INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 12, Issue 6, (2022) E-ISSN: 2222-6990

Cyber Crime in Business: Review Paper

Ashour A. N. Mostafa

Senior Lecturer at The Higher Institute of Science and Technology – Tobruk, Libya

Email: Ashour.Mostafa@thist.edu.ly

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i6/13865 DOI:10.6007/IJARBSS/v12-i6/13865

Published Date: *07* June 2022

Abstract

The criminals of cyber, nowadays, are exploiting software that aims to damage or disable computer systems, i.e., malware, viruses, bots and other forms of complicated attacks or threats, to breach considerable organizations. Those threats could be for various goals, such as financial revenue, disruption of business, or political trend. The situation used by the cybercriminals is to attack diverse organizations and multiple targets for raising the likelihood ratio of success. It could be spread the viruses and malware programs that designed on daily basis. The influence of cybercrimes in business is shown in this paper by surveying some studies which were conducted in some countries.

Introduction

Organizations strive and struggle to defend own assets and sensitive data by fighting the threats separately, but most of the attacks are unidentified and unrecorded. However, hackers or cybercriminals are often working under the supervision of well-structured organizations with money support. They employ high-skills black hat hackers and supply them the goals and motivations to attack. This essay is going to show the influence of cybercrimes in business by surveying some studies were conducted in some countries like the United States, the United Kingdom, Germany, Hong Kong and Brazil. In turn, the study focuses on addressing the risks that organizations meet by getting the experience of practitioners of IT and business executives. It assists in setting up the precautions for future threats. The findings can be summarized that the cybercrimes risks levels differ among countries, sixty-six attacks and disruption per week are the average that organizations meet, the motivation for a hacker, the cost paid by organizations that caused by cybercrimes is continuous, the effect of mobile on security risks, and last but not least, lack precautions that adopted by countries. In this study, it has been surveyed 2,618 highly experienced business leaders and IT security practitioners located in the United States, United Kingdom, Germany, Hong Kong and Brazil.

Risk management has never been easy. Finding efficient mitigating measures is not always straightforward. Finding measures for cyber crime, however, is a really huge challenge because cyber threats are changing all the time. As the sophistication of these threats is growing, their impact increases. Moreover, society and its economy have become increasingly

dependent on information and communication technologies. Standard risk analysis methodologies will help to score the cyber risk and to place it in the risk tolerance matrix. This will allow business continuity managers to figure out if there is still a gap with the maximum tolerable outage for time-critical business processes and if extra business continuity measures are necessary to fill the gap.

Key Findings of the Impact of Cybercrimes on Business

Five Different types of Cyber Crimes:

There are five main types of cybercrimes that concern the countries conduct the study. It includes denial of service (DoS), botnet, advanced persistent threats (APTs), social engineering, and malicious programs i.e., viruses, worms and Trojans (Ponemon, 2012).

The mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

Denial of Service (DoS)

This kind of attack is more effective than other attacks because it differs in the forms and goals of the attack that target the computers and networks. Cybercriminals and attackers often aim to breach the information systems intentionally. Their goals might be to extract the critical information, steal credit cards, modify sensitive data, or making fraud operations to exploit services are not allowed to be used. All of those operations involve in one goal that is disruption the victim (Shui, 2013).

The process of denial of service is conducted through the malicious control of the targeted system and deny offering services to legitimate users. It is not to steal sensitive data, or steal numbers of credit cards, or damage the machine of the victim. It is just stop available services from the victim to the normal client within the organization. It is implemented via occupying the victim in the attack traffic, hence the large numbers of clients are compromised by the attacker itself. He uses them as attackers in unauthorized access (Mirkovic et al., 2004; Tan et al., 2014).

Such damages of DoS attacks can be outlined as follows:

- Sites that have online orders can be accessed in unauthorized way through the services offered to their clients to gain money.
- Majority of websites offer services for marketers to show its advertisements on websites to the public. The attack aims to loss the revenue that websites profit from the marketers.
- Create fake webpages and exploiting users who have lack knowledge on cyber security.

Botnet

Botnet simply can be defined as utilizing a malicious program to attack private computers or a network to be controlled as a group without the user to realize, such as sending a spam. In other meaning, the difference between the hacker and the client in a botnet is the ability of client in a botnet to take actions without allowing the hacker to log into the client's operating system. In addition, the clients in a botnet include any client with its machine execute a specific goal with others in a coordinated role. Those clients are considered in a botnet because of no interference from the hacker (Schiller & Binkley, 2014).

Advanced Persistent Threats (APTs)

It is a threat relating to the attacks on networks to facilitate the intruder to access to the network and stay for long time or period without ability of detection. The aim of this process is to steal sensitive data and not to damage the system physically. Those attacks usually occur on the ministries of defense and the sectors related to manufacturing and financial. The mechanism of detection through the intrusion detection system (IDS) cannot detect the intruder due the rapid access to the network or the system and getting out. It aims the availability to access a long period of time, not to be discovered. Some techniques used in this mechanism that the intruder writes codes to gain access to the system such as the social engineering, spear fishing and create a back door (Chen et al., 2014).

Social Engineering

From the term "social", social engineering can be defined as some of the users who have bad intentions chat with legitimate users to get information of a system to able to access the targeted system without any notice of legitimate users. Therefore, most of the researchers and security practitioners realized that the vulnerabilities of the systems can be come from the same users who are working in that organization. Some of the attacks can be occurred by phone. A hacker who pretends an officer working in an authority and tells the victim to pull out the information easily, e.g. password of the system and a credit card number (Krombholz et al., 2015).

Malicious Programs

This terminology has become known to the public in which these programs are deployed and inserted into the system to harm it. Two types of malicious programs which needs a host, and the other executed independently such as viruses, logic bombs and backdoors. The other type can be scheduled and run by the OS, for instance, worms and zombies (Stallings, 2014).

In simple definition of some examples of malicious program, it can be summarized as follows (Stallings, 2014):

- Virus: it is a program that can infect the programs through modifying the good programs for creating copies of the virus and continuing the infection into the system.
- Worm: it is a program that able to create replicas in any media and transfer the copies over the network.
- Backdoor: in other term called "trapdoor". It is a point in the program the intruder can exploit it to gain access to the system. Programmers usually use the trapdoors to test and debug the programs that often have authentication procedures.
- Logic bomb: it is one of the oldest types of threats. It depends on inserting a code into the programs to trigger the actions when a particular condition occurs.
- Trojan horses: it is the most useful viruses for cybercriminals. It has embedded code that called/invoked to accomplish particular functions. One of the objectives of deployment is the data destruction.
- Zombie is used in denial of services attacks because it takes over the computers connected to Internet to start the attacks.

Figure.1 explains the ranking of the five types of cyber security in each country, in which ***"5"*** refers to the highest level of the risk.

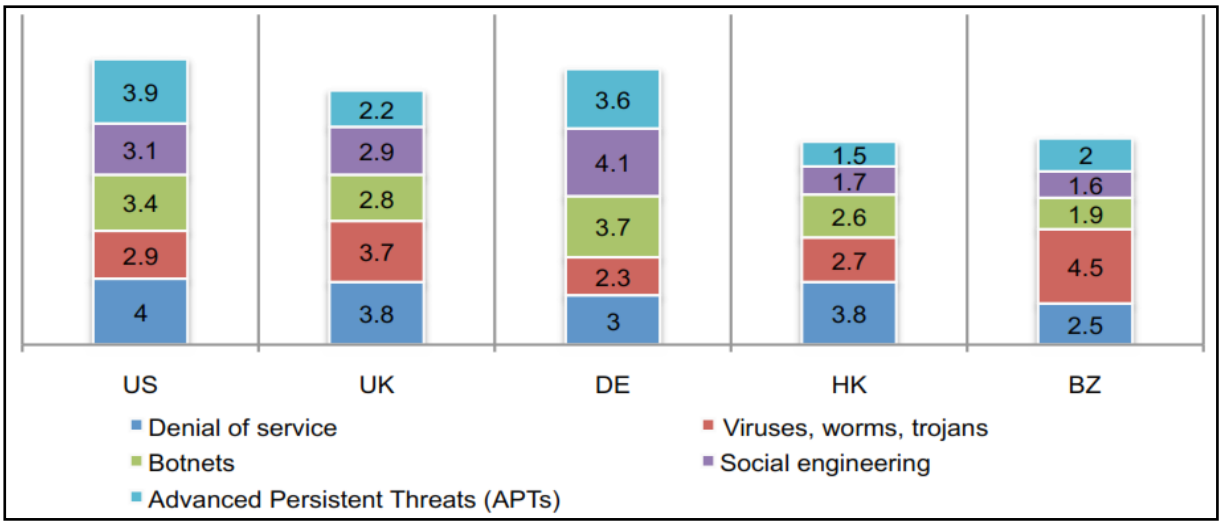

Fig. 1: Cyber Security Rank

As illustrated in the figure, the respondents who are IT practitioners and organizations senior executives in each country stated the USA the most risk comes from the denial of service, and the United Kingdom is the same to the USA. The social engineering in Germany (DE "Deutschland") is the most critical one. In Brazil, the viruses and various malicious programs are the highest risk (Ponemon, 2012). In this study, it has been surveyed 2,618 highly experienced business leaders and IT security practitioners located in the United States, United Kingdom, Germany, Hong Kong and Brazil. The present survey questions were part of a larger omnibus survey instrument (a.k.a. Meta survey) fielded on a quarterly cycle in all five countries.

Figure.2 shows the countries' concerns of the cybercrimes risks and how much they implement precautions of security.

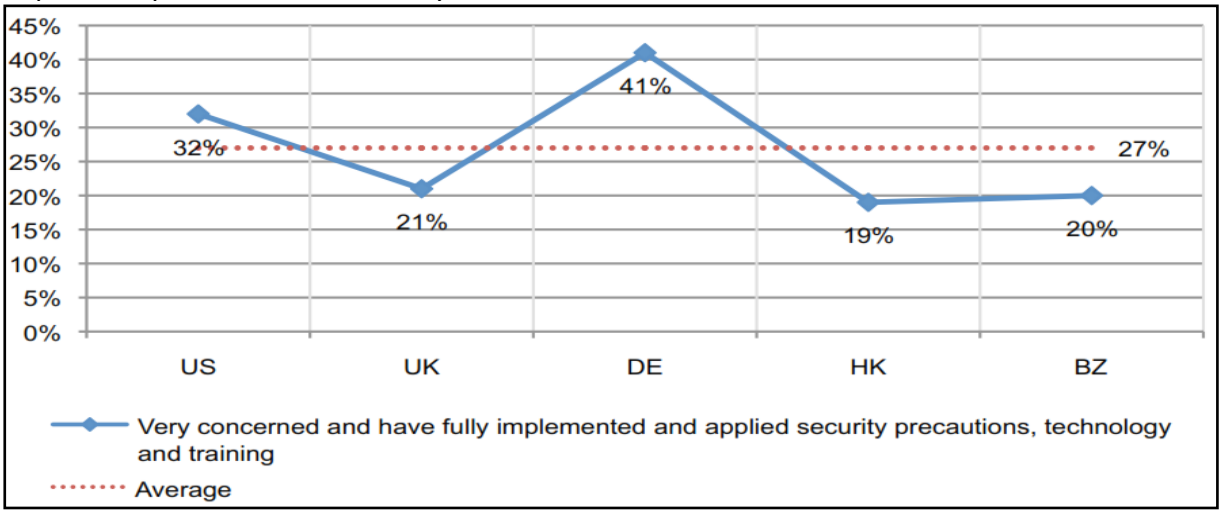

Fig. 2: Countries' Concerns of Cyber Security (Ponemon, 2012)

As illustrated in the chart, the dotted line in red color clarifies the average of countries concerns of the risks. Two countries implement precautions of the security such as the adopted security technologies, and training the individuals and organizations related to the field are USA and Germany.

In the United Kingdom, the majority of the practitioners stated that the country is concerned of the security risks, and they increased the precautions implementations, technology adoption and staff training. In addition, they implemented the security measures that assist in protection against the threats like utilizing the firewalls and anti-bot technologies.

In contrast, Brazil and Hong Kong mentioned that the firewalls are the most technology implemented for protection as a security measure, and utilizing the intrusion detection system.

The following table (Table. 1) shows the most security measures that adopted and implemented by the five countries, added to the percentage of level of usage to fight the attacks.

Table 1
Security Measures Adopted in the Countries

Security Measures	US	UK	DE	HK	BZ
Firewall	98%	90%	97%	92%	89%
Additional manual procedures and controls	97%	95%	94%	84%	82%
Anti-malware	93%	89%	96%	91%	82%
Intrusion prevention systems	86%	74%	88%	84%	70%
Strengthening of perimeter controls	87%	86%	79%	59%	32%
Web protection such as URL Filtering	74%	66%	75%	61%	50%
Training and awareness programs	81%	76%	80%	44%	41%
Application control	61%	47%	83%	62%	37%
Endpoint security	57%	49%	68%	59%	49%
Encryption technology	60%	51%	79%	41%	45%
Identity and access management	60%	51%	78%	52%	34%
Anti-bot technology	56%	44%	59%	45%	40%
Security intelligence systems	53%	42%	72%	33%	38%
Security certifications or audit	23%	39%	51%	25%	29%
Data loss prevention	40%	29%	44%	21%	24%
Other	3%	2%	0%	2%	1%
Average	64%	58%	71%	53%	47%

It is noticed that Germany is the highest rank in adopting different security measures to prevent the attacks followed by the United States.

Frequency of Attacks

According to Ponemon institute that reported the study in 2016, they pointed out the most types of attacks or infections for precede two years. Every day the organizations in those countries meet the challenges of cyber-attacks (Ponemon, 2012).

As illustrated in the chart, the United States has 54% of SQL injection attacks while 47% for advanced persistent threats and 11% for denial of services. Unlike Brazil that has lowest percentage of SQL injection attacks among the five countries, but it has an increment in the denial of service attacks higher than the United States. This denotes to the policies that followed in these countries for the security measures. It also the attacks differ from a country to another according to the nature of the organizations and firms followed by the security

measures adopted, for instance, USA and UK has similar percentage of SQL Injection attacks and both are higher among the others (Shar & Tan, 2013).

SQL injection is one of the vulnerabilities exploited and utilized in web 2.0 area. Web 2.0 refers to the web applications. Intruders and cyber criminals are using SQL injection to steal the sensitive data from online websites for organizations. The weakness in the web application occur when the application misses the validation of input of the users. Therefore, the hacker insert statement s into the databases driven web applications to be run (Shar & Tan, 2013).
The database driven web apps is used in the websites related to the e-commerce. Such websites need to sell products online and promote services as well. Therefore, there are some technologies and tools used to scanning the vulnerabilities of the web applications and protect its databases.

Loss of Information and Sensitive Data
Loss of critical information is one of the critical challenges that organization face it. The organizations and firms that are attacked then losses sensitive information would impact on the productivity that probably declined. Then it causes the so-called the business disruption as illustrated in Figure.3.

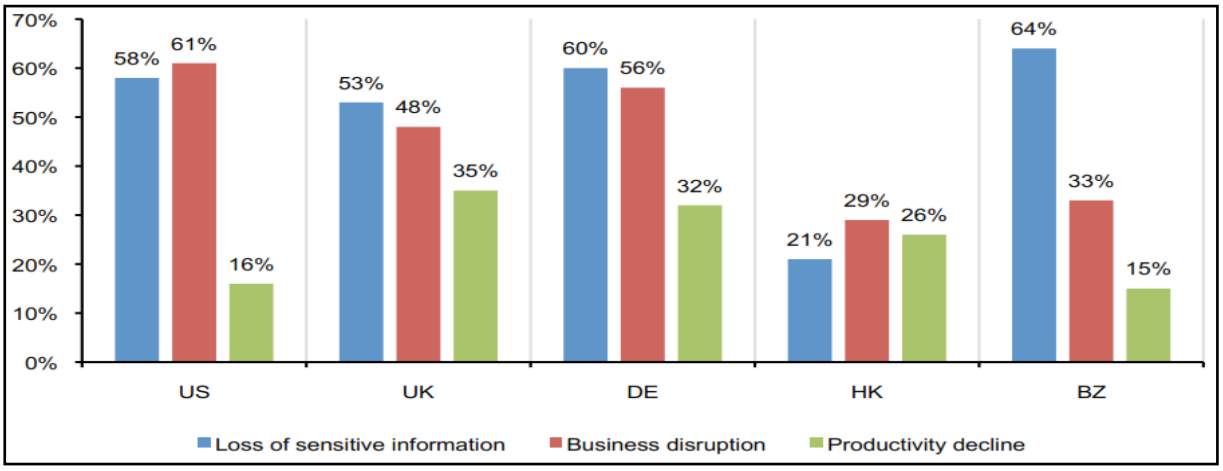

Fig. 3: Major Cyber Attack Percentage (Shar & Tan, 2013).

As illustrated in the chart, loss of information has highest percentage among others because of the adopting of security measures. In Germany and the United States are quite similar to Brazil because they attacked more than others. In turn, the productivity decline has minor impact each. The mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. As a member of the Council of American Survey Research Organizations (CASRO), they uphold strict data confidentiality, privacy and ethical research standards. They do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Mobile Devices usage in the Workplace

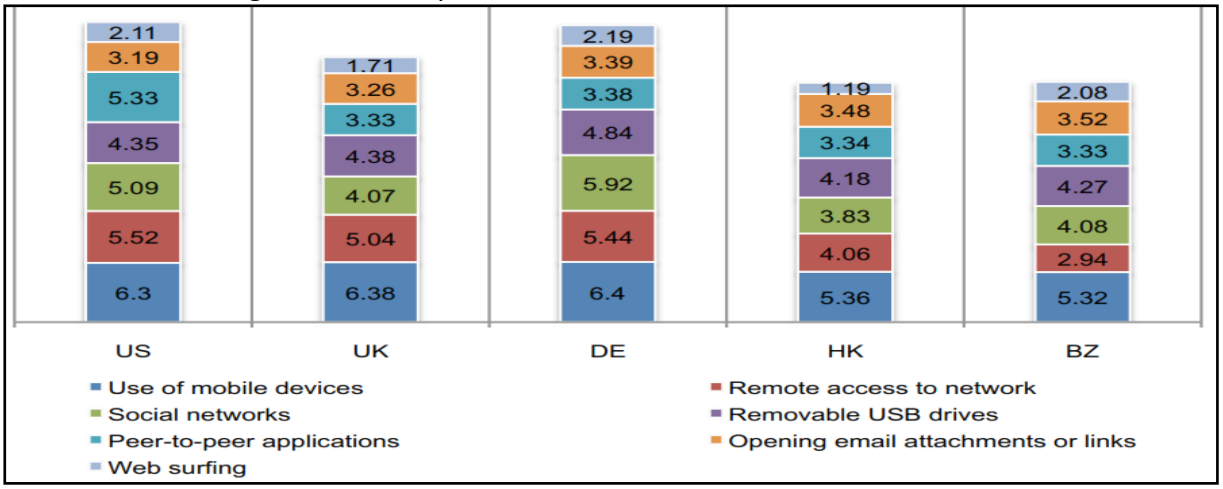

Fig. 4: Mobile Device and Threats in the Workplace (Shar & Tan, 2013).

According to the information technology and business leaders that the study conducted on them, they stated that the use of mobile phones in the workplace is a critical issue that make a concern for the organization in all countries. The benefits of mobile device divers from web surfing to reading email, and from downloading the mail attachments to use the social networking apps. The issue relates to the lack of security for mobile as well as using the removable devices in the workplace. This chart ranked from "1" that is the lowest risk to number "7" that is the highest risk as illustrated in Fig. 4 (Shar & Tan, 2013).

Financial Fraud

This Fig. 5 is describing the motivation for the cyber criminals to commit the financial fraud. The highest percentage in all countries relates to the financial fraud, followed by the disruption of operations, then theft of customer's data.

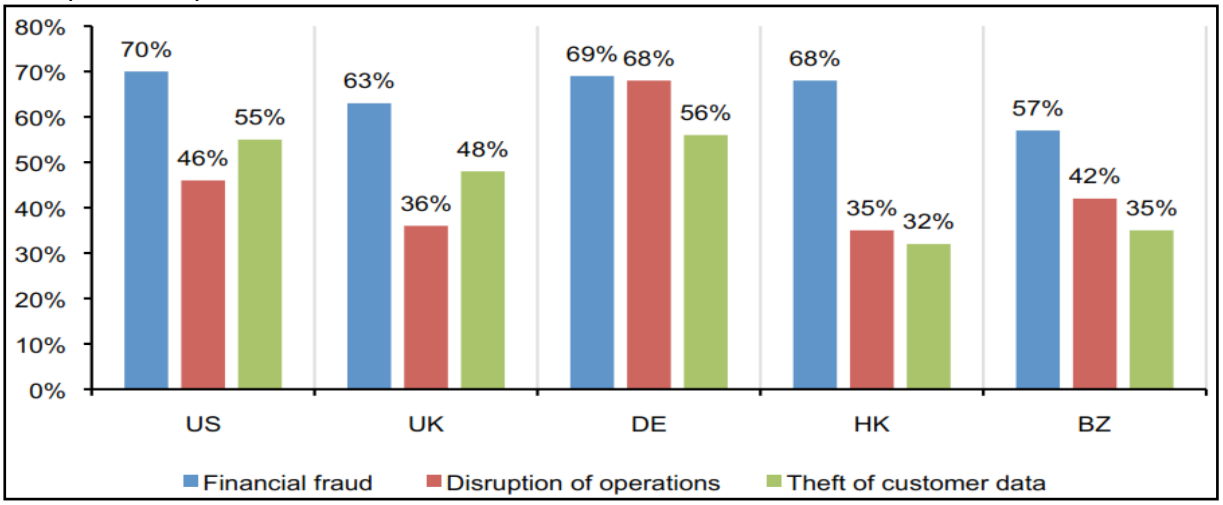

Fig. 5: impact of Attacks on the Organizations

The Average Cost of Cyber Attacks

According to the Table. 2 above with the Table. 1 in the previous section, Germany has the highest cost estimation due to the cyber-attacks unlike Brazil that is the lowest ones. This results in Table. 1 and Table. 2 are because of the highest implementation and adopting of the security measures, technologies and training comparing to Brazil.

Table 2
Average Cost of Cyber Attacks

Dollar range	US	UK	DE	HK	BZ
< 10,000	2%	5%	2%	15%	10%
10,000 to 50,000	9%	18%	9%	21%	19%
50,001 to 100,000	10%	27%	12%	28%	26%
100,001 to 200,000	13%	31%	33%	15%	15%
200,001 to 300,000	30%	9%	27%	8%	9%
300,001 to 400,000	22%	5%	5%	9%	5%
400,001 to 500,000	7%	3%	8%	3%	8%
500,001 to 1,000,000	4%	1%	3%	1%	5%
> 1,000,000	3%	1%	2%	0%	3%
Total	100%	100%	100%	100%	100%
Extrapolated value	$276,671	$229,560	$298,359	$159,244	$106,904

Figure.6 shows the chart of the distribution for the industrial sectors that conducted the study on their individuals in their organizations (Shar & Tan, 2013).

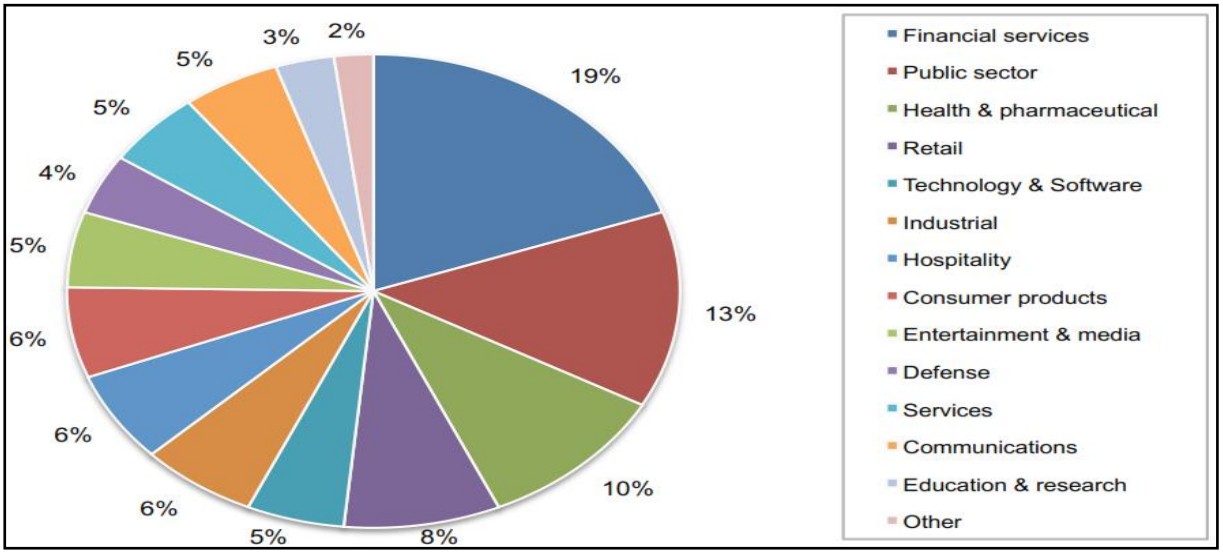

Fig. 6: The Study conducted of the Industrial Sectors (Shar & Tan, 2013)

In addition, 47% of the samples/participants are working in organizations that have more than 1000 employees. Also, 63% of the reports surveyed from IT Technicians and leaders rather than chief risk officer and others because they are more connected to the IT field.

Conclusion

As conclusion of the study, the participants have focused on the common types of the security risks represented in the five attacks: denial of service (DoS), botnet, advanced persistent threats (APTs), social engineering and malware programs such as viruses and worms. Those five has been surveyed according to the experts and practitioners of the information technology and business leaders as well. It was to address the impact of cybercrimes on business, the motivations for cybercrimes to commit such threats, the highest cost of implementing the security measures for protection, and the level of risks that major organizations within countries face it. The survey was addressed in five countries as the United States, the United Kingdom, Germany, Hong Kong, and Brazil.

The risks levels differ among the five countries in which the denial of services (DoS) is the most critical threat that US and UK meet. In turn, Brazil has threats represented in malware programs such as Trojan horses, viruses and worms. Last, Germany struggles from the social engineering. Organizations in these countries face SQL injection as the most attack followed by advanced persistent threats. These cybercrimes affect the organizations in loss of sensitive data, reduction in productivity and hence the business disruption. Losses represented in the intellectual property and the secrecy of trades transactions. The motivation for cybercrimes to commit such these crimes can be either political or ideological. Most of the cybercriminals are doing the job for financial purposes as fraud or steal sensitive data. Such these crimes conducted either destruction purposes or for competing. The cost resulted because of the attacks found out the United States, Germany and UK have the highest cost of prevention of such threats either applying security measures or due to the losses resulted by the attacks. Use the mobile devices in the workplace are considered as the most concerns that face the business administrators from their employees. In addition, the social media and removable USB devices in the workplace are critical threats, too.

References

Ali, L. (2019). *Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC)*. The Journal of Developing Areas, 53(1).

Bressler, M. S. (2009). *The impact of crime on business: A model for prevention, detection & remedy*. Journal of management and Marketing Research, 2(1), 12-20.

Burrows, J., & Hopkins, M. (2005) *Business and crime* in Tilley, N. (2005) (Ed.) *Handbook of crime prevention and community safety*. Devon, Willan Publishing.

Caravelli, J., & Jones, N. (2019). *Cyber Security: Threats and Responses for Government and Business*. ABC-CLIO.

Chen, P., Desmet, L., & Huygens, C. (2014). *A study on advanced persistent threats*. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer Berlin Heidelberg.

Chowdhry, D. G., Verma, R., & Mathur, M. (Eds.). (2020). *The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security*. CRC Press.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). *Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts*. Computers in Industry, 114, 103165.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). *Cybercrime Business Digital in Indonesia*. In E3S Web of Conferences (Vol. 125, p. 21001). EDP Sciences.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). *Advanced social engineering attacks*. *Journal of Information Security and applications*, *22*, 113-122.

Levi, M., Morgan, J., & Burrows, J. (2003). Enhancing Business Crime Reduction: UK Directors' Responsibilities to Review the Impact of Crime on Business. Security Journal, 16(4), 7-27.

Levisohn, B. (2009). Experts Say Fraud Likely to Rise. Business Week Online [serial online].

January 12, 2009: 14-14. Available from: Business Source Complete, Ipswich, MA. Accessed February 18.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

Mirkovic, J., Dietrich, S., Dittrich, D., & Reiher, P. (2004). "Internet Denial of Service Attack and Defense Mechanisms". Pearson Education: The Radia Pertman Series in Computer

Networking and Security. Retrieved from January 13, 2017, *https://books.google.com/books?isbn=0132704544.*

Ndeda, L. A., & Odoyo, C. O. (2019). CYBER THREATS AND CYBER SECURITY IN THE KENYAN BUSINESS CONTEXT. GSJ, 7(9).

Nwekpa, K. C., Ezezue, B. O., & Ibeme, C. C. N. P. N. Effect of Cybercrime on Performance of e-business in konga. com.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

Ponemon Institute. (2012). *The Impact of Cybercrime on Business. Studies of IT Practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil.* Retrieved January 7, 2017, from *https://www.ponemon.org/local/.../Impact_of_Cybercrime_on_Business_FINAL.pdf*

Renu, P. (2019). Impact of Cyber Crime: Issues and Challenges.

Sakban, A., Kasmawati, A., & Tahir, H. (2020). The role of Indonesian National Cyber Bureau in monitoring mining business companies. In IOP Conference Series: Earth and Environmental Science (Vol. 413, No. 1, p. 012032). IOP Publishing.

Schiller, C., & Binkley, J. R. (2011). *Botnets: The killer web applications*. Syngress.

Shar, L. K., & Tan, H. B. K. (2013). Defeating SQL injection. *Computer*, *46*(3), 69-77.

Shui, Y. (2013). "Distributed Denial of Service Attack and Defense." Chapter 1, p. 1-5. Springer Brief in Computer Science. Springer.com: Google Books Online. Retrieved from January 10, 2017, *https://books.google.com.tr/books?isbn=1461494915.*

Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. The transnational dimension of cyber crime and terrorism, 1-34.

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. Pearson Higher Ed.

Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2014). A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE transactions on parallel and distributed systems*, *25*(2), 447-456.

Putte, V. D., & Verhelst, M. (2014). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers?. Journal of business continuity & emergency planning, 7(2), 126-137.