:2013 Information Security Management System*. International Organization for Standardization (ISO), Switzerland, p. 23, 2013.

[12] ISO/IEC27002, "Information Technology -- Security Techniques -- Code of Practice for Information Security Controls," *Code of Practice for Information Security Controls*. International Organization for Standardization (ISO), Switzerland, p. 80, 2013.

[13] M. Alshawabkeh, M. M. Saudi, and N. H. M. A. Alwi, "Computer security factors effects towards online usage of internet banking system," in *Advancement in Information Technology International Conference - ADVCIT (Theme: Towards Innovation in Information Technology)*, 2015, vol. 10, no. 2, pp. 532–539.

[14] M. Alshawabkeh, M. M. Saudi, and N. H. M. A. Alwi, "Computer security factors effects towards online usage of internet banking system," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 2, pp. 532–539, 2015.

[15] K. Brotby, *Information security governance: a practical development and implementation approach*. Hoboken, New Jersey: John Wiley Sons, 2009.