Cyber Security in Business Organizations

Name

Institution

Cyber Security in Business Organizations

Advanced computer technology has certainly improved lives in many aspects. There are better medical services, online shopping that has enabled door delivery of products, distance learning modules for universities and colleges, and many other things. In today's world, it is easy to learn how to do anything and obtain whatever it is one may want without having to move from one's resting zone (Goodman, 2014). However, it has also made increased the vulnerability of people to unsuspecting breaches of privacy and theft of personal data left in online websites and retail portals (Himma, 2007). In the recent past, there have been various security breaches in some of the most used websites where subscriber data, including financial transactions, credit card information and addresses are stolen. Some of the most publicized hacks include Myspace, eBay, Anthem, JPMorgan Chase, and Ashley Madison, among others in the recent past (www.informationisbeautiful.net, 2016). Target, a retail company that has over 1700 stores in the USA became a victim of an avertable hack from Russian hackers (Riley, Elgin, Lawrence, & Matlack, 2014). As mentioned, this breach of the company's clients' transaction records was avoidable. However, there are various issues that led to the occurrence despite various red lights that were raised regarding the incident before it happened.

The most significant issue that permitted the hack was negligence. Negligence, by definition is the lack of proper response, if any, in light of looming fatality, danger, or any unwarranted activity. According to the report of events leading to the attack and the reaction afterwards, as published in Bloomberg online (Riley, Elgin, Lawrence, & Matlack, 2014), the Thanksgiving attack on the company's servers that served its 1797 outlets, malicious activity had been noticed well in advance before the attack. Many Americans use cards to make payments at convenience stores and other shopping areas. The malware used to deploy this hack would

capture credit card numbers and other details, after which it would run virtual computer environment on Target servers, giving access to the attackers. An exfiltration malware was planted on the 30th of November that would that would then be used by the hackers to pot the stolen data to three US centers before it was then transported out to Russia. Target had contracted FireEye to beef up security alongside the company's team of specialists in Bangalore. The two security surveillance forces would then inform the team in Minneapolis of any suspicious activities noticed on their systems. When the installation of the malware occurred, the two agencies sent numerous alerts to the company's headquarters, which were all ignored. This inaction caused the loss of about 40 million credit card numbers with 70 million addresses and phone numbers to unauthorized parties. Such an occurrence has an impact on the level of trust that the customers will bestow upon the retailer; the company may not recover from the damage of the breach.

Another challenge is the deployment of security platforms that the company specialists hardly trust. According to Jim Walter, a director at McAfee, "The malware utilized is absolutely unsophisticated and uninteresting", meaning that it would have been deleted by the anti-malware protection system in place. However, the automatic deletion feature of FireEye had been turned off, apparently for observation before full deployment. Being a company that deals with public data, this move was dangerous. It is better to perform evaluation on test data rather than live environments in which eminent threats are more destructive.

Overlooked Red Flags

Ignoring security breach warnings. The management of security at the company appears to have been very loose and hands-off. The fact that the security team began combing through various alerts issued through the system and other notification platforms after the federal agency

means that the alert system was not properly managed. Therefore, having turned off the auto-deletion on the Anti-malware software and failing to properly utilize alert mechanisms shows a lot of recklessness. This means that the company loses a lot of money in funding a dysfunctional security team which failed to monitor notifications of suspicious activity and disables the malware attack prevention mechanism.

Unusual behavior and practice of the cyber security personnel went uninvestigated. The fact that the individuals who managed the security of the company had the capacity to stop, and perhaps, help with the investigation in tracing the file destination before the attack, shows that they might have acted as part of an inside job or did so out of vendetta. The company, after getting the news of the breach, should have made the point to investigate these individuals to find out whether they had the right competence or why they failed to prevent the attack despite all the information at their disposal.

After the Attack

Once alerted by the Department of Justice about the breach, Target Company went ahead to delete the malware. The next step was to have its cyber security team help with the investigations that lead to the tracking of the IP addresses to Russia. This was the right move, letting the relevant investigative authorities conduct their evaluation of the company's servers and computer systems. This exercise, according to the company's executives, was conducted in order to prevent another attack in future.

The company also went ahead to reassure the customers that none of them would pay any fees related to the attack; the management even set up an ad-hoc customer relations entity, which was a positive move in saving face for the company. In the face of crisis, the reassurance of the

clients would may have reduced the massive loss of public trust in the company's services and security of their data.

Conclusion

Target company hack attack happened as a result of carelessness and ineptness of the company's security organ. From the discussion above, the company had the right infrastructure in terms of external support as well as equipment required to avert attacks of any kind, especially the kind described. However, security of a firm is human-driven, which means that despite the level of sophistication involved, if the operation from the control end fails, then the cyber environment fails the safety test. The security management, due to some of the reasons that have been highlighted above, including the failure to act in light of red flags and the mismanagement of a live customer environment shows how incompetent the whole team was. The department, while it had the resources required to block attacks and trace the probable source, or forward the case to relevant cybercrime authorities, they fail to do so and ignore the threat alerts and updates from Bangalore and FireEye. The attack is thus to be blamed on the cyber security division of Target.

References

Goodman, P. (2014, August 12). *Advantages and Disadvantages of The Internet Revolution*. Retrieved from http://hubpages.com/technology/Advantages-and-disadvantages-of-the-internet

Himma, K. E. (2007). *Internet Security: Hacking, Counterhacking, and Society.* Jones & Bartlett Learning.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 17). *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*. Retrieved from http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data#p1

www.informationisbeautiful.net. (2016, August 8). *World's Biggest Data Breaches*. Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/