MANAGING SECURITY RISKS IN INTERNATIONAL BUSINESS

Nikola Brzica[13] & Ivana Brzica[14]

UDC / UDK: 004.738.5:339.5:005.334
JEL classification / JEL klasifikacija: F23, L81, O33
DOI: https://doi.org/10.22598/pi-be/2021.15.2.87
Scientific review / Pregledni znanstveni rad
Received / Primljeno: May 25, 2021 / 25. svibnja 2021.
Accepted for publishing / Prihvaćeno za tisak: November 11, 2021 / 11. studenog 2021.

Summary

This paper examines the existing theory of risk management in international business, as well as the effects that the globalization and digital transformation have on the development of contemporary security risks. Besides the analysis of the key elements of globalization and digital transformation, this paper points out that the imperative for success in international business is a systematic approach to security risks, and the new categorization of risks in international business. While the pandemic has provided an impetus for the rapid and widespread adoption of digital technologies, it has also created new opportunities for hostile threat actors leading to an increase in cybercrime and thus reinforced the demand for robust and responsive security measures. The paper argues that more now than ever, there is a burning need to address the problem of security risks properly. Initial efforts to address these risks have sought to include the aforementioned security risks in existing risk mitigation practices and to address them through existing business risk processes, but it has become evident that success risk mitigation requires new and adapted approach. The authors present the review of existing theory of security analysis and propose the new categorization of risks in international business to include security risks. Security risks include, but are not limited to threats such as loss of data and intellectual property, fraud, disruption of business processes, and the possible endangerment of the physical security of both employees and assets.

Keywords: *international business; e-commerce; security risks; risk management.*

[13] dr.sc. Nikola Brzica, Head of Expert Committee, Business Security Academy, Zagreb, Croatia. Email: nikola.brzica@gmail.com
[14] mr.sc. Ivana Brzica, Doctorate student, Faculty of Economics and Business, Zagreb, Croatia. Email: ibrzica@net.efzg.hr

1. INTRODUCTION

One of the most important contributing factors in contemporary international business is a secure environment, equally important for both businesses and their customers. The systematic mitigation of security risks associated with international business contributes to confidence that the transactions will be secure, that goods purchased will be delivered, and that data will not be destroyed or misused, especially for fraudulent ends. This has proven itself particularly true in recent years with the rapid explosion of digitally enabled e-commerce. Namely, the last decade, with an additional impetus by the onset of the COVID-19 pandemic, has seen accelerating transition towards a digital economy in which social media and the internet, as well as information and communications technologies play a growing part in the production, consumption and exchange of goods and services. However, alongside new opportunities, new risks have also arisen. Perhaps more now than ever, there is a burning need to address the problem of security risks properly. While the pandemic has provided an impetus for the rapid and widespread adoption of digital technologies, it has also created new opportunities for hostile threat actors leading to an increase in cybercrime and thus reinforced the demand for robust and responsive security measures. It is becoming increasingly apparent that sustaining the growth of international business seen in recent years requires that business become aware of existing and evolving security risks, as well as their possible impacts, and position themselves to mitigate those risks effectively and efficiently. Initial efforts to address these risks have sought to to include the aforementioned security risks in existing risk mitigation practices and to address them through existing business risk processes, but it has become evident that successful security risk mitigation requires a new and systematic approach to the subject. Security risks include, but are not limited to threats such as loss of data and intellectual property, fraud, disruption of business processes, and the possible endangerment of the physical security of both employees and assets.

This paper is structured as follows. Section 2 reflects on globalization and the new business environment from the security perspective. Section 3 outlines the existing theoretical framework of the security science and the security risk management. Section 4 proposes a new categorization of risks in international business. In Section 5 it is discussed how the pandemic and the rise of E-commerce have created a new security landscape. Section 6 concludes the paper and outlines directions for future wo

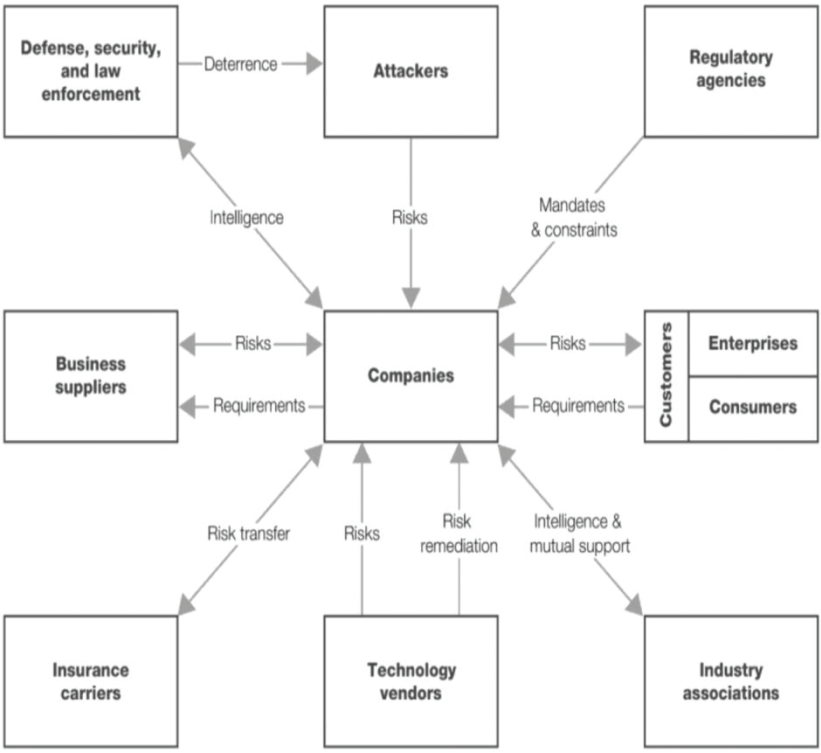
2. GLOBALIZATION AND NEW BUSINESS SECURITY ENVIRONMENT

International business is a term used to describe all commercial transactions (public and private, the sale of goods, services and resources, investments, etc.) which occur between two or more countries, and are facilitated by global resources (Radebaugh & Sullivan, 2007). The motivations and objectives of commercial entities that do business internationally are generally twofold; achieving economic gains, as well as gaining

experience with which they hope to enable further business operations on the international market (Ristovska, 2014). Unfortunately, commercial entities that decide to do business internationally face a disparate, unfamiliar and often insecure environment. However, despite the associated risks, the internationalization of business has produced previously unthinkable gains in recent decades. Globalization has proven to be an important driver of economic growth, inclusive trade and job creation that has had a positive correlation on both economic prosperity and social welfare. Together, globalization and technological advances have "erased national borders," and it appears that the responsibility for maintaining security is now largely outside the realm of traditional national authorities. In recent years, global security threats such as ethnic conflict, terrorism, climate change, cyber-attacks and pandemics are no longer isolated, geographically constrained events that can be easily contained and managed within the borders of one or two states. On the contrary, although contemporary security threats still often manifest themselves in geographically isolated areas as a result of long simmering political, economic, social and other instabilities, their impacts in a globalized world often greatly transcend the spatial dimension and can be shockingly far-reaching.

One thing that should be kept in mind is that today we face a contemporary global security environment which is merciless in its handling of all actors who are not prepared for the existential and operational conditions associated with contemporary international business operations. This new security environment is characterized by insecurity, rapid changes, the eradication of traditional boundaries, the quick distribution of information, and an increasing reliance on information-communication infrastructure for business operations. In these circumstances, both public and private enterprises conducting business are exposed to a new type of risk - that of security risk, and must be able to manage and mitigate the same.

Figure 1. Wide range of security risks and engaged actors



Source: Rezek, Chris, O'Halloran, Derek, Kaplan, James M., Marcus, Alan, Bailey, Tucker. (2015). Beyond Cybersecurity : Protecting Your Digital Business . Hoboken, New Jersey: John Wiley & Sons.

Security risks can have consequences not only for countries (the traditional national security actors and guarantors of international security), and not only within a specific geographical area, but for all commercial entities (such as enterprises, consumers, business suppliers, technology vendors, regulatory agencies) that exist and participate in the international market (see Figure 1). As such, these commercial entities can be directly or indirectly exposed to the consequences of a security incident. A good example of the paradigm shift described above is the recent proliferation of unethical hacking and use of malicious software in attacks on the ICT infrastructure of both public and private sector entities. These attacks have been conducted for a wide variety of motivations, but have often targeted e-commerce companies and enterprises. Demonstrating this new "world without borders," in some cases, attacks have been launched at targets from opposite ends of the globe. (Sulmeyer, 2017). As mentioned above, e-commerce is a rapidly growing form of business in which information technologies are used to increase sales, business

efficiency, and provide a basis for new products and services (Išoraite et al., 2018:2). E-commerce lies at the heart of the digital economy, defined by the Organization for Economic Cooperation and Development (OECD) as the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders (OECD, 2020a). E-commerce represents a complex and growing range of economic activity. It includes transactions between businesses (B2B), between businesses and individual consumers (B2C), and between governments, businesses and citizens (G2B, G2C). Also, it includes the direct provision of services that can be traded digitally, as well as the facilitation of ongoing and additional trade in goods, international commerce, between continents and across land borders, as well as domestic transactions, both wholesale and retail (UN, 2021: 13). When communicating with each other and/or with customers, businesses engaged in international trade typically exchange various types of sensitive information whose compromise can result in negative consequences. Thus, commercial entities must take measures to protect information about products and services, information pertaining to negotiations regarding the terms of transactions, exchange contracts and other documents, transmit and accept orders and complaints, press releases, etc. Indicative of the increasing importance of protecting information are recent statistics on cybercrime, with the FBI reporting a 300% increase in reported cybercrimes since the onset of the COVID-19 pandemic. It is estimated that by the end of 2021, cyber security threats will cost the world $6 trillion USD per year (Williams et al, 2020:547). In addition to increased frequency, increased complexity has also been noted. In the case of sophisticated attacks (commonly known as APT's - Advanced Persistent Threats), once attackers have gained access to enterprises 'networks, they can collect and exfiltrate intellectual property, business plans, forecasts, financial transaction data, and other valuable business related data over extended periods of time.

3. REVIEW OF EXISTING THEORETICAL FRAMEWORK

The contemporary security studies aim to reach a consistency with the knowledge domain of security and to demonstrate the underlying principles applied in the security risks management to those of the scientific method. In these attempts, theorists are focused on the development of a theoretical context and a knowledge base which can be applied to security aspects that can be operationalized protect the organizational resources. According to Meushaw, security science as an emerging discipline should give us an understanding of the limits of what is possible, by providing objective and qualitative or quantitative description of security properties and behaviors (Meushaw, 2012). Smith and Brooks (2013) argue that security science in its most simplistic knowledge areas include security management, security theories and principles, the built environment, and security risk management. According to the same authors, security risk management is a core knowledge category of the security function and such a function should provide the organization with articulated and consensual threats and risks that inform and direct the security effort (2013:41). It is a widely accepted premise in

contemporary risk management theory, security breaches (frequently intentional) represent the major part of all possible risks, so the management of particular security risks today became the main part of risk management process (Szmit, 2015). When discussing the existing risk methodologies, Terje argues that probability is the most common tool, but other tools also exist, including imprecise (interval) probability and representations based on the theories of possibility and evidence, as well as qualitative approaches (Terje, 2016: 4). However, in security risk management, where qualitative assessments are often performed on the basis of judgments of actors' intentions and capacities, without reference to a probability scale, lies a potential for significant improvements in the way security risks are assessed. Theorists agree that this can be achieved by developing frameworks that integrate the standard risk methodology, contemporary security science and new ways of assessing and treating uncertainty (Brooks, 2011; Cubbage and Brooks, 2012; Szmit, 2015; Terje, 2016). On the other side, authors Herley and van Oorschot (2017: 1) deny the development of security science in their comprehensive academic perspective by claiming that "[T]he security community is not learning from history lessons well-known in other sciences, and that the practices on which the rest of science has reached consensus appear little used or recognized in security, and a pattern of methodological errors continues unaddressed". However, it is less important to quibble over whether security is a science than it is to lay out a, efficient model for assessing security risks. It is certainly the case that security has moved to the forefront of societal concerns, and by that it deserves to be discussed within the contemplations of new risk management approaches.

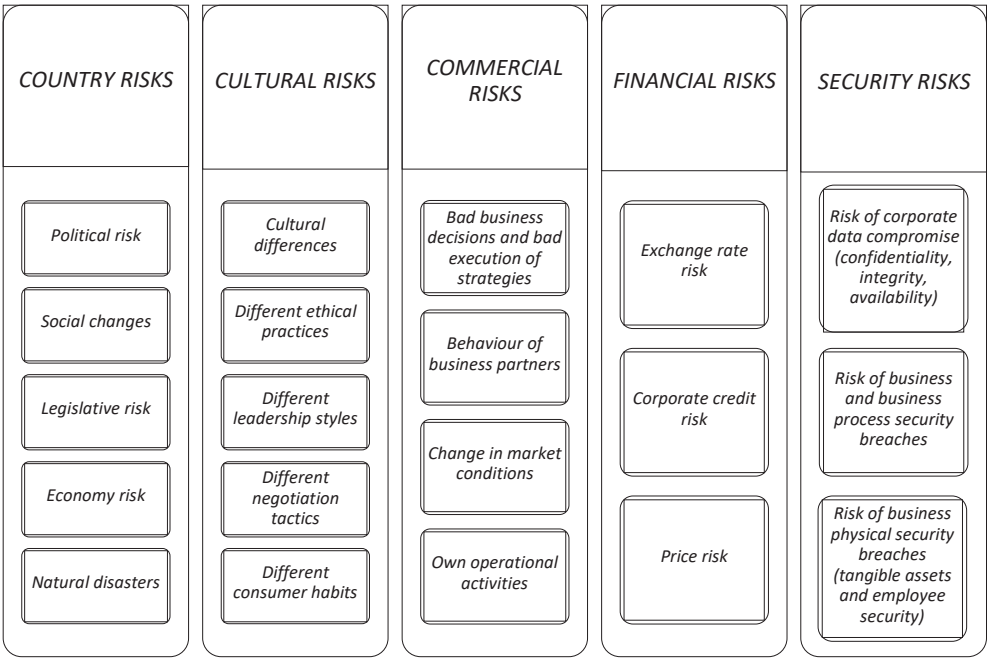
The concept of risk management as a formal discipline emerged throughout the corporate sectors and has become a well-established discipline. The Risk Management International Standards Organization (ISO) 31000:2009 standard, considered the international benchmark should question for its suitability for security risk management, as it fails to address the specific security risk concepts such as threat, vulnerability, and criticality. The majority of risk management models are two dimensional, and a comprehensive security risk management model could be considered multidimensional (Jouni et al, 2015). Therefore, there is an evident need to develop security risk management as a standalone risk management process, incorporating core security risk concepts of threat, criticality, and vulnerability, and to address contemporary business security considerations. Traditionally, the risks associated with international business operations are divided into country risk, cultural risk, commercial risk and financial risk (Lazibat et al, 2020: 394). Security risk is often integrated into one of these traditional risk categories based on their effects on a particular aspect of business, but this fails to recognize the reality of the contemporary risk landscape. In other words, the security considerations of contemporary business operations are too extensive and complex field for examination through the traditional and existing risk categorization. But perhaps it is best to start with an overview of traditional understanding of the risks associated with International Business operations. According to Lazibat et al (2020: 394-404), country risk is the primary category of risk and refers to the possibility that changes in the environment in a foreign country result in a negative impact on business operations, profitability or value of company assets. Cultural risk refers to the risk that

misunderstandings caused by cultural differences will have a negative effect on business. According to the same source, commercial risk refers to the failure to achieve business goals due to poor business decisions, and financial risk refers to the possible instability of the financial market and the adverse impact of the same on the profitability of the company. Although the above classification of risks covers almost all aspects of international business, as well as a broad range of risk events and their consequences, recent experiences suggest that contemporary threats can cause extremely negative effects on businesses and business operations that far surpass those encompassed by the traditionally defined individual categories. Central to the specificity of security risk is its fundamental character. Namely, apart from the fact that it is highly complex and can have disproportionate negative effects on multiple aspects of a business, security risk is much more unstructured than other risks in international business. Security risks are constantly evolving and are comprised of threat actors who act against public and private entities with malicious intentions. Quite often risk mitigation efforts provide effective countermeasures for only a limited time.

4. NEW CATEGORIZATION OF RISKS IN INTERNATIONAL BUSINESS

Newsome (2014) and Szmit (2015), argue that security is considered a form of risk, applied within the management approach of risk management. Therefore, it is to conclude that the security risk management should be a subdomain of risk management, and it should represent a more thorough approach than the generic risk management. Others like Stroie and Rusu (2011) and Smith and Brooks (2013) define the risk is the possibility of incurring loss, misfortune or an undesired outcome, which is certainly distinct from security. However, all of them agree that any of the existing generic risk management models lack key concepts and processes necessary for effective design, application, and mitigation of security risks (Smith and Books, 2013: 52). The dispersion of security risks and their incorporation into the existing categorization of risks in international business makes it impossible to effectively and comprehensively consider this issue, and ultimately prevents the effective management of this type of risk. Security risks have matured to the point that they require its own "philosophy" to navigate challenges of risk methodology, ethics, decision making, modelling choices, and interpretations. Therefore, security risks, due to their complexity, seriousness and possible consequences for business, require their own classification in the division of business risks in international business.

Figure 2. Classification of risks in international business and the new security risk



Source: Lazibat T., i dr. (2020). Međunarodno poslovanje. Sveučilište u Zagrebu, Ekonomski fakultet, p. 394. and authors' addition of "security risks".

Based on the contemporary theoretical approaches to security risk management, as a separate category of risk in international business, security risk should as a minimum include the risk of data security compromise[15], the risk of business and business process security breaches, as well as the risk of business physical security breaches (loss of tangible assets and employee security).

4.1. The risk of data security compromise

The risk of data security compromise refers to the risk of compromise of intellectual property and other sensitive data owned by the company. The possible compromise of intellectual property and other sensitive data can have negative effects on

[15] Data security compromise refers to the traditional definition of compromise from an information security perspective: confidentiality, integrity, and availability. It is important to understand that data does not have to be destroyed (when integrity is compromised) in order for businesses to suffer negative consequences. Businesses can suffer negative effects from "leaks" (when confidentiality is compromised), as well as from "Denial of Service" attacks (when availability is compromised).

commercial entities in the international market, including reduced competitiveness, decreased profitability and damaged prospects for future growth. Unauthorized access to company-owned data through cybercrime violates the secrecy of business contracts, operations, financial transfers, as well as damaging the reputation of the company. For example, digital payment systems are important facilitators of international business and e-commerce as its integral parts. Successful employment of these digital payment systems, however, besides appropriate regulatory environments and cooperation between governments and banks, requires the implementation of security mechanisms which are intended to protect businesses and their customers (personal information, bank and credit card information, and other sensitive data). As such, compromise of such systems can result in great damage to both public and private enterprises, as well as to their customers. ISO 27001 standard outlines the requirements for and information security management system, and provides an outline for information security risks assessment. However, recent study shows that 71 percent of medium-sized business (250 to 550 employees) do not have an information security policy in place (Kaspersky Lab, 2020), which is, in context of digitalized economy, unacceptable. Damaging consequences of data security compromise include, but are not limited to financial loss (drop in share price, penalties, and customer compensation), reputational damage, and possible legal actions (lawsuits). In efforts to protect against this type of security risks, companies operating in the international market are responsible for taking all necessary measures to protect their data and intellectual property from unauthorized access according to the World Intellectual Property Organization (WIPO, 2019). In addition to registering intellectual property through defined procedures, commercial entities manage this risk to their data by signing Non-disclosure (NDA) contracts with partners, clients, and employees in the international marketplace (Hyatt, 2018). Data risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires a careful analysis of threat and vulnerability of information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur (Jouini et al, 2015: 508).Furthermore, the implementation of certain "best practice" security measures in business is recommended and in some cases required, such as the protection of information systems on which data is stored (business plans, financial data, projections, projects, personal data on employees and partners, etc.). Also, as defined by the theory of risk management, this risk can be mitigated through the transfer of risk, either to insurance companies or to specialized companies that deal with the protection and supervision of information systems, avoidance of risks, or reduction of risks (Boban et al, 2003: 84).

4.2. The risk of breaches to the security of business and business processes

This security risk refers to the risk of third parties targeting the company through the disruption of its business processes, often with the intention of furthering their own financial or ideological aims. Common examples of such breaches are third-party interference in business communication (so-called Business Email Compromise Fraud - BEC) and the diversion of financial payments to fraudulent the bank accounts of malicious actors. According to a EUROPOL report, between the 2nd and 3rd quarters of

2020, there was a marked increase in the quantity of this type of corporate fraud compared to the period before the onset of COVID-19, and the amount of funds lost by companies was significantly higher than had previously been recorded. Business email compromise is an advanced type of attack that leverages identity deception through phishing schemes to use company's employees or its customers to make fraudulent payment requests (Pomerleau, 2020: 67). The attack on INA d.d. [16] is also a good example of this type of security risk, as the attackers not only gained unauthorized access to INA's ICT network and data, but also disabled all Point of Sale devices, and thus disrupted key business processes and caused financial and reputational damage to the company. Studies show that in average it takes 23 days for an organization to recover from such an attack (Pomerleau, 2020: 68). Additionally, complicating matters is the recent trend of increased telework (remote work). Research shows that the United States has experienced a 300 percent increase in the use of videoconferencing platforms since the start of the pandemic, while in Thailand, data traffic from Zoom and Skype increased by 828 and 215 per cent respectively between 01 January and 19 March 2020 (UN, 2021: 38). In adapting to conditions mandated by COVID-19, companies are increasingly exposed to the risk of business and business process security breaches, as it is not possible to equally protect the ICT resources and communication channels of employees who operate outside the company's security infrastructure, as those that are physically located on company premises. This security risk is in direct correlation with the development of the Business Continuity Management (BCM) function. As Smith and Brooks argue, BCM is not subservient to risk management, but rather is a function that can support risk management with a mitigation strategy, and the most effective approach is to use risk management as the "informing" process, much like a threat assessment informs the "likelihood" component of security risk management (Smith and Brooks, 2013: 205).

4.3. The risk of business physical security breaches

Physical or corporate security is the function in charge of avoiding or mitigating a specific type of risks that affect an organization's personnel, goods, and knowledge through a wide range of activities, both preventive and reactive (Garcia et al., 2021: 4). The risk of business physical security breaches (to include employee security breaches) is the type of security risk that can be most associated, but not equated, with traditional interpretations of security risk. Namely, the security risk to the physical property and security of employees does not focus on the financial aspects of risk, but only the physical security aspect. This category of risk can be closely linked to political instability and social change. Of course, as with country risk, not all businesses are exposed to this type of risk by default. This type of risk can occur for all businesses that are physically present in a potentially unstable country, only for those businesses that belong to a particular industry, or only for specific companies or specific industries (Lazibat et al., 2020: 398).

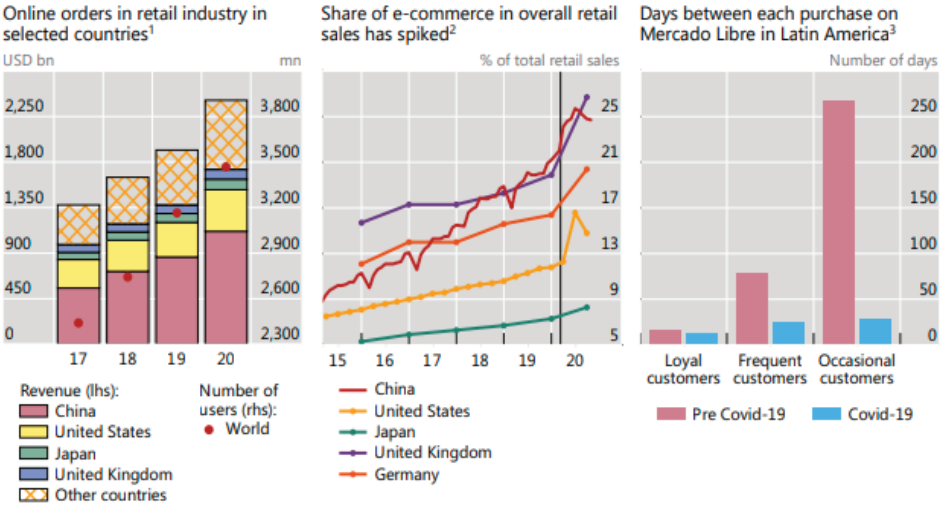
[16] Attack on INA d.d. network happened in October of 2019. Namely, although the attack was discovered in February of 2020 when a number of business processes came to a standstill thus triggering alarms, publicly available sources indicate that INA's ICT network was compromised with malicious code at least four months earlier.

Physical security encompasses the security of enterprise-owned infrastructure, control of access to infrastructure, and compliance with national legislation regulating employee safety. Furthermore, depending on the activity of the company and the countries in which it is physically present, there may be specific risks related to employee safety (and health if working in a country with a high incidence of infectious diseases, or if they are engaged in work involving hazardous materials). Furthermore, companies present in politically and economically unstable environments must perceive this risk in terms of exposure to terrorist or other radical activities. In such cases, a proactive approach in mitigating this risk is necessary to avoid potential catastrophic consequences.

5. PANDEMIC AND THE NEW SECURITY LANDSCAPE

As outlined earlier, globalization in economic terms is primarily a business opportunity, but companies operating in the contemporary international market must consider security risk as a new category of business risk. Although security risks are faced by all companies, including those operating solely in national markets, the globalized nature of international markets make for greater security risk exposure. It is true that e-commerce companies that operate exclusively in national markets, in their own language and within a national cyberspace, are rarely attacked by cybercriminals due to their limited business reach. But it is also true that such companies are increasingly rare, and that it is increasingly difficult to find a company that is not involved in international business in at least one of its segments. Contemporary companies that operate in the international market, although not necessarily physically present in a particular geographical area, are more visible and exposed to a number of malicious actors that can be positioned anywhere in the world. Businesses involved in e-commerce are particularly exposed to these security risks. Since the appearance of COVID-19 in 2020, the coronavirus pandemic has accelerated the digital revolution and increased the role of the ICT technologies and infrastructure for even the most basic business processes, without which even the most basic outlines of the new business normalcy would be unthinkable. It is the combination of these two factors that has led to the highest growth in online sales on record in the past twelve months.

Figure 3. Rise of e-commerce in the pandemic



The black vertical line in the centre panel indicates 11 March 2020 (World Health Organization declares the Covid-19 to be a pandemic).

[1] Data as of August 2020. [2] Data as of November (US), October (CN) and September 2020 (DE, JP and UK). [3] Pre Covid-19: from 24 February 2019 to 23 February 2020. Covid-19: from 24 February 2020 to 19 April 2020.

Source: Bank for International Settlements (2021): "E-Commerce in the pandemic and beyonf", BIS Bulletin, No. 36., January 2021., pg.2. Available on: https://www.bis.org/publ/bisbull36.pdf

To put things in an empirical perspective, in 2016 only about 400 mil. people purchased goods or services via the internet globally, while in the 2020 that number increased to more than one billion. Further illustrating this trend, studies show that in 2020, e-commerce represented 21,3 per cent of all retail sales, with a clear tendency towards increasing (Digital Commerce 360, 29 Jan 2021). In parallel, an exponential increase in cybercrime was reported. The VPN provider Atlas reports that the number of phishing sites more than trebled between January and the middle of March 2020, as the pandemic spread globally. Google reported a global surge in phishing sites, reaching a total of more than two million by late 2020, which was a 19 per cent increase over 2019 (Lyons, 2020). Amidst this unprecedented growth, it is interesting to note that according to same reports, 86 per cent of breaches were financially motivated and 10 per cent were motivated by espionage. Additionally, it is a generally accepted belief that the level of participation in the digital technology and the quality of available internet services are the best indicators of an economy's capacity to leverage e-commerce (UN, 2021: 32). But in the new environment, success does not depend on the quality of infrastructure alone. Increasingly, the security of business operations is playing as important a role as the quality of infrastructure. The pivots that the businesses made since the start of pandemics

to keep up with customers' shifting needs and the need to institute innovative ways of staying relevant on the market, constitute a new strategic approach to security. This approach must be able to accommodate a new security landscape

6. CONCLUSION

Risk assessment and risk management are established as a scientific field and provide important contributions in supporting decision-making. Security as a field is still developing, and whether it will be further developed as a science or it will remain a sub-discipline is irrelevant for the topic. However, security risks have developed to the point that they deserve their own philosophy. Basic principles, theories and methods of security risk management exist and they are continuously developing. This review paper has placed its focus on recent work and advances covering the fundamental ideas and thinking on security risk management. Given the various forms of risk to which business participating in international trade are exposed, and due to the increasing need to protect employees, assets and customer data, it is necessary to develop security mechanisms and practices that will protect public and private enterprises, as well as their ICT infrastructure in order to maintain the continuity of international business. At the forefront of these risks are the risks associated with contemporary security threats such as transnational cybercrime and as such represent a new form of security risk. Fortunately, the challenge posed by these risks is not without precedent, and previously developed methods and practices do shed light on appropriate courses of action. As risk management methodology prescribes, these types of risk can be effectively mitigated through the development and implementation of new policies and risk response capabilities at the enterprise level. In this sense, it is important that companies operating in the international market perceive emerging risks in a timely manner and focus on minimizing the negative effects on business operations from the occurrence of a risk event. The contemporary concept of security risk management and mitigation in international business must be focused on preventive action and partnership, with the active participation of both public and private entities. These actors must strive to implement preventative security practices and minimise the harmful effects of security risk events. In addition, evidence suggests increased security and data risks in countries that have weak legal and regulatory frameworks for cyber security and data protection. Thus, success in mitigating business security risks also depends on governments and business working together to create legislation that will improve digital infrastructure, facilitate digital payments and establish appropriate legal and regulatory frameworks for online transactions and security. The pandemic has demonstrated the dependence of the entire society on information technology and digital economy. To be able to efficiently participate in the new environment and successfully manage the uprising security risks, businesses must disseminate information from various sources to facilitate responses to emerging threats. Fundamentally, those engaged in international business must address these simple questions: What are the weaknesses of our existing security infrastructure? How will new digital business practices influence our position on the international business market?

What are the costs and benefits of our security investments? How can we improve security of business operations with our existing resources? What priorities should shape further security investment? Thoroughly answering these questions will provide a solid grasp of which security risks need to be addressed, and in which order of priority. The answers to these questions provide an overview for identifying the status of current risks, as well as their effects on business objectives. From this overview it is possible to develop solutions that specifically meet those needs can be assessed. This paper has highlighted the need for a more systematic approach to mitigating security risks in international business, and proposed an improvement of the existing risk categorization. This paper also presents an opportunity for further scientific research which should investigate the correlation between the success of the companies with international presence and their approach to security risks.

REFERENCES:

1. Bank for International Settlements (2021): "E-Commerce in the pandemic and beyonf", BIS Bulletin, No. 36., January 2021., pg.2. Available on: https://www.bis.org/publ/bisbull36.pdf
2. Boban, M., Požgaj, Ž., Sertić, H. (2003). "Strategies for successful software development risk management", *Managemen: Journal of Contemporary Management Issues*, 8(2), pp 77-91.
3. Brooks, D.J., 2011. Security risk management: A psychometric map of expert knowledge structure. International. Journal of Risk Management 13 (1/2), 17–41.
4. Cubbage, C., Brooks, D. (2012). *Corporate Security in the Asia-Pacific Region*. Crisis, Crime, Fraud and Misconduct. CRC Press: Boca Raton.
5. Garcia, J.E:, Encias, L.H., Dominguez, A.P. (2021). A Comprehensive Security Framework Proposal to Contribute to Sustainability. *Sustainability 2021*, 13, 6901. https://doi.org/10.3390/su1312690
6. Herley, C., Van Oorschot. P.C. (2017). SoK: Science, Securita and the Elusive Goal of Security as a Scientific Pursuit. IEE. Available on: https://ieeexplore.ieee.org/document/7958573
7. Hyatt, P. (2018). 4 ways to protect your intellectual property in foreign markets. Available on: https://www.tradeready.ca/2018/topics/feasibility-of-international-trade/4-ways-protect-intellectual-property/
8. Išoraitė, M. & Miniotienė, N. (2018). "Electronic Commerce: Theory and Practice". *IJBE (Integrated Journal of Business and Economics)*. Vol2. No73. 10.33019/ijbe.v2i2.78.
9. Jouini, Mouna & Ben Arfa Rabai, Latifa & Khédri, Ridha. (2015). A Multidimensional Approach towards a Quantitative Assessment of Security Threats. Procedia Computer Science. 52. 507-514. 10.1016/j.procs.2015.05.024.
10. Kaspersky Lab (2020). Kaspersky Security Bulletin 2020 Statistics. Available on: https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/

11. Lazibat T. i dr. (2020). *Međunarodno poslovanje*. Sveučilište u Zagrebu, Ekonomski Fakultet Zagreb.
12. Lyons, K. (2020). "Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week". The Verge (News item). Available at: https://www.theverge.com/2020/4/16/21223800/google-malwarephishing-covid-19-coronavirus-scams.
13. Meushaw, R. (2012), What is security science?, Oct 19, 2012. http://cps-vo.org/node/6041.
14. Newsome, Bruce. (2014). A Practical Introduction to Security and Risk Management.C A: Sage.
15. Pomerleau, P.L., Lowery, D.L. (2020). *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection*. Palgrave MacMillan, Panama City, FL.
16. Radebaugh, ., Sullivan, D. (2007), International Business: Environments and Operations (11th ed.). Pearson/Prentice Hall.
17. Rezek, Chris, O'Halloran, Derek, Kaplan, James M., Marcus, Alan, Bailey, Tucker. (2015). *Beyond Cybersecurity : Protecting Your Digital Business* . Hoboken, New Jersey: John Wiley & Sons.
18. Ristovska, K (2014). *The Impact of Globalisation on Business*. Available on: https://core.ac.uk/download/pdf/33812244.pdf
19. Smith, L.C., Brooks, J.D. (2013). *Security Science: The Theory and Practice of Security*. MA: Elsevier.
20. Stroie, E.R., Rusu, A.C. (2011). Security Risk Management - Approaches and Methodology. *Informatica Economică*, vol. 15, no. 1. Available on: https://core.ac.uk/download/pdf/6612749.pdf
21. Sulmeyer, M. (2017). "What the Rise of Russian Hackers Means for Your Business". *Harvard Business Review*, 12. svibnja 2017. Available on: https://hbr.org/2017/05/what-the-rise-of-russian-hackers-means-for-your-business#
    World Intelectual Property Organization (2019). Intellectual Property Issues in International Business. Available on: https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_uln_13/wipo_smes_uln_13_t_park.pd
22. Szmit, M (2015). Security Management and Risk Management Approach in Cybersecurity and Information Security Management. Available on: https://www.researchgate.net/publication/277009090_SECURITY_MANAGEMENT_AND_RISK_MANAGEMENT_APPROACH_IN_CYBERSECURITY_AND_INFORMATION_SECURITY_MANAGEMENT
23. OECD (2020a) E-commerce in the times of COVID-19. Paris: OECD. Available at: https://read.oecd-ilibrary.org/ view/?ref=137_137212-t0fjgnerdb&title=E-commerce-in-the-time-of-COVID-19.
24. Terje Aven (2016). Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, Volume 253, Issue 1, p. 1-13

25. UN (2021). "Covid-19 and E-commerce: A Global Review". United Nations Conference on Trade and Development. NY. Available on: https://unctad.org/system/files/official-document/dtlstict2020d13_en.pdf
26. US Commerce grows 44% in 2020. Digital Commerce 360, 29 January 2021. Available on https://www.digitalcommerce360.com/article/us-ecommerce-sales/#:~:text=Online's%20share%20of%20total%20retail,2019%20and%2014.3%25%20in%202018.
27. Williams, C.M:, Chaturvedi, R., Chakravarty, K. (2020). "Cybersecurity risks in the pandemic*", Journal od Medical Internet Research* 22(9). Available on: https://www.jmir.org/2020/9/e23692/

UPRAVLJANJE SIGURNOSNIM RIZICIMA U MEĐUNARODNOM POSLOVANJU

Nikola Brzica & Ivana Brzica

Sažetak

U radu se analizira postojeća teorija upravljanja rizicima u međunarodnom poslovanju, kao i učinci globalizacije i digitalne transformacije na razvoj sigurnosnih rizika. Pored analize ključnih elementa globalizacije i digitalne transformacije, ovaj rad ističe sustavno upravljanje sigurnosnim rizicima u međunarodnom poslovanju i zasebnu kategorizaciju u identifikaciji rizika kao imperativ za sustavno upravljanje sigurnosnim rizicima. Sustavno upravljanje sigurnosnim rizicima daje sigurnost svim dionicima poslovnih procesa da će se novčane transakcije biti sigurne, da će se kupljena roba isporučiti, i da podaci neće biti uništeni, i/ili dostupni neovlaštenim trećim stranama. Suvremeni koncept upravljanja sigurnosnim rizicima u međunarodnom poslovanju mora biti usmjeren na preventivno djelovanje i partnerski odnos, pri čemu se očekuje aktivno sudjelovanje svih poslovnih entiteta uključenih u međunarodno poslovanje u realizaciji sigurnosne prakse i sprječavanju štetnog učinka rizika. Rad ističe kako se ovom vrstom rizika se može učinkovito upravljati kroz razvoj i implementaciju novih politika i sposobnosti odgovora na rizike na razini poduzeća. U tom smislu, bitno ga je da ga poduzeća koja posluju na međunarodnom tržištu pravovremeno percipiraju, i usmjere se na minimiziranje negativnih učinaka na poslovanje. Autori iznose teorijski pregled upravljanja sigurnosnim rizicima i predlažu novu kategorizaciju rizika u međunarodnom poslovanju. Kao zasebna kategorija u identifikaciji rizika u međunarodnom poslovanju, sigurnosni rizik bi trebao obuhvatiti rizik od narušavanja sigurnosti podataka, rizik od narušavanja sigurnosti poslovanja i poslovnih procesa kao digitalne sigurnosne rizike, te fizički rizik od narušavanja fizičke sigurnosti poduzeća (gubitka materijalne imovine i sigurnosti zaposlenika).

Ključne riječi: *međunarodno poslovanje; e-trgovina; sigurnosni rizici; upravljanje rizicima.*