YEARBOOK OF UNWE (2021), PUBLISHING HOUSE – UNWE
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2021.2.08

ABOUT THE CHALLENGES OF CYBERCRIME IN THE DIGITAL AGE

Diyana Bankova[1]
e-mail: diyanabankova@gmail.com

Abstract

With the COVID-19[2] pandemic and The Fourth Industrial Revolution: Digital Transformation, society is facing a global problem – cybercrime. Every single day, the management of different companies experiences more difficulties in ensuring prevention from hacker attacks. Prevention from cyberattacks is becoming an international problem for businesses, causing significant financial losses. For the aim of the article, some sectors were analyzed – the insurance and banking industry which face the challenge of "cybercrime" because their activities are almost completely digitalized. It is important to notice the arguments of the competent authorities investigating cybercrime. The whole digitalization of the business processes in enterprises requires additional resources for combating this kind of crime. The anonymous nature of these acts also threatens international security. Operational authorities also face these challenges. A change in international law regulation is necessary, in the management directed against digital risks and anomalies in IT security in administration and business.

Key words: cybercrimes, security, management, digitalization, control

JEL: K24, F50, G32, F38

Introduction

With the onset of the COVID-19 epidemic, the employees of enterprises began to work even more actively online from their homes. Services and processes began to be digitized en masse. Klaus Schwab coined the term "The Fourth Industrial Revolution". That process is characterized by: nanotechnology, biotechnology and other digital technologies. That fact has brought many changes in business cycles in the enterprises. For example, bank transfers are now made entirely online, and all the information at their disposal is implemented in banking software. Nowadays, there is a tendency for a wider use of electronic money, cryptocurrency and others, compared to other financial standard currencies. This change is also noticeable in the insurance sector. The information is again entirely

[1] PhD, Department of Counteraction to Crime and Public Order Protection, Faculty of Police, Academy of the Ministry of Interior of Bulgaria and International Business School – Botevgrad.

[2] COVID-19 is an infectious disease caused by a coronavirus.

digital, and users are extremely affected by personal data leaks and the possibility of hacker attacks. Even in some countries, innovative cyber insurance products are available.

The auditing and accounting professions are also changing. All procedures and tests performed by accountants are fully digitized. In accounting practice, the creation and development of appropriate digital skills is directly related to the development of technology and the implementation of innovative software applications and products that support the activity, according to Georgieva and Georgieva (2020, p. 147). Softwares are being developed that completely store and save the information. This also applies in full to internal auditors in the public sector. The administration is making a smooth transition to digitalization in their practice.

The process of digitalization affects every sector of the economy that uses IT technologies. In addition to the time-saving advantage, protection against corona virus, etc., there are also some significant problems with the so-called "cyberterrorists". The public authorities responsible for the security of society have reported frightening information about crimes with our personal data.

Applied methodology

The mission of any competent authority responsible for public security is to use preventive measures and approaches against crime, including cybercrime. It would be difficult to define the term "cybercrime". The reason is that it involves a number of predicate crimes, and could be realized in different ways.

For example, money laundering is not what it used to be. Teicher (2018) is of the same opinion. He mentions in his article that "money laundering is easily achieved with electronic money. Through the digital payments, we don't really know who is the user in the end. There have been cases of financing terrorists placing payments with electronic platforms such a Paypal and Airbnb. For these reasons, we need to be extremely meticulous about them, as there is a claim that the new money is a genius scam" (Вейсел, 2018, p. 131).

Yet the flexibility of hackers does not end here. It is a common practice to steal personal data and racketeer their victims. One example is *Postbank South Africa*. There are reports of personal data breaches and the replacement of 12 million bank cards. The reason is the theft of credit and debit card numbers (Bizga, 2020).

A similar business that is subject to the risk of cyber-attacks on personal data is the insurance industry. In 2020, the insurance company *Shirbit Company* in Israel suffered a cyber-attack. The company's owners have been racketeered for $3.8 million so as not to misuse consumer data (Graham, 2021). Examples can continue to be listed and analyzed. However, it is more important to seek a solution to the problems associated with cyber-attacks. There is a clear need to increase internal controls in companies. Due to their weakness, we are dependent on the

activities of law enforcement agencies. For the aim of the article, information will be provided in this regard on the expression of financial losses from different types of cyber crime. The table below is summarizes statistical information from the *Federal Bureau of Investigation (FBI)* in the United States for 2020.

Table 1: Financial losses from cybercrimes about the period 2016 – 2020 in the USA

Year	**Financial losses**	**Kind**
2016	$ 1.5 Billion	Identity Theft
2017	$ 1.4 Billion	Personal Data Breach
2018	$ 2.7 Billion	Extortion
2019	$ 3.5 Billion	Non-payment/ non-delivery
2020	$ 4.2 Billion	Phishing
Total	**$ 13.3 Billion**	

All listed expenses are in the billion USD.
Source: Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (2020, p. 5-6).

From the presented data in the table, there is an obvious trend of increasing losses from cybercrime in the last five years. In addition, the nature of that crime is of different kinds:

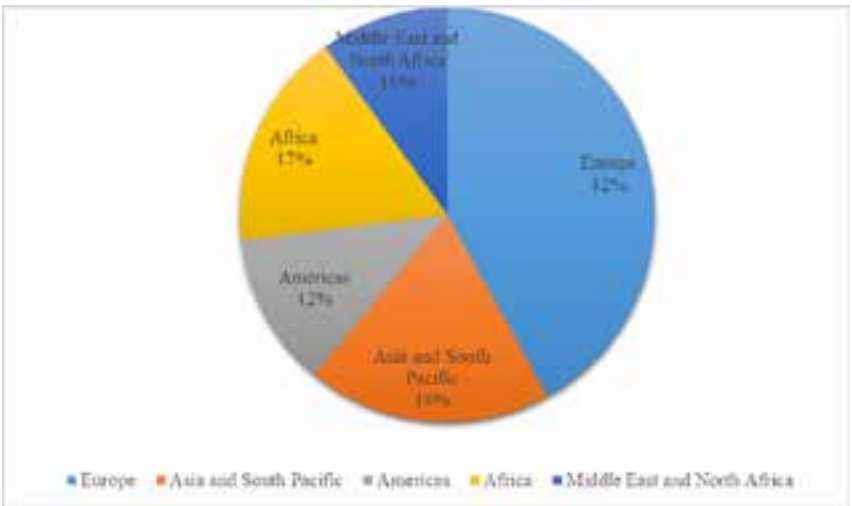
- Identity Theft – form of theft of another's identity;
- Personal Data Breach – General Data Protection Regulation (GDPR)[3];
- Extortion – the practice of obtaining benefit through coercion;
- Non-payment/non-delivery – a kind of fraud concerning the delivery of goods or failure to ship merchandise;
- Phishing – a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

Each of these cyber methods inflicts colossal losses on society. They indicate weaknesses in governance and internal control in the public and private sectors in the United States. This report also applies to the institutions exercising supervision over the activities. For these reasons, it is necessary to consider the introduction of additional national IT security, as well as crime prevention. Currently, cloud technologies in the Internet are used as an alternative way to store a database. In this way, even with a system breakdown, the information will be stored elsewhere. Experts in the field divide the clouds into: *public, private and hybrid clouds,* to that way determines the access to the information.

[3] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

The report of FBI presents that one of the reasons for the increase in cybercrime was the outbreak of the pandemic with COVID-19. It panicked society and transformed it into "victims". Also it is much easier to manipulate anyone can becomes a victim to such manipulation and attack. Even large corporations cannot protect their corporate and IT security from hacker attacks.

Other collegial police bodies, like Interpol also pay special attention to cybercrime committed during COVID-19. In order to gain a broader view of global issues, will be present a figure of cybercrime in different regions in percentage terms.



Source: Interpol (2020, p. 4).

Figure 1: Interpol Global Cybercrime Surveys

During the COVID-19 pandemic based on the study of *Interpol*[4] the following cybercrimes have occurred:

- Phishing;
- Disruptive Malware (Ransomware and DDoS) – attacks typically block access to a computer system or files until the victim pays a certain amount of money;
- Data Harvesting Malware – malicious software that steals information from the user;
- Misinformation – false, asymmetrical or inaccurate information, especially one which is deliberately intended to deceive.

[4] The International Criminal Police Organization is an inter-governmental organization. They have 194 member countries, and help police in all of them to work together to make the world a safer place.

The expert groups of Interpol noticed that corona virus induce the people to use internet more often and it is easy for the hackers to commit a crime. In order to minimize crimes of this kind, financial losses, the competent bodies shall encourage: timely information sharing, enhance police collaboration and cooperation with different countries, strengthen public-private partnerships, develop and implement national cybercrime strategies. Society needs to be better informed on how to react to such an attack, and which competent authorities to turn for help.

Within the European Union the responsible collegial body is *Europol*[5]. They also explore these problem areas. After the pandemic wave they raised concern regarding the need for people to have reliable information and new computer knowledge. The Agency noticed the other problem about crime with cryptocurrencies. The institution is challenged by crimes with international character across the EU border.

A Europol survey presents methods for the Safe Teleworking (according to the term from the Cambridge Dictionary it is an activity of working at home, while communicating with your office by phone or email, or using the internet) between business and for employees. For the business they recommend the following:

- Establishing corporate policies and procedures;
- Providing secure remote access;
- Keeping device operating systems and apps updated
- Securing your teleworking equipment;
- Securing your corporate communications;
- Raising staff awareness about the risks of teleworking;
- Increasing your security monitoring;
- Regularly check in with staff (Europol, 2020, p. 12).

For the safety of the employees they recommend:

- Accessing company data with corporate equipment;
- Using secure remote access;
- Keeping business and leisure apart;
- Being careful when using private devices for telework;
- Avoiding giving out personal information;
- Thinking before connecting;
- Staying alert;
- Developing new routines;
- Protecting your teleworking equipment and environment;
- Reporting suspicious activities (Europol, 2020, p. 12).

In order to minimize crime of all kinds, European legislation is actively enforcing agreements on *Joint investigation teams (JIT)* according to Nikolov

[5] Europol is the European Union's law enforcement agency. The mission of the Agency is to ensure a safer Europe for the benefit of all the EU citizens. It's based in The Hague, the Netherlands. They support the 27 EU Member States in the EU.

(2021). This method can involve different specialists and different competent authorities, and even non-EU countries to stop the crime, including cybercrime. This approach saves money and time.

Society is becoming increasingly dependent on information technology and electronic payment methods. Additional financial investments need to be made. The focus of criminals is entirely on cybercrime, due to their anonymous type. Hackers are constantly developing their skills, and are increasingly taking advantage of the fear, insecurity and naivety of the average user. Corporate organizations also suffer from constant hacking attacks. It is therefore essential that we report to the competent authorities which have the resources to resolve and decide the international cybercrime pandemic.

Results

With growing cybercrime, we need to take proactive and preventive action against them based on the good practice of competent authorities – FBI, Interpol, Europol. Some of these activities may focus on the following implementation in the public and private sectors:

- Increasing the internal and external control in the enterprises;
- Saving funds for cybersecurity;
- Updating internal policies and rules;
- Improving the coordination and subordination between law enforcement agencies in order to prevent cybercrime;
- Submitting signals by citizens to the competent authorities;
- Creating legislative reforms in favor of cybersecurity.

Discussion

Are there a number of working groups (at international and European level) discussing how cyber-attacks can be minimized? The working group „*European Crime Prevention Network*“ attaches importance to the motives that provoke the occurrence of these kinds of crime. Some of them are: money, emotion, sexual impulses, politics or religion, just for fun. With the outbreak of the COVID-19 epidemic wave, hackers can be even more cruel to their victims.

In such a critical situation, we need to use good practices. This is how Interpol acts. In the report “*Guide for criminal justice statistics on cybercrime and electronic evidence*“ good practices are noted by police forces. For example, *Association of Chief Police Officers (ACPO)* publishes the: *Managers Guide on Good Practice and Advice Guide for Managers of e-Crime Investigation* and the *ACPO Good Practice Guide for Digital Evidence,* etc.

It is important to remember that not everything depends on the competent police authorities. However, the state mechanism must take care of our national security by providing additional funds against cybercrime in the state budget, according to Goleva, Mircheva (2020, pp. 16-42). It is necessary to implement innovative approaches to cybercrime and also for business owners. In the study "*Innovate for cyber resilience*" (2020), cybersecurity practitioners share their experience in combating these crimes. They focus on financing in the IT security sector so that the business processes in organization can be normally continued.

Acknowledgements

The author is grateful to the organizers from the University of National and World Economy (UNWE) – Sofia, and to the colleagues from the Academy of the Ministry of Interior of Bulgaria, and to the General Directorate Combating Organized Crime, Department "Cybercrime".

References

Вейсел, А. (2018). Счетоводни аспекти на криптовалутите, Дигитални измами и киберсигурност, първа международна научно-практическа конференция, ИК-УНСС, София. (Veysel, A., 2018, Schetovodni aspekti na kriptovalutite, Digitalni izmami i kibersigurnost, parva mezhdunarodna nauchno-prakticheska konferentsia, IK-UNSS, Sofia).

Георгиева, Т., Георгиева, Д. (2020). Извършваните от счетоводителите дейности и задачи като фактори за определяне на необходимите дигитални компетенции, седемнадесета международна научна конференция Цифровата трансформация – бизнес, образование, наука, „Издателство на МВБУ", Ботевград. (Georgieva, T., Georgieva, D., 2020, Izvarshvanite ot schetovoditelite deynosti i zadachi kato faktori za opredelyane na neobhodimite digitalni kompetentsii, sedemnadeseta mezhdunarodna nauchna konferentsia Tsifrovata transformatsia – biznes, obrazovanie, nauka, Izdatelstvo na MVBU, Botevgrad).

Николов, П. (2021). Съвместни екипи за разследване, „Авангард Прима", София. (Nikolov, P., 2021, Savmestni ekipi za razsledvane, „Avangard Prima", Sofia).

Accenture Security. (2020). Innovate For Cyber Resilience, Lessons From Leaders To Master Cybersecurity Execution, Third annual state of cyber resilience, available at: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf (accessed 01 June 2021)

Association of Chief Police Officers (ACPO). (n.d.). Managers Guide on Good Practice and Advice Guide for Managers of e-Crime Investigation, available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_

Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf (accessed 01 June 2021)

Association of Chief Police Officers (ACPO). (2012). Good Practice Guide for Digital Evidence, available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (accessed 01 June 2021)

Bizga, A. (2020). South Africa's PostBank is Replacing 12 Million Bank Cards After Major Security Breach, available at: https://securityboulevard.com/2020/06/south-africas-postbank-is-replacing-12-million-bank-cards-after-major-security-breach/ (accessed 01 June 2021)

European Crime Prevention Network. (2016). Theoretical Paper Cybercrime, Cybercrime: A theoretical overview of the growing digital threat, available at: https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf (accessed 01 June 2021)

Europol. (2020). Internet organized crime threat assessment (IOCTA), European Union Agency for Law Enforcement Cooperation, available at: https://www.europol.europa.eu/iocta-report (accessed 01 June 2021)

Federal Bureau of Investigation (FBI), Internet Crime Complaint Center. (2020). Internet crime report 2020, available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (accessed 01 June 2021)

Goleva, V., Mircheva, V. (2020). Constitutional and Financial Legal Aspects of the State Budget in the Republic of Bulgaria, Economics and Law, Volume II, Issue I, pp. 16-42.

Graham, C. (2021). Israel shaken by data leak after ransomware attack at Shirbit insurance company, available at: https://hotforsecurity.bitdefender.com/blog/israel-shaken-by-data-leak-after-ransomware-attack-at-shirbit-insurance-company-24786.html (accessed 01 June 2021)

Interpol. (2020). Cybercrime: Covid-19 Impact, available at: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats (accessed 01 June 2021)

Interpol, European Union, Council of Europe. (2020). Guide For Criminal Justice Statistics On Cybercrime And Electronic Evidence, available at: https://rm.coe.int/3148-3-1-12-guide-for-criminal-justice-statistics-on-cybercrime-and-ee/1680a0250a (accessed 01 June 2021)

Teleworking, available at: https://dictionary.cambridge.org/dictionary/english/teleworking (accessed 23 December 2021)

Teicher, R. (2018). Transaction Laundering – Money Laundering Goes Electronic in the 21st Century, available at: https://www.finextra.com/blogposting/15423/transaction-laundering---money-laundering-goes-electronic-in-the-21st-century (accessed 01 June 2021)