Cyber Security Risk Management Strategy for VG Trading Company

Chaewon* & Jiyoung**

*Associate professor, Department of Management, Hanyang University, South Korea. E-Mail: cha.12won@yahoo.com
** Professor, Department of Management Hanyang University, South Korea. E-Mail: youngmba@gmail.com

Received : 14.02.2019 **Revised : 25.05.2019** **Accepted : 18.07.2019**

***Abstract*---** For governments, large enterprises, individuals, small businesses, and other parties participating in modern society, one of the major concerns is the aspect of cyber security. With cyber attacks and criminals complicating the nature of this field via sophisticated approaches, it is apparent that the need for a deeper focus on cyber security risk management cannot be overemphasized (Abomhara & Koien 2015). Whereas investments in perimeter defences have increased, internal threats emerging from third parties such as vendors and contractors and even company employees add to security incidents (Amoroso 2013).

***Keywords*---** Risk Management, Cyber Security, Investment

I. INTRODUCTION

MAJOR approaches that have been advocated in a quest to reverse this trend include solid employee training in relation to cyber security and embracing a close management and monitoring of third parties that include contractors and vendors, poised to curb enterprise level security breaches (Crowell 2010). This paper formulates a cyber security risk management strategy, focusing on a small-medium business, VG Trading Company.

II. RISK MANAGEMENT PLAN

The plan is grounded in security prioritization and, operational and thought leadership. The main aim is to harmonize risk management language, methodologies, and technologies across the selected enterprise. In addition, the plan seeks to improve the company's visibility into its cyber security risk landscape via the identification of strengths and opportunities for improvement. By steering a better-informed risk tolerance culture, the aim of the plan is to identify potential security solutions, develop operational and capital expenditures, and better set cyber security priorities at the company. Hence, specific objectives include:

- To create a set of best practices and reusable tools for utilizing the cyber security management plan towards assessing infrastructure risks
- To communicate a cyber security that is aligned to senior leadership needs and preferences
- To inform the prioritization and budget planning process surrounding VG Trading Company's cyber security
- To establish an organizational alignment of VG Trading Company's objectives of risk tolerance

One of the areas of focus will be the people. Specifically, company employees will receive regular training and briefings to gain an awareness of company security escalation paths and resources. This provision of staff awareness pipeline is deemed important because they are expected to be in charge of strategy implementation towards assuring cyber security. Another area of focus concerns the process. To achieve risk-informed procedures and processes, the strategy seeks to ensure that the target firm actively adapts to sophisticated and evolving threats, a changing cyber security landscape, and predictive indicators to assure preparedness for future uncertainties. In addition, focusing on the process of strategy implementation will aid in ensuring that the company responds to events in a timely manner. The third area of focus will concern the technology. Specifically, the strategy seeks to ensure that the tools deployed in the company and industry's environment are reviewed regularly for coverage against changes in internal ecosystems and the threat environment. Indeed, the focus on technology is informed by the need for the strategy to ensure that the company's tools deployed anticipate any emergent threats. The last area of focus concerns the ecosystem, constituting third parties and other industry players. Indeed, the strategy seeks to advocate for the organization's success in risk management and active sharing of data with partners in a quest to ensure that the current and accurate information leads to improved ecosystem cyber security prior to the occurrence of events. In summary, major components of the strategy include the ecosystem, technology, process, and the people (company employees). From the perspective of compliance, the strategy will ensure that the target groups' right to privacy (such as company employees and third-party vendors and contractors) is not contravened.

Risk Management Plan and Implementation

The Selected Risk Identification and Evaluation Methodology

The central approach adopted is the qualitative cyber

10.9756/SIJCSEA/V7I4/03010020402
ISSN: 2321-2381

security risk assessment. According to Goolsby (2013), this method implies that the subjective qualities associated with the respective risks are used as key predictors and aid in indicating merit in relation to other or related risks. As affirmed by Liff (2012), one of the alternatives is to assess risks as high, medium, or low. Therefore, this methodology is informed by the probability that a risk is likely to occur. The approach also centers on the probability that the perceived impact is likely to pose on the targeted firm. Therefore, this plan seeks to categorize risks based on their source and the effect or vulnerabilities that they are likely to have on the enterprise, as well as the organization's stakeholders. From the context of cyber security, the adoption of a qualitative methodology in the current plan implies that focus will be on the discovery and review of the company's assets (such as human resources, processes, software, and hardware) to establish known weaknesses against potential vulnerabilities' databases. By measuring the respective risks against relative scales, the plan seeks to determine the probability that the perceived threats could exploit VG Trading Company's vulnerability. Indeed, this method (qualitative methodology of identifying and evaluating cyber security risks at VG Trading Company) has been selected because it is not only less expensive and faster but also enables companies to streamline their timetables while minimizing the respective budgets (Porche, Paul & York et al. 2013).

In situations where the cyber security risks are low, it has been documented that it is very difficult to circumvent or pass through the device or control and the system requires experienced experts or very high skill levels. In addition, low risks imply that little or no sensitive data is lost or leaked and poses very little impact on system users and company critical infrastructure. Thus, low risks are marked by an existence of log management and related controls responsible for reporting, blocking, and detecting intrusion with ease (Reddy & Reddy 2014). In situations where risks are deemed by the qualitative approach as moderate, the attacker could circumvent or pass through the system successfully only in the existence of certain conditions, requiring moderate skill. In such a case, full breach is improbable and sections of system users or critical infrastructure may be affected, depicting the presence of insufficient log management and related controls responsible for the detection and blockage of intrusions (Sabrine, Muriel & Stéphane 2015). Lastly, high risks imply that the attackers not only circumvent or pass through the device or control successfully but also require little skill and are likely to gain full access to critical infrastructure and operate the system users' accounts, depicting probable breach. As observed by Tabor (2013), high cyber security risks depict an absence of adequate detection controls. With VG Trading Company emerging as a smaller scale enterprise, the qualitative methodology of risk identification and evaluation is deemed cost-effective or economical, ensuring that the company's adoption and implementation of strategies such as recommended controls do not make it cash-strapped.

A Risk Assessment of VG Trading Company's Cyber Security Using the Qualitative Methodology

Table 1: Risk Assessment

Identified threat/ VG Trading Company functions	**Systems**	**Impact (1-5) (high, medium, low)**	**Likelihood (1-5)**	**Risks**	**Risk rating (high, medium, low)**	**Priority rating (high, medium, low)**
Unauthorized access (accidental or malicious)	Onsite server environment	5	5	Loss of brand image or company image due to the resultant breach	High	High
Data misuse by authorized users/employees	Payment gateway service	3	3	Compromised company confidential data	Medium	Medium
Unintentional exposure/data leakage of customer information	Customer service and support	2	2	Loss of customers due to security-related fears surrounding leakage of personal data	Medium	Medium
Customers	Field area network, routers, bridges, head-end collector	4	4	Loss of company revenue and possible attack-vectors into the company's back-end systems	High	High
Corporate services	Stock-inventory systems and the online store	3	3	Lost ability to run the company's day to day functions	Medium	Medium

III. CONCLUSION

From the case description, VG Trading Company deals in high-end micro-electronic components and, through online sales, distributes these products directly via purchase orders and contracts. Similarly, the customer base of VG Trading Company entails large corporations but the process of supporting, maintaining, and managing in-house systems is conducted by a small IT team and the management of the

10.9756/SIJCSEA/V7I4/03010020402
ISSN: 2321-2381

company's externally hosted systems and the hosted services, a trend that threatens to prompt malice, should a cyber security risk management strategy not be implemented. With several services hosted onsite and acting as the dominant environment for the company's stock-inventory systems, financial and planning processes, help-desk, and Customer Management System (CMS), it is evident that the information environment at this company is prone to security threats; exacerbated by the arrangement to enable the gateway form a platform for making customer payments. As documented by Van Niekerk and Maharaj (2012), such a small-medium business could experience massive damage to its reputation and not only lose assets but also incur significant expenses towards fixing the resultant damage, should it fail to implement a cyber security risk management strategy.

REFERENCES

[1] Abomhara, M., & Koien, G.M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security*, 4, 65-88.

[2] Amoroso, E.G. (2013). Cyber attacks: Protecting national infrastructure. *Elsevier, Waltham, M.A.*

[3] Crowell, R.M. (2010). War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare. *Newport: Naval War College*

[4] Goolsby, R. (2013). On Cybersecurity, Crowdsorucing, and Social Cyber-Attack. *Arlington: Office of Naval Research.*

[5] Liff, A.P. (2012). Cyberwar: A new "absolute weapon"?: The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428.

[6] Porche, I.R., Paul, C., York, M., Serena, C. C., Sollinger, J.M., & Axelband, E. (2013). Redefining information warfare boundaries for an army in a wireless world. *RAND Institute, Santa Monica*.

[7] Reddy, G.N., & Reddy, J.U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *International Journal of Engineering and Technology*, 4(1), 48-51.

[8] Sabrine, S., Muriel, C., & Stéphane, B. (2015). Infowar on the Web. *Proceedings of the ACM Web Science Conference on ZZZ - WebSci '15*, 1-3.

[9] Tabor, R. (2013). NATO Information Operations in Theory and Practice: Battling for Hearts and Minds in Afghanistan. *AARMS*, 12(1), 155-164.

[10] Van Niekerk, B. & Maharaj, M.S. (2012). Mobile devices and the military: Useful tool or significant threat? *Journal of Information Warfare*, 11(2), 1-11.

10.9756/SIJCSEA/V7I4/03010020402
ISSN: 2321-2381