A Case Study of Credit Card Data Breach at Target Corporation: Implications for the Future of Company Information System Security

Kristoffer* & Marius**

* Instructor, Computer Applications, University of South-Eastern Norway, Norway. E-Mail: kristofferapp@outlook.com
** Assistant Professor, Computer Applications, University of South-Eastern Norway, Norway. E-Mail: mariusstain@yahoo.com

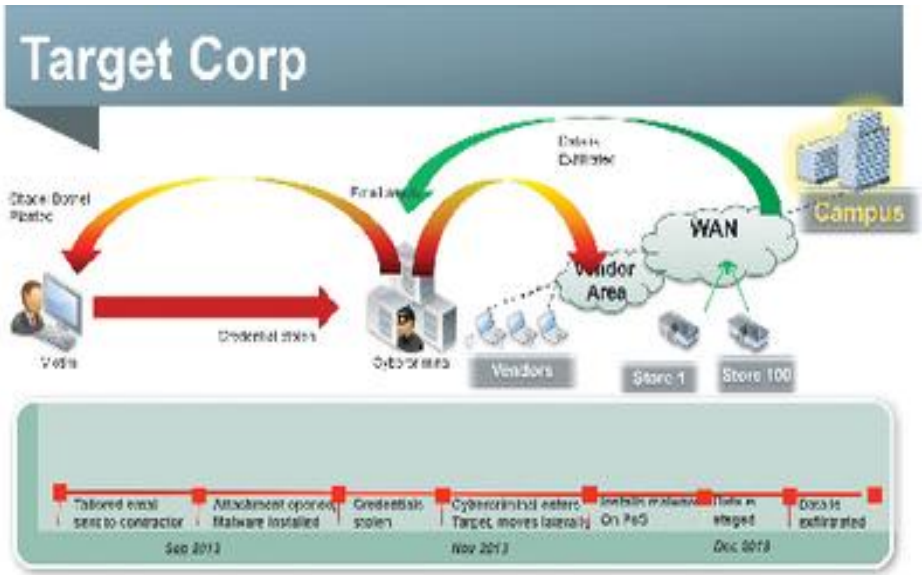
Received : 02.01.2019 **Revised : 20.03.2019** **Accepted : 05.08.2019**

***Abstract*---** Crisis management refers to a process through which organizations handle situations deemed to be sudden emergencies. With quick decision making inevitable, crisis management seeks to limit potential damages that could accrue from perceived adversities. In this paper, the aim is to focus on crisis management from a practical illustration to understand issues such as potential causes, trends, and possible interventions that could be adopted to control emergencies.

***Keywords*---** Crisis Management, Credit Card, Decision Making

I. EVENT ANALYSIS

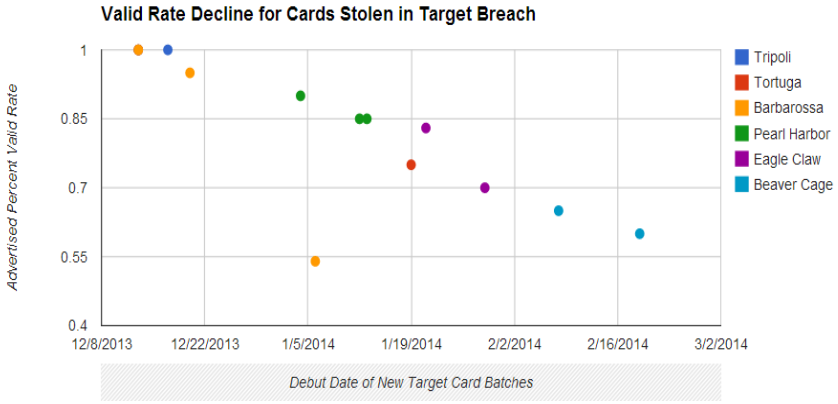
THE chosen organization is Target Corporation. Specifically, the issue under discussion is that which involved a credit card data breach that has not only compromised the organization's brand in the face of customer bases but also sensitized security management agents regarding issues affecting information security. Coming in the wake of 2013's holiday's height, the cyber attack was documented as the largest in the corporate history of America



In December 2013, it was reported that about 2000 Target stores had fallen victim of a cyber attack. Specifically, more than 40 million credit cards were stolen through unauthorized access to customer data on the point of sale (POS) systems. The shoppers received such unwelcome holiday surprises that would not only threaten their relationship with the business firm but also unrelated security-related adversities in their lives (Krebs, 2013). Later, the corporation revised these numbers to incorporate private data affirmed to reflect information for 70 million customers, with the breach transpiring between the months of November and December (Poulin, 2014). With internal alerts missing, Target established the breach after receiving information from the Department of Justice (Elgin, 2014). Thus, the cost of the breach was felt by banks, employees, customers, and Target. Specifically, the customers' losses due to the credit

10.9756/SIJCSEA/V7I4/03010020404
ISSN: 2321-2381

card loss were refunded by banks while groups such as the CIO and CEO lost their jobs (Gonsalves, 2014).



As mentioned above, one of the responses involved making adjustments to the corporation's organizational hierarchy. In addition, the company's executives held consultations with the U.S. Justice Department before hiring forensic teams whose role would be to conduct an in-depth investigation into the hacking exercise (Warner, 2014).

By hiring a third party to engage in the investigation, it can be inferred that Target sought to identify and respond to the threat with accuracy. One of the issues justifying this stand is that a third party was likely to be neutral, should they have been independent from possible contacts of the hackers. In addition, it has been indicated that the company made adjustments to its organization hierarchy as shown in the loss of jobs by the CIO and the CEO, among other executives. Thus, the action was accurate because it can be perceived as that which sought to avoid possible interference (by these executives and others employees) with the ongoing investigations. By seeking to identify trends and possible causes of the cyber attack, Target would not only establish forces behind the breach but also establish and implement stringent measures regarding data security and user privacy. Thus, the initial response was not targeting symptoms of the threat. Rather, the third-party hiring process and the adjustments made to the employees' hierarchy sought to identify and respond to the threat with accuracy.

II. Implication for the Future of Computer Science

The crisis affected groups such as Target's employees, banks and customers. For high-ranking employees, the impact was felt in terms of the loss of jobs. On the other hand, banks were forced to refund the money stolen from customers after the credit card data was accessed. Similarly, the banks had to pay the replacement fee and this process accounted for over $200 million in expenditure (Target, 2014; Krebs, 2013). Corporation was also affected in such a way that the wake of a new year witnessed a significant decline in customer visits; a trend that was attributed to the compromised brand image resulting from the cyber attack.

One of the related responses involved placing daily limits on withdrawals and spending for customers holding debit cards and affected by the breach, with other cards reissued. Whereas this step sought to address the short-term adversity by reducing potential losses, the action remained inadequate because of its deviation from the main threat, the Target breach, to a symptom which concerned potential losses accruing after the breach. Additionally, Target left 700 positions unfilled while 475 employees worldwide, especially in Minneapolis, were laid off. On the one hand, the action could aid in reducing possible interference to the ongoing investigations, especially in cases where the breach may have involved information leakage from sources within the firm. On the other hand, the action compromises the company's vision of serving customers with diligence and a user-centered strategy whose role is to attend to the concerns of product and service users with promptness (Shostack, 2014; Webb, 2014). It is also worth noting that the last weekend before Christmas witnessed the retailer offer a 10-percent discount off in-store purchases. Whereas these efforts might have aimed at regaining the brand image or value, they seem to target symptoms, rather than the real issue concerning the causes, possible effects, and some of the solutions that could be adopted to prevent a future recurrence of the breach.

From the above trend, the company did not seem to have a clear plan of action. Instead, it engaged in responsive measures that sought to regain its brand image at the expense or real issues accruing from the cyber attack. For example, the sales-killing breach saw the company let its employee groups wear polo t-shorts and jeans in a quest to boost their morale in March 2014. In addition, the CFO stated in the month of February that the firm had invested hundreds of millions towards enhancing and assuring data security and rejected claims that Target's system s remained below par, yet the security systems in place had been breached. Indeed, the company was struggling to adapt to changes in the intensity of the crisis while responding to public concerns, rather than establish a clear plan of action. With discounts offered to customers in the U.S. and material possessions such as polo t-shirts and jeans used as possible avenues for regaining the company's image, it can be inferred that Target concentrated on short-term solutions at the expense of long-term solutions.

On November 27, 2013, details such as phone numbers, mailing addresses and names of about 40 million customers

10.9756/SIJCSEA/V7I4/03010020404
ISSN: 2321-2381

were exposed to fraud. This pointer prompted a meeting between the U.S. Justice Department and Target's executives on December 3rd, with a third-party forensics team hired on 14th. On December 15th, Target confirmed a criminal infiltration into its system. However, the installed malware was removed from almost all registers in the U.S. stores but the public remained unaware. As such, KrebsOnSecurity, a data and security blog, was the first site to report the data breach and, in turn, prompted investigations by the Secret Service (Schwartz, 2014). Brian Krebs, the security blogger, broke the story on December 18th and prompted Target's initial announcement on December 19th.

III. CONCLUSION

From Krebs' response and definition of the crisis, the process can be deemed to have been effective. The blogger began by stating that several smaller banks had contacted him, reporting fraud rates. Upon receiving the information, Krebs visited a site responsible for selling stolen credit cards, coincidentally realizing that the latter had just received an enormous shipment. By matching the Bank Identification Numbers on the cards of issuing banks, Krebs confirmed that the institutions had stolen cards on the market. As the blogger asked the banks to indicate whether their point of purchase was common, the institutions affirmed that the cards had been used at Target, specifically between Thanksgiving and December 15, 2013. The blogger was also effective in such a way that he proceeded to point to the website where Target's cards were sold. With price and purchase buttons arranged next to each credit card, details included passwords, names, card numbers, and other personal details.

REFERENCES

[1] Elgin, B. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew It. *Bloomberg Businessweek*.

[2] Gonsalves, A. (2014). Target CEO resignation highlights cost of security blunders. *CSO*.

[3] Krebs, B. (2014b). A first look at the Target intrusion malware. *Krebs on Security*.

[4] Poulin, C. (2014). What retailers need to learn from the Target breach to protect against similar attacks. *Security Intelligence*.

[5] Schwartz, M.J. (2014). Target, PCI auditor Trustwave sued by banks. *Dark Reading*.

[6] Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons, Inc.

[7] Target. (2014). Target provides update on data breach and financial performance. *Target*.

[8] Warner, G. (2014). Target "hacker tools" provide breach insight. *Malcovery Security*.

[9] Webb, T. (2014). Target lawyer suggests mediation for resolving data breach lawsuits. *TwinCities.com*.

10.9756/SIJCSEA/V7I4/03010020404
ISSN: 2321-2381