

ACCOUNTING IMPACTS OF TARGET DATA BREACH

Edwin O. Amuga

Executive summary

In the third quarter of 2013, Target Corporation suffered a colossal data breach that resulted in large amounts of personal information and huge financial losses, which affected tens of millions of Americans and adversely impacted the 2014 annual report. The 2014 annual

financial statements of the company were adversely affected by the breach. This paper aims to discuss the effects of the company data breach on the 2014 annual financial report and the losses suffered the impact it had on the financial statements, March 13, 2015, Ernst and Young, and the weaknesses in the company's information system. The cyber accounting challenges and mitigation measures and trends in the face of cybersecurity are also examined.

Keywords: Security, Network, Assessment, Technology, Cyber, Intrusion

Introduction

Information risk and security issues have increased to a phenomenal concern for every organization regardless of the size. This risk escalation is due to the increased information systems development, and their consequences lead to financial, operational, and reputational losses. Computer forensics, therefore, plays an imperative role in counteracting computer-related crimes by obtaining and analyzing digital information use to ensure an organization's computer network system security. Therefore, organization heads must implement best-suited evaluation methods and assessment for a well-elaborated risk mitigation process to better control business practices, thereby improving the business process. Quantitative and qualitative have been developed for security evaluation. These methods include creating and updating security policies, analyzing data, reviewing documents, identifying risk, scanning for vulnerabilities, briefing, and reporting.

The Data Breach

An intruder installed malware on the united states store customers' point of sales systems and stole a significant amount of payment card and guest information from the company's

network. The intruder successfully made away with over 40 million guest debit and credit card accounts who shopped in stores in the United States between November 27 and December 17, 2013. The intruder also had unauthorized access to data of over 70 million guests, including email addresses, names, mailing addresses, and phone numbers. A forensic investigation into the intrusion found that the network art responsible for handling payment card data did not comply with relevant payment data security standards. As a result of the data breach, the company has suffered a financial loss of \$252 million in cumulative expenses, which were partially paid off by \$90 million insurance recoveries for the cumulative expenses of \$162 million. Additionally, due to the data breach announcement, the company saw a sales decline as a result. The information disclosure of the data breach was done in the company's 2014 annual report signed by the CEO and Company chairman, Mr. Brain Cornell, and Executive Vice President and CFO, Mr. John Mulligan (Target, 2015).

Ernst and Young Audit report

An audit was conducted on the financial statements and financial reporting internal controls of the Target Corporation by Ersnt and Young as unqualified opinion, which showed that the financial statements were fairly represented in all aspects, according to the Public Company Accounting Oversight Board standards (Uwadiae, n.d). Per the PCAOB regulations, all public accounting firms have to be registered as the body establishes the standards related to accounting, including quality control, auditing companies' independence, and ethical adherence. Ernst and Young, as unqualified opinions imply that the judgment f an independent auditor on the financial statements of the company are appropriately and fairly represented without

exception and complies with the Generally Accepted Accounting Principles (Plachkinova and Maurer, 2018).

Ernts and Young additionally conducted a financial reporting internal control audit for the company. They posited that Target had fully maintained efficient internal controls on their financial statements report under the COSO guidelines in an unqualified opinion in the march 13 2015 report. With the COSO framework, companies are able t establish, assess and enhance internal controls as it is crucial n financial reporting due to the fact that it offers investors with reasonable assurance on the accuracy of the financial statements.

The vulnerability of information systems

The point of the sales system suffered vulnerabilities that paved the way for the data breach. Utilizing this weakness in the point of sales systems, the intruder installed malware to allow them to acquire debit and credit card information and millions of United States Target shoppers' data. The company suffered a POS software vulnerability starting as a third party vendor, resulting in the intrusion on the point of sales system that combined weaknesses in the supply chain, vulnerabilities in the information security, and cyber awareness weaknesses. Because the intrusion began as a third party vendor, it was treated as a weakness in the supply chain. The intruder used an email to attach a malware and sent it to Fazio Merchant Services employee, a third party vending company that supplied mechanical and refrigeration services to Target. A malware named dubbed Citadel was then installed to steal login credentials from the computer system. It was also alleged that the employee replied to the email using a commercial Malwarebytes Anti-Malware software version, which did not provide real-time anti-malware protection. Fazio mechanical lacked security measures in its network and system, which

created the supply chain weaknesses for Target Corporation. Target, on its part, did not examine the security system of the vendor, which also added to the vulnerability in the system supply chain.

The resultant difficulty accessing the point of sales terminals of Target across the whole network upon getting into the Target network raised the alarm for the intrusion and information security weakness upon investigation. Citadel was able to enter Target's network and access all the POS system information due to lack of additional security levels, POS weakness security controls, and weak passwords used by Target for several internal systems and storage of a range of credentials in the servers of Target. The investigation also revealed that Target Corporation used outdated web servers that did not have critical patches that allow attackers to access the affected systems without using credentials. As part of the weaknesses, Target did not respond to numerous malware notifications from November and December, resulting in security control vulnerabilities.

All the weaknesses highlighted herein enabled the intruder through Citadel to hack the POS system easily and get hold of debit and credit card information and other personal customer information in the United States. The weaknesses were not satisfactorily highlighted in the annual report of Target Corporation but the compromised POS system and the number of affected people and the information stolen.

Cyber Accounting Challenges and Emerging trends

Target Corporation conducts its accounting according to FASB and IFRS. The United States has a long traditional accounting history, and its accounting environment has experienced

changes over the years in light of national laws, regulations, and international accounting standards. There have been questions on how to quickly adapt to GAAP to coexist with international accounting standards that have an increasing influence. The newly developed enforcement regulations enhance investor protection and efficiency in the market. The American requirement for all listed companies to prepare consolidated financial statements following the International Financial Reporting Standards has also contributed to adjusting accounting practices among companies in the country.

These adjustments in the accounting environment have different effects on different accounting practices. Among the accounting areas affected by the IAS are cybercrime-related losses in an accounting process. The international accounting standards have a criterion for investments and expenses but not cyber-related losses as these are new and emerging problems. The IAS 38 classifies cybercrime costs as identifiable non-monetary liabilities. This case requires careful consideration since there is no consensus on the matter among different accounting platforms. This paper looks into the international guidelines for cybercrime-related costs and how they can be applied at Target Corporation. The application of international accounting standards at the company will add to handling the practice in many companies.

Accountants are striving to adjust to the new technological demands in the face of the digital age. A gamut of softwares have been used by the ever-growing number of accounting professionals, including Tableau, IDEA, and Quickbooks, in their daily accounting work. Cloud computing and data storage is also gaining prominence in the accounting field, among other technology uses that come with cybersecurity risks. It is estimated that financial institutions are three times more likely to be targeted by cyber attackers than any other company due to the fact that these companies handle large sensitive financial information volumes daily, with phishing

and hacking being the most common cyber attacks. In many cases, employees are lured into falling for harmful emails laden with malware due to a lack of cybersecurity awareness and password management. It is estimated that over 90% of employees use predictable passwords crackable within six hours, with 18% of employees sharing their passwords with others (PCAOB, 2013).

The increasing risk in cyber threats and attacks is pushing accountants to be aware and understanding the mode of identifying and responding to cyber threats and attacks. In this regard, accountants must understand information technology security policies in their firms to ensure safe online dealings and appropriate reporting and handling of data breaches. It is, therefore, imperative for companies to train employees on cybersecurity and cyber awareness.

Future Threats Mitigation

Target must increase and enhance network security levels by providing appropriate training and education to its employees, third-party vendors, management, and suppliers to prevent and manage future attacks on its networks (ACAT, 2020). Cyber awareness training to be considered by the company should include cybersecurity threat education, threat management, password management, authentication, and provision of additional resources to system users. An effective training program follows systematic steps to meet organizational objectives and participant expectations. The development of management and supervisory skills, defining organizational missions, goals, and objectives as we assess situations and improve the performance of work must be achieved through researched-based solutions through the use of consultants. Additionally, they can identify training and operational needs, improve communication within an organization

On cyber threat training, employees, third-party vendors, and suppliers should be trained on potential cyberspace threats, including social engineering, malware, spam, phishing, and other possible threats and their impacts on systems and networks to identify and manage the risks when they occur. The company should educate its employees not to open or download unidentified emails, software, or links on threat management. On password management, the employees should be educated and guided to create strong, unpredictable, and hard-to-identify passwords. The company should mandate a two-factor authentication, which increases the storage and crucial information access security level on authentication. Target should also provide additional training resources, such as the SANS Institute, which offers in-person and online training.

To further fortify its information technology, the company should take a range of measures and awareness, including ensuring that the software in use is up to date, screening for suppliers, and third-party vendors on cybersecurity measures before being allowed to access credentials and the network. The company should also ensure that its security measures comply with applicable standards and regulations. Additional security layers in systems and networks should also be added to ensure that the information is not easily accessible by attackers or any potential threats. Target should also ensure that it has a well-trained team that acts on alerts and notifications upon detecting cyberattacks or threats.

Accounting Methodology

IISAB38 demands that costs related to cybercrime losses be deemed as not having future economic benefits, and therefore its capitalization does comply with the accruals concept. As a result, the treatment of this kind of expenditure is to write it off to the incurred profit and loss

account. Consequently, spending on the costs of development, as a basic rule, should be computed in the profit and loss account and written off as obtained as with the expenditures. Under ISAB38, there is an option to defer spending and carry it forward as business losses as it has such characteristics as not being clearly defined, commercially impracticable, and technically infeasible. The separately identifiable expenditure, there are resources available for project completion, and the project's income outweighs the project cost. If the requirements were fully met, the company could capitalize on the costs, bring them onto the balance sheet, and maintain the policy to write expenses off to the income statement. If the business decides to adopt an accounting approach on capitalization, the same application should be consistent and replicated in the treatment of cyber-related losses meeting the requirements.

Accounting of cyber loss costs according to FASB and IFRS

Investment in research and development can be referred to as an intangible business asset with no physical form. Tangible assets, consequently, can be seen or touched with transparent outcome predictability. In business, intangible assets are of two types: those that are internally generated and those purchased. Accounting treatment of the purchased ones is straight forward with its purchase capital obtained in the same way as tangible assets. Internally generated assets require careful consideration. Research and development costs in business are categorized as internally generated intangible assets and, therefore, must be carefully looked at before accounting with recognition to the host country and international regulations and standards.

In the United States, treating cybercrime losses in accounting is not different from many places worldwide. Its accounting standards govern the treatment even though they are an investment in technology being tangible in the United States.

Evaluation criteria

Economically, it will be reasonable to capitalize on technology investment costs even though its benefits cannot be estimated. For asset value to be assessed for capitalization, the number of years needed for the investment to generate profit has to be determined. It will be subject to amortization period assumption. Amortization life differs from one asset to another and reflects the economic viability of investments. For the amortization life of technology, the investment must be estimated, information is gathered in the past years' expenses on the investment. The costs incurred during the amortization life are obtained as a way of evaluation.

The cost of intangible assets separately acquired, according to IAS 38, comprises of its purchase price, together with import duties and non-refundable taxes, fewer rebates and discounts, and any directly attributable costs or asset preparation for the intended use. The subsequent measurement of intangible is a very similar property like equipment, plant, and property. For the following evaluation, two models, the cost model and revaluation models, can be used. The cost model demands its cost less accumulated amortization assesses intangible costs, just like depreciation is handled, less any accumulated impairment loss. In the revaluation model, intangible assets are carried at fair value at revaluation date less accumulated amortization less any accumulated impairment loss (Dinh, Kopf and Schultze, 2017). The revaluation model is not frequently applied for intangible assets since it demands the existence of an active market, which is rare.

Designation criteria

Under IFRS rules, cyber crime losses are classified under administrative expenses, as it is done under GAAP. By contrasting IFRS and GAAP, costs spent on technology are capitalized when the company established that it is commercially viable. The IFRS approach is that some

technology investment and cybercrime loss costs can be utilized instead of being incurred as an expense in the profit and loss statement. IFRS requires subjectivity and judgment, which creates risk management gives room for optimism. Technology is a long term investment in the company. The results will be seen in successive years to come in revenue increase, cash flow, and profit and thus, should be capitalized, rather than being listed as an expense. Without the capitalization of technology spending, it won't be easy to compare with companies in the industry. Losses due to cybercrime significantly impact other companies' yearly bottom lines. In the research phase, it is impossible to demonstrate the future economic benefit of the investment. The IAS 38 states that the expenditure incurred here are written off to the income statement as an expense and should not be capitalized as an intangible asset (Dinh, Kopf and Schultze, 2017).

Conclusion

Vulnerabilities emanating from weak cybersecurity protocols and lack of cybersecurity awareness result in security breaches, leading to substantial financial and information losses. Target suffered the data breach due to many weaknesses in the management of its information technology, as highlighted in the 2014 annual report. The breach adversely affected the financial statements to be audited by Ernst and Young (Tuovila, 2019). In the March 13, 2015 report, Ernst and Young offered an unqualified opinion that posited that Target had fairly represented its financial statements and financial reporting internal controls on the impacts of the data breach on the financial statements. Target in the 2014 annual report disclosed the material effects of the 2013 data breach on its financial statements after the occurrence and presented its losses and material amounts that impacted its financials in the year.

References

- Annual Cybersecurity Awareness Training. (2020). Lecture. Retrieved July 17, 2020, from <https://www.wapa.gov/jobs/Documents/annual-cyber-security-training-new-hire.pdf>
- Dinh T., Kopf K. & Schultze W. (2017). Springer. Controlling & Management, ework.pdf

Plachkinova, M. & Maurer, C. (2018). Teaching Case: Security Breach at Target. Journal of Information Systems Education, 29(1), 11-20. Retrieved July 17, 2020, from

<https://jise.org/Volume29/n1/JISEv29n1p11.pdf>

Public Company Accounting Oversight Board (PCAOB). (2013, January 16). Retrieved July 17, 2020, from <https://www.sec.gov/fast-answers/answerspcaobhtm.html>

Target 2014 Annual Report. (2015). Retrieved July 17, 2020, from

<https://investors.target.com/static-files/25786cd8-19a2-4895-938d-519c02157000>

Tuovila, A. (2019, May 23). Unqualified Opinion. Retrieved July 17, 2020, from

<https://www.investopedia.com/terms/u/unqualified-opinion.asp>/FinancialReporting/ng-coso-an-approach-to-internal-control-fram

Uwadiae, O. (n.d.). COSO - An Approach to Internal Control Framework. Retrieved July 17,

2020, from <https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/audit>