Computer Information Insecurity: Insights from a Case Study of Visa Inc

Jacob* & Daniel**

*Lecturer, Department of Information Technology, Chapman University, California. E-Mail: jacobit24@yahoo.com
** Lecturer, Department of Information Technology, Chapman University, California. E-Mail: danielchamp@outlook.com

Received : 14.03.2019 **Revised : 29.06.2019** **Accepted : 20.07.2019**

***Abstract*---** The field of crisis management continues to receive attention due to significant changes that have arrived with globalization. The latter is attributable for changing lifestyles and developments such as invention and innovation in which the emergent technologies have fostered interaction among members across the world. With such an increasing trend in the frequency and duration of interaction, sections of firms or organizations and individuals have ended up falling prey in such a way that the issue of data privacy or confidentiality has been compromised (Claeys & Cauberghe, 2012). For example, the interactions have led to the players in cyberspace fall victim of cyber attacks in which adversities such as losses, interference or tampering, and malware attacks have exposed the affected product and service users in terms of personal information that includes physical addresses, identity card numbers, banking information or transactions, and purchasing histories (Coombs & Holladay, 2012). According to Frandsen and Johansen (2011), such crises have not only yielded a loss of trust among consumers but also hampered the state of brand image progress.

***Keywords*---** Insecurity, Consumers, Image progress

I. INTRODUCTION

IN both cyberspace and unrelated cases, recent trends have witnessed crises such as the credit card data breach at Target Corporation, the Sewol Ferry Tragedy that led to losses of life and exposed lapses in country levels of disaster preparedness in South Korea, and credit card data breaches at FACC (an Austria-based manufacturer of aerospace parts), the University of Central Florida, Premier Healthcare, the Medstar Health Inc., Yahoo, and LinkedIn (Holladay & Coombs, 2013). From this trend, it is evident that technological developments have arrived in the wake of increasing cyber insecurity and only organizations that embrace dynamic operations that are responsive to the prevailing conditions in cyberspace might keep abreast with the ethical conduct involving user data privacy. This paper focuses on the subject of crisis management, with insights gained from the credit data breach at Visa Inc. In so doing, it is projected that valid and reliable recommendations will be made towards the improvement of user data security at the firm, upon which the customers' trust might be restored and re-ignite the company's brand image.

II. COMPUTER SYSTEM CRISIS DEFINITION AT VISA INC

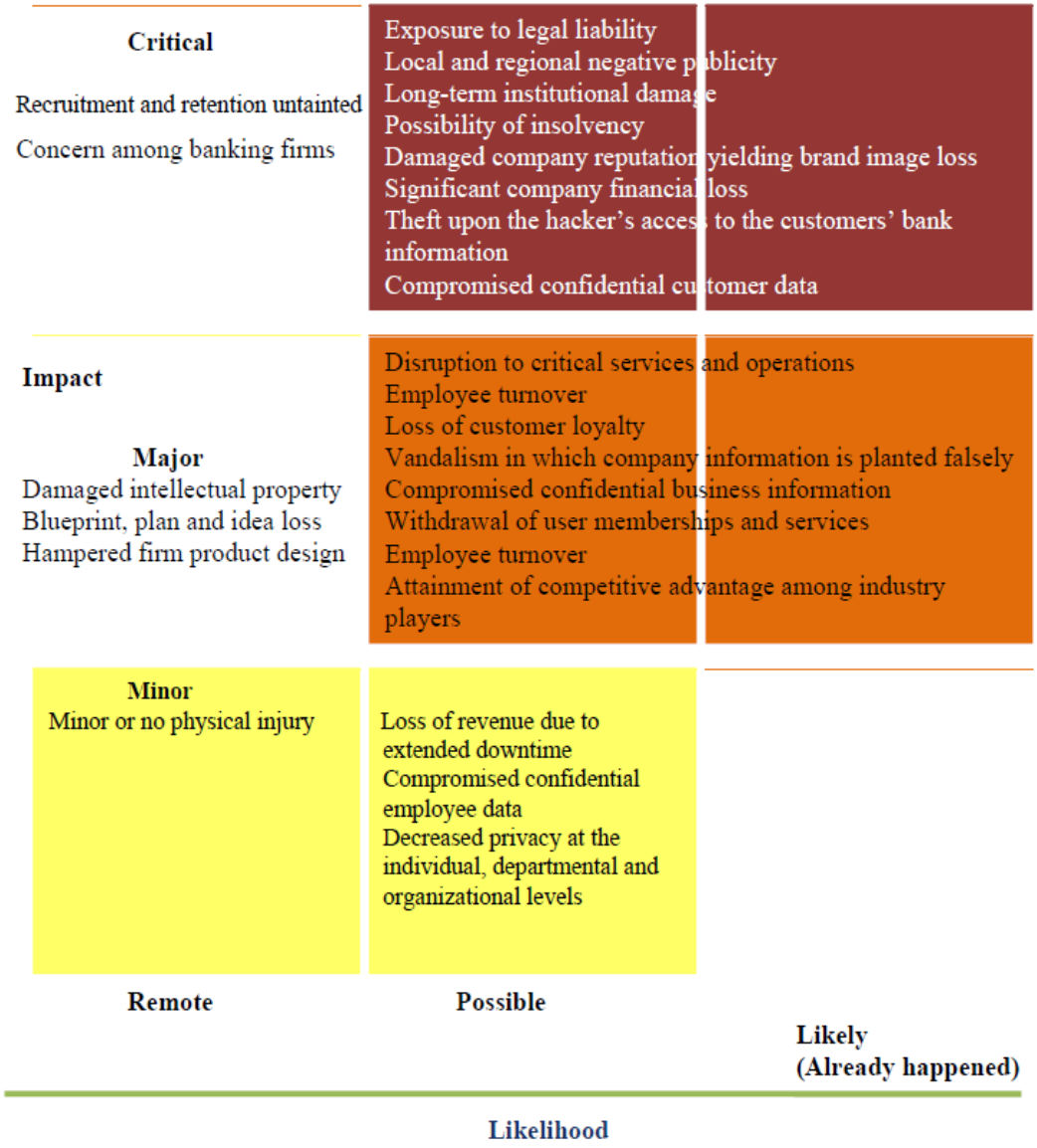
At Visa Inc., a cardholder information security program has been implemented with the central aim of protecting service users during payment card processing activities. Thus, only company employees involved in the payment processing division can access the users' information in terms of Personal Identifiable Information (PII) and the latter includes the cardholders' identities such as biometric records, Social Security Numbers, and their names.

In a recent credit card data breach at the firm, an employee compromised the information system security and stole a significant amount of information belonging to cardholders. Imperative to note is that the employee stole the information from the firm's database just before leaving the company. According to Jin (2014), ex-employees have continually become a menace to organizations and the question that most of the managers ought to ask before allowing such task force groups to walk out of the company doors for the last time (as employees) is what organization data could these groups be taking with them as they leave? At Visa Inc., the ex-employee is perceived to have accessed the Payment Card Industry- Personal Identifiable Information (PCI-PII) information. What remains unearthed is the amount of data that may have been lost, a dilemma that prompts the impact analysis procedure to not only determine the actual value but also to design strategies that could be adopted to ameliorate the adversity.

Whereas the history of the company indicates that a cyberspace insecurity event involving credit card data breach has not occurred before, this event forms an awakening call that sensitizes groups such as the top management and employees charged with the security system regarding the delicate nature of their departmental operations, as well as the question of employee trust within and outside the organization. Similarly, an impact analysis of the case presented at Visa Inc. is important because of the need to prevent a nearly inevitable loss of a significant number of

10.9756/SIJCSEA/V7I4/03010020406
ISSN: 2321-2381

customers, as well as the need to restore the brand image of the global firm. Lastly, an analysis of this event is important because it enables other firms engaging in operations of electronic card payments to not only monitor the behavior of their employees while examining their security systems' level of credibility but also form a platform from which new and responsive data security systems can be adopted and implemented to shun possibilities of falling prey to cyberspace attacks.



III. PERCEIVED STAKEHOLDERS

In the case presented, the primary stakeholder exhibiting direct effects of the data breach is the affected firm itself, Visa Inc. in addition, the top management, middle managers and other employees in the lower levels of the organization's hierarchy form critical stakeholders that the crisis affects. It is further notable that the crisis affects specific departmental heads in charge of user information monitoring at Visa Inc., besides the employees involved in the payment processing division. Apart from these internal groups, cardholders at Visa Inc. form another group of direct stakeholders affected by the data breach crisis. In addition, the banks charged with crediting or debiting the cards held by these customers are affected in such a way that they risk losing significant amounts of data, should the hacker(s) access financial information of the customers and possibly prompt online withdrawals. Similarly, other firms providing electronic card payment services are affected due to the fact that some customers may have linked their credit cards to these groups and allow an inter-agency transfer of funds. The complexity of the matter stretches further beyond competitors and banking institutions to affect businesses and business partners with whom the affected cardholders may have engaged in business-related operations, as these firms not only face the risk of experiencing significant financial losses or stalled progress due to the stand-off and halted business operations but also pose the risk of having their past transactions with

10.9756/SIJCSEA/V7I4/03010020406
ISSN: 2321-2381

the affected cardholders exposed and yield an additional danger in terms of confidential data loss.

Government regulators and the general public will also be affected by the crisis. For example, the general public constitutes potential customers who may have planned to seek services at Visa Inc. As such, it is predicted that this group might end up questioning or losing confidence in the credibility of user information privacy systems at Visa Inc.; a trend that could make them to shy away from seeking the company's services. Regarding government regulators, the group might be affected in such a way that the sections of agencies that Visa Inc. might have contracted to collaborate with its internal personnel in monitoring user data privacy will end up being questioned regarding the resultant lapses that may have prompted the breach.

IV. Stakeholder Expectations

As mentioned above, the affected stakeholders include customers, employees, government regulators, competitors, the customers' business firms, the management (and the department charged with user information monitoring), and the general public. Given the magnitude of the crisis, it is projected that the customers would expect the company to compensate the affected cardholders any financial losses that they may have incurred while the banking institutions would expect Visa Inc. to compile and send a detailed report regarding the lists of affected customers, as well as the respective losses that each customer may have undergone. Similarly, Visa's competitors are expected to seek information regarding inter-agency or intra-industry breaches that may have resulted from the crisis to avoid a ripple effect in which these groups' customer bases could also have their data exposed, as the hackers' knowledge regarding possible inter-agency transactions conducted by the affected card holders could offer a possible link to the internal security mechanisms that these intra-industry operators may have put in place.

On the other hand, government regulators are likely to anticipate a request for collaborative efforts towards understanding the causes and possible degree of loss that the breach may have caused while the employees at Visa might expect the firm to hire an external and independent task forces that could look into possible links that may have enabled the ex-employee to access the data security system of the company. Lastly, the general public will expect Visa Inc. to share details regarding the actual number of cardholders affected using forums such as print media and television, as well as social media platforms. This anticipation by the general public is attributed to the fact that a clarification could reduce possible tensions that might arise, should the firm handle the crisis with ambiguity. However, it is expected that, care will be taken to avoid releasing information that could sensitize the suspected hacker regarding the mechanisms laid by security agencies while addressing the adversity. Similarly, customers are likely to expect the firm to send information through channels such as emails or letters to the affected cardholders; detailing the extent to which the breach might have occurred and some of the strategies that the company has put in place to compensate the affected groups. Overall, the aforementioned stakeholders are likely to anticipate a swift reaction to the breach in such a way that Visa relays information in a timely manner while engaging relevant authorities or agencies to not only understand the cause, culprit and magnitude of the breach but also strive towards compensating the affected cardholders respectively – while seeking to restore customer trust and the company's brand image.

V. Conclusion and Recommendations

To guide the crisis response, one of the issues that should be investigated concerns the ex-employees criminal history and the nature of conduct at the institution. Whether the employee had a criminal record or disciplinary issues while serving Visa Inc. could act as a lead towards understanding the motive of the hacking event. In addition, there is a need to examine the former employees' communication trend with other employees and external groups to understand the potential source of the hacking (whether internal or external), upon which further analyses will aid in understanding whether the incident involved the mentioned ex-employee or a network of hackers. It is also imperative to understand the relation between the ex-employees line of operation with that of the payment processing division and, the user data security department. In so doing, the results might inform about possibilities of an internal link to the incident. Lastly, an internal cyber security agency should be consulted to avoid tampering with evidence in situations where the existing data security group at the firm was used; as this group could be part of the hacking network and remain unreliable in conducting credible investigations.

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] Holladay, S.J., & Coombs, W.T. (2013). Successful prevention may not be enough: A case study of how managing a threat triggers a threat. *Public Relations Review*, 39(5), 451-458.

[5] Jin, Y. (2014). Examining publics' crisis responses according to different shades of anger and sympathy. *Journal of Public Relations Research*, 26(1), 79-101.

10.9756/SIJCSEA/V7I4/03010020406
ISSN: 2321-2381