Cyber Security Lessons from Malware Installation in Companies: Insights from the Aftermath of Target Corporation's Attack

Ekrem* & Emine**

*Assistant professor, Dept of Computer, Ankara University, Turkey. E-Mail: sssekrem21@gmail.com
** Assistant professor, Dept of Computer, Ankara University, Turkey. E-mail: emine_ne@yahoo.com

Received : 22.03.2019 Revised : 10.06.2019 Accepted : 04.07.2019

Abstract--- As the attackers began installing malware on Target Corporation's system, the firm appears to have failed to embrace an effective response process, especially that which emanated from the firm's anti-intrusion software that sent multiple automated warnings (Krebs, 2014).

Keywords--- Cyber, Software, Response Analysis

I. Introduction

THE attackers moved from less sensitive areas of the company's network to those that stored consumer information but the company would still not isolate the most sensitive network assets. It is also notable that the firm did not respond to multiple warnings arising from the anti-intrusion software that detected possible escape routes that the attackers planned to use after exfiltrating information from the company's network (Gonsalves, 2014). Therefore, Target's initial response is that which depicts a firm that did not treat the crisis with seriousness.

II. Outcome/Response Analysis and Cyber Security Lessons

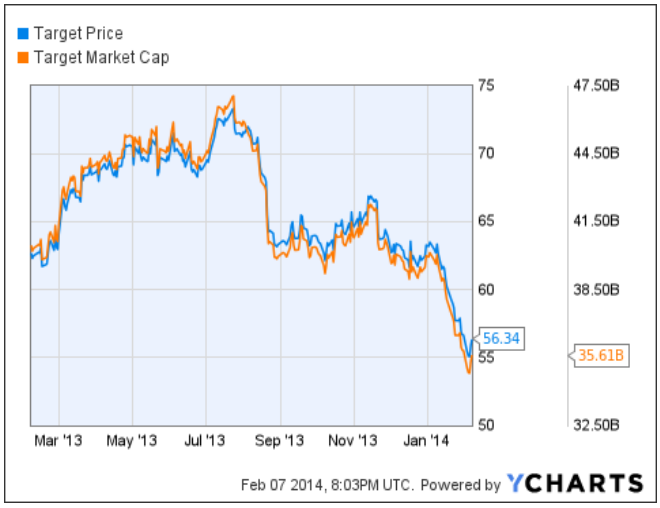

Figure 1: Impact of the Data Breach

Source: Gonsalves (2014)

Some of the actions that Target took include placing daily limits on withdrawals and spending for the affected customers holding debit cards, card reissuance, laying off sections of employees (475 across the world) while leaving 700 positions unfilled, provision of polo t-shirts and jeans to boost the employees' morale, and an allowance of 10-perent discount off in-store purchases made by U.S. customers over the last weekend to Christmas (Fazio, 2014). Similarly, the company committed $100 million towards technological update and an introduction of chip-and-PIN technologies, an action that was to be implemented on its credit and debit cards by early 2015. Furthermore, the company replaced sections of its top management, including the CIO position that was taken by Bob DeRodes, a former technology adviser (Elgin, 2014).

Based on the prevailing policies governing contracts among card holders, banks, and Target Corporation, the financial institutions engaged in compensation exercises regarding the money lost by Target's customers, as well as the replacement of similar cards. As such, the banks did a commendable job. Similarly, Target's decision to offer discounts for U.S.-based user groups is commendable because it was likely to restore consumer confidence to a desirable extent.

Mixed outcomes arise regarding Target's executives' public statements. For instance, the company's announcement to invest in further improvements in its data security system on both the short-term and long-term bases has been implemented. In addition, the company's organizational adjustment in terms of the employee groups to shun possibilities of recurrences of similar lapses has been addressed to a desirable extent. However, the questions of

10.9756/SIJCSEA/V7I4/03010020405
ISSN: 2321-2381

whether the company will implement these changes and sustain the trend for a substantial period continues to be a point of concern, especially given the current and rapid changes in technology (that demand firm flexibility in the cyber security sector).

Overall, it is worth acknowledging that Target's statements and actions that have followed these statements or plans have contained the damage to a significant extent. For instance, the company's brand image has been restored to a significant extent. However, the fear caused by the crisis continues to pose reluctance among some of the prospective credit card users and, in situations where new user groups have been secured, the amount of money extended to Target's products and services seems to be lower than the initial case (D'Innocenzio, 2014).

Target's response was effective because it not only sought to determine the cause of the hacking incident but also sought to address the needs of employees and customers. For example, customers had their cards replaced while banks compensated accordingly and, the employees' morale was restored. Furthermore, the response was effective because the corporation's decisions were preceded by relevant consultations with various security agencies to contravening regulations guiding security-related investigations in the corporate sector. Imperative to note is that the organization did not sensitize members of the public regarding specific details and the extent of the harm in time. However, this decision could be attributed to the need to avoid alerting the hackers about the company's mechanisms in place (towards recovery).

Whereas it is evident that Target Corporation was not the first firm and neither were its members of the top management the first individuals to alert the public arena regarding the credit card breach, it stepped in accordingly and admitted about the fraud. Necessary steps were also taken by consulting relevant authorities while making possible connections between internal and external security mechanisms, steps that led to the laying off of sections of employees to pave way for investigation (Dell Secure Works, 2014). As such, it can be inferred that appropriate steps were taken to not only identify the cause and participants of the breach but also to formulate strategies towards realizing lasting solutions. Moments before and after the incident, Target Corporation's executives provided scanty information about the incident. This trend was in consideration of possible and unintended consequences that could have been witnessed, should the firm have revealed full details surrounding the hacking incident. For example, disclosing the fraud in full detail would alert the culprits regarding the firm's plans to address the situation and end up compromising the investigators' efforts (Clark, 2014). On the other hand, possible resultant trauma that could have been experienced by millions of customers, whose financial plans may have been tampered significantly, remained unpredictable and attracted the firm's decision to take a less active role; especially as depicted in its public statements. Lastly, the preceding and proceeding moments marred by a dominance of Target executives' silenced are likely to have been intentional to avoid tainting the company's brand image.

Some of the actions taken by Target were timely while others were untimely. For example, warning systems kept sending automated messages but relevant departments failed to intervene. On the other hand, the company's consultation with the U.S. Justice Department and other relevant security agencies after news about the crisis went public was timely. Similarly, the company's focus on the needs of employees and customers was timely. However, statements were untimely and all the hints came after Krebs' report on the previous day (Capacio, 2014).

III. Alternative Course of Action

Option 1: Appointing an experienced crisis management team. Professional crisis management leadership implies that the personnel at Target would be characterized by extensive data security expertise whose complementation with public relations and strong communication skills could translate into desirable outcomes. By appointing a crisis management team, effects might be felt in each department while the team composition is likely to reflect the impact. Specifically, this action implies that the sales leadership documents and scripts to explain situations to the current user groups and prospective customers while customer service representatives could access accurate information while advising the non-impacted and the impacted customers.

Option 2: Managing uncertainty forms another option. Given the extensive nature of data breach at Target, it is inevitable that true facts could take weeks or months to be uncovered. For instance, the nature of the attack and the exact number of impacted records may take time to be pinned down. As such, the company's early release of inaccurate information translated into an increase in negative public responses, yielding significantly adverse impacts on its reputation (Baldwin, 2014). As such, the uncertainty could be managed by informing the customers about the incident but delaying the release of exact numbers pending verification. Lastly, uncertainty could be managed by allowing communication to focus on specific actions that might have had potential impacts on specific customers, notifying the affected group with accuracy and specificity, rather than provide general information to the public arena.

The effectiveness of these courses of action would be determined by examining their consequences on the affected groups, including the concerned company, product and service users, and other related agencies in the rest of the world. In addition, the strategies' effectiveness would be determined by focusing on context-specificity to understand their state of feasibility based on the available resources for implementation. Lastly, action plan effectiveness would be determined by comparing possible outcomes to those realized or experienced during the past implementation of alternative courses, aiding in understanding potential strengths and weaknesses of the respective approaches.

At Target, the first option, which involves appointing an

10.9756/SIJCSEA/V7I4/03010020405
ISSN: 2321-2381

experienced crisis management team, is recommended. The current corporate sector is highly competitive and companies whose reputations are tainted by data security lapses such as those experienced at Target are unlikely to attract large consumer pools. Thus, appointing an experienced crisis management team is likely to pose longevity in security system consistency while embracing flexible approaches that are responsive to the dynamic state of technology faced in the current, globalization-driven world. Indeed, this team is likely to gather relevant data from groups such as employees, customers and the rest of the public in an intelligent manner and curb looming crises in time. By implementing this strategy, Target is projected to regain its competitive advantage in the global retail marketplace.

IV. CONCLUSION

The dilemma witnessed at Target Corporation sounds alarm regarding the great extent to which cyber insecurity could harm the retail sector, as well as other players in the business sector. As such, the company's delay to release full information to the public remains relevant due to the perceived need to avoid disclosing critical information to the hackers. However, lapses preceding the hacking process when security alerts were sent by automated systems raise questions regarding a possible compromise among internal company groups. It is also worth noting that the company's technology experts might have lapsed to an extent so significant that the leakage reached Krebs, a blogger, yet not public statement had been made by the firm. Therefore, embracing corporate social responsibility becomes inevitable, should Target strive further to regain its strategic location and competitive position. Similarly, a collaborative approach between internal security systems and experts and external agencies is highly encouraged to trace trends in cyber attacks and ameliorate adversities in time – by monitoring warning systems and responding accordingly.

REFERENCES

[1] Baldwin, H. (2014). The other shoe drops for Target's CIO. *Forbes*.

[2] Capacio, S. (2014). Target breach: Security warning ignored before heist. *myFOX9.COM*.

[3] Clark, M. (2014). Timeline of Target's data breach and aftermath: How cybertheft snowballed for the giant retailer. *International Business Times*.

[4] Dell Secure Works. (2014). The 20 critical security controls. *Dell Secure Works*.

[5] D'Innocenzio, A. (2014). Target data breach cost banks more than $200 million. *The Huffington Post*.

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

[7] Fazio, R.E. (2014). Statement on Target. *Fazio Mechanical Services*.

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

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

10.9756/SIJCSEA/V7I4/03010020405
ISSN: 2321-2381