THE HARMFUL EFFECTS OF CYBER CRIME IN BUSINESS AND ECONOMIC SUSTAINABILITY

Navneet Kaur Popli [1]
Dr. Anup Girdhar [2]

Abstract

Businesses today, both nationally and internationally are moving towards digitization at a fast pace. With the recent digital initiative by the Modi government in India, the entire global business economy is eying our nation anxiously to see how the country benefits from this new development. Digitization, however, is a path to be trodden cautiously. It is ridden with different types of attacks on business in the cyber world. Cyber crimes committed by worms, viruses, trojans, botnets, shellcodes etc. cause a great deal of damage to businesses both small and large. In this paper, we try to access the harmful impact that cyber crimes and cyber espionages have in business and economic sustainability.

Keywords Digital Economy, Cyber threats, malware, cyber criminals, economic instability, cyber espionage, ransomware, denial of service, identity theft, phishing.

Introduction

Cyber Security may not be your first priority when one starts establishing a business. However, neglecting it can cause serious damage to your organization. The losses cybercrime can cause to your business may be direct or indirect. Also it is wrong to believe that only online businesses face a threat from cybercriminals. You may have an offline business but the very fact that you are connected to the Internet (which every organization today is) in some way or the other pose a threat to your company. It provides a door to the cyber criminal to enter into your company and then place himself at a position where intensified harm can be done to your system. Information must be considered as an important resource and appropriate care has to be taken for its security. All organizations, whether big or small suffer because of malware attacks of some type or the other. Losses range from financial to reputational to political etc. either fully or partially [1].

II. TYPER OF CYBER CRIME

It is a myth that only large organizations are hit by cyber crimes. Small and mid size organizations are also hit hard by cyber criminals. They are an attractive target especially because most of them do not have the required funds and time to devote to cyber security activities.

Cyber crime generally falls under two broad categories [2]-

1) Information theft
2) Vandalism

Information theft means stealing of important company information like data about customers, vendors or products, business plans, research analysis, transactional histories, proprietary information, financial information etc. Phishing is a form of information theft in which a person is lured into leaking his personal information like credit card details, account numbers etc. When they click on a malicious link in a seemingly legitimate e-mail.

Digital vandalism involves denial of service attacks, virus, trojans, bots etc. which normally leads to disruption of business causing a lot of harassment to the organization and its customers as well as vendors.

According to a report by FBI in 2014 on the type of cyber attacks, notable among them are [3]:

1) Viruses
2) Trojan Logons
3) Employee abuse of internet privileges
4) Denial of service
5) Unauthorized access by insiders
6) Theft of proprietary information
7) Sabotage of data and networks
8) Financial frauds
9) Manipulating data integrity
10) Installing a sniffer
11) IP spoofing
12) Data diddling
13) Salami attacks
14) E mail bombing
15) Web jacking
16) Logic bombs

The types and complexities of cyber attacks keeps increasing day-by-day and thus huge costs, time and trained manpower is required to combat the attacks.

iii. Losses to a business caused by cyber crime

There are a number of ways cybercriminals are a threat to business.

1) **Loss due to cyber-espionage**- cyber-espionage means spying on business to get important information like patents, business plans, blueprints, sales strategies, merger/acquisition data, product designs, formulas, research analysis, customer and vendor information etc. The information is not stolen and still lies within the company. The company may not even be aware that it is being spied upon. The losses are not direct because there is no theft of information but this can be used by a rival company in any possible manner. It may pull out your employees, use your business plans and may try to disrupt your business in varied ways. The rival may try to influence your loyal customer base in buying their products instead of yours. The impacts can be many and can be quite dangerous as well.

[1]Research Scholar, Tilak Maharashtra Vidyapeeth, Pune
[2]CEO, Founder, Sedulity Solutions and Technologies

2) **Loss due to theft-** to cause more vandalism, the rival may steal the information after spying. This means important data no longer lies with the company. A company invests billions of dollars on collecting, analyzing and using information. Once the information is stolen, it causes a direct financial loss to the company. Also precious contacts are lost leading to loss of business from both customer and vendor side. In addition to that, smooth functioning even within a company is barely possible without accurate data.

3) **Loss due to Ransomware**- Ransomware is any malware that enters a system covertly and looks like legitimate code[4]. After installing itself into the system, it encrypts all files and databases and asks ransom payment to decrypt the files. The ransome may cost thousands to millions of dollars. This leads to heavy direct financial losses, in addition to a sense of fear and insecurity in the employees.

4) **Security cost**- with cybercimes on the rise, more and more money has to be invested for protecting a business' cyber property. The cyber crime methodologies keep changing and a company has to invest a lot in keeping up to date with these changes and devising ways to get rid of cybercrime [5]. Thus cyber crime protection is indeed a very expensive affair.

5) **Loss of Reputation and Customer trust**- It takes years of good business practices to build a company's reputation and a single cyber attack to destroy it[6]. If customers suffer financial losses on a company's site, they are never going to return to that site again. If the home page is defaced even for some hours, the company's reputation among customer's and vendor's mind is maligned. The company loses trust which ultimately leads to loss of business.

6) **Cost incurred in solving the problem**- Once an attack has happened which may be theft of information, cyber espionage, defacing the site, phishing attack etc.; it is important to fight the attack. Huge amounts of time and money go into setting things right. Repairing the site, decrypting the encrypted information, getting the lost data back all incur lots of cost.

7) **Cost of legal suits**- When important customer or vendor data is lost, an individual has every right to fight a legal suit against the company. These legal difficulties cost dearly to any business. In case of any kind of security breach, if a legal action is taken, unprecedented losses may be incurred by the company in defending itself [7].

8) **Loss due to Denial of Service attack**- Malware can stalk a company's working for an indefinite time. During this period, the company is unable to give its services to consumers. This denial of service leads to huge direct and indirect losses to the company. Denial of service is done using e-mail barrages, viruses or overflowing the company's server by repeated and incessant service-requests causing slow down of servers or complete shutdown of computer systems [8].

9) **Loss due to Identity Theft**- is one of the most serious thefts which directly impacts individuals and thus businesses. According to FBI, 30 million credit card security numbers were stolen through computer security breaches during 1999-2003 resulting in US $15 billion in losses [9].

10) **Loss incurred in paying penalties**- many a times if customer loses his important information or has to suffer some financial loss because of cyber crime, it becomes the responsibility of the company to pay him penalty. Even if nothing tangible is lost, if the customer had to wait long for a service, then the company is liable to compensate for the inconvenience and the delay caused.

III. STATISTICS ON LOSSES DUE TO CYBER CRIME

The tsunami of cyber crime is sweeping across the world with a high speed. According to IBM Corp.'s Chairman, CEO and President Ginni Rometty, cybercrime may be the greatest threat to every company in the world [12].

In 2013, the Wall Street Journal estimated the cost of cyber crime in the U.S. to be approximately $100 billion. In 2015, the British Insurance company Lloyd's estimate was $400 billion a year loss to business because of cyber attacks.

From 2013 to 2015 the cyber crime costs quadrupled and it is predicted that there will be another quadrupling from 2015 to 2019. Juniper Research predicted that the rapid digitization of business will increase the cost of breaches to $1.2 trillion globally which is almost four times the cost of breaches in 2015 [13]. The cost of committing the crimes however is astonishingly low. A typical phishing attack for 500,000 e-mails would normally cost only $30. Hosting a phishing site is almost free. Thousands of credit cards can be stolen in only $100.

IV. SAFETY FROM CYBER ATTACKS

In this paper many situations were discussed where cyber criminals can disrupt business, steal information and can harm any business big or small with different ranges of severity. However, digital business is the need of the hour and our ultimate future. Therefore, instead of getting scared, we must gear ourselves and fight cyber crime with all our might. Here some good business practices are suggested which help us do just that.

All business organizations must keep their operating systems, browsers and all system software regularly updated. Any patch, if suggested should be implemented. New malware keep getting invented to attack these software and patches are a way to protect the software from latest malware; in addition to enhancement to the software. Also firewalls, antivirus and other Intrusion detection prevention systems must be in-place and updated at all times to counter any kind of malware.

All required encryptions must be done on important data to secure it further. There should be strict and well defined administrative rights given to employees which restrict software installation without authorization. Also passwords, filtrations etc. must be applied without fail.

Some sites which are found to be malicious must be blocked so that malicious content does not get into your organization's network. Strict policies must be made for usage of external memory devices like pen drives or CD's. Employees must not be allowed to carry them home or bring them to the office. Sometimes an employee can be an attacker so as a policy all employees should be searched for external memory devices both while coming and going from the company premises.

REFERENCES

- Das, S., & Nayak, T. (2013). Impact of cyber crime: issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142-153.
- Egeland, B, (2015), *4 Ways Cyber Crime Can Hurt Your Small Business*, Retrieved from http://www.businessknowhow.com/security/cybercrime.htm
- Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.
- Malhotra, V & Malik, S,(2010), Global Economic Instability Because of Cyber Crime, *International Journal of Computer Applications*, 1(2), 5-10.
- McAfee, (2014), *Net Losses: Estimating the Global Cost of Cybercrime* , Center for Strategic and International Studies, Retrieved from http://www.mcafee.com/in/resources/reports/rp-economic-impact-cybercrime2.pdf .
- Mohr, A, *3 Ways Cyber Crime Impacts Business*, Retrieved from www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.asp.
- Morgan, S,(2016), *Top 5 Industries At Risk Of Cyber-Attacks, Retrieved from https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/&refURL=https://www.google.co.in/&referrer=https://www.google.co.in/*
- O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Symantec Corporation.
- Ponemon Institute (2012). *The Impact of Cybercrime on Business*, Retrieved from https://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf>
- Report, FBI, |(2014). *Internet Crime Report*, 'Retrieved from https://pdf.ic3.gov/2014_IC3Report.pdf>,
- Reuters,(2014), *Cyber crime costs global economy $445 billion a year*, Retrieved from www.cio.com/article/2908864/security0/5-costly-consequences-of-smb-cybercrime.html
- Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-9.