Impacts of Financial Cybercrime on Institutions and Companies

آثار الجرائم الإلكترونية المالية على المؤسسات والشركات

BY

Dr. Dina Taman

PhD in Political Science - Faculty of Economics and Political Science - Cairo University

Doi: 10.21608/ajahs.2024.341707

استلام البحث ١١/ ١٢/ ٢٠٢٣

قبول البحث ٢٠٢٣/ ١٢ /٢٨

Taman, Dina (2024). Impacts of Financial Cybercrime on Institutions and Companies. ***The Arab Journal of Literature and Human Studies***, The Arab Institute for Education, Science and Letters, Egypt,8(30), 477-488.

http://ajahs.journals.ekb.eg

Impacts of Financial Cybercrime on Institutions and Companies

Abstract:

Since the invention of the Internet, the face of the world has changed beyond imagination. It represents a revolution in the field of communication between humans, and the transfer of all information and services we might need. Despite all the positive impacts of the Internet in our lives, there are negative impacts that emerged as a result of the digital transformation, especially during the period of Covid 19 , in which people's dependence on working through the Internet increased as a result of the preventive measures taken to confront the deadly virus. We find that the world incurred huge losses in 2021, approximately 6 trillion dollars today as a result of cybercrime, after it was 3 trillion dollars in 2015. Which is equivalent to the third largest economy in the world after the United States and China. It is worth noting that the cost of global cybercrime is expected to increase by 15% annually over the next five years, to reach $10.5 trillion annually by 2025. It is expected that these losses will be borne by companies and institutions, whether large or small, due to the changing patterns of cybercrime as they target more companies and organizations instead of focusing on individuals since 2020. Therefore, this research paper discusses the main question "what are the impacts of cybercrime on companies and institutions? "Firstly, by studying the cybercrime and its different forms and challenges. Secondly, the ability to implement cyber security in companies and institutions in the light of international experiences.

Keywords: Cybercrime – cyber security – financial crimes – digital Transformation.

المستخلص:

تغير وجه العالم بشكل يفوق الخيال منذ اختراع الانترنت. فلقد كان بمثابة ثورة في مجال الاتصالات بين البشر، ونقل المعلومات والخدمات. وعلى الرغم من كل الاثار الايجابية التي شكلها ظهور الانترنت فى حياتنا الا ان هناك اثار سلبية ظهرت نتيجة التحول الرقمي وخاصة في اثناء فترة كورونا والتي زاد فيها اعتماد الناس على العمل من خلال الانترنت كنتيجة للإجراءات الوقائية المتخذة لمواجهة الفيروس الفتاك. فنجد أن العالم تكبد خسائر طائلة في ٢٠٢١ تقارب اليوم ٦ تريليونات دولار جراء الجرائم الالكترونية، بعد ان كان ٣ ترليون دولار فى ٢٠١٥. وهو ما يعادل ثالث أكبر اقتصاد في العالم بعد الولايات المتحدة والصين. وجدير بالذكر انه من المتوقع أن تزداد تكلفة الجرائم الإلكترونية العالمية بنسبة ١٥% سنوياً خلال السنوات الخمس المقبلة، لتصل إلى ١٠.٥ تريليونات دولار سنوياً بحلول عام ٢٠٢٥. وجدير بالذكر انه من المتوقع أن تزداد تكلفة الجرائم الإلكترونية العالمية بنسبة ١٥% سنوياً خلال السنوات الخمس المقبلة، لتصل إلى ١٠.٥ تريليونات دولار سنوياً بحلول عام ٢٠٢٥. ومن المتوقع ان تتحمل هذه الخسائر الشركات والمؤسسات سواء الكبيرة او الصغيرة نظرا لتغير أنماط الجريمة الإلكترونية حيث صارت تستهدف بشكل أكبر الشركات والمؤسسات بدلا من التركيز على الأفراد منذ عام ٢٠٢٠. ومن ثم تأتى اهمية هذه الورقة البحثية لمناقشة اثر الجريمة الإلكترونية على الشركات و المؤسسات؟ وذلك عن طريق التعرف على الجريمة الالكترونية و اشكالها وانماطها المختلفة. ثانيا كيفية تحقيق الامن السيبراني في الشركات و المؤسسات فى ضوء التجارب الدولية.

الكلمات الدالة: الجرائم الإلكترونية - الأمن السيبراني - الجرائم المالية - التحول الرقمي.

Introduction

The Internet has changed the world beyond imagination. It represents a revolution in the field of communication between humans, and the transfer of all information and services we might need. Despite all the positive impacts of the Internet in our lives, there are negative impacts that emerged as a result of the digital transformation, especially during the period of Covid 19 , in which people’s dependence on working through the Internet increased as a result of the preventive measures taken to confront the deadly virus. In 2021, the world lost approximately 6 trillion dollars as a result of cybercrime, after it was 3 trillion dollars in 2015. Which is equivalent to the third largest economy in the world after the United States and China.

The cost of global cybercrime is expected to increase 15% annually over the next five years, to reach $10.5 trillion annually by 2025. It is expected that these losses will be borne by companies and institutions, whether large or small, due to the changing patterns of cybercrime as they target more companies and organizations instead of focusing on individuals since 2020. Therefore, this research paper discusses the main question "what are the impacts of cybercrime on companies and institutions?"
Firstly, by studying the cybercrime and its different forms and challenges. Secondly, by discussing the ability to implement cyber security in companies and institutions in the light of international experiences.

I. Definitions & Types of Cybercrime

1.1. Definitions

The term of cybercrimes is vague (ZAVRŠNIK) that's why there is no single and determined definition to describe the cybercrimes. This paper presented some definitions of some experts and other definitions of international organizations. First of all, the definitions of experts such as the definition of Debarati Halder and Jaishankar who defined cybercrimes as being
"Offences that are committed against individuals or groups of individuals with
a criminal motive to intentionally harm the reputation of the victim or cause
physical or mental harm, or loss, to the victim directly or indirectly, using
modern telecommunication networks such as Internet (Chat rooms, emails,

notice boards and groups) and mobile phones" (SMS/MMS)
in addition, the definition of S.T. Viswanathan who classified the definitions of cybercrimes in three categories: (Viswanathan, 2001)
Firstly, any illegal action in which a computer is the tool or object of
the crime i.e., any crime, the means or purpose of which is to influence the
function of a computer. Secondly, any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain. Thirdly, computer abuse is considered as any illegal, unethical, or unauthorized behaviour relating to the automatic processing and transmission of data.

On the other hand, there are other types of definitions, which are the international organizations definitions such as The 10th UN Congress on the Prevention of Crime and the Treatment of Offenders,2000, presented two definitions: Cybercrime in a narrow sense (computer crime)covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. (Rajput, 2020)

1.2 Categories of Cybercrimes

There are 3 categories of cybercrimes: crimes against individuals, crimes against property and crimes against governments.

1.3 Types of Cybercrimes

Most of electronic financial crimes focus on gaining profits by obtaining or stealing data, then selling it or using it to illegally gain control of funds, accounts, or assets. Although it is difficult to identify a specific list of cybercrimes due to the continuous development in technology and tactics, we will list some common types of cybercrimes including:

1. cyber fraud - including phishing, spear phishing, vishing, and whaling.
2. DDoS Attacks: distributed denial-of-service attacks
3. Botnets
4. Malware attacks: including viruses, worms, trojans, spyware, rootkits, etc.
5. ransomware attacks
6. Identity Theft
7. drive-by downloads
8. Cyberstalking
9. Hacking
10. Password decryption
11. Online Scams

II. Cybercrimes affected the largest economics in the world:

According to the US government 3 thousand companies were hacked in 2013. In one of the most dangerous bank robberies ever, a global cybercrime gang managed to steal $45 million from two Gulf banks by hacking credit card processing companies and withdrawing money from ATMs in 27 countries (Reuters, 2013). According to Indian government officials, cybercrime caused a loss of Rs 1.25 crore in 2019 to the Indian economy. It is expected that cyber threats will continue to increase, especially as the country begins developing smart cities and deploying the 5G network, in addition to a number of other initiatives (PTI, 2020).A British company reported that it lost $1.3 billion from a single attack. Brazilian banks say their customers lose millions annually to cyberfraud (CenterforStrategicandInternationalstudies, 2014).

III. Cyber Security in companies and institutions.

There are some measures that businesses should take to reduce the risk of cyber-attacks.

3.1 Measures taken by Companies:

Nowadays, security is considered as the key to any company. The Internet and new technologies, in general, created a complex environment which is detrimental to the protection of the information we store. For this reason, in this part some guidelines will be mentioned to avoid companies to become victims of cybercrime. These points should be entered into the company protocols and the employees should be urged to comply with them to protect data and information from being lost. These points are: (Kernellegal, 2022)

1. Maintaining: all the devices and all software used in the company should be kept up to date in the first step to work in a safe environment, in which our data is not in danger. Cybercriminals find systems with outdated software a weak point through which they create an entry route.
2. Data back-up: using several back-up methods to guarantee the data safety, including daily, weekly, quarterly, and annually server back-ups.
3. Securing network and data: Operating systems and security software should be updated automatically without disregarding to fix security flaws.
4. Avoiding unknown programs. Ads that warn about the risks that threaten our computer or those that urge us to update certain software are themselves the gateways for malware to

our computers. The employees should avoid downloading them.

5. Avoiding strange Wi-Fi networks: the employees should avoid strange Wi-Fi networks, which expose the equipment and make it easier for cybercriminals to work.
6. Activating data encryption: which means to convert data into a secret code before it is sent over the internet, by turning on network and data encryption when storing and sharing data.
7. Using multi-factor authentication: users should provide two or more proofs of their identities to access their accounts, to provide different layer of security.
8. Using passphrases stronger than passwords: a weak password is still the main gateway for cybercriminals. Therefore, passphrases are highly recommended instead of passwords, particularly for the important accounts that hold important business information and data.
9. Comprehensive monitoring system: all the equipment and software should be recorded. Also, all important information should be removed from any device and software that is no longer in use and disconnect these devices from its network.
10. Implementing security policies: companies and enterprises should have clear cybersecurity policies to inform their employees about the acceptable steps when sharing data, using computers and other devices, and accessing internet sites.
11. Cybersecurity training: one of most important step that should be taken into account to protect customers data is to train the employees on how to identify, avoid, and deal with a cyber threat.
12. Confirming customer protection: all companies and enterprises should work on keeping the private information of their customers safe. In addition, they should provide a

secure online environment in which different transactions can take place.

10. Providing cyber insurance: A cyber insurance policy should cover the financial losses resulting from a cyberattack, especially for individuals or groups that may have been harmed because of a business's action or inaction

3.2 Measures taken by Governments:

The developing countries should exert more efforts to protect their people against cybercrimes and to meet international standards for the security of computerized information by:

1. Enacting laws that criminalize the cyber-attacks. Here we will review the case in Egypt as an example to the measures that should be taken to protect the institutions and individuals from cyber-attacks:

The Egyptian government has taken serious steps towards developing the cyber security in Egypt and developing the information security industry, whether software and hardware with Egyptian expertise and international specifications. In addition, the government is keen to prepare distinguished human cadres in this field and to support projects and companies specialized in this field to fight cybercrimes. Therefore, the government has adopted several strategies, including a strategy to develop the appropriate legislative framework for cyber security, a strategy to develop an integrated system to protect cyber security, a strategy to protect the digital citizenship program, a strategy to support scientific research and development and develop the cyber security industry, a strategy for community awareness and preparation of human cadres and expertise (Vapadmin, 2019). Since banks represent the backbone of the movement of funds electronically, it has become necessary to upgrade the insurance system for everything that is a financial information infrastructure. For this reason, in 2022 the Central

Bank of Egypt announced the establishment of the first integrated information security centre, which helps to predict cyber-attacks before they occur and warn banks of them. In addition to a series of legislations issued in recent years that strengthen and control the digital financial system in Egypt such as: the Law on Combating Information Technology Crimes. the Personal Data Protection Law, as well as a new law that was issued for the Central Bank and the banking system, in which we find for the first time a complete chapter on regulating payment methods and financial technology. Moreover, the House of Representatives finally approved a law regulating and developing the use of financial technology in non-banking financial activities, which was submitted by the Financial Supervisory Authority (Ahmed ElBatran ; Fatma Eman, 2022).

2. Setting risk management policies, and ICT security regulations.
3. Expanding training to employees to be able for establishing and maintaining effective security programs.
4. Supporting technical and political cooperation between developed and developing countries for provide better defences against cybercrimes all over the world.

Conclusion

The Internet has become the backbone of work in the twenty-first century, but the risks faced by companies and institutions have increased to protect the data and information of their customers from electronic crimes. Therefore, the world began to give more attention to the means of data protection in companies through measures taken by companies and measures taken by governments to protect the cyber security of working through the Internet. In the end, it is a joint work between the state and the private sector and between the developing and developed countries of the world to achieve more international progress in the field of electronic work.

References:

Ahmed ElBatran ; Fatma Eman. (2022). Bankers: The Cyber Security Center is a necessary step to upgrade the financial information infrastructure system. *El Maal*.

CenterforStrategicandInternationalstudies. (2014). *Net Losses:Estimating the Global Cost of Cybercrime Economic impact of cybercrime II.* intel Security.

Kernellegal. (2022, February 20). *5 consejos para proteger a tu empresa de ciberdelitos*. Retrieved from Kernel Legal: https://www.kernellegal.com/5-consejos-proteger-empresa-ciberdelitos/

PTI. (2020). Cyber crimes in India caused Rs 1.25 lakh cr loss last year: Official. *The Economic Times*.

Rajput, B. (2020). *Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation.* Springer Nature Switherland AG2020.

Reuters. (2013). Oman, UAE banks fall victim to global cyber crime ring. *Arabian Business*.

SMS/MMS. (n.d.). Retrieved from 6 http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

Vapadmin. (2019, August 8). *Cyber Security in Egypt*. Retrieved from Vapulus https://www.vapulus.com/ar/%D8%A7%D9%84%D8%A7%D9%85%D9%86D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%81%D9%8A-%D9%85%D8%B5%D8%B1/

Viswanathan, S. (2001). *The Indian Cyber Laws with Cyber Glossary.*

ZAVRŠNIK, A. (n.d.). Cybercrime Definitional Challenges and Criminological Particularities. *Masaryk University Journal of Law and Technology*.