DE GRUYTER OPEN
RIGA TECHNICAL UNIVERSITY 1862

Information Technology and Management Science

ISSN 2255-9094 (online)
ISSN 2255-9086 (print)
December 2017, vol. 20, pp. 64–68
doi: 10.1515/itms-2017-0011
https://www.degruyter.com/view/j/itms

Data Analysis of Cybercrimes in Businesses

Shilpa Balan[1], Joseph Otto[2], Edgar Minasian[3], Arun Aryal[4]
[1–4] *California State University, USA*

Abstract – **In the current digital age, most people have become very dependent on technology for their daily work tasks. With the rise of the technological advancements, cyber-attacks have also increased. Over the past few years, there have been several security breaches. When sensitive data are breached, both organisations and consumers are affected. In the present research, we analyse the cyber security risks and its impact on organisations. To perform the analysis, a big data technology such as R programming is used. For example, using a big data analysis, it was found that the majority of businesses detected at least one incident involving a local area network (LAN) breach.**

Keywords – **Big data, cybercrime, R, security.**

I. Introduction

In today's digital age, people have become dependent on technology to complete their tasks electronically. The use of computers, laptops, tablets and smartphones has become very common. For example, people send out documents through e-mail, make phone calls through wireless devices, share pictures through Facebook, Instagram and Snapchat, and connect with the world through Twitter and LinkedIn. In this environment where user engagement with devices is increasing, businesses are adapting as well. As an example, many firms now sell their products online. Some may accept that these online platforms are secure. Moreover, with technological advancements, many believe that cyber security has strengthened and cyber-attacks have decreased. Unfortunately, cyber-attacks are increasing regardless of all the cyber security programs that have been developed.

The cyberspace has caused unethical practices [16]. Cyber-attack is defined as "the exploitation of cyberspace for the purpose of accessing unauthorised or secure information, spying, disabling of networks and stealing both data and money" [16]. Such attacks have only been increasing over the past few years. There is a lack of knowledge regarding these attacks causing many individuals and organisations to become susceptible to them.

The aim of the research is to perform a study of the cyber-attacks to create an awareness of the various types of cyber incidents so that appropriate defence measures can be initiated by organisations against such attacks.

The research questions in the present study are:

1) What is the percentage of cybercrime incident types?
2) What are the risks of inadequate security in an organisation?
3) How are businesses impacted by cybercrimes in terms of monetary loss and system downtime?

To perform the analysis on these research questions, we use a big data technology such as R in this study. This is further detailed in the methodology section. The analysis and results are presented in the results section. The literature review on cyber security and cybercrimes is described in the background section.

II. Background

The Internet has made communication much easier. The cyber space is an outcome of the Internet which has impacted several industries and services. Examples include banking, hospitals, education, emergency services and the military [12]. Across these industries, there have been several cyber incidents causing data breaches, for example, at Target [8], JP Morgan [1], and Home Depot [13]. The attack at JP Morgan Chase affected nearly 76 million households [1]. Most often, the damage already occurs before a breach is detected. This indicates that if the breaches could have been predicted or detected early, significant damages could have been avoided.

Furthermore, cyber-attacks and cybercrimes are not always done by outsiders, but also by the "insiders". Insiders to the organisation could be employees, contractors, or vendors. When these insiders become responsible for the cybercrimes and cyber-attacks [7], these types of attacks are characterised as an insiders' attack. The "insiders" are a greater threat as they are more familiar with the system. They can attack the system to destroy or steal information. The "insiders" can attack the system more easily than the outsiders. The FBI estimates that 80 % of the cyber security accidents arise from the insiders, and the cost of an inside attack is fifty times higher than that of an external attack [7]. This forces companies to find ways to prevent these types of attacks.

Moreover, the evidence for a cybercrime is difficult to gather and evaluate. Unlike the physical evidence of traditional crimes, the evidence of cybercrimes is digital. This difficulty increases the rate of cyber-attacks globally. Digital evidence is subject to manipulation which makes it difficult for investigators to track the origin of the crimes [3].

Several standards on cyber security information exchange have now been developed. ENISA (European Network and Information Security Agency) supports its member states with the European Information Sharing and Alert System (EISAS) [4]. The White House has outlined a cyber strategy for the United States of America [15].

Despite the importance of security and the development of standards, studies conducted in the years 2009 and 2011 by McAfee, a computer security firm, revealed that companies were investing very little in cyber-defence [14]. Many firms neglect security because they find it very expensive. In particular, McAfee found that companies often had weak authentication requirements [14]. Only few firms have systems that can monitor a network activity. Other studies reveal that some companies’ defence systems are so weak that they do not even know when a cyber-attack occurs [14].

Thus, the need for security is essentially to protect the assets in an organisation from various threats. These assets are related to the safety of either the individual or society at large [15].

At present, there is still a relative lack of understanding about the various types of cybercrimes and attacks. In this paper, we analyse the impact of cybercrimes on organisations. Further, we analyse the different cyber incident types and the areas of inadequate security in organisations.

III. Methodology

The cyber security dataset analysed in this study is an open dataset published by the Bureau of Justice Statistics and the National Cyber Security Division of the U.S. Department of Homeland Security [2].

The dataset contains a survey sample of 35 596 businesses including those with more than 5000 employees and fortune 500 companies. The businesses in the dataset represent several industries such as agriculture, chemical and drug manufacturing, finance, healthcare, telecommunications, transportation, insurance, retail, advertising and others. The dataset includes the risk level of businesses providing their services online, the number of cyber-attacks, the number of cyber-attacks detected, the monetary loss to the organisations due to the cyber-attacks, the system downtime caused due to the cyber-attacks and the patterns of attacks caused by insiders and outsiders.

The dataset studied was first converted to a CSV (comma-separated values) format. The data were then cleaned to remove any missing value, duplicate entries, etc. We used R programming to analyse the cleaned data. R is an open source program for statistical computing that is used for a big data analysis [10]. The Results section discusses the details of our findings from the data.

IV. Results and Analysis

We used R programming for our analysis. By using R programming, one can visualise the data to better understand the big picture of a large dataset [10]. Figure 1.b. and Figure 2.b. show the R code used to generate the visualisations in Figure 1.a. and Figure 2.a.

One of the critical aspects of computer security is determining which networks were accessed in an incident. Most of the businesses detected at least one incident involving a local area network (LAN) as seen in Figure 1.a. The figure also indicates that the majority of the incidents happen in the LAN (Local Area Network) network which is internal to the organisation.

Some researchers make a distinction between cyber theft and cyber-attack. Cybercrimes, such as Internet fraud and intellectual property piracy, are typically classified by most researchers as a cyber theft. A cyber-attack aims to steal or hack the information of an organisation or government office [17]. Some researchers also classify a cyber-attack as an attack made for a political or national security purpose [6].

Figure 2.a. shows the areas of risks or areas of inadequate securities in organisations. The greatest need for change to protect against inadequate security is for authorisation. Another area of inadequate security is “internal control”. Internal control is defined as processes that are designed to provide quality. While even companies with the strongest internal controls are not immune to fraud, strengthening internal control policies, processes and procedures allow companies to be more successful in their fight against cybercrimes.

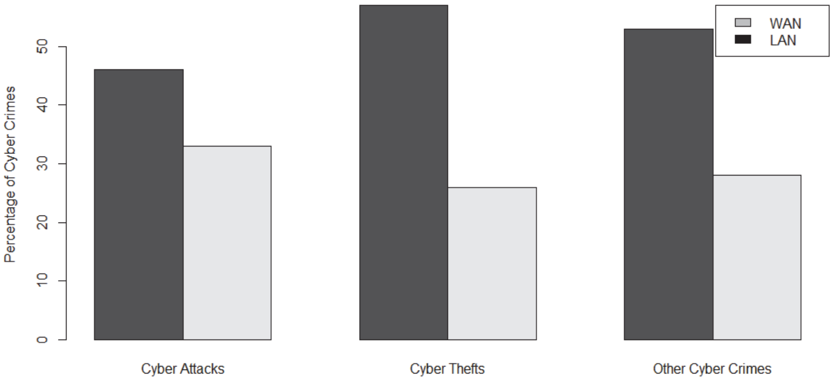

Fig. 1.a. Analysis of cybercrime incident types.

```
barplot(CyberAttacks,beside = TRUE,names.arg = c("Cyber Attacks","Cyber Thefts","Other Cyber Crimes"),ylab = "P
ercentage of Cyber Crimes",legend("topright",legend = c("WAN","LAN"),fill =  c("gray","black")))
```

Fig. 1.b. R code for the corresponding analysis in Fig. 1.a.

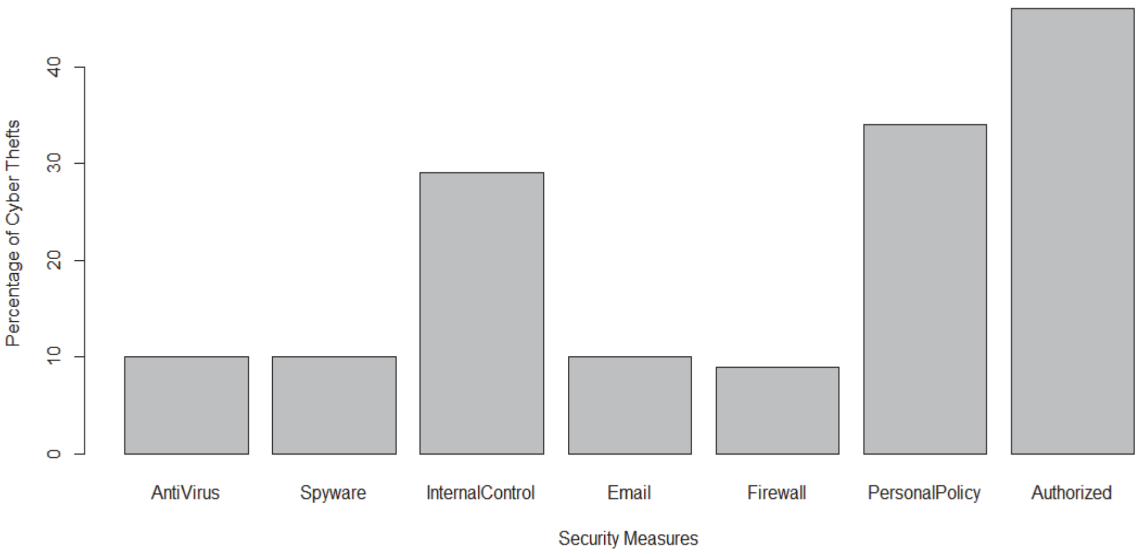

Fig. 2.a. Analysis of incident types in security insufficiencies.

```
barplot(Attack$CyberTheft, horiz = FALSE,names.arg = c("AntiVirus","Spyware","InternalControl", "Email",
"Firewall", "PersonalPolicy", "Authorized"), ylab = "Percentage of Cyber Thefts", xlab = "Security Measures")
```

Fig. 2.b. R code for the corresponding analysis in Fig. 2.a.

V. Discussion

Table I shows some of the businesses impacted by system downtime and monetary loss. Using R programming, we were able to find summary statistics of the impact of the cyber thefts on businesses. We found that an average of 11.7 % of businesses incurred a monetary loss of more than $ 100 000. Table 1 also indicates that businesses faced a downtime of more than 25 hours due to cybercrimes.

Table II indicates the percentage of businesses that incurred some amount of monetary loss due to cybercrimes. Table II shows that 91 % of all businesses incur some kind of monetary loss due to cybercrimes and as seen in Table I, 13 % of all businesses incur monetary loss of $ 100 000 or more.

Organisations should take actions to implement appropriate cyber security measures and practices to help decrease the number of cyber incidents. Encryption and authorisation to log in with password features are a recommended practice [11]. It is also important to regularly update firewalls and anti-virus programs. Any illegal communication via the Internet should be reported [11]. As most of the information today is in digital form, organisations need to make data theft a top security issue.

We computed the summary statistics in Figure 3 using R programming. Figure 3 shows that approximately 21 % of businesses are impacted by cyber thefts.

```
>mean(data_attack$CyberTheft)
[1] 21.14286

>sd(data_attacks$CyberTheft)
[1] 15.08231
```

Fig. 3. Summary statistics in R of cyber thefts to businesses.

TABLE I

Statistics of Businesses Impacted by Cyber Crimes (Source: Bureau of Justice Statistics, 2017)

Critical infrastructure	Percentage of businesses with monetary loss – $100 thou. or more	Percentage of businesses with system downtime of 25 hours or longer
All businesses	13	40
Agriculture	4	46
Chemical and drug manufacturing	18	33
Computer system design	13	41
Finance	29	38
Health care	14	39
Petroleum mining and manufacturing	12	30
Real estate	6	39
Telecommunications	12	47

Transportation/pipelines	11	40
Retail	18	42
Scientific research and development	12	43
Accounting	13	29
Advertising	12	26
Architecture and engineering	11	40
Business and technical schools	5	45
Insurance	20	41
Construction	8	41
Food services	11	33
Forestry, fishing, and hunting	8	50

TABLE II

STATISTICS OF BUSINESSES IMPACTED BY CYBER CRIMES WITH SOME MONETARY LOSS

Critical infrastructure	Percentage of businesses with some monetary loss
All businesses	91
Agriculture	90
Chemical and drug manufacturing	91
Computer system design	98
Finance	93
Health care	91
Petroleum mining and manufacturing	89
Real estate	94
Telecommunications	91
Transportation/pipelines	90
Retail	94
Scientific research and development	93
Accounting	90
Advertising	88
Architecture and engineering	91
Business and technical schools	88
Insurance	96
Construction	92
Food services	87
Forestry, fishing, and hunting	87

VI. CONCLUSION

While the Internet has enabled the world to connect with each other, it can also cause problems to organisations and people. Cybercrime is now widespread and is growing having major impacts on organisations and society as a whole. Billions of dollars are being lost every year due to these attacks. The effects are even more detrimental to small and medium sized businesses, sometimes ending with the company going bankrupt.

As technology advances, cybercrimes have increased in their technical sophistication as well, making cyber security a greater priority for organisations. The cyber-attacks in organisations are becoming more commonplace. The attacks are destructive and more sophisticated making it harder for organisations to try to protect themselves from such attacks. While some companies try to secure their systems against attackers, other companies neglect the importance of cyber security. It is all the more challenging to detect and prevent an attack from an insider of an organisation [3]. Moreover, with the limitations in collecting evidence against cyber-criminals, cybercrimes have increased further.

Firms should develop cyber security measures to protect and defend their systems from attackers. Simple measures such as disconnecting virus infected computers from the Internet to prevent spreading the malware, and backing up data, should be performed by organisations.

While the field of cybercrimes and cyber security is very popular, open data sets are still very limited for an analysis in this field of study. If more data in this field are available, then for future research, the different types of viruses from cybercrimes and their impact on organizations can be explored. The impact of cybercrimes on other industries can be investigated as well. One could also make an analysis of the cybercrimes in different regions.

REFERENCES

[1] T. Agarwal, D. Henry and J. Finkle, "JPMorgan hack exposed data of 83 million, among biggest breaches in history," 2014 [Online]. Available: http://www.reuters.com/article/2014/10/03/usjpmorgan-cybersecurity-idUSKCN0HR23T20141003

[2] Bureau of Justice Statistics, "Data Collection: National Computer Security Survey (NCSS)," [Online]. Available: https://www.bjs.gov/index.cfm?ty=dcdetail&iid=260#BJS_data_experts

[3] D. Chaikin, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence," *Crime, Law and Social Change*, vol. 46, no. 4–5, pp. 239–256, Mar. 2007. https://doi.org/10.1007/s10611-007-9058-4

[4] ENISA, *EISAS (enhanced) report on implementation*, 2011.

[5] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political*," IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, 2011. https://doi.org/10.1109/mts.2011.940293

[6] O. Hathaway and R. Crootof, "The Law of Cyber Attack," *Faculty Scholarship Series*, p. 3852, 2012 [Online]. Available: http://digitalcommons.law.yale.edu/fss_papers/3852

[7] S. Hinde, "Computer Security: Mapping the Future," *Computers and Security*, vol. 22, no. 8, pp. 664–669, 2003.

[8] B. Krebs, “The target breach, by the numbers,” 2014 [Online]. Available: https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[9] N. Kshetri, “Diffusion and Effects of Cyber-Crime in Developing Economies,” *Third World Quarterly*, vol. 31, no. 7, pp. 1057–1079, Oct. 2010. https://doi.org/10.1080/01436597.2010.518752

[10] R Project, “The R Project for Statistical Computing,” [Online]. Available: https://www.r-project.org/

[11] R. Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society,” *International Journal of Scientific & Engineering Research*, vol, 3, no. 6, Jun. 2012 [Online]. Available: https://www.ijser.org/researchpaper/Study-of-Latest-Emerging-Trends-on-Cyber-Security-and-its-challenges-to-Society.pdf

[12] T. Shimeall, *Cyberterrorism*. Software Engineering Institution Carnegie Mellon University Pittsburgh, pp. 1–18, 2002.

[13] R. Sidel, “Home depot’s 56 million card breach bigger than target’s,” 2014 [Online]. Available: https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

[14] N. Sales, “Regulating Cyber-Security,” *Northwestern University Law Review*, vol. 107, no. 4, 2013.

[15] R. von Solms and J. van Niekerk, “From Information Security to Cyber Security,” *Computers & Security*, vol. 38, pp. 97–102, Oct. 2013. https://doi.org/10.1016/j.cose.2013.04.004

[16] M. Uma and G. Padmavathi, “A Survey on Various Cyber Attacks and Their Classification,” *International Journal of Network Security*, vol. 15, no. 1, pp. 390–396, 2013.

[17] J. Vijayan, *Targeted Cyber Attacks Testing IT Managers*, 2010.

Dr. Shilpa Balan is an Assistant Professor at the Department of Information Systems of California State University, Los Angeles. Her research interests include big data, business intelligence and healthcare informatics.
E-mail: sbalan@calstatela.edu

Dr. Joseph Otto is the Chair and Professor at the Department of Information Systems of California State University, Los Angeles. His research interests include information systems and business analytics.
E-mail: jotto@calstatela.edu

Edgar Minasian is a senior undergraduate student at the Department of Information Systems of California State University, Los Angeles. His research interests include business intelligence and data visualisation.
E-mail: eminasi@calstatela.edu

Dr. Arun Aryal is an Assistant Professor at the Department of Information Systems of California State University, Los Angeles. His research interests include the areas of emerging technologies, data analytics, and enterprise systems.
E-mail: aaryal@calstatela.edu