Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

ASSESSMENT OF DIFFERENT RISK EVENTS UNDER A COMMON PLATFORM

Dragoș Danțiș
Bucharest University of Economic Studies, Romania
dragos.dantis@gmail.com

Ana Gabriela Anuțoiu
Transylvania University of Brașov, Romania
gabriela.anutoiu@yahoo.com

Abstract
The authors desired to approach inside this study possible risks emerging in different areas of research, like environment and finance. As the ranges of investigation are quite different, the writers have tried to find a common driver in the construction of the message. This has been achieved, by addressing to a shared hierarchical level, under the pyramid of Maslow, the second one linked to safety and security needs. Through the examples provided will be shown that even if the areas of research are different, the risks emerging are linked to infrastructure and / or technological innovation and are impacting on the safety and security areas. Collection of the data has been done through interrogation of dedicated open-source information specific to each field of research, legislation or addressing to specialized reports for the technical findings. Through the examples provided the research will show there may be relevant risks emerging in environment area, when meeting with brown bears or in finance, when facing threats linked to cybercrime and cybersecurity. Readers of this article should understand, that risks may occur based on a probability scale and on the appetite for risk of each one of them. In case of manifestation, the level of research and preparation for that particular case of each person or organization may influence on the impact measure and on the outcomes.
Keywords: brown bear, environment, finance, risks, safety and security.
DOI: https://doi.org/10.24818/beman/2022.S.I.3-05

1. INTRODUCTION

Inspiration for the construction of this paper has arrived from three directions. The first one has been given by the information and communication flow experienced by the authors in their field of research. They have seen that data for input is being collected, recorded and registered mostly through technological or digital channels, is being read and analysed by various stakeholders in dedicated virtual settings and transmitted as output under various digital forms.

The second one has been given by the fact that in most of the cases, the news appearing in official media or social networks were regarding the security field, independently of the fact, the announcements were about outdoor trips (e.g., risks arising while meeting the brown bear) or about finance (e.g., risks emerging from cybercrime or cybersecurity).

Even though there are constantly news regarding the risks occurring in outdoor trips or in the financial services, still not many people or companies are aware about them, or even if aware, their conduct goes into a direction with unwelcome outcomes. As an indirect result, many situations could have been or may be prevented, with a proper level of education and research.

Last inspiration point, possibly the significant and the connection one, among all the arguments, was linked to the identification of a common driver, serving as central platform for the construction of the message.

With this paper the authors decided to focus their attention on the possible risks, which could happen in environment and finance and are linked to technological innovation having as common driver of research the second level in the pyramid of Maslow, the one belonging to security and safety needs.

In the same time the authors wanted to express different requirements can be encompassed in a common cluster, like the one, mentioned in the upper paragraph. This is a result of the brainstorming, showing clearly, that a shared cluster can be used for the creation of a common message to address the various backgrounds (Figure 1).

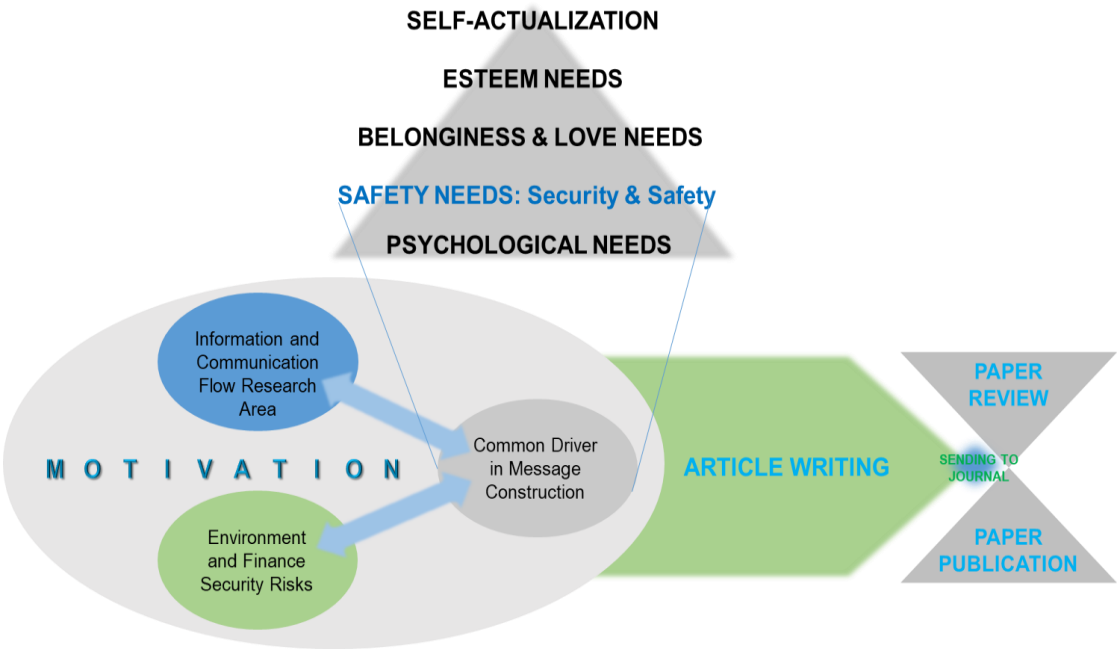

FIGURE 1. MOTIVATION FOR ARTICLE WRITING

Source: Author's own representation (including Maslow five level Needs Pyramid)

Aim of the research for the authors is to familiarize even more the people or the organizations with risks, linked to technical innovation, which could arise in environment or in financial services. Technology today is present, more or less in all the aspects of our life, as a result, some risks related to it could appear even in areas, which are normally the territory of wild animals.

In such cases, acknowledgment of the situation can be a first step towards the prevention or limitation of negative results.

The approach used by the authors, in putting together different fields of research in arriving to a common goal can be put under the portfolio of interdisciplinary research. This term is understood by the authors as follows (Tobi and Kampen, 2018): "interdisciplinary research may involve different disciplines within a single scientific culture, and it can also cross-cultural boundaries as in the study of humans and their environment".

Without reason of doubt, the interdisciplinary research has been used already extensively by researchers worldwide to advance on their key topics of interest. The authors have already tested this approach in few occasions, submitting several papers for reviewing, increasing each time, with the experience developed, the complexity level of the technical information provided.

This article will continue in the same direction, providing useful content in the understanding of possible risks emerging in technology range, in two different areas of research: environment and finance.

2. LITERATURE REVIEW

2.1. Brief considerations on the Safety-Security Needs level definition

The authors will address in this section several considerations on the main concepts, which have been used as skeleton in the construction of the article.

As already stated, the main pillar for the shaping of the message is linked to the second hierarchal level in the pyramid of Maslow, as a consequence the review will concentrate on this level.

In his well-known book, Maslow (1943) proposed a model for the classification of the human needs in: psychological, safety-security, love, esteem and self-actualization, an architecture which was followed by academia for further research.

The first level in this framework can be identified quite easily and is linked to immediate needs like hunger and thirst (Kenrick et al., 2010) and is depending on basic factors the human beings require, like food, air, water. The same study (Kenrick et al., 2010) mentions the idea highlighted even by Maslow, once the first level of basic needs has been fulfilled, the humans will go for the accomplishment of the next one, the safety-security.

To define the second level in the pyramid, the authors bring into discussion two interesting points expressed by Taormina and Gao in their article published in American Journal of Psychology (2013). According to their remark the definition of this scale has to be linked to the identification of the impacting threats and perceive them as a mix of tangible and intangible factors. Furthermore, the mentioned work, provides examples of menaces like wild animals, unforeseen events, social disorder, financial security or unemployment.

The hypothesis with the understanding of the safety-security needs level in relation with the risks impacting on human environment and communities is also mentioned by Aruma and Hanachor (2017) and is further developed through analysis, stating that insecurity has an impact on progress and society growth. Most of the above-mentioned ideas and examples are confirmed as well in a recent work (Uysal et al., 2017), being stated that one dimension of safety is strictly linked to economy.

In authors' opinion, taking into consideration the statements expressed, the following ideas can emerge:

- analysing the representation of the concept of the pyramid, from a logical angle, can be concluded that with each level the human requirements are more specialised;
- the hierarchical stages are interconnected between them;
- needs classified under particular level may be present in different aspects of the human life, like environment or finance;
- requirements classified under a certain level can appear in different moments (e.g., performing a trip into the forest; being subject to a fraud tentative).

2.2. Cyber Risk a new threat towards the digital finance

With the development of the financial market and the integration of new channels in performing the activity with customers, the financial institutions had to integrate in their structure, new components in the field of technology and innovation.

Consequently, with the opportunities arising to this new model of business enhancement arrived the risks, to a large extend identified as cyber risks.

European Systemic Risk Board (2020) associates to the cyber risk "three key features that, when combined, fundamentally differentiate it from other sources of operational risk: the speed and scale of its propagation as well as the potential intent of threat actors". To complete the understanding of this statement, should be understood that cyber risk is part of the operational risk, seen as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Bank for International Settlements, 2019).

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

Furthermore, the European Systemic Risk Board (2020) defines the cyber as "relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems", while the cyber risk represents "the combination of the probability of cyber incidents occurring and their impact".

In a document issued in 2021 the National Institute of Standards and Technology defines the cyber risk as "the risk of depending on cyber resources (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace)". The same source mentions this type of risk "overlaps with security risk, information security risk, and cybersecurity risk, and includes risks due to cyber incidents, cybersecurity events, and cyberspace attacks".

An interesting link is being provided by the definition advanced by National Institute of Standards and Technology, highlighting the perimeter where the cyber risk is occurring, in the cyberspace. To this extent the cyberspace represents "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (National Institute of Standards and Technology, 2021).

Referring to this concept, Mr. Juhan Lepassaar, the Executive Director of ENISA mentions that "member States have come to agree on the need to increase cooperation and make joint efforts to develop a common approach meant to strengthen the European cyberspace". (ENISA, 2019). This last statement represents a clear indication on the need to strengthen the prevention and protection of the perimeter, as more or less all the economic sectors are depending on the digital area, including the financial services.

3. RESEARCH METHODOLOGY

The research will head in the presentation of two different scenarios in diverse areas of research, with possibility of being impacted by the emerging risks in the field of technology and innovation.

First one, will be linked to an assessment of the situation in Romania regarding the interaction with the brown bear *(Ursus arctos)* in the environment. This focus is justified by the large number of individuals at country level compared to the other states of the European Union. Representation will be accompanied by brief available data, obtained from official sources, national legislation in place and specialized reports.

Second scenario will have a look at the cyber risks emerging in financial background at European level, as more or less the manifestation occurs on a wider area. The evaluation will benefit from quantitative and qualitative information, collected from technical studies issued by regulators or dedicated agencies.

In both cases, particular ideas can be considered by readers for their acknowledgment and further study.

4. RESULS AND DISCUSSIONS

4.1. Technological risks occurring in environment while meeting the brown bear

When speaking about the environment research area, the writers take into account, the situations when people arrive to meet wild animals, especially the brown bear *(Ursus arctos)*.

As indicated and detailed in a previous article (Anuțoiu and Danțiș, 2021) the number of brown bears has increased at national level and for some time has become a central theme in daily media communication.

In practice, due to the broadening of the bear population and reduction of the available territory the number of encounters with the people has increased constantly and has several causes:

- the wild animals are in search of food and arrive close to the local communities or local infrastructure;
- humans practicing various open-air activities enter into the bear habitat;
- the expansion of the urban area;
- large sporting events organized in nature.

An overview on the situation of the brown bear has been advanced by the Government Emergency Ordinance no. 81/2021 on the approval of immediate intervention methods to prevent and combat attacks by brown bears on persons and their property, and amending and completing certain normative acts, which mentions that between January 2016 and June 2021, 6.400 phone calls were made to the emergency number 112, managed by the Special Telecommunications Service, representing reports on the presence of the brown bear.

The preamble of the above-mentioned normative act shows that most of the emergency calls have been registered during 2019 and 2020 years, while for the considered time period of 2021 there were 1.493 phone calls, and also that the number of phone calls has increased several times in the last years in the following counties: Brașov, Covasna, Prahova, Harghita, Argeș, Mureș.

The same source (Government Emergency Ordinance no. 81/2021) shows that in 2019 and 2020, more than 1.000 immediate interventions, provided by the cited normative act, were registered, three times more than in previous years.

Considering the cases with unwanted results, when it is required a different course of action, the public authorities, issued and published the Order no. 723/2022 which mentions the maximum level of intervention and prevention in case of brown bear species (Ministry of Environment, Waters and Forests, 2022).

In front of such a complex scenario, the people need to have a good understanding on the way to behave close to brown bears, to prevent human life, domestic animals or economic losses.

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

The primary focus for any person, present in the bear habitat or encountering such an animal is to adapt a mix of reactive and proactive measures to stay safe and to protect its body and life safety.

Consulting the opinion of a specialist in mountain trips risk management, the mobile phone has been identified as a proper mitigation action to call the emergency services to signal the presence of a bear, to ask for support and evacuation or to allow terrain orientation and positioning.

Between the lines can be understood that in wildlife the mobile phone represents probably the main technological pillar for the accomplishment of the safety and security needs. Nevertheless, the mobile phone can be impacted by the following risks, which can be seen as risks towards second level needs in the pyramid of Maslow:

- battery life duration impacting only partially or on all the functions of the mobile phone;
- lack of network coverage with effect on the messages and audio communication function;
- absence of internet network coverage influencing the terrain orientation and positioning;
- broken screen with impact on the utilities of the mobile phone.

To prevent such occurrences and to have the proper capabilities to intervene in case of need, the people should act in a responsible manner while doing an outside trip, which could result in meeting with brown bears:

- information in advance on the touristic routes and on the weather present in the areas to be visited;
- there should be consulted the web pages of the emergency services for useful information;
- the trip should be done in a group of people and the excursion should be made exclusively on marked tourist routes;
- battery of the mobile should be fully charged at the start of the trip and a backup should be available;
- the use of the mobile phone should be done in an accountable manner to guarantee the availability of battery resources in case of need;
- a navigation application should be installed on the mobile phone to allow a proper positioning on the terrain;
- close friends or family should be informed about the area to be visited.

Nevertheless sometimes, with all the mitigation actions considered by a person before an outdoor trip, there can appear events impacting on the functioning of the network in that geographical area. If such an incident occurs the risk will be present at the level of the infrastructure of a utilities provider, impacting partially or totally on the functioning of services offered.

Such events can occur and are available through a study issued by National Authority for Management and Regulation in Communications of Romania, identified as ANCOM (2022). According to this report for the year 2021 the most impacted services due to incidents have been the ones of mobile phone and

SMS and the ones of mobile internet and transmission of mobile data. As a result, the authors will present, information available only for these two categories that can be linked to the perimeter of current article (Figure 2 and Figure 3), for the period 2019 – 2021.

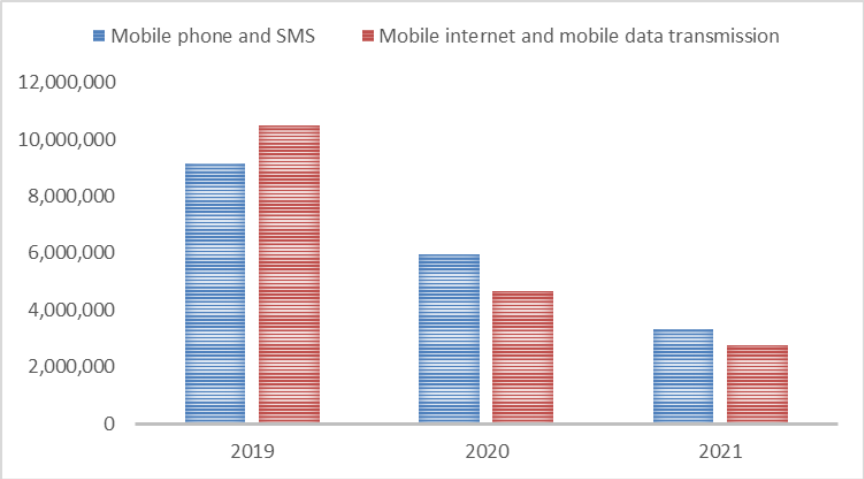

FIGURE 2. NUMBER OF CONNECTIONS IMPACTED PER SERVICE

Source: Author's own representation based on ANCOM report data

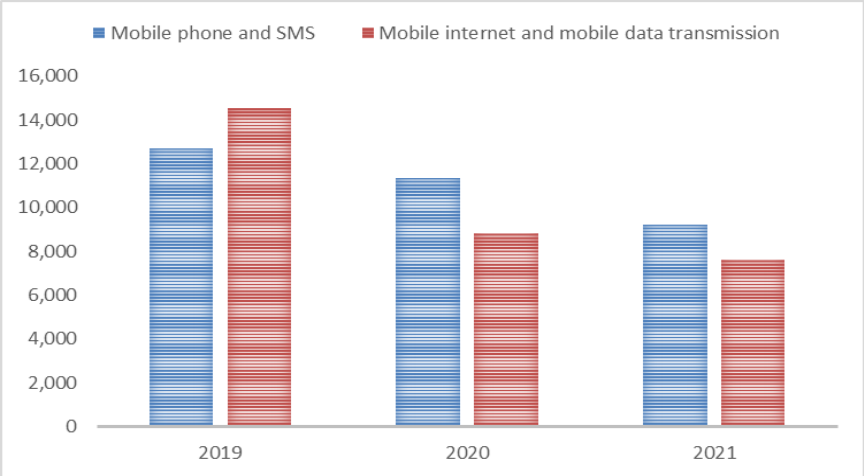

FIGURE 3. AVERAGE NUMBER OF CONNECTIONS IMPACTED BY AN INCIDENT PER SERVICE

Source: Author's own representation based on ANCOM report data

From the two figures shown above can be seen clearly that the number of connections impacted has decreased from one year to the other, as a total sum and as an average number per incident.

The same report, citing the Decision 512/2013 of the National Authority for Management and Regulation in Communications of Romania indicates that the providers of communications have to inform if it was affected the capability to call the emergency number due to an incident. Based on the information

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

arrived from the operators, "if the emergency calls were impossible to be placed using the own infrastructure, the users have been able to access the infrastructure of other networks with coverage in the area", resulting that in most of the cases a backup solution has been available.

4.2. Cyber Risks emerging on the financial market

Focusing on the financial market, the authors have seen the evolvement of the background in the last years with the development of the digital alternative channels, enrichment of the services provided by classical banks and launch of decentralized finance, also known as DEFI.

To the directions stated above can be added more specialised ones, as indicated by the President of the European Central Bank in a speech delivered in November 2000, highlighting a course of action which has maintained the dynamics even now: "The theme of this panel discussion is a topical one. In recent years, financial markets have undergone some of the most rapid and extensive changes in any markets…Other interesting developments in world financial markets include the continued broadening and expansion of derivatives markets. The broadening of these markets has largely come about because rapid advances in technology, financial engineering, and risk management have helped to enhance both the supply of and the demand for more complex and sophisticated derivatives products" (European Central Bank, 2000).

With digitalization the way of doing business and the interaction between banks and clients changed substantially and moved into the cyberspace. The new environment paved the way not only to numerous opportunities, but as well to new situations, which can be seen as threats.

Banks, Fintech companies or other financial actors have been subject to cyber-attacks resulting in business disruptions, reputational or financial losses, data breach, and client discontent.

The changes registered at the level of European Union area for example, provided the input to the public authorities to start and broaden the definition associated to the perimeter of the financial ecosystem, to monitor and in some cases even intervene in situations, which several years ago were out of scope.

For the representation of the cyber threat landscape will be used mainly the rich portfolio of papers published by ENISA, The European Union Agency for Cybersecurity, and other official European Union bodies, which has evolved overtime in an extensive source of information for practitioners and researchers (ENISA).

The findings and recommendations of security experts are established on current realities, in which more or less in average every person is owner of an electronical device connected to the internet, in most of the cases a smart phone or a computer. This can serve not only as a communication tool, but as well as a financial platform for various services offered by Fintech companies or banks. This

assessment enriches the statements regarding the redefinition of classical financial perimeter and brings into attention the high number of devices and users that can be subjects of cybersecurity attacks. As the mobile phones are used extensively for a wide typology of functions, ENISA ranks in second place the treats associated to mobiles – threats will become fully mobile (ENISA, 2020).

ENISA mentions clearly in one of the research papers that "the number of incidents with financial organizations and not necessarily banks, increased substantially during the reporting period" (ENISA, 2020). In the same brochure, the security agency indicates the financial data as one of the most desired assets by cybercriminals (ENISA, 2020).

Without any doubt the conclusions of ENISA at European level have been present in other areas, outside of EU, as the financial area represents a profitable target for cybercriminals. Among the objectives of cyber attackers have been clients, financial institutions or even European authorities.

For example, while still a member of the European Union, Great Britain revealed a case similar to other earlier situations, in which have been used modules associated to the SWIFT international financial system. The entity impacted was the Far Eastern International Bank, target in October 2017 to a cyber-enabled fraud. The malware was sent in the ecosystem of the financial institution through a spear-phishing email, tainting the ICT systems used for SWIFT payment network. Managing to obtain valid credentials the attackers initiated several transactions to be sent through the SWIFT system in foreign countries, for an overall amount of 60 million US dollars. Though as the financial messages were configured in wrong manner the real loss reached only a total value of 500.000 US dollars (National Cyber Security Centre and National Crime Agency, 2017-2018).

Based on an earlier remark regarding the targeting of European authorities by the cyber groups, is brought into attention the event happened in March of 2021, when European Banking Authority was the subject of a cyber-attack against its Microsoft Exchange Servers. A communication was put in place by the authority informing on the occurrence and the investigations in place (European Banking Authority, 2021).

In completion of the above-mentioned examples, the Europol, is highlighting the so-called SIM Swap fraud and the joint actions of various law enforcement forces to investigate and prevent such a threat (Europol). In detail such a scenario allows the criminals to replicate the SIM card of the mobile phone of the victims and obtain through several actions the ownership of the SIM card and to use it for financial frauds.

While presenting the underwent investigations, the Europol law enforcement agency, advances to the readers some key statements, in order to protect themselves from such situations, which can be seen

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

very useful, in front of such a complex operational model. The guidelines of Europol are complemented by the advices of ENISA (2021) to prevent such a situation occurrence.

To the scenarios indicated, ENISA (2022) adds the ransomware risk, which represents "a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality". The study advances the idea that this threat has evolved gradually throughout the years and aside the classical actions of encryption and locking, currently performs as well deletion or stealing of data. The investigation advances the following technical information for the analysed perimeter, with an average of 518 GB of stolen data per incident and an average of 10 TB per month.

Report from 2021 of ENISA provides an overview on the evolution of the ransomware incidents, the cybersecurity agency performing a collection of data from various sources (Figure 4). It can be seen clearly a general increase trend in the number of threats from the initial period of the analysis, April 2020, even if there can be noticed months with decrease in the values registered.

The evolution of this type of risk is strictly linked to the development of the scenario known as RaaS, or ransomware-as-a-service, an operating method used by groups of malicious attackers to obtain financial advantage

Another main idea coming out of the analysis performed by ENISA is the change of behaviour in the preferences of cybercriminals regarding the pay-out method for the ransomware attack, replacing Bitcoin with Monero. This approach is linked to the characteristics of this cryptocurrency, which provides improved anonymity. The extensive nature of ransomware is recognised even by European Commission, stating that such an attack is impacting on an organization around the world every 11 seconds (European Commission, 2022).

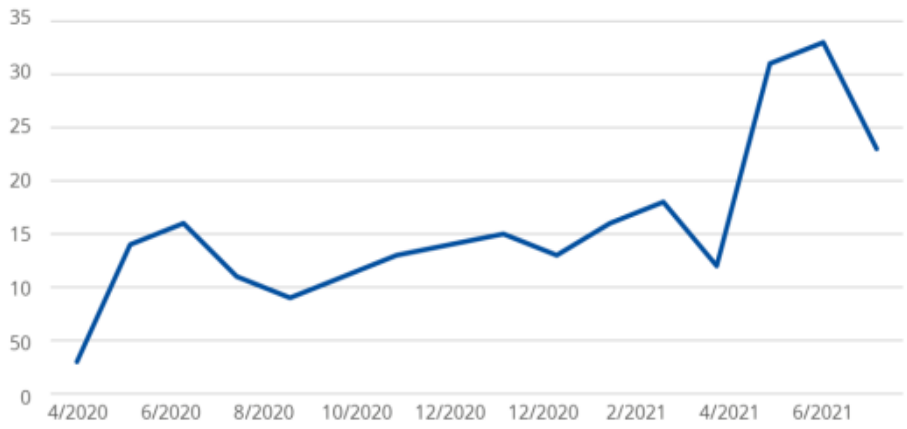

FIGURE 4. RANSOMWARE INCIDENTS OBSERVED BY ENISA (APRIL 2020 - JULY 2021)

Source: Extract from ENISA Threat Landscape 2021 report

Presented examples represent only a portion of the scenarios in place impacting on the financial industry digital ecosystem. In fact, to the above-mentioned cybercriminals can use phishing, DDos, malware, spyware, card skimming, smishing, "zero-days" software vulnerabilities, advanced persistence threat, third party data breach, ATM fraud, botnets.

Referring to the existing cyber threats, ENISA mentions the most popular ones: web application attacks, insider threat (unintentional abuse), malware, and data theft. The same source indicates as a general evaluation a stable incidents trend for financial / banking / insurance sector (ENISA, 2020).

Such a complex portfolio of existing and emerging cyber risks has to be associated with a rough quantitative representation to show there is a strong financial motivation behind the actions of cybercriminals.

In a paper issued in 2020 the European Systemic Risk Board, brings forward estimates of the industry, going from USD 45 billion to USD 654 billion for the global economy in 2018. The statement expressed by the authors regarding the difficulty in establishing the total costs of cyber incidents are well founded on the two conditions stated: not all incidents are reported and not all the losses can be identified (European Systemic Risk Board, 2020).

Furthermore, in front of so many cyber risks impacting the financial industry, Mrs. Alexandra Maniati, Director of Innovation & Cybersecurity of the European Banking Federation was stating: "There can be no successful digital innovation in banking or any other sector, if it's not based on cybersecurity and digital operational resilience" (European Banking Federation).

Above mentioned citation offers an overview on the importance of the cybersecurity and the impact of cyber risks, which are being present across all the domains of a society. This statement is covered as well by a representation advanced by ENISA in one of agency's studies (ENISA, 2021), providing a synthesis of cyber incidents / attacks (Figure 5). Among the first areas targeted by the cyber events are public administration / government and digital service providers.

In the list of sectors impacted by the cyber incidents, can be seen that finance / banking is ranked at position number 5 in the preferences of the attackers, showing once more the interest towards data acquisition and financial gains obtained from cybercrime.

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022

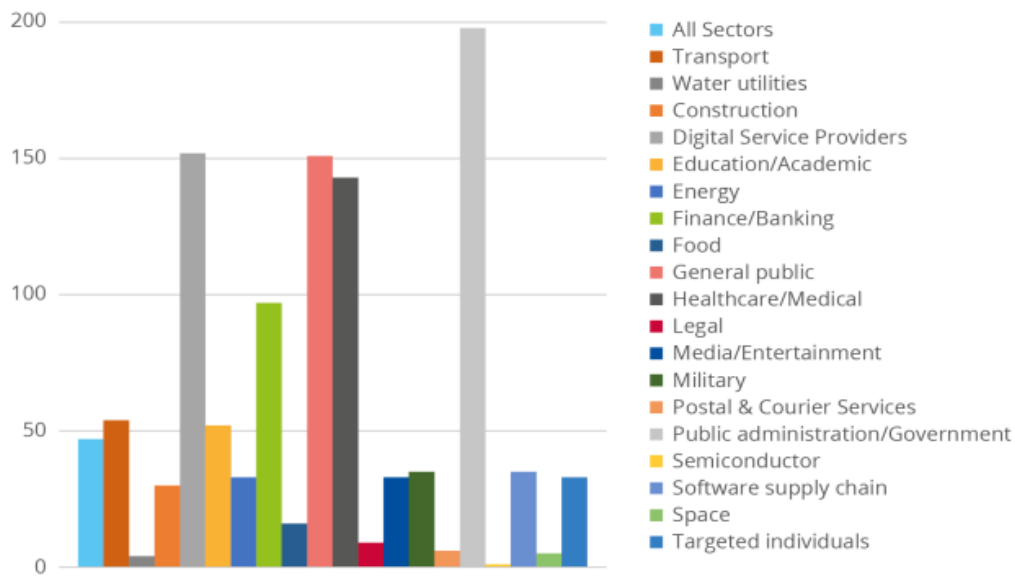

FIGURE 5. TARGETED SECTORS PER NUMBER OF INCIDENTS (APRIL 2020 - JULY 2021)

Source: Extract from ENISA Threat Landscape 2021 report

5. CONCLUSIONS

What can be noticed from the examples provided by the authors is the fact that risk management is a concept, which has to be understood properly by the people or organizations, even more when particular activities or scenarios imply a different behavioural scenario.

Risk can be present as an event even when the activity or the scenario as such imply the presence of technology, as not in all the cases, as shown, the innovation guarantees the absence of risk.

Rather, in the presence of technology, there can be present risks specific to the digital ecosystem and in such situations is needed an understanding and awareness on the nature of such technological hazards.

The manifestations of technological threats can have an impact on the safety and security needs of people, being translated in physical injuries or in economic losses.

In terms of economic losses, the European Commission (2022) is offering in one of its documents the following assessment, which is raising some attention points. The ransomware attacks across the globe may be evaluated to 20 billion Euro in 2021, while the annual cost of the cybercrime may have arrived to 5,5 trillion Euro in the past year.

Currently the European Union is concentrating the attention on the Cyber Resilience Act, an extensive legislation to “introduce mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle… Once adopted, economic operators and Member States will have two years to adapt to the new requirements”.

The risk events will continue to be present in the human activities and will accompany the performance of value chains of the organizations.

It can be even concluded that risk as an event will manifest itself at some moment in time in any given scenario. What can be changed instead is the risk awareness level of people or organizations and to prepare as best as possible for the risk manifestation and mitigation of the impact.

In this regard, the content of the article comes to enrich the information available to the readers in being aware on particular situations linked to environment or finance.

REFERENCES

Anuțoiu, A.G., Danțiș D. (2021) Brown Bear Population Management in Romania: Pilot Project Using the Benefits of Technology. Proceedings of the 38th International Business Information Management Association (IBIMA), 23-24 November 2021, Seville, Spain, ISBN: 978-0-9998551-7-1, ISSN: 2767-9640

Aruma, E.O., Hanachor, M.E. (2017) ABRAHAM MASLOW'S HIERARCHY OF NEEDS AND ASSESSMENT OF NEEDS IN COMMUNITY DEVELOPMENT. International Journal of Development and Economic Sustainability Vol.5, No.7, pp.15-27, December 2017. Published by European Centre for Research Training and Development UK (www.eajournals.org)

Bank for International Settlements (2019). Retrieved September 22, 2022 from https://www.bis.org/basel_framework/chapter/OPE/10.htm?tldate=20221231&inforce=20220101&published=20191215

ENISA (2022). The European Union Agency for Cybersecurity. Retrieved September 01, 2022 from: http://www.enisa.europa.eu

ENISA (2020). Emerging trends. 2020. Retrieved September 10, 2022 from: http://www.enisa.europa.eu/publications

ENISA (2022). ENISA threat landscape for ransomware attacks. 2022. Retrieved September 20, 2022 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

ENISA (2021). How to avoid MOBILE SIM SWAPPING? Retrieved September 10, 2022 from https://www.enisa.europa.eu/publications/how-to-avoid-sim-swapping-leaflet

ENISA (2020). Main incidents in the EU and worldwide. 2020. Retrieved September 10, 2022 from: http://www.enisa.europa.eu/publications

ENISA (2020). Main incidents in the EU and worldwide. 2020. Retrieved September 10, 2022 from: http://www.enisa.europa.eu/publications

ENISA (2020). Sectorial/thematic threat analysis. 2020. Retrieved September 10, 2022 from: http://www.enisa.europa.eu/publications

ENISA (2019). The EU Agency for Cybersecurity welcomes its new Executive Director: Mr. Juhan Lepassaar. 2019. Retrieved September 10, 2022 from https://www.enisa.europa.eu/news/enisa-news/welcome-to-the-new-ed

ENISA (2021). The Threat Landscape. 2021. Retrieved September 22, 2022 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Banking Authority (2021). Cyber-attack on the European Banking Authority. 2021. Retrieved September 10, 2022 from: https://www.eba.europa.eu/cyber-attack-european-banking-authority

European Banking Federation (2022). Retrieved September 20, 2022 from: https://www.ebf.eu/priorities/innovation-cybersecurity/cybersecurity/

European Central Bank (2000). Recent Developments and Trends in World Financial Markets. Speech delivered by Dr. Willem F. Duisenberg, President of the European Central Bank, on the occasion of the 75th anniversary of the Banco de Mexico, Mexico, 14 November 2000. Retrieved September 22, 2022 from https://www.ecb.europa.eu/press/key/date/2000/html/sp001114.en.html

European Commission. (2022) Cyber Resilience Act – Factsheet. PDF ISBN 978-92-76-56557-4 doi: 10.2759/543836. Retrieved on 28th of September 2022 from https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

European Commission (2022) Press release. State of the Union: New EU cybersecurity rules ensure more secure hardware and software products. Retrieved September 21, 2022 from https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

Europol. The SIM hijackers: how criminals are stealing millions by highjacking phone numbers. Retrieved September 10, 2022 from: https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers

European Systemic Risk Board (2020). European System of Financial Supervision. Systemic Cyber Risk. February 2020. ISBN 978-92-9472-131-0 (pdf). DOI 10.2849/566567 (pdf). Retrieved September 21, 2022 from: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9

Government Emergency Ordinance no. 81 from 21st of July 2021 on the approval of immediate intervention methods to prevent and combat attacks by brown bears on persons and their property, and amending and completing certain normative acts.

Kenrick, D.T., Griskevicius, V,, Neuberg, S.L., Schaller, M. Renovating the Pyramid of Needs: Contemporary Extensions Built Upon Ancient Foundations. Perspect Psychol Sci. 2010 May;5(3):292-314. doi: 10.1177/1745691610369469. PMID: 21874133; PMCID: PMC3161123.

Maslow, A. (1943). A Theory of Human Motivation. Psychological Review, 370-96.

Ministry of Environment, Waters and Forests (2022). Press Release. Order which mentions the maximum level of intervention and prevention in case of brown bear species has been put in public debate. Retrieved September 15, 2022 from http://www.mmediu.ro/articol/comunicat-de-presa-ordinul-care-stabileste-nivelul-maxim-de-interventie-si-preventie-in-cazul-speciei-urs-brun-a-fost-lansat-in-consultare-publica/4923

National Authority for Management and Regulation in Communications of Romania. ANCOM. (2022) Raportul privind incidentele care au afectat securitatea rețelelor și serviciilor de comunicații electronice în anul 2021 al Autorității Naționale pentru Administrare şi Reglementare în Comunicaţii

National Authority for Management and Regulation in Communications of Romania. ANCOM. (2013). Decision number 512 on 2013

National Cyber Security Centre and National Crime Agency (2017-2018), The cyber threat to UK business. 2017-2018 Report. Retrieved September 15, 2022 from: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

National Institute of Standards and Technology (2021). U.S. Department of Commerce. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. December 2021. Retrieved September 22, 2022 from https://doi.org/10.6028/NIST.SP.800-160v2r1

Order no. 723 from 4th April 2022 on the approval of the level of intervention and prevention in the case of the brown bear species (*Ursus arctos*), in the interest of the health and safety of the population and in order to prevent significant damage

Taormina, R.J., Gao, J.H. (2013) Maslow and the Motivation Hierarchy: Measuring Satisfaction of the Needs. American Journal of Psychology. Summer 2013, Vol.126, No. 2 pp.155–177

Tobi, H., Kampen, J.K. (2018) Research design: the methodology for interdisciplinary research framework. Qual Quant 52, 1209–1225 (2018). https://doi.org/10.1007/s11135-017-0513-8

Uysal, H.T., Aydemir, S., Genc, E. (2017) MASLOW'S HIERARCHY OF NEEDS IN 21ST CENTURY: THE EXAMINATION OF VOCATIONAL DIFFERENCES. 2017. In book: Researches on Science and Art in 21st Century Turkey (pp.211-227) Edition: Volume 1 Chapter: 23 Publisher: Gece Kitaplığı Editors: Hasan Arapgirlioğlu, Robert L. Elliott, Edward Turgeon, Atilla Atik

Business Excellence and Management
Volume 12 Special Issue 3 / October 2022