Study on Cybersecurity Risk and Business Management

Ye Wang [1,a,*]

[1]*AB. Freeman School. Tulane University, Congtai Road, Handan, China*
a.wangye7272@163.com
**corresponding author*

Keywords: cybersecurity risk, cyber-attack, business management

Abstract: Cybersecurity risk is a common risk that companies must pay attention with. In the fiscal year 2017, Equifax suffered a serious cybersecurity incident. The cybersecurity incident brought a series of damage to the company operation. In order to better carry out cybersecurity risk management and risk avoidance, this paper starts with the classification of cybersecurity risks, analyses the consequences of cyber attack from financial perspective and operational perspective, and summarizes the solutions from the macro strategy and micro strategy.

1. Introduction

According to the Equifax 2017 annual report, Equifax, a leading company which provides payroll-related and human resource management business, suffered a serious cybersecurity incident. Criminals got unauthorized access to Equifax's network through cyber attack, and stole the personal information of Equifax's consumers, such as names, Social Security numbers, birth dates. Even more seriously, criminals stole around 209,000 U.S and Canadian consumers' credit card numbers. This event brought very harmful consequences for the Equifax. In the 2018, Equifax reported operating income decreasing from 831 million dollars to 448 million dollars[1]. The cyber attack resulted 50 percent decrease revenue. Because of numbers of similar cybersecurity incidents that happened in the past years, the cyber attack risk now becomes one of the biggest problem which brings a sense of fear and costs millions dollar loss to the financial institution and companies. In order to understand better about the effects of cyber attack, this paper will introduce the which types of institutions that have large probability to experience attack and conclude effects of cyber attack on the finical institutions and companies and find ways to help finical institutions to cut loss.

2. The Background of Cybersecurity Risk

2.1. What Is Cybersecurity Risk

In current, cybersecurity risk is a very common risk that companies must pay attention with. Otherwise, it can bring very serious problems to that company. According to the Larry Satucci, Cyber security risk is defined as any risk of financial loss, disruption, or damage to the reputation of an organization from a failure of its information technology systems" [2]. Basically, cyber security

risk is a risk that hacks can stole valued information. If information were stolen, that event will harmfully affect companies' operation and hurt companies' reputations.

2.2. The Classification of Cybersecurity Risk

The CERT Program developed a taxonomy of cyber security risks for the all companies. It concluded cyber security risks in four main classes: 1. actions of people, 2. systems and technology failures. 3. failed internal process. 4. external events. The CERT program also decomposed these four classes into many subclasses [3]. Basically, the CERT program divided cyber security risk into four divisions through analyzing the instances that result cyber risk. First, that the companies' management neglect and inaction about the cyber risk can result the cyber security risks. Second, the companies' backward cyber system can make companies very vulnerable to the cyber attack. Third, lack of processes such as monitoring cybersecurity, controlling the cyber system, and updating the new technology can result cyber security risk. The last, some external factor, such as, natural disaster, business issues, and legal issues can attract cyber attack to the companies. Moreover, Shinichi Kamiya concluded which types of firms have more chances getting cyber attacks. Hackers target firms that hackers can get valuable information, such as the finical institutions, finical agencies. Second, firms that have more intangible and highly valued assets have large chance suffering cyber risk. Third, Hackers may also target on the firms which have less attention on the cyber security management. In addition, firms with the monopoly profits can get cyber attack more often [4].

3. The Consequences of Cyber Attacks on Businesses

In order to fully understand the adverse consequences of cyber attacks, this paper analyzed Equifax and Yahoo' operation performances through their balance sheet, income statements, and cash flow statements.

3.1. The Consequences of Cyber Attack from Financial Perspective

Cyber attacks lead company losing billions dollars. Equifax and Yahoo had some common characteristics. First, they all engaged in the losing profit and decreasing their stock value. For examples, Equifax's operating income dropped from 831.7 million dollars in 2017 to 448 million dollars in 2018. The operating margin drop from 24.7% to 13.1 %. Moreover, Target also decreased in its EBIT. In the year 2014, Target's EBIT growth is -11.3% [5]. Those numbers indicate that successful cyber attack will hurt the companies' financial performance. Moreover, successful cyber attack also will increase the cost of the companies. For example, Equifax spend around 70 million dollars to offset their customers' losses because the cyber attack. Even more serious, Yahoo is still struggling with their cybersecurity from year 2013.

Through above analysis, we got conclusion that cyber attacks have big impact on the companies' operational and financial performances. All companies have decreased their EBIT, their ROA, and their stock prices. Those companies lose tons of money because of the cyber attack. Moreover, companies have to spend more money to eliminate the effects of cyber attack.

3.2. The Consequences of Cyber Attack from Operational Perspective

This paper will mainly introduce the operational challenges that Equifax has to overcome. After 2017 cyber security incident, Equifax have faces three operational challenges. First. their

reputations were damaged. According to the Wall street journal in 2017, the Equifax has stunned many consumers who are suddenly aware of their own vulnerability to the country's financial plumbing [6]. Many customers and stakeholders suspend the securities of their businesses. If they cannot gain their reputations back, it will result negative impact on Equifax business. Second, their ISO certifications were suspended. It is very important for their business. If they fail to maintain or regain these certifications, they may stop doing business, and cannot to get new business. Third, Equifax spend abundant money and provided free services to assist their customers who were effected by the cyber attack. For example, Equifax provided free services for their impacted consumers to monitor their credit and identity information in the U.S. Moreover, Equifax also faced many lawsuits. Government officials and agencies invested and created several claims. Those claims and investigations brought significant external and internal legal costs and expenses. If Equifax were unable to obtain sufficient financing to meet their obligations as the time duo, those claims and investigations fee would adversely effect their business. Not only Equifax needs to face those challenges, but also other companies who suffered from cyber attacks will face those problems. Those problems can significant adversely affect company's operational performance, and damage companies' profits. In order to avoid the big losses from cyber attack, what the companies should do?

4. Solutions and Further Questions

Faced with such huge losses, companies have to find out ways to reduce the losses and to reinvigorate. Following passages will introduce some advises before the cyber risk, and remedy for losses after cyber attack.

Federal Financial Regulators gave some enhancements of the cyber risk management on the Oct 16, 2016. It suggested that cyber risk management into three independent functions: Business units, independent risk management, and audit [7]. The business units should know how to manage those risks; Independent risk management should have its owe line to reporting to the board about the cyber security risk; Audit should have an audit plan to decide whether companies' risk control is rational. This is the whole functions for the company. For more specifically, business units should attach the importance to the cybersecurity risk. Business units should also fully understand the ways to cope with the aftermath of the cyber attack. Independent risk management should assess the cyber risk quantitatively through the company. Audit should design the experiments to test the vulnerability assessments with the size of companies, the types of operations, and the likelihood of occurrence.

For the macro-strategy, companies should establish a board to monitor the inherent cybersecurity risks. In addition, those board of directors should have adequate expertise in cybersecurity in order to fully accomplished their duties. For example, the Jet Propulsion laboratory of NASA has designed a board with independent technical experts. Those experts should decide the cycle of the risk happened. Then, they set meeting once or twice a year. The reason of the meeting is to "forcing engineers to think about whether they have the sufficiently considered likely failures and defects". For cybersecurity risk management, company can do the same [8]. Company should set a board meeting periodically, and board should discuss about the failures and defects of their progress of managing cybersecurity risk. Company should also hire agencies who can ensure the governance. James Fox, a leading authority on cybersecurity in the Financial services industry also shared his idea to help controlling the cybersecurity risk management [9]. He suggested firm should have a cybersecurity risk management plan first, and then firms should fully execute the plane. Firm should also establish a simple and fully risk appetite statement and based on the risk appetite

statement to allocate investment dollars for the cybersecurity risk. This risk appetite statements will help company to minimize the costs and also help company to control the cybersecurity risk as much as possible.

Companies should also develop some micro strategy based on their companies' circumstances. There are five steps that leading regulators in financial markets have given out the cybersecurity guidelines [10]. The financial industry regulatory Authority suggested firms to layer several independent securities to control company's IT system. It also suggested to restrict the numbers of employees to access their database. Also it suggested companies to make complicated security code to protect their data. In addition, firm should find a third party to test any potential cybersecurity weakness. It will help firm to find the insufficient of controlling cybersecurity. For example, some information system security association will help company to managing cybersecurity risk.

Moreover, buying cybersecurity insurance is one of the most helpful way to decrease the losses. Cyber insurance may cover the damages that cybercrimes created and may also cover the customers' losses. Some argued that buying cyber insurance will increase the cost of company a lot, and the insurance could not fully cover the companies' losses. However, in the Equifax case, during the year ended December 31, 2017, Equifax had $125 million of cybersecurity insurance coverage to limit their losses that related to the cybersecurity attack [11]. Although those 125 million could not cover all the losses, but it really helped Equifax to reduce their losses. Cyber insurance helps company to transfer its risks to insurance companies. Those cyber insurance policies can cover many perspectives of losses, such as credit tracking, media responsibility, computerized data loss and its recovery, lawsuit compensation, and etc.

Through above analysis, in order to prevent the cybersecurity risk, company should understand how cybersecurity management works and understand three functions which include business units, independent management and audit. Then from macro perspective, company should set boards, build plan and risk appetites. Boards can help monitoring companies to execute the plane and risk appetites. For more specific, companies should follow above five steps to prevent the cybersecurity risk. Moreover, buying cybersecurity insurance will help company to mitigate the losses that cyber attack resulted.

5. Conclusion

Cybersecurity risk is one of the harmful risks for the companies. Companies need to pay attention and prevent this risk in the future. This paper introduced the cybersecurity risk's definition, and the classification of the cybersecurity risk. Moreover, this paper had an analysis about the consequences that cyber attacks lead. Last, it gave some advices to prevent the cybersecurity risk and to mitigate the losses from the cyber attacks. Cybersecurity risk is unavoidable problem in the company risk management, if companies fully understand the risk and take precautionary measures, companies can minimize the losses and prevent future cyber attack.

References

[1] *Equifax Annual Report. (2018). Equifax, 15.*

[2] *Larry Santucci. (November 2018) Quantifying Cyber Risk in the Financial Services Industry. Federal Reserve Bank of Philadelphia Consumer Finance Institute, 6.*

[3] *L.R. Young, (2010) "A taxonomy of Operational Cyber Security Risks". Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.*

[4] *Shinichi Kamiya, Jun-Koo Kang, et al. (July 2018) What Is the Impact of successful cyber attacks on Target firms? National Bureau of Economic Research, 4.*

[5] *Target Annual Report. (2015). Target, 17.*

[6] AnnaMaria Andriotis, Michael Rapoport and Robert McMillan. (Sept. 18 2017) 'We've Been Breached': Inside the Equifax hack. Wall Street Journal.
[7] Luke Dembosky, Jeremy Feigelson, et al. (2016) Federal Financial Regulators to Propose Enhanced Cyber Risk Management Standards. Banking and Financial Services Policy Report, Volume 35, Number 11, 18.
[8] Robert S. Kaplan and Anette Mikes., (June 2012) Managing Risks: A New Framework. Harvard business.
[9] Larry Santucci. (November 2018) Quantifying Cyber Risk in the Financial Services Industry. Federal Reserve Bank of Philadelphia Consumer Finance Institute, 29.
[10] Kristin N. Johnson. (2011) Cyber Risks: Emerging Risk Management Concerns for Financial Institutions, 140.
[11] Equifax Annual Report. (2018). Equifax, 33.