Crisis Action in Computer Information System Attacks: A Case Analysis

Jhonny Jim* & Michael**

*Instructor, System Engineering, Brunel University, London. E-Mail: jim_jhonny11@gmail.com
**Assistant professor, System Engineering, Brunel University, London. E-Mail: Michael_20el@gmail.com

Received : 29.02.2019 **Revised : 02.04.2019** **Accepted : 25.07.2019**

***Abstract*---** This study analyzed the nature of crisis action that followed computer information system attacks at Visa Inc. The study aimed to recommend some of the alternative actions that the companies and other firms could take to avoid significant information loss in the future. Indeed, the most notable group that the crisis is expected to affect constitutes the customers.

***Keywords*---** System attacks, Information, Credit card

I. INTRODUCTION

THE credit card data breach implies that the users' personal information is at risk and could translate into other insecurity issues; especially when the cardholders' physical addresses and personal contact information such as mobile phone numbers is accessed. Therefore, the chief goal that seeks to curb the ripple effect arising from the breach is to maintain the current user base at Visa Inc. while seeking to attract additional customer bases. Another goal is to maintain the current competitive advantage that Visa Inc. enjoys through the prevailing brand image. The third organizational goal is to prevent a future occurrence of similar credit card data breaches while restoring public confidence in Visa's services. The last organizational goal is to foster an effective user data monitoring system on a collaborative basis involving internal and external information security management departments.

II. STRATEGIES AND TACTICS TO ATTAIN THE ORGANIZATIONAL GOALS

In response to the credit card data breach incident and the fulfillment of the organizational information security goals above, a six-step strategy is recommended. According to Johansen, Aggerholm and Frandsen (2012), the first step requires companies to establish committees or teams. In this case, representative stakeholders will be those perceived to understand the value of Visa's services, processes, systems, and data. The role of such groups will be to examine aspects of vision articulation and mission implementation processes in relation to the core objectives and goals of Visa Inc. the second step entails ensuring the group is informed (Liu, Austin & Jin, 2011). Apart from understanding the business environment at Visa, the selected team that constitutes a risk management group will be expected to be advised regarding any policy, regulatory, legal, or other sector-specific operational, security, or privacy requirements. As avowed by Liu, Jin and Austin (2013), the next step requires organizations (such as Visa) to identify any security or business constraints, as well as assumptions that could stall progress towards effective crisis management while seeking to assure customer data confidentiality. For example, constraints that could face Visa Inc. include the company's view of legal mandates and success, time deadlines, and budget approvals. On the other hand, common company assumptions include the firms' judgment that most of the task force groups are law abiding or loyal, and that the security technologies of an organization can be relied upon towards operation in relation to the existing design (lliott & Macpherson, 2010). At Visa Inc., success in effective crisis management following the credit card data breach incident demands the concerned team to review and capture these aspects on a period basis to determine, over time, whether their validity holds.

The fourth strategy entails communicating decisions about cyber security risks in clear terms that are not ambiguous. As documented by Mazzei and Ravazzani (2011), the process of establishing a comprehensive crisis management strategy such as that which involves cyber attacks requires organizations to broadcast firm risk governance, risk tolerance, and risk priorities based on aspects of likelihood and impact. Thus, at Visa Inc., an accomplishment of the organizational goals (above) requires the senior leadership team to consider an adoption of risk tolerance statements that are driven by major risk categories that communicate the firm's appetite (in a clear manner) for foregoing opportunities or accepting harm.

The fifth strategy requires organizations to embrace an enterprise risk management process that incorporates cyber risk management (Mazzei, Kim & Dell'Oro, 2012). Therefore, Visa's general framework responsible for risk communication, acceptance, prioritization and identification is expected to operate uniformly both at the IT system

10.9756/SIJCSEA/V7I4/03010020407
ISSN: 2321-2381

management level and the enterprise level. Lastly, aspects of strategy modification, review, measurement and management are expected to be conducted regularly to improve possible gaps that could emerge (Schwarz, 2012).

Therefore, dynamism will be embraced based on changes that the organization undergoes to remain responsive while aligning with flexible cyber space operations that demand for system updates to match technological changes.

III. Strategy Execution and Evaluation

To execute the formulated strategies, data classification is important. This step helps in curbing ambiguity through a clear understanding of locations and types of data sets that the company maintains based on importance (Sohn & Lariscy, 2014). The completion of a data classification process is core and is projected to enable the firm to determine the cost and effort required to secure information perceived to be a critical asset in a proper manner. Upon accomplishing the data classification initiative, Utz, Schultz and Glocka (2013) documented that the next step of strategy execution in risk management involves making managerial decisions to balance expenditures on the part of security with the business' real value of the information protected. At Visa Inc., this process will be achieved by identifying information that deserves protection, assigning a value to this information, cataloguing sites that house the critical information, and identifying either the persons having the information or those who need to access the information.

The next stage in the execution exercise will involve security control implementation. According to Veil, Sellnow and Petrun (2012), most of the hackers are unlikely to submit change requests or fill out user request forms. Thus, the manner in which a firm needs to foster a control environment that is prepared to handle unseen and unknown threats cannot be overemphasized. Whereas no one specific framework could be implemented over another three frameworks from which security control implementation could be achieved include SANS Critical Security Controls, *ISO 27001*, and Security Privacy Controls for Federal Information Systems and Organizations (NIST 800-53) (Weber, Erickson & Stone, 2011).

The third step in the execution process will involve verifying security control performances regularly to obtain assurance over the capacity of the security control systems to operate effectively and determine whether these controls' operations align with organizational intentions. Breach preparedness testing and planning is also ideal (Claeys & Cauberghe, 2012). Given that the current technological evolutions imply that most of the organizations either expect or are prone to hacking (Coombs & Holladay, 2012), companies such as Visa Inc. ought to devise breach response procedures. To achieve this execution objective, processes will include an identification of individuals or departments that ought top be notified internally, establishing response teams, tracking intruder activity by implementing monitoring protocols, notify respective legal authorities, and establishing egress prevention. Other procedures will involve estimations of the degree of compromise, coordinating with insurance carriers and legal counsel, and implementing security remediation after analyzing root causes, an.

The last execution procedure will entail risk transfer and risk acceptance. According to Frandsen and Johansen (2011), even robust security processes have continued to fall prey to cyber attacks. Potential financial impacts that may occur include fines assessed by regulatory agencies, increased transaction processing costs, and credit monitoring for the affected customers; including cardholders at Visa Inc. therefore, the execution process will culminate in risk transfer and risk acceptance by evaluating the overall effectiveness of the cyber security strategies outlined and decide whether to accept some of the risks or transfer them via cyber-liability policies (in the wake of fast-evolving insurance carriers).

Regarding resource requirements, it is evident that the strategies designed demand for expertise. As such, the cost or budgetary allocations extended to security will be expected to rise while preparing to accommodate the additional expertise. Additional costs are also expected to be directed at the purchase of new or updated software (systems) that keep abreast with technological evolutions, and the costs extended to external agencies collaborating with Visa's internal group during the regular monitoring exercises aimed at examining the effectiveness of system controls. To evaluate the effectiveness of these strategies, data outcomes obtained during the risk preparedness testing and risk preparedness planning will be used as a basis to inform about program success while highlighting some of the weaknesses or challenges that could accrue to foster an early intervention. Similarly, the success of the program will be evaluated by examining trends in the activities of hackers and the capacity of the control system to detect unseen or unknown threats, upon which critical reductions or preventions of incidents of cyber attacks will mark a crucial predictor of success in credit card data security at Visa Inc.

References

[1] Claeys, A.S., & Cauberghe, V. (2012). Crisis response and crisis timing strategies, two sides of the same coin. *Public Relations Review*, 38(1), 83-88.

[2] Coombs, W.T., & Holladay, S.J. (2012). Amazon. com's Orwellian nightmare: exploring apology in an online environment. *Journal of Communication Management*, 16(3), 280-295.

[3] Frandsen, F., & Johansen, W. (2011). The study of internal crisis communication: towards an integrative framework. *Corporate Communications: An International Journal*, 16(4), 347-361.

[4] Johansen, W., Aggerholm, H.K., & Frandsen, F. (2012). Entering new territory: A study of internal crisis management and crisis communication in organizations. *Public Relations Review*, 38(2), 270-279.

[5] Liu, B.F., Austin, L., & Jin, Y. (2011). How publics respond to crisis communication strategies: The interplay of information form and source. *Public Relations Review*, 37(4), 345-353.

10.9756/SIJCSEA/V7I4/03010020407
ISSN: 2321-2381

[6] Liu, B.F., Jin, Y., & Austin, L.L. (2013). The tendency to tell: Understanding publics' communicative responses to crisis information form and source. *Journal of Public Relations Research*, 25(1), 51-67.

[7] lliott, D., & Macpherson, A. (2010). Policy and practice: Recursive learning from crisis. *Group & Organization Management*, 35(5), 572-605.

[8] Mazzei, A., & Ravazzani, S. (2011). Manager-employee communication during a crisis: the missing link. *Corporate Communications: An International Journal*, 16(3), 243-254.

[9] Mazzei, A., Kim, J.N., & Dell'Oro, C. (2012). Strategic value of employee relationships and communicative actions: Overcoming corporate crisis with quality internal communication. *International Journal of Strategic Communication*, 6(1), 31-44.

[10] Schwarz, A. (2012). How publics use social media to respond to blame games in crisis communication: The Love Parade tragedy in Duisburg 2010. *Public Relations Review*, 38(3), 430-437.

[11] Sohn, Y.J., & Lariscy, R.W. (2014). Understanding Reputational Crisis: Definition, Properties, and Consequences. *Journal of Public Relations Research*, 26(1), 23-43.

[12] Utz, S., Schultz, F., & Glocka, S. (2013). Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster. *Public Relations Review*, 39(1), 40-46.

[13] Veil, S.R., Sellnow, T.L., & Petrun, E.L. (2012). Hoaxes and the Paradoxical Challenges of Restoring Legitimacy Dominos' Response to Its YouTube Crisis. *Management Communication Quarterly*, 26(2), 322-345.

[14] Weber, M., Erickson, S.L., & Stone, M. (2011). Corporate reputation management: Citibank's use of image restoration strategies during the US banking crisis. *Journal of Organizational Culture, Communications and Conflict*, 15(2), 35-55.

10.9756/SIJCSEA/V7I4/03010020407
ISSN: 2321-2381