CYBER RISKS, THE GROWING THREAT

[1]Muthu Dayalan
Researcher & Software Professional

Abstract: In the recent time, cybercrime is the most crucial issue that has a significant impact on the economy of the businesses especially those who are functioning online. This economic loss is effecting all the sectors including government and conventional businesses. Cybercrime, also referred as computer crime, is the use of computer devices and networks to advance other ends and commit illegal activities, such as committing fraud. The main source of all these activities is internet. The basis of this research paper is to identify the growing threats to businesses of all the sectors due to increase in cybercrime. Aspects explored in this research paper are the impacts of cyber threat and how it has caused worldwide disruption. In addition to this, what are the major threats, which can harm an enterprise in various ways? It further explores that how these cyber criminals are expanding into organized groups. Moreover, the various techniques that they have used in recent time to exploit the property of organizations. The results of this study will suggest that businesses need to revaluate their security policies in order to protect their confidential data.

INTRODUCTION

In the recent time, it is essential for businesses to shift from the conventional computing system to Cyber System. However, computer security threat has emerged as the most pressing problem for businesses due to lack of knowledge (Yadav & Gour, 2014). Cybercrime losses estimates about $300 billion to 1 trillion to world's economy (McAfee, 2013). With advancement in the technology, unauthorized users are finding new ways to harm the data from the computer system (Ahmad, 2016). Moreover, the difficulty has increased due to unidentified threats, which halt to select an approach for the solution. The internet availability around the globe has further triggered the threats as according to the data, the number of internet users has increased by 45% over the last decade to the global penetration level of 29% (Argaez, 2012). According to Euro Stat (2010), broadband access has increased from 4% to 64% within 8 years in the United States. Whereas, the public sector is being pressurized to use the internet for transparency and accountability. Regardless, globalization and the internet are providing new opportunities for businesses to improve the overall functioning; on the contrary, it is exposing more towards risks, which indicate the importance of Cyber Security (Andreasson, 2012).

DISCUSSION

The Business Impacts

All types of cyber-attacks affect the economy of an organization; however, the resulting impact of incident still does not depict an accurate picture. It varies from usual to invisible cost that include customer breach notifications, attorney fees, litigation, technical investigation (Deloitte, 2016, p.1), loss of IP, operational disruptions/destruction. Most commonly, attacker may interpret the stock price of the organization in order to negatively affect the image and value of the organization by using different malwares (Yadav & Gour, 2013). Moreover, there is a high risk of loss of sensitive data; especially financial competitors to harm the organization can use data as its access to unauthorized users. According to Ellen Messmer (2012), the financial Cyber-heist ''Operation High Roller'' was launched from servers in three countries: Albania, China and Russia (Watkins, 2014). This attack caused $78 million and $2.5 billion losses from the bank accounts plus notable damage to the global banking system. Moreover, 614 organizations across different sectors, including health, finance, education, and majorly government have publicly revealed the data breaches which accounts for almost 92 million (Center, 2013).

The Cyber-attacks are not only limited to small organizations but also have a potential to distress large corporations and government institutions causing global disruption (Smith, 2016). However, small businesses are under the deception that they are not under attack and have approached for lesser defense. Whereas, according to the latest report, nearly three-quarters (74%) of small organisations reported a security breach in last year which is an increase on the 2013 and 2014 survey. Digital attackers (Survey Government Security., 2015) are now pinpointing sMEs. However, according to Toni Allen (2015), "SMEs have not historically been the target of cybercrime but in 2015 something drastically changed". One of the key reason for attacking SME's is that hackers find it as an easy target plus they have a sheer chance to penetrate to larger corporations through SME's who are difficult to attack directly. Therefore, it is essential that SME's follow steps to reduce Cyber Risks. Even though some small businesses have started to recognize the potential severity of cyber-attacks but many still have a long way to go in implementing good risk management.

Major Cyber Threats

In recent times, every organization regardless of belonging to any sector should be prepared for unpredictable events. As recently, it was reported that yearly cost to the world-wide economy from cyber-crime is more than $400 billion which indicates that industry of cyber crime is the most growing industry because the risks involved are low whereas the returns are high (McAfee, 2016). This is why; businesses should take this threat seriously, as they are not only protecting themselves and their customers' data but also securing a competitive advantage (Vaizey, 2015). Deniel of service, malicious insiders, and web-based attacks are considered as the most common type used by attackers (Ponemon, 2014). Whereas, on the other side, the major threats include, ransom ware, which is a software that infects a digital device or system, shutting it down until the user meets the cyber criminal's monetary demand. Secondly, hack attack where the attacker is able to access the company data/network. This attack is common for identifiable information (PII) on the customers of the organization, especially credit card information. Thirdly, CEO fraud in which hacker is able to hack the email account of the authorized senior people and through that, they pose and convinces finance authority to make the payments (Krach, 2017).

In addition to this, denial of service attack is also becoming a threat due to its easiness to use and cheap cost. In this, a volume of data pushed to its servers in a malicious manner floods the website of the organization. Moreover, human error is also the most common and weakest link in the security chain where the data is breached either it is leaked to unauthorized people or important information is lost (Streetwise, 2016). All these threats are making companies struggle in cyber risk management else, they are at a great chance of highly visible breaches happening with growing regularity. Conversely, few technological executives have a view that they are losing tracks of the hackers, which is why companies are unable to quantify the impact of the risk and mitigation plans (Bailey, Miglio & Richter, 2014). Even though, it is essential to quantify intangible damages to anticipate business impact. A recent report by Fire-Eye (2015) reveals that hackers, especially from China are spying on government and business targets over the past few years (Hamzah, 2015). Thereby, cyber-crime has become a global concern as well. As quoted "Every CIO and CISO wake up each day knowing that if they don't get security right and breaches are suffered, their program can be perceived to be ineffective, and their citizens may suffer direct harm." (Deloitte, 2012, p.1).

The Cyber threat does not revolve around financial or any particular risk in this time, it is a real threat to performance and survival because most of the major large corporations are now technology-driven, and therefore they have the high chance of being vulnerable and hackers can easily penetrate. However, less than 40% of cyber-crime was reported in a survey because most of the companies do not realize and log the cyber-element of economic crime qualified (Survey Financial Services, 2014). This shows lack of management and awareness within the organizations due to which the chance of exposure to cyber threats increases regardless of having the cyber defense. Because cyber-crime is not accurately identified then is difficult to respond to it and come up with suitable solutions. On the other side, a report by PWC (2014) highlighted that companies are now considering cyber risk the highest level threat globally along with other business risks. This shows that companies are now investing resources to combat these threats. PWC (2014) also indicated 48% of CEOs in its latest Global CEO Survey informed that now their major concern is to secure the data and eradicate all kind of cyber threats (PWC, 2014).

The major reasons to increase in these threats include lack of cyber security policies as the target market of hackers is not only limited to finance but they are threatening every single company out there. Secondly, they are unable to differentiate between compliance and cyber security policy which is because of lack of employee training and awareness. And due to this, the companies are unable to come up with a recovery plan. A report observed the trend of incidents since 2013, that there has been slight progress in readiness and even till in 2015, there was a little or no increase in organizations that were not ready and had no proper plan to react to the incident (Zaharia, 2016).

How Cyber Criminals Operate

Cybercrime in today's time is not solely the realm of rogue hackers operating alone instead cyber criminals are now forming into formalized and organized groups (Singleton, 2013). The techniques and tricks of cyber-crime are making it difficult for companies to get immune to it. It is also observed that new techniques are revealed for masking exploits, specifically with the use of encryption protocol to make the detection of malicious codes more difficult. Additionally, cyber criminals are increasingly using Bit coin to make transactions in order to avoid detection. Furthermore, it is evident that the major factor behind cyber-crimes are monetary benefits and it indicates how lucrative this business is (Kaspersky, 2017). Consequently, it is expanding at such a rapid pace. Moreover, the cost of entry in this is very low and cheap. For instance, if the hacker is able to attack the date of 100 people, they can earn up to $10,000 by selling sensitive data to relevant people.

It has been observed that cyber criminals are looking for the more lucrative return on the investment through more cost cutting techniques which are why complex malicious programs are used rarely as they cost a lot, for instance; Rootkits and Boot kits. This huge investment may result in less return as they do not give the required result. Due to this, organized hacker groups are looking after mass produced malware that is tailor-made for cyber-crime. In addition, the small corporations that have the large corporation as clients are at a higher risk of being attacked as it is easy access to the load of information that some large enterprises have. As small organizations invest less on security due to budget restrictions. This is why hackers are well aware that even though their real target may have shored up their security, the vendors and service providers that serve them may not have been as vigilant. They take this opportunity to lapse as their point of entry (Aseef, 2005).

These days, most cyber criminals are operating like well-oiled machines and there are four most common types of hackers that include, cyber criminals who understand the importance of corporate information and how companies are sensitive towards it. Secondly, Cyber mercenaries who extract data from anyone on behalf of clients. Then there are Hacktivists who blackmail companies by leaking confidential information that may cause damages to the organization. And lastly, Nation States or Government Agencies which can be government contractors, who focus on collecting tactical information or unsettling business facilities in hostile countries. According to a report issued by Cyber Security Intelligence Index (2016), that 60% of all cyber-attacks were supported out by insiders and approximately one-quarter inadvertent actors and, three-quarters involved malicious intent (IBM, 2016). All this indicates that hackers around the globe are looking for efficiency, cost cutting techniques and high returns. This is why they are already on the market to make sure they succeed in it. Figure 1 indicates the number of web attacks blocked decreased slightly in July, down from 1,159,398 per day to 1,158,985 per day and this marks four months of elevated web attack activity (Corporation, 2017).

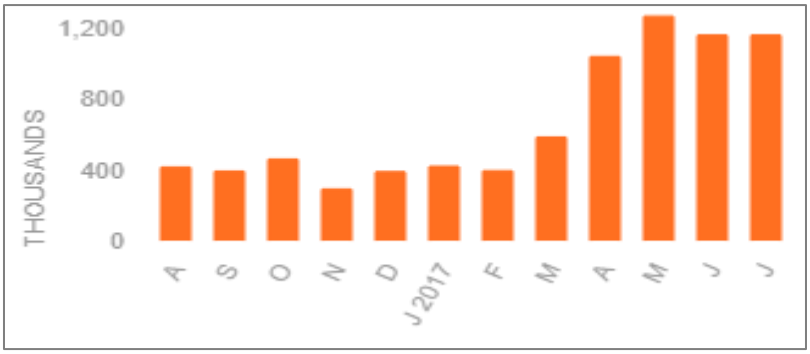

Figure 1: Web Attacks

CONCLUSION

In the era of technological development, technology has been a key enabler to better and more productive living, whereas on the contrary, it has its own consequences and it does bring its fair share of challenges as increasingly sophisticated cyber threats become a key concern in this connected world. Regardless of constant efforts from organizations, these attacks show no sign of slowing down. Thereby, it is extremely crucial to understand hackers' level of sophistication and determination. Moreover, Cyber Security teams along with organizations need to find effective ways to tackle these issues and a proper understanding of the actors.

REFERENCES

[1] Ahmad, A. (2016). Type of Security Threats and It's Prevention. Int J Comput Technol Appl, 750-752.
[2] Andreasson, K. J. (2012). Cybersecurity: Public Sector Threats and Responses. CRC Press .
[3] Argaez, E. d. (2012). New 2011 Year-End World Stats. 69. Data retrived from http://www.internetworldstats.com full on August 28 2017
[4] Aseef, N. (2005). Cyber-Criminal Activity and Analysis.White Paper .
[5] Bailey, T., Miglio, A. D., & Richter, W. (2014). The rising strategic risks of cyberattacks. Berlin: WEF; McKinsey,Company.
[6] Center, I. T. (2013). 2013 Data Breach Stats. San Diego:Identity Theft Resource Center. Data retrived from http://www.idtheftcenter.org/ full on August 16 2017
[7] Company, Mckinsey. The rising strategic risks of cyberattacks. Data retrieved from http://www.mckinsey.com/ full on August 17 2017
[8] Corporation, S. (2017). Security Response Publications United States:Symantec Corporation. Data retrieved from https://www.symantec.com full on August 17 2017
[9] Decker. (2012). Deloitte-NASCIO Cybersecurity Study: State government at risk: a call for collaboration and compliance. United Kingdom : Deloitte & Touche Enterprise Risk Services Pte Ltd. Data retrieved from https://www2.deloitte.com full on August 20 2017
[10] Deloitte. (2016). Responding to cyber threats in the new reality Australia:Deloitte & Touche Enterprise Risk Services Pte Ltd. Data retrieved from https://www2.deloitte.com full on August 17 2017
[11] Deloitte. (2016). Business impacts of cyber attacks. Australia:Deloitte & Touche Enterprise Risk Services Pte Lt.
[12] Euro Stat. (2010). Cyber Security and privacy hot topics 2015. Data retrieved from http:// ttps://www.pwc.se/ full on August 18 2017.
[13] Ellen, T. (2015). Huge rise in hack attacks as cyber criminals target small businesses. Data retrieved from https://www.theguardian.com full on August 21 2017.
[14] Forum, Mckinsey. The rising strategic risks of cyberattacks. Data retrieved from http:// http://www.mckinsey.com/ full on August 18 2017.
[15] Hamzah, Z. (2015). Responding to cyber threats in the new reality;A shift in paradigm is vital. United Kingdom : Deloitte & Touche Enterprise Risk Services Pte Ltd.
[16] IBM. (2016). IBM X-Force Threat Intelligence Index. United States:Cyber Security Intelligence Index.
[17] Kaspersky, l. (2017). Cybercriminals:Exposing the villains. Kaspersky Lab. Data retrieved from http:// http:// http://go.kaspersky.com full on August 20 2017
[18] Krach, K. (2017). 10 of the Biggest Cybersecurity Threats to Watch for in 2017. California:A Medium Corporation.
[19] McAfee. (2013). The Economic impact of Cybercrime and Cyber Espionage. Santa Clara: McAfee. Part of Intel Secuirty.
[20] McAfee. (2016). 2016 Threats Predictions. Santa Clara: McAfee. Part of Intel Security.
[21] Ponemon. (2014). Cyber Risk. Insurance Information Institute. Data retrived from http://www.iii.org/ full on August 21 2017
[22] PWC. (2014). Threats to the Financial Sector. The United States. PwC network.
[23] Singleton, T. (2013). The top five Cyber Crimes. New York: American Institute of CPAs.
[24] Smith, M. (2016). Huge rise in hack attacks as cyber-criminals target small businesses. London: Guardian News and Media Limited.
[25] Smith, M. (2017). Huge rise in hack attacks as cyber-criminals target small businesses. The Guardian News and Media Limited.
[26] Streetwise, C. (2016). Britons urged to take cyber security as seriously as home security. United Kingdom:Cyber Aware.
[27] Survey, Financial Services. (2014). Threats to the Financial Services Sectors. Price water house Coopers LLP.
[28] Survey, Government Security. (2015). Government urges business to take action as cost of cyber security breaches doubles. United Kingdom:Digital Economy Minister Ed Vaizey.
[29] Vaizey, D. E. (2015). Government urges business to take action as cost of cyber security breaches doubles. United Kingdom : Department for Business, Innovation & Skills Ed Vaizey .
[30] Watkins, B. (2014). The Impact of Cyber Attacks on Private Sector. MindPoint Group. Data retrieved from https://www.mindpointgroup.com full on August 16 2017.
[31] Yadav, H., & Gour, S. (2014). Cyber Attacks: An impact on Economy to an organization. International Journal of Information & Computation Technology, 937-940.
[32] Zaharia, A. (2016). 10+ Critical Corporate Cyber Security Risks – A Data Driven List. København K: Heimdal Security.