Case Study

Name

School or Institution Name (University at Place or Town, State)

**Target Data Breach**

**Introduction:**

 With the advancement in information and communication technologies and their prevalence in our lives, it is hard to imagine any business without the inclusion of information technology. Information and communication technologies play the role of utilities in modern business. Exponential penetration of modern technologies into businesses have made them a potential target of cyber-attacks. Hacking is the most common theme of exploiting information systems for monetary benefits. Hackers can penetrate a system to steal critical information that is required for ensuring business continuity. Most of the data breaches in the history of the information systems involve hacking. Hackers exploit the vulnerabilities present in the system to breach the valuable data. Businesses pay white hat hackers to locate security holes in their systems and to suggest security enforcement. Black hat hackers, on the other hand, penetrate the networks with the intention of gaining financial benefits from their penetration practices (Manworren, Letwat, & Daily, 2016). One such hacking attempt that shook the world of cybersecurity is known as the Target data breach. Retail network of the Target Corporation was hacked and compromised by the criminals to harvest personally identifiable information. The attack was successful at a massive scale and compromised almost 40 million records of credit card information. The paper describes the causes of successful penetration of the network, consequences of the breach, and recommendations to prevent future incidents.

**Discussion:**

One of the most significant data breaches of all times was reported in 2013 by Target Corporation. They revealed that a massive amount of almost 40 million credit card details from their networked are compromised by the hackers including 70 million records or other personally identifiable information. Detailed investigations and reports of the Target data breach revealed many weak points in retail networks relying on internet and information technology solutions for their operations. Although most of the organizations operating or providing services online require access to personally identifiable information of their customers for various purposes (Shu, Tian, & Ciambrone, 2017). Such information is required by retail or online stores for successful delivery of the order. Similarly, Target Corporation was storing personally identifiable information of their customers using their point of sales terminals into their database systems.

 Such kind of systems can prove to be a heaven for the hackers if they are successful in penetrating the system without notice of the owner. It has happened in the case of the Target Corporation data breach. Hackers were able to compromise their point of sale network using vulnerabilities in the system. The attack was undetected for a fairly long period of time allowing the hackers to collect huge amounts of the data. Hackers did not attack the network of the Target Corporation (Weiss & Miller, 2015). In fact, they initially penetrated into the network of Fazio mechanical services, a business partner of the Target Corporation. The networks of both organizations were interlinked at the point of sales machine network. After successfully compromising the network of Fazio mechanical services, hackers got the credentials to access the core network of Target organization.

 Hackers probed the network of Target using the stolen credentials from Fazio mechanical services and were able to successfully penetrate the network. After initial penetration into the network, they discovered vulnerabilities in point of sale terminals of Target Corporation. Hackers exploited the vulnerabilities to deploy malware in the machines named "BlackPOS. (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Rao, 2016)” Malware was programmed to scan the memory of the point of sale terminal for credit card information and data related to order stored in the memory of the machine. Instead of transferring the data directly to the hackers they decided to accumulate the data into the network of Target Corporation. They were successful in their efforts and then using other vulnerabilities in the network they built a bridge to upload the data to hacker owned command and control servers. Whole analysis of the attack approach used I target data breach reveals several weak points and practices used by the large-scale enterprise businesses.

 Hackers designed the point of sale malware to intelligently encrypt the stolen data before moving it to internal repositories. Hackers controlled servers were traced to Miami and Brazil in later investigations. Hackers used file transfer protocol channels to drop data loads to these locations. When the breach was publicly announced, the Target Corporation suffered severe reputation loss in the market. While investigating the actual cause of the successful compromise of the network, it was discovered that the Target Corporation was not unaware of the security of their information systems (Kashmiri, Nicol, & Hsu, 2017). They have installed a cyber-security solution known as FireEye to protect their assets against such attacks. Deeper analysis revealed that many of the preventive protection technologies of the FireEye solution were turned off by the system administrators due to lack of knowledge. The penetration of the network and attack could be stopped at various points of the attack cycle, but system administrators did not report the security incidents and ignored the alerts of the cyber-security solution installed on the machines.

 The answer to the question that even if the security policies were bypassed by the hackers how he was able to steal massive amounts of critical data, is that due to the poor segregation of data. Target used poor network segregation between the operational data and critical data related to credit card details of the customers. If appropriate segregation of network resources is used then such network penetrations will not end up in severe consequences. Depending on the lessons learned by the massive breach in history the target Corporation opted for chip-based credit card solutions instead of standard cards (Sigholm & Bang, 2013). These cards contain electronic chips capable of providing encryption mechanisms to secure personally identifiable and financial information. They also started to educate their system administrators about the deployed information security systems along with patching of the security vulnerabilities in their point of sale network to protect against future attacks.

**Conclusion:**

Most businesses rely on personally identifiable information of customers for their business operations. However, dealing with such information impose further responsibility for information assurance on the organizations. Information assurance is a practice to ensure the confidentiality, integrity, availability, and non-repudiation of the data. Confidentiality means that the information must not be compromised by criminals or hackers. Since in the above discussion the systems of Target Corporation lacked the capabilities of information assurance suffered a massive data breach. The data breach of Target Corporation and any similar attacks can be prevented by making information assurance strategies a part of the business plans. It is hard to install a system to protect the first system without even the guarantee of value addition to the investments. Organizations must consult white hat hackers to patch vulnerabilities in their systems before their exploitation by the black hat hackers or malicious actors (Gray & Ladig, 2015). Financial benefits are the primary driving force behind the ever-growing cyber-crimes industry. Enterprise and small to medium-sized businesses as well must ensure the protection of their network by patching discovered security holes as soon as possible. Otherwise, the results of the breach and successful hacking can be catastrophic for the business as it is evident from the hacking attack on Target Corporation in 2013.

References

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47–56.

Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber security accelerates in the US following target corporation’s data breach. *International Journal of Business Administration*, *6*(2), 60.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, *45*(2), 208–228.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257–266.

Shu, X., Tian, K., & Ciambrone, A. (2017). Breaking the target: An analysis of target data breach and lessons learned. *ArXiv Preprint ArXiv:1701.04940*.

Sigholm, J., & Bang, M. (2013). Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. In *2013 European Intelligence and Security Informatics Conference* (pp. 166–171). IEEE.

Weiss, N. E., & Miller, R. S. (2015). The target and other financial data breaches: Frequently asked questions. In *Congressional Research Service, Prepared for Members and Committees of Congress February* (Vol. 4, p. 2015).