Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 2250-2260

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

Analyzing the Playstation Network Hack Through PMBOK Lenses

Anastazry Faidzli[1], Duurgashini P Balan[1],Nuvanehsan M Selvan[1], Jonathan Joseph[1],Mathushini Kathiraveloo[1], Thaswin Muralikaran[1],Vimalla Subramaniam[1], Danish Hossman Abd Rahman[1], Siti Hajar Arbain[1]*

[1]Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2023.04.02.132
Received 15 November 2023; Accepted 16 November 2023; Available online 30 November 2023

Abstract: The PlayStation Network outage (sometimes referred to as the PSN Hack) was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and PlayStation Portable consoles from accessing the service. This report dives into the many facets of the PSN hack, exploring the circumstances that led to the breach, the ramifications, and the responses. This case study highlights the need to incorporate these knowledge domains into complete risk mitigation and recovery strategies, reinforcing the importance of proactively handling and aligning stakeholders' interests. The focus of the report will be on how each of these knowledge domains contributed to considering, dealing with, and eventually recovering from the PlayStation Network attack. In the context of a global-scale data breach, this research serves as a sharp reminder of the consequences of poor procurement management, insufficient risk assessment, quality control, and stakeholder involvement. The insights gathered from this case study will provide significant lessons for organizations across industries, underscoring the crucial relevance of rigorous management practices in protecting the interests of all stakeholders against unanticipated dangers.

***Keywords**: PlayStation, PSN, Hacking*

1. Introduction

Issues of security and privacy data breaches were hardly widespread or viral back in the day as they are in today's era of globalization and advancements in the field of information technology. But when they did occur, it was highly likely to have happened on a huge scale and were published in mainstream media. Such was the case in 2011 when Sony PlayStation's PSN online services (PlayStation Network) had been reportedly breached and allowed hackers to obtain the private and sensitive data of nearly 77

**Corresponding author: sitihajara@uthm.edu.my*

million users[1]. Although the crisis had been averted swiftly due to the effective procedures by Sony, it has raised questions over personal and privacy data encryption and storage, and how far can we trust third parties with invaluable private data such as identification cards, bank & and credit card information, and others.

Amongst the key factors that allowed this data breach or hack to occur was due to the insufficient and 'bare-bones' online infrastructure of the PSN Network during its early days of operations. As explained by Atlantis Press Journal style in this explanation the release of PlayStation 3 together with the inclusion of the PSN online services garnered widespread attention from people around the globe in 2005 [2]. But problems started to arise after its eventual release; direct comparisons by their fellow competitor console, the Xbox 360, with its simplistic yet secure and rewarding online services, deemed the PSN's lackluster and not-so-user-friendly interface to not just being disliked by owners of PS3's and PSP's, but also attracting the attention of fellow hackers too.

Through multiple thorough discoveries and research, experts eventually found that the PSN's weak online store infrastructure was also benefited by the shockingly unsecured private user data that were left out in the open on Sony Computer Entertainment's database with little to minimal encryption. This had become apparent after a hacker syndicate group known as Anonymous had performed the data breaches repeatedly in 2011 which had prompted Sony to take proper evasive measures once and for all; they had halted their PSN servers temporarily and performed a week-long maintenance to strengthen their online infrastructure and privacy database of their consumers [2]. Although this issue was rectified during the end of the PlayStation 3's lifecycle and being further improved on for the PlayStation 4's PSN ecosystem, it was a lesson well-learned not just for Sony, but also for the public consumers as well.

The 2011 PlayStation Network (PSN) breach serves as a multifaceted case study that highlights the interconnected nature of project management knowledge areas and their critical role in preventing and managing organizational crises. Sony Interactive Entertainment, in the context of the PSN breach, could have benefited from a more comprehensive approach as outlined in the PMBOK, particularly in the knowledge areas of procurement management, risk management, quality management, stakeholder management, and cost management.

This issue largely deals with the low amount of awareness by the public towards the private encryption and storage of sensitive data during the early days of online services and interconnectivity. Thus, some of the takeaways from this issue include the caution and awareness that we must approach a third-party service before trusting them with our personal and private data. We must also do thorough background checks about their prior history with cyberattacks and the effective countermeasures they have managed to perform to tackle these issues. We must also set additional security questions to enhance our login security and enable two-step verification on online platforms in order to prevent information breaches from important accounts. Here in lies a dilemma whether we can trust everything we see on the Internet, but no matter to what degree of genuineness it implies, it is always advisable to be careful and mindful at all times because, at the end of the day, you can never be too careful in a dark, exposed and dangerous ecosystem like the World Wide Web.

2. Knowledge Areas

The Project Management Body of Knowledge (PMBOK) is an all-inclusive framework that describes accepted terms and best practices for efficient project administration. In this framework, procurement management, risk management, quality management, stakeholder management, and cost management are the five critical knowledge areas that are essential to project success and efficiency. There are a total of nine knowledge areas in the PMBOK but only five are chosen for this report.

Procurement Management is a critical aspect of PMBOK, focusing on the processes necessary for purchasing or acquiring products, services, or results from outside the project team. This area is essential for ensuring that the procurement contributes to the project objectives in terms of quality, timeliness, and cost-effectiveness [3]. Effective procurement management not only aids in acquiring necessary resources but also aligns these acquisitions with the project's goals and timelines.

Risk Management, another vital area, involves identifying, analyzing, and responding to project risks. This process includes maximizing the outcomes of positive events and minimizing the consequences of adverse events. Effective risk management is crucial as it helps in anticipating potential problems and planning responses, thereby reducing project uncertainties [3]. By foreseeing potential risks and establishing mitigation strategies, projects can maintain a steadier path towards their objectives.

Quality Management in PMBOK encompasses activities and processes required to ensure that the project satisfies the needs for which it was undertaken. This includes managing both project and product quality through planning, managing, and controlling project and product quality requirements. Meeting stakeholders' objectives through quality management is essential for the overall success of the project [3]. It ensures that the project's deliverables are of a standard that meets or exceeds stakeholders' expectations.

Stakeholder Management is about identifying and analyzing stakeholder expectations and developing strategies for engaging them effectively in project decisions and execution. Since stakeholders have a big say in how the project turns out, controlling their expectations and involvement is essential to its success [3]. Stakeholder management that is effective makes sure that everyone participating in the project is communicating clearly, knowing what is going on, and supporting it.

Last but not least, cost management entails organizing, projecting, funding, managing, and regulating expenses to guarantee that the project is finished within the permitted budget. This area is key to delivering a project on budget, a critical component of project success [3]. Effective cost management ensures that resources are used efficiently and that the project delivers value within its financial constraints.

In summary, these five knowledge areas of PMBOK - Procurement Management, Risk Management, Quality Management, Stakeholder Management, and Cost Management - are integral to the successful delivery of projects. They ensure that projects are well-planned, executed efficiently, and meet their intended objectives while satisfying stakeholder requirements and staying within budgetary limits.

2.1 Procurement Management

Procurement management involves securing goods or services for a business by engaging in purchasing, leasing, or entering into contractual agreements with external sources to fulfill project requirements [4]. According to the PMBOK, it starts with procurement planning, solicitation and the source selection phase and finally, contract closure that formalizes the end of the procurement [3]. There are a few things relating to procurement management that Sony should have done to prevent this disastrous incident from occurring in the first place.

The Playstation network is one of the biggest gaming networks available on the market. Being that, the company is expected to deal with sensitive user data such as passwords, credit card details and much more. It was expected that Sony would take this matter seriously by performing regular risk assessment on their network, identifying potential risk and fixing the issues. Unfortunately, this was not performed or performed poorly as seen when the data breach occurred in 2011. Sony has announced the enlistment of an external cybersecurity firm to probe the incident [1]. This is a great response taken by Sony by accepting the fact that the company has messed up and needs to outsource the services from other

companies. The firms procured by Sony were tasked to investigate the incident. Due to the fact that these companies are not their staff, this can help ensure that the investigation is impartial and unbiased, especially if the breach may have involved internal security lapses. Cybersecurity firms are also experienced in responding quickly to security incidents. Their prompt involvement can help Sony identify and address the breach more effectively. By procuring the services of experts, Sony can also demonstrate its commitment to protecting customer data and rebuilding trust among its user base.

But what is done, is done. Sensitive user data has already been stolen at that time. To make matters worse, after a few months apart from the incident, Sony Pictures was hacked by an organization called Lulzsec. The organization's intentions were clear. They claimed to have executed a basic attack with the intention of exposing Sony's "shameful" security [5]. The group only did a simple successful SQL injection attack and then they are in the network. Even worse, the data obtained are not even encrypted. In their statement, LulzSec remarked that none of the data they obtained was encrypted. They pointed out that Sony had stored more than 1,000,000 customer passwords in an unencrypted format, essentially making it easily accessible. LulzSec implied that Sony's lax security practices made this outcome inevitable. During the procurement process, Sony should have included in the procurement documents by specifying that the cybersecurity company should not only respond to incidents but also play a proactive role in enhancing overall security. The reasons that Sony did not include this in the scope of services is unknown but given the consequences that already occurred, it is mind boggling how this was not done. Cybersecurity incidents can seriously damage an organization's reputation. Taking proactive security measures demonstrates a commitment to safeguarding customer data and can help rebuild trust with the user base.

2.2 Risk Management

Risk management involves the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events as highlighted in Njogo's analysis of risk management in the Nigerian banking industry [6]. In Sony's case, the article suggests that there might have been shortcomings in anticipating the risk of a hack and in implementing adequate measures to prevent such a significant breach, or at least mitigate its impact. The incident led to a considerable loss of trust among stakeholders, and Sony had to take several steps to manage the crisis, communicate with affected parties, and try to restore confidence.

2.2.1 Risk Mitigation Action Points

In the event of a security breach or data theft, it is crucial to have a well-defined set of actions to mitigate the risks and minimize the impact on the organization and its stakeholders. The following figure which is Figure 1 illustrates the sequence of risk mitigation action points taken by Sony during the PlayStation Network (PSN) hacking incident in 2011, where personal data of approximately 77 million users was stolen.

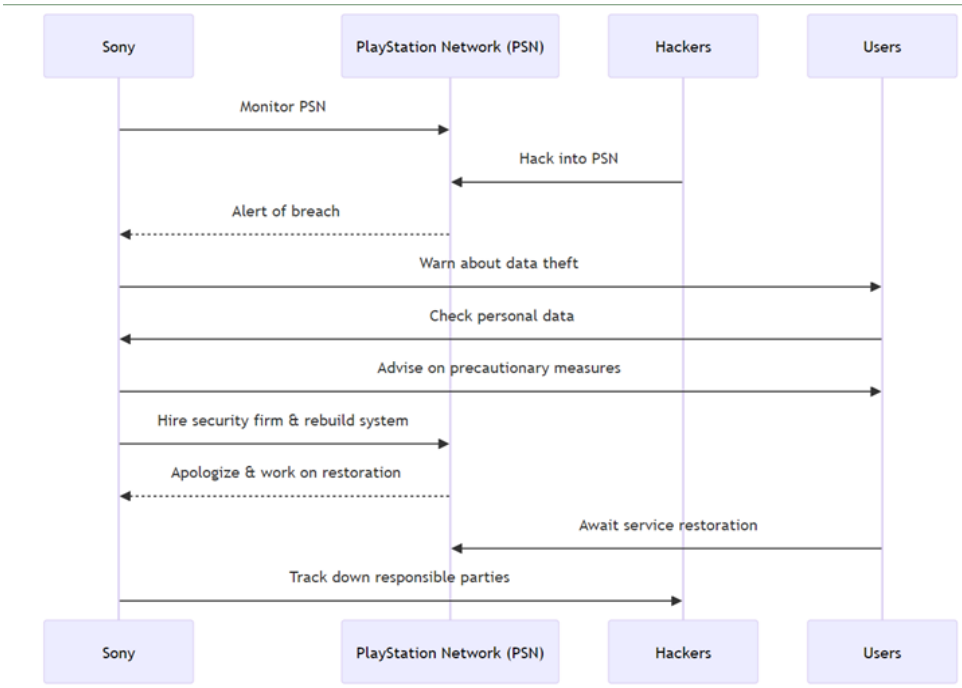

Figure 1: Risk Mitigation Action Points

- **Sony Monitors PSN:** Sony continuously monitors the PlayStation Network (PSN) to ensure its security and functionality.
- **Hackers Attack PSN:** Hackers initiate an unauthorized attack on the PlayStation Network, gaining access to user data.
- **PSN Alerts Sony:** The PlayStation Network system detects the security breach and alerts Sony of the incident.
- **Sony Warns Users:** Sony promptly informs its users about the data theft and the potential risks associated with the breach.
- **Users Check Personal Data:** Users take action by checking their personal data and account activity to identify any unauthorized access or changes.
- **Sony Advises Precautions:** Sony advises users to take precautionary measures, such as monitoring their credit card statements and being vigilant against potential scams.
- **Sony Hires Security Firm & Rebuilds System:** Sony hires an external security firm to investigate the breach and takes steps to rebuild its system to enhance security measures.
- **PSN Apologizes & Works on Restoration:** The PlayStation Network apologizes to its users and works diligently to restore its services.
- **Users Await Service Restoration:** Users await the restoration of PlayStation Network services.
- **Sony Tracks Down Hackers:** Sony commits to tracking down the individuals or groups responsible for the hacking incident.

The Risk Mitigation Action Points outlined in the figure and the subsequent steps taken by Sony during the PlayStation Network hacking incident exemplify the importance of a robust and well-structured risk mitigation plan. The ability to promptly identify, assess, and respond to risks is crucial in safeguarding an organization's assets, reputation, and stakeholder trust. By implementing effective risk mitigation strategies, organizations can minimize the impact of adverse events, ensuring the continuity and resilience of their operations [7].

2.2.2 Risk-level Matrix

The PlayStation Network hacking incident was a significant event that had far-reaching implications for both Sony and its user base. In order to fully understand the impact of this incident, it is important to analyze the various risks that were involved, and assess their likelihood, impact, and overall risk level. The Risk-Level Matrix is a valuable tool in this analysis, providing a clear and concise visual representation of the different risks associated with the incident. By categorizing each risk and evaluating its potential consequences, we can gain a better understanding of the incident's overall impact and identify the areas that require the most attention and mitigation efforts as shown in Table 1.

Table 1: Risk-Level Matrix for PlayStation Network Hacking Incident

Risk Event	Likelihood	Impact	Risk Level
Unauthorized access to user data	High	High	Critical
Financial implications due to potential credit card theft	Medium	High	High
Loss of trust among stakeholders	High	Very High	Critical
Legal implications and potential lawsuits	Medium	High	High
Damage to brand reputation	High	Very High	Critical
Temporary suspension of services	High	Medium	Critical
Potential phishing or scam attempts post-breach	Medium	Medium	Medium

The Risk Scale and Necessary Actions for the PlayStation Network Hacking Incident is a structured approach to address the risks associated with the incident as shown in Table 2. The scale categorizes risks into four levels: critical, high, medium, and low, each with its own description and necessary actions.

Table 2: Risk Scale and Necessary Action for PlayStation Network Hacking Incident

Risk Level	Description	Necessary Actions
Critical	Risks that have a high likelihood of occurrence and can have severe consequences.	● Immediate action required. ● Engage senior management and stakeholders. ● Allocate maximum resources to mitigate.
High	Risks that are likely to occur and can have significant consequences.	● Prioritize action. ● Engage relevant teams for mitigation strategies. ● Monitor closely.

Medium	Risks that may or may not occur and have moderate consequences.	● Schedule for review. ● Implement standard procedures to mitigate. ● Regularly monitor
Low	Risks that are unlikely to occur and have minimal consequences.	● Monitor periodically. ● Implement preventive measures as part of routine operations.

By categorizing risks into these four levels and outlining the necessary actions for each, project managers can effectively prioritize and address the risks associated with the PlayStation Network hacking incident. This structured approach ensures that resources are allocated efficiently, and risks are managed effectively to minimize their impact on the project.

2.3 Quality Management

Quality management is the process of overseeing all the necessary tasks and activities to uphold a specific level of excellence. This includes creating a quality policy, implementing quality assurance and planning, as well as incorporating quality control and improvement measures [8]. According to PMBOK, quality management is broken down into three main phases which are quality planning, quality assurance, and quality control. These three phases should be taken seriously by Sony Interactive Entertainment in managing the quality of PlayStation Network's security to avoid this disastrous hack from happening in the first place.

The massive hack exposed the possibility that Sony's early security measures were insufficiently thorough to safeguard its users' personal information and credit or debit card information. A careful evaluation of potential threats and the implementation of strong security measures to reduce such risks are essential components of quality planning. Sony should have identified the quality requirements for security of PlayStation Network (PSN) which includes data protection, user authentication, encryption standards, and threat detection. These quality requirements are important for securing user data. For the purpose of identifying potential security threats and weaknesses that the PSN might encounter, Sony should have carried out a comprehensive risk assessment which helps in understanding potential risks. Moreover, Sony should have established quality metrics to measure the quality of PSN's security. Quality metrics such as intrusion attempts, incident response times, and encryption strength should be monitored and reported from time to time to get an insight of PSN's security effectiveness.

Quality assurance process is linked to continuous improvement and analysis process [9]. Sony's security measures did not prevent unauthorized access and data breaches, indicating a gap in quality assurance processes. Sony should have established a system that continuously monitors PSN's security protocol to find any weaknesses. This will regularly evaluate the effectiveness of security measures. Next, to find and fix possible security flaws, Sony should have implemented regular security audits carried out by in-house and outside specialists. It would have been easier to evaluate the continued effectiveness of security measures with regular reviews. Moreover, Sony should have introduced continuous training initiatives to ensure that employees, particularly those in charge of overseeing and protecting the PSN, were up to date on the newest security risks, recommended procedures, and the

significance of following security guidelines. By implementing these processes, quality assurance of PSN's security could have been strengthened and able to prevent the massive hack.

Quality control involves overseeing the project metrics established during the quality planning phase to verify their satisfactory performance [9]. The incident proved clearly that Sony's quality control systems were unable to identify and address security flaws in a timely manner. Implementation of strict access control should be implemented and monitored by Sony to ensure that only authorized persons had access to sensitive data and the system's important part. Moreover, Sony could have ensured that industry standard encryption and data protection measures are implemented and works effectively. Quality control means making sure that systems stay current with the newest security updates and patches. Sony should have set up a robust system to promptly apply security updates, including patches to fix software vulnerabilities which ensures PSN's security remains secured.

Overall, the importance of implementing effective quality management can be seen in Sony' case. Following quality management phases like quality planning, quality assurance, and quality control assists organizations in identifying potential threats, strengthening the security, and maintains the effectiveness of the system's security. By implementing effective quality management can prevent security breaches and protect user data from being compromised.

2.4 Stakeholder Management

The 2011 Playstation Network (PSN) breach is a notable case study in the realms of cybersecurity and crisis management, providing a wealth of insights on how stakeholder management plays a vital role in the response and recovery phases of an organizational crisis [10]. The PMBok (Project Management Body of Knowledge) framework serves as a complete lens for examining the dynamics of stakeholder management throughout this high-profile incident.

Sony employs a wide range of communication activities through an established set of public relations protocols to create and maintain favorable relationships with various stakeholders, such as employees, PlayStation users, shareholders, suppliers, investors, government agencies, and gaming society in general. Stakeholders that require information about Sony can easily obtain it via the company's website [11]. Sony creates a single platform(touch-point) for mutual relationships with its stakeholders, including providing for its consumer's needs and demands.

One of the key principles of stakeholder management is communication. It is important to communicate regularly with stakeholders about the project's progress and to ensure that stakeholder's needs are being fulfilled. In the case of the Playstation Network Hack, Sony could have communicated with its clients more quickly and transparently about the incident. Sony could have provided regular updates on the status of the investigation and on the steps that the company was taking to protect the client's data. Another principle of stakeholder management is engagement. Engaging stakeholders in the project planning and decision-making process helps to build trust and reliability. Sony could have engaged with its clients by asking the clients for feedback on how the company should respond to the hack. Sony could have also engaged with security experts to develop a more robust cybersecurity plan.

Furthermore, it is important to manage stakeholder expectations. Stakeholders should have a clear understanding of the project's goals and objectives, as well as the timeline and budget. Sony could have managed stakeholder expectations by setting realistic expectations about how long it would take to resolve the hack and how much it would cost to protect the client's data.

The Project Management Body of Knowledge (PMBOK) is a set of standards and guidelines for project management. By using PMBOK, Sony could have applied stakeholder management principles to the Playstation Network Hack. For example, Sony could have used PMBOK to develop a stakeholder management plan that identified all of the key stakeholders in the hack, assessed stakeholder's needs and expectations, and developed a plan for communicating with the stakeholders

and managing their expectations [12]. Furthermore, Sony could have used the PMBOK's risk management knowledge area to identify, assess, and respond to the risks associated with the hack. For example, Sony could have identified the risk of losing customer trust and taken steps to mitigate that risk by communicating with customers quickly about the incident.

Finally, by applying stakeholder management principles and using the PMBOK as a framework, Sony could have improved its responses to the Playstation Network Hack and reduced the negative impact of the incident on its reputation and business.

2.5 Cost Management

The process of project cost estimation, budgeting, and control is known as cost management. Cost management is a process that starts in the planning stage and lasts the whole project as managers keep an eye on, review, and make adjustments to expenses to make sure the project stays within the allocated budget [13]. Cost management is a continuous, fluid process. However, there are four main elements or functions that can be found in any cost management plan which are resource planning, cost estimating, cost budgeting, cost control. Resource planning is the first phase in any cost management process where the cost manager looks over the project's specifications and scope to determine what resources the project will need. Estimating the cost of resource acquisition is the next step after compiling a list of required materials. Cost budgeting is a thorough strategy that outlines how much, for what, and by when you want to spend money on a project. And finally, the act of tracking and accounting for expenses as a project moves along, making necessary adjustments, and notifying stakeholders of issues as they arise is known as cost control [13].

PlayStation Network is an online service that allows users with a PlayStation account and an Internet connection to access various services for their PlayStation consoles and other devices. During April 2011, the PlayStation Network, or PSN, was unavailable, and players worldwide have been vocal about their frustration on the Internet [1]. Upward of 77 million registered PlayStation Network users had their personal information, passwords, and potentially credit card numbers stolen by cybercriminals. These days, data breaches are the most talked-about topic worldwide. In certain places, they are also closely related to the global economy [14]. Millions of user passwords were exposed which stopped many users from using playstation. This incident also resulted in financial and reputation loss to the Playstation Network.

During the cost management process, Sony should have prioritized the cost management area to avoid hacking, data breaching, and to make sure the personal data of their users are safe. In the cost management, cost estimates and budgets are developed based on the project risks. The costs associated with potential data breaches. system downtime, and reputation damage need to be considered in cost estimation and budgets. This process recommends the inclusion of contingency reserves in the project budget to account for unforeseen events. Investing in cybersecurity measures, such as firewalls, intrusion detection systems, and employee training, incurs costs. After a cybersecurity incident, there are costs associated with recovering compromised systems, conducting forensic analyses, and implementing security improvements. These recovery costs should be considered in the overall project budget.

By integrating these considerations, project managers can develop a more comprehensive understanding of the financial implications of cybersecurity issues and incorporate effective cost management strategies to address them. This approach helps ensure that the financial aspects of cybersecurity are integrated into the overall project cost management framework, contributing to a more secure and resilient project environment.

3. Conclusion And Recommendation

The remarks highlight the multiple issues and repercussions involved with the PlayStation Network (PSN) attack in 2011. The case study serves as a sharp reminder of the vital role that defined risk

mitigation plans, good quality management, thorough cost management, and stakeholder involvement have in protecting organizations against and limiting the consequences of security breaches. The inquiry into Sony's data breaches focuses on procurement and cybersecurity problems, emphasizing the importance of regular risk assessments and preemptive steps. External cybersecurity firms are recognized for conducting neutral investigations. The Sony Pictures tragedy that followed emphasizes the significance of encryption and preventive security measures. The inclusion of cybersecurity standards in procurement contracts is indicative of a forward-thinking approach to security.

Stakeholder management is highlighted as critical, with an emphasis on communication, engagement, and expectation management. The PMBOK framework is provided as a beneficial tool for analyzing stakeholder interactions, arguing that stakeholder management concepts should be applied during the PSN hack. The risk management knowledge area from the PMBOK is suggested for recognizing and managing hack-related risks. Cost management is seen as a constant and dynamic process, with an emphasis on prioritizing cybersecurity measures and analyzing associated expenditures. The recommendation to incorporate cybersecurity issues into the overall project cost management framework is intended to guarantee a thorough grasp of the financial consequences of cybersecurity difficulties.

In summary, the aggregate findings emphasize the need of taking a comprehensive and integrated approach to risk reduction, quality control, cost management, and stakeholder involvement when dealing with cybersecurity concerns. In an increasingly linked and digital society, the lessons acquired from the PSN disaster give significant guidance for organizations to reinforce their systems, safeguard user data, and preserve stakeholder confidence.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia and especially our instructor, Ts. Dr. Mazidah binti Mat Rejab for the support.

References

[1] PlayStation Network hackers access data of 77 million users," The Guardian. [Online]. Available: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data. [Accessed: 12-Nov-2023]

[2] B. A. Olaniran, "A Gamer's Nightmare: An Analysis of the Sony PlayStation Hacking Crisis," Journal of Risk Analysis and Crisis Response, vol. 4, pp. 151-159, September 2014.

[3] Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Sixth Edition, Project Management Institute, 2017.

[4] "What is Procurement Management? Why it Matters [2023]," Asana. [Online]. Available: https://asana.com/resources/procurement-management.

[5] "Hackers attack another Sony network," The Guardian. [Online]. Available: https://www.theguardian.com/technology/2011/jun/03/sony-network-hackers-lulzec. [Accessed: 12-Nov-2023].

[6] B. O. Njogo, "Risk management in the Nigerian banking industry," Arabian Journal of Business and Management Review (Kuwait Chapter), vol. 1, no. 10, pp. 100-109, 2012.

[7] R. Starr, J. Newfrock, and M. Delurey, "Enterprise resilience: managing risk in the networked economy," Strategy and Business, vol. 30, pp. 70-79, 2003.

[8] A. Barone, "Quality Management: Definition Plus Example," Investopedia, Mar. 23, 2022. [Online]. Available: https://www.investopedia.com/terms/q/quality-management.asp#:~:text=Quality%20management%20is%20the%20act,quality%20control%20and%20quality%20improvement.

[9] H. Rever, "Quality in project management—a practical look at chapter 8 of the PMBOK¬¬® guide," in PMI® Global Congress, North America, Atlanta, GA. Newtown Square, 2007.

[10] Bailey, T., Miglio, A. Del, & Richter, W. (2014). The rising strategic risks of cyberattacks. Retrieved 16.

[11] Sony Corporation. (2023). Sony website. Retrieved November 11, 2023, from https://www.sony.com/

[12] A Guide to the Project Management Body of Knowledge (PMBOK Guide) (6th ed.). Newtown Square, PA: Project Management Institute, 2017.

[13] T. D. Jainendrakumar and P. Margin, "Project Cost Management for Project Managers Based on PMBOK," PM World Journal, vol. 4, no. 6, pp. 1-13, 2015.

[14] D. P. Mozumder, M. N. Mahi, and M. Whaiduzzaman, "Cloud Computing Security Breaches and Threats Analysis," ResearchGate, 2017. [Online]. Available: https://www.researchgate.net/publication/320124329_Cloud_Computing_Security_Breaches_and_Threats_Analysis