Entrepreneurship
ISSN: 2738-7402
DOI: 10.37708/ep.swu.v12i1.2 *Volume: XII, Issue: 1, Year: 2024, pp. 8-20*

EXPLORING BIVARIATE CORRELATIONS IN CYBER RISK ON AN INDUSTRIAL LEVEL: EMPIRICAL EVIDENCE FROM GREECE AND THE EUROPEAN ECONOMIC AREA

Maria Koutsari[1]

Received 31.03.2024, Accepted: 29.04.2024

Abstract

In the rapidly evolving domain of cybercrime, understanding the intricate dynamics between industry-specific characteristics and cyber risk ramifications is critical for developing robust risk management strategies. This study delves into the bivariate relationships between annual cyber-attack rates and various industry attributes. Utilizing time-series data as well as both Pearson and Kendall correlation analyses, we assess the linear and ordinal associations across a comprehensive dataset encompassing multiple industries. Our findings reveal that the telecommunications and digital infrastructure industries display a significant inverse relationship between cyber incident rates and systemic risk, an unexpected observation indicating that improved awareness or control of systemic risk may lead to reduced incident rates. On the other hand, the banking sector's direct correlation suggests that as systemic risk rises, so do incident rates, likely because of the sector's attractive high-value data targets. The outcomes of this bivariate exploration complement our previous empirical analysis presented in the article The Financial Impact of Cyber Risk: Empirical Evidence from Greece and the European Economic Area, conducted by the same author, offering a granular view of the cyber risk landscape. This paper aims to inform stakeholders on the pivotal interactions between industrial dynamics and cybersecurity outcomes, fostering informed strategies to mitigate risk and safeguard economic interests.

Keywords: *cybersecurity; incident rate correlation; systemic cyber risk; cyber-attack costs; Greece; European Union.*

JEL-Codes: *G32, L86, O32, C81, G38*

Introduction

Cyber threats not only pose individual risks but also have the potential to disrupt entire industries and economies thus a new definition emerged over the past decades, that of cyber risk. The attacks themselves are often labeled as cyber incidents, which can subsequently manifest in various types, each carrying distinct risks and potential impacts. Some of the most common types include data breaches, malware encrypted attacks, phishing and insider threats. A data breach or privacy violation is the

[1] PhD Student at the Faculty of Economics, South-West University "Neofit Rilski", Blagoevgrad, E-mail: mkoutsari2@gmail.com, ORCID ID: 0000-0003-1847-0556

unauthorized access to or disclosure of personal information, such as financial records, health information, or personal identifiers, while a malware is a malicious software that encrypts the victim's files, with the attacker demanding a ransom to restore access. Phishing, which has become very famous over the past recent years, is defined as the fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communication. The industrial, technological and digital revolutions, which began in 1780 and are still going strong today, have led among others to the rise of cyber risk (Todorov et al., 2023). Hence, as we navigate the complexities of the digital age, understanding the implications of this type of cybercrime becomes increasingly indispensable not only for public sectors around the world but also for businesses operating in cross-markets.

Cyber-attacks matter significantly not only for individuals but also for organizations and industries at large. For individuals, a cyber-attack can lead to identity theft, financial loss, and privacy violations. For organizations and industries, the stakes are even higher. Cyber-attacks can disrupt business operations, lead to significant financial losses, damage brand reputation, and erode customer trust. Moreover, in certain industries, such as healthcare and finance, cyber incidents can also pose risks to national security and economic stability. The financial implications of cyber incidents are particularly alarming. The direct costs include expenses related to incident response, forensic investigation, data recovery, legal fees, and regulatory fines. Indirect costs can be even more substantial, encompassing long-term reputational damage, loss of customer trust, and competitive disadvantage. Additionally, systemic risks may arise when multiple organizations within an industry or supply chain are impacted, potentially leading to broader economic disruptions. To protect against these risks, modern industries and the public sector must adopt a multifaceted approach to cybersecurity. This involves not only investing in technology-based defenses like firewalls, antivirus software, and intrusion detection systems but also implementing comprehensive risk management strategies. Key components of an effective cybersecurity strategy include risk assessment, employee training, data encryption practices and incident response planning.

For years, both Greece and the European Union have been attempting to tackle the consequences caused by cybercrime. The European Union's decentralized Agency for Cybersecurity (ENISA) has been collaborating with thousands of European private and public entities since 2004. This collaboration aims to gather and record dependable data concerning data breaches, security incidents, privacy infringements, and phishing attacks. Furthermore, the Hellenic CSIRT, under the National Cyber Security Authority (NCSA), coordinates Greece's cybersecurity incident responses, collaborates nationally and internationally to bolster defenses against cyber threats, and operates a 24/7 response center to address reports from agencies, businesses, and citizens.

Last but not least, Artificial Intelligence (AI) has become a pivotal ally in combating cyber threats, opening up innovative avenues for bolstering cybersecurity measures in Greece and abroad. By researching through multidimensional datasets, AI can uncover patterns and irregularities hinting at potential cyberattacks. This capability enables proactive threat identification and rapid mitigation efforts. AI-enhanced security frameworks automate the scrutiny of network behavior, pinpoint weaknesses, and even forecast imminent attack strategies by analyzing prevailing trends. Additionally, AI contributes to bridging the cybersecurity expertise void by streamlining standard operations, thereby freeing up human specialists to tackle more intricate issues. Nonetheless, it is crucial to recognize that as AI technologies evolve, cyber adversaries might also exploit these advancements for malicious aims, underscoring the need for continuous innovation and evolution in cybersecurity tactics, ensuring that defenders remain consistently a step ahead of attackers.

1. Literature Review

Modern markets open up new opportunities for radical changes in the organization of the economic system (Stavrova et al, 2021). The dynamics of contemporary business development, which are linked to the pursuit of avenues for future innovation and growth, as well as the enhancement of businesses' financial standing and competitiveness, establish the necessity of their digital transformation (Filipova et al, 2023). According to Stavrova (2021a), with the introduction of intelligent technologies, the technological revolution has seriously affected people's lives by integrating them into every social aspect. The influence of cybercrime across various sectors of the economy has only become a significant area of study in the past twenty-five years. Despite growing awareness and proof of the damages caused by cyber risk, academic research on this topic has been scarce, particularly concerning Greece, with most studies being conducted by consultancy agencies, cybersecurity firms, and private institutions. A study conducted by Anderson et al. (2013) concluded that society is highly inefficient in combating cybercrime, comparing cybercriminals to terrorists or metal thieves in terms of the disproportionate costs they impose. The authors suggest that, based on their findings, resources should shift from preemptive measures (like antivirus software and firewalls) towards more active responses, such as pursuing and prosecuting cybercriminals. However, most studies reveal an actual lack of agreement on how to define and quantify cyber risk and its implications. A key consideration in understanding cybercrime is determining if its effects can be quantified financially. Hence, the notion of cyber risk emerged through the financial analysis. Based on Cebula & Young (2010) cyber risk can be said to be the risk to the operations of information and technology assets that could compromise the confidentiality, availability, or integrity of information systems. Aldaroso et al. (2022) attempted to identify the driving factors of cyber risk in the modern world. They found that larger companies and incidents affecting multiple organizations simultaneously incur greater costs. Interestingly, events driven by malicious intentions (such as cyber-

attacks) generally result in lower costs, except when they are among the most severe losses. Research and technological development are often presented as the only way to product innovative goods on the market and a way to make a company competitive (Yuleva, 2019). A pivotal research study conducted by Romanosky (2016) examined over 12,000 cyber incidents in the US only. His findings reveal that the financial damage to firms from such incidents is considerably lower, while calculating the average cost of a cyber-incident at ca. $200,000, which is comparable to the annual IT security budget of a firm, and this only constitutes 0.4% of their anticipated yearly income. In the meantime, Dreyer et al. (2018) developed a flexible and transparent method for estimating current and future global costs of cyber risk, acknowledging the significant uncertainty in the incidence and financial impact of cyber events. This approach identifies potential financial risks by country and industry sector, calculates direct costs by examining financial exposures and their vulnerability to cyber incidents, and assesses systemic costs across sectors in over 60 countries using OECD data. The model incorporates uncertainty through various probability distributions and allows for extensive customization to explore different scenarios, including the impact on GDP and potential effects of cyber controls. It also suggests areas for future research, such as exploring downstream systemic effects and enhancing the model with sector-specific data or expert insights. Das & Nayak (2013) argue that while government involvement is crucial, the primary responsibility for preventing cybercrime falls on commercial software developers and entities capable of combating fraud.

Digital financial services, offered by both the public and private sectors, play a crucial role in the modern economy's growth but have been consistently targeted by ongoing cyber incidents. In a pivotal empirical research, Bederna & Szadeczky (2023) introduced the "Effect of incidents" metric to gauge the financial impact of unplanned incidents against budgeted plans and the "Incidence of incident recognition" metric to measure the discrepancy between an incident's perceived impact by owners and its actual effect on asset value. On the same page, again Aldaroso et al. (2022) conclude that the financial sector, despite experiencing a higher frequency of cyber-attacks, typically faces lower costs on average. Utilizing cloud services correlates with reduced costs, particularly for smaller-scale cyber incidents. However, as reliance on cloud services grows, it may increase the risk of significant losses. Moreover, as someone would logically deduce, the banking institutions appear to be at the epicenter of the cyber events. An article by Kiss & Gulyas (2023) highlighted the critical role financial institutions play in the global economy and how their attack surface has expanded due to digitalization and increased remote work. They also concluded that currently no-one is immune to cyber-attacks, underscoring the importance of constant vigilance and adopting "zero-trust" policies, despite technological advancements that may help reduce threats, with the acknowledgement that hackers often remain a step ahead.

Cybercrime has significantly impacted both the public and private sectors in Greece as well. In a study conducted by Papanikolaou et al. (2013), the researchers highlight that the telecommunications and government sectors were the primary targets of cyberattacks during the period surrounding the Greek crisis outbreak, namely 2010-2012. They specifically note that Greek governmental bodies are particularly vulnerable due to inadequate cybersecurity defenses, leading to more frequent attacks. Drivas et al. (2020) confirmed a substantial rise in reported incidents over the last ten years, prompting the local authorities such as the NCSA, to implement all necessary measures to combat cybercrime in Greece. Maglaras et al. (2020) concluded that the rapid pace of digital transformation has left legal authorities struggling to keep pace with technological advancements and, consequently, the rise in cyber risk events. In addition, Vagena & Ntelis (2019) urge the European Union to take immediate actions; EU cybersecurity legislative framework has gaps that need to be filled.

2. Research Methodology

As also happened in the article *The Financial Impact of Cyber Risk: Empirical Evidence from Greece and the European Economic Area* by Koutsari (2023), the present study utilizes annual time-series data spanning 2014-2021 comprising information from Greece and various European countries such as the UK, the Nordics, Italy, Germany and France. To determine the yearly count of cyber incidents, this study utilized annual reports from the European ENISA & Hellenic NCSA, while the average financial impacts of cyber incidents by type and industry were sourced from the IBM annual data breach report, employing a detailed accounting approach known as activity-based costing (ABC method). It' is crucial to underline the assumption made in this research that Greek and European accounting standards are compatible, particularly in applying the ABC method. This assumption allows for the adaptation of financial data to the specific context of the Greek business sector for the period between 2014 and 2021. Consequently, the study focuses on seven major sectors of the Greek economy: energy, telecommunications, healthcare, retail, banking & finance, digital infrastructure, and government services. These sectors are composed of various for-profit entities, differing in size, structure, and revenue, and are collectively referred to as "players" within this analysis. The research examines the total number of reported cybersecurity incidents in each sector, broken down by the type of incident and the nature of the information compromised. Additionally, the incident rate (IR) is used to gauge the extent of cyber risk's impact on each sector, following a straightforward equation:

$$IR = \#\ cyber\ incidents\ /\ \#\ industry's\ players \quad (1)$$

To examine the systemic risk across various sectors, we employ a crucial metric termed the debt-to-revenue ratio. Our analysis concentrates on four key sectors:

energy, communications, banking/finance, and digital infrastructure. Within these sectors, we pinpoint the organization deemed "too big to fail" (TBTF) as the leading entity. We assess their exposure to credit risk in relation to the total revenue of the industry by calculating their net short-term and long-term liabilities. As also shown in the article *The Financial Impact of Cyber Risk: Empirical Evidence from Greece and the European Economic Area* by Koutsari (2023), this process incorporates the consideration of yearly fixed effects and is guided by a straightforward formula:

$$SR_{i,t} = Debt_{i,t} / Revenue_{j,t} \quad (2)$$

Here, SR denotes the systemic risk of the leading corporation (i) for the year (t) in relation to the revenue of industry (j). To determine the SR for the retail, health, and public service sectors, a different methodology is necessary, one that integrates macroeconomic indicators such as GDP and national external debt. These sectors contribute differently to the country's overall output and, by extension, to its national debt. To accurately reflect this, specific weights are allocated to each sector: a) Government services: 0.23, b) Healthcare: 0.05, and c) Retail sector: 0.25. As also shown in the article *The Financial Impact of Cyber Risk: Empirical Evidence from Greece and the European Economic Area by Koutsari (2023),* these weights are then applied to the national external debt to assess the weighted credit risk for each relevant sector. The systemic risk for each sector is subsequently calculated using a specified formula:

$$SR_{j,t} = CR_{j,t} / Revenue_{j,t} \quad (3)$$

In this formula, SR signifies the systemic risk associated with industry (j) for the year (t), and CR denotes the weighted credit risk for the same industry in that year.

The Pearson correlation coefficient measures the linear relationship between two continuous variables and is defined (1896) mathematically as:

$$r = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}} \quad (4)$$

Where r is the correlation coefficient, n the number of pairs of scores and x and y are the observed scores between variables X and Y respectively.

Kendall's tau is a non-parametric measure of relationships between two variables. It assesses the ordinal association between two non-linear measured quantities. The formula for Kendall's tau is typically expressed as:

$$\tau = \frac{2}{n(n-1)} \Sigma(i < j) sgn\big(x(i) - x(j)\big) sgn(y(i) - y(j) \quad (5)$$

Where τ is the coefficient, n the number of observations, sgn is the sign function, which is -1 if the argument is negative, 0 if the argument is zero, and 1 if the argument is positive. x(i) and x(j) are the values of the first variable while y(i) and y(j) are the values of the second variable. Last but not least the summation Σ(i<j) is over all pairs of distinct observations.

3. Analysis

We choose six correlation bundles for each of the seven industries in focus. Bearing in mind that, the decision to use Pearson's or Kendall's correlation tests hinges on the data's distribution and the relationship's linearity, we ultimately choose Pearson's r coefficient everywhere (i.e., scale variables) except for the bundle incident rates (IR) and total number of employees (i.e., non-linearity assumption). Therefore, table 1 presents the coefficient results associated with cyber risk across four Greek industrial sectors.

Overall, results suggest that each sector has unique cyber risk profiles; the relationship between cyber incidents and other factors varies widely. The energy sector appears to be impacted the least among the four, with a strong positive statistically significant correlation between incident rates and the industry's revenue.

Table no. 1. Correlation coefficients for 6 bundles across 4 Greek industries

Correlation bundle / Industry	Energy	Comm.	Banking	Digital
IR/SR (r)	0.025	-0.764*	0.59*	-0.595*
	(0.918)	(0.000)	(0.003)	(0.003)
IR/Rev (r)	0.71*	0.829*	-0.508*	0.55*
	(0.001)	(0.000)	(0.01)	(0.007)
IR/Cost (r)	-0.123	0.217	0.376***	-0.106
	(0.616)	(0.309)	(0.07)	(0.629)
IR/Emp (τ)	0.383	0.791*	0.095	0.564*
	(0.106)	(0.000)	(0.665)	(0.000)
Cost/Rev (r)	0.155	-0.005	-0.901**	0.122
	(0.527)	(0.983)	(0.047)	(0.579)
Cost/SR (r)	-0.076	-0.018	0.014**	-0.113
	(0.756)	(0.935)	(0.02)	(0.609)

Note *,** & *** indicate statistical significance at 0.01, 0.05 & 0.10 levels

Source: Authors calculations with IBM SPSS

Hence, higher incident rates correlate with higher revenue, suggesting that as energy companies grow in revenue, they may experience more cyber incidents, possibly due to increased attractiveness as targets or more systems to manage. As for the telecommunications sector, there is a strong negative and statistically significant correlation between incident rates and systemic risk. Telecommunications sector shows the strongest negative correlation, suggesting that high systemic risk correlates with fewer incidents.

This could suggest effective risk management practices are in place, or that higher systemic risk awareness leads to better preventative measures. Additionally, there is a clear, positive, and statistically significant link between the number of incidents and the revenue of industrial companies, highlighting that as telecommunications firms expand their earnings, they might face an increased number of cyber-attacks. This increase can be attributed to their enhanced digital sophistication, which paradoxically makes them more susceptible to such threats.

The finance and banking sector in Greece presents a compelling case study, particularly in the wake of the severe financial downturn that began in 2010. Greek banks have undergone substantial recapitalization efforts to withstand the turmoil caused by the debt crisis, which resulted in widespread financial instability. In terms of cyber threats, Greek financial institutions are notably at risk, contributing to a moderate systemic risk. This risk escalates alongside rising cyber incident rates. Contrarily, banking revenues, unlike other sectors, appear to be well-protected, indicating that banks with higher earnings may have more effective security measures in place, thus experiencing fewer cyber-attack consequences. Furthermore, the banking sector stands out as the singular industry in which average costs per incident exert a tangible influence on industrial revenues and systemic risk. This relationship underscores the reality that financial losses from cyber threats directly affect the financial sustainability of the banking sector. Within the context of Greece, where the lion's share of the market is held by four major so-called systemic banks, the average costs borne by any one of these institutions can have extensive repercussions across the entire sector. Last but not least, the digital infrastructure sector serves as the foundational support for the operations of all other industries, acting as a critical backbone. Based on the results of table 1, a higher systemic risk seems to correlate with fewer cyber incidents, which may indicate that companies are more vigilant and perhaps better at mitigating risks. Same moderate magnitude is also observed in the relationship between incident rates and industrial revenue; higher sector revenue is associated with more incidents, a pattern consistent with findings in the energy and communications sectors. Notably, in both telecommunications and digital industries, cyber risk appears to be linked with the total number of employees in the sector, indicating that industries with larger workforces tend to experience more incidents.

Table 2 summarizes the correlation coefficient results for the public services, the healthcare sector and the retail sector. For government services and healthcare, the economic impact of cyber risk appears to be less directly correlated with the factors considered, pointing towards a potential divergence in how cyber risk is managed and its consequent economic impact within these sectors. This suggests that cyber risks are neither increasing with higher systemic risks nor are they leading to significantly higher costs per incident. However, there is a statistically significant moderate positive correlation between cyber incident rates and the number of employees. This relationship may indicate economic implications where larger departments or more

populous government services could be more susceptible to cyber incidents, potentially due to a larger attack surface or the challenge of managing security across a broader employee base.

Table no. 2. Correlation coefficients for 6 bundles across 4 large Greek industries

Correlation bundle / Industry	GovServ	Health	Retail
IR/SR (r)	-0.038	-0.270	0.036**
	(0.848)	(0.223)	(0.035)
IR/Rev (r)	0.077	0.136	0.121*
	(0.695)	(0.547)	(0.000)
IR/Cost (r)	-0.014	0.249	-0.137***
	(0.943)	(0.264)	(0.078)
IR/Emp (τ)	0.481*	-0.031	0.110
	(0.001)	(0.892)	(0.418)
Cost/Rev (r)	-0.200	-0.197	0.016**
	(0.307)	(0.379)	(0.020)
Cost/SR (r)	0.206	0.066	0.197
	(0.293)	(0.770)	(0.280)
Note *,** & *** indicate statistical significance at 0.01, 0.05 & 0.10 levels			

Source: Authors calculations with IBM SPSS

In the Greek healthcare sector, none of the correlations reach statistical significance, indicating that at the moment cyber risk has minimal or no effect on the country's health infrastructure. The retail sector presents, however, a totally different picture. There is a weak positive correlation between cyber incident rates and systemic risk that is statistically significant. This indicates that, unlike in government services and healthcare, in the retail sector, as systemic risk increases, there is a slight but notable increase in cyber incidents. This could have economic implications such as the need for increased investment in cybersecurity measures as retail businesses grow in scale and systemic importance. Furthermore, there is a statistically significant weak positive correlation between incident rates and revenue, implying that larger, possibly more successful retail entities may face more cyber threats, a trend that aligns with the idea that more profitable businesses can become bigger targets for cyber-attacks. This relationship is economically significant as it points to the need for successful retail businesses to proportionally scale their cybersecurity efforts with their revenue growth. Interestingly, the retail sector shows a statistically significant negative correlation between average costs per incident and incident rates. This could mean that although incidents become more frequent, the cost per incident decreases, perhaps due to economies of scale in addressing cybersecurity issues or more efficient incident management as the frequency increases. This suggests a potential economic benefit in terms of incident management cost reduction as retail entities gain more experience dealing with cyber incidents.

When comparing across the three sectors, the retail sector stands out for having statistically significant correlations that imply a relationship between systemic risk and incident rates, as well as between revenue and incident rates. In contrast, in government services and healthcare, these relationships are either not significant or inversely correlated. The implication here is that retail may be more economically impacted by cybersecurity issues, requiring targeted investment and strategies to manage the associated risks effectively. Moreover, the trend in the retail sector regarding the cost per incident could reflect more mature cyber risk management practices, which could serve as a benchmark for the other sectors.

4. Conclusions and Recommendations

The present paper provides a comprehensive bivariate analysis within the realm of cyber risk across diverse industrial sectors in Greece. Our study delineates the intricate relationships between cyber incident rates and various economic indicators, including systemic risk, revenue, costs per incident, and employment figures, yielding a multifaceted perspective on the cyber-economic landscape.

The telecommunications and digital infrastructure sectors manifest a pronounced negative correlation between cyber incident rates and systemic risk, a counterintuitive finding suggesting that higher awareness or management of systemic risk could coincide with lower incident rates. Conversely, the banking sector's positive correlation in this regard intimates that increased systemic risk corresponds with heightened incident rates, possibly due to the sector's high-value data targets. This divergence underscores the complexity of cyber risk management and the necessity for sector-specific cyber risk strategies. Revenue, as an economic driver, appears to exhibit a consistent positive correlation with cyber incident rates in most sectors, implying that greater financial success might increase vulnerability to cyber threats. The banking sector, however, demonstrates an intriguing negative correlation, suggesting that higher revenue can be associated with fewer incidents, potentially indicative of more robust security measures and risk management strategies being implemented as financial stakes escalate.

When considering the average costs per cyber incident, a noteworthy sector-specific trend emerges. The retail sector is unique in displaying a negative correlation, indicating a potential reduction in the cost per incident as their frequency increases, perhaps due to improved response efficiency. In contrast, the banking sector reveals a weak positive relationship, hinting at increased complexities and associated costs of incidents within this domain. The number of employees further informs our understanding of cyber risk, with sectors such as telecommunications and digital infrastructure indicating a significant positive correlation between workforce size and incident rates. This could suggest that larger employee numbers contribute to increased cyber risk exposure, emphasizing the need for comprehensive personnel training and robust security protocols. Drawing comparative insights, the retail sector emerges as particularly sensitive to the dynamics of cyber risk, demonstrating

economic repercussions tied to both systemic risk and revenue. This sector's adeptness at managing cost per incident with rising incident rates may offer strategic lessons for other industries. These patterns and correlations, unique to each sector, provide a nuanced understanding of the economic implications of cyber risk at an industrial level.

The evidence suggests a compelling interaction between cyber risk and economic factors that necessitates a bespoke, sector-sensitive approach to cybersecurity. Such an approach should integrate risk awareness, financial robustness, and human capital considerations, thereby fortifying respective industries against the evolving landscape of cyber threats. As industries continue to grapple with the challenges posed by the digital revolution, our findings highlight the importance of not only recognizing the distinct cyber risk profiles of each sector but also tailoring prevention and mitigation strategies to these specificities. This tailoring is paramount for safeguarding economic stability and resilience within Greece and, by extension, the broader European Economic Area.

REFERENCES

Aldaroso, I., Gambacorta, L., Giudici, P. & Leach, T. (2022). The Drivers of Cyber Risk. *Journal of Financial Stability*, 60(1). DOI: 10.1016/j.jfs.2022.100989, https://www.researchgate.net/publication/359020072_The_drivers_of_cyber_risk

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). *Measuring the Cost of Cybercrime*. The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-39498-0_12

Bederna, Z. & Szadeczky, T. (2023). Managing the Financial Impact of Cybersecurity Incidents, *Security & Defense Quarterly*, 41(1), 15-35, DOI: 10.35467/sdq/159625, https://www.researchgate.net/publication/368904873_Managing_the_financial_impact_of_cybersecurity_incidents

Cebula, J., & Young, L. (2010). *A Taxonomy of Operational Cyber Security Risks*. Technical Note CMU/SEI-2010-TN-028. CERT Program, https,://apps.dtic.mil/sti/tr/pdf/ADA537111.pdf

Center for strategic and international studies-CSIS & McAfee. (2014). Net losses; estimating the global cost of cybercrime, https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime

Drivas, G., Maglaras, L., Janicke, H. & Ioannidis, S. (2020). Assessing Cyber Security Threats and Risks in the Public Sector of Greece. *Journal of Information Warfare*, 19(1), pp. 96-112. https://www.jstor.org/stable/27033611

European Union Agency for Cybersecurity – ENISA (2020). Annual report on data breach and other threats landscape. Threat Landscape, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/enisas-threat-landscape-and-the-effect-of-ransomware?gad_source=1&gclid=Cj0KCQjwir2xBhC_ARIsAMTXk860eABLiNi5Cq59cIzSrJuc4ynEud9DtxgHrO3mbpzCNx9sGs-ze6EaAmToEALw_wcB

Filipova, M., Yaneva, D. & Mierlus-Mazilu, I. (2023). Specifics of digital transformation in business. *Economics and Management*, 10 (2), 110-121. DOI: 10.37708/em.swu.v20i2.7

IBM & Ponemon Institute - ENISA (2021). The annual report on the costs of a data breach worldwide. Threat Landscape, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/enisas-threat-landscape-and-the-effect-of-ransomware?gad_source=1&gclid=Cj0KCQjwir2xBhC_ARIsAMTXk860eABLiNi5Cq59cIzSrJuc4ynEud9DtxgHrO3mbpzCNx9sGs-ze6EaAmToEALw_wcB

Kiss, G. & Gulyas, O. (2023). Impact of Cyber-Attacks on the Financial Institutions. *Procedia Computer Science*, 84-90. https://www.researchgate.net/publication/375597364_Enhancing_Cyber_Security_in_the_Banking_Sector_with_Chatbot_Assistance

Koutsari, M. (2023). The Financial Impact of Cyber Risk: Empirical Evidence from Greece and the European Economic Zone. *Finance*. 1(1), 69-82. https://espisanie.financebg.com/wp-content/uploads/2024/02/finance-br-1-2023.pdf

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis C. and Ioannidis, S. (2020). Cybersecurity in the Era of Digital Transformation: The case of Greece, *2020 International Conference on Internet of Things and Intelligent Applications* (ITIA), pp. 1-5. https://www.researchgate.net/publication/344819170_Cybersecurity_in_the_Era_of_Digital_Transformation_The_case_of_Greece

Nayak, T. & Das, S. (2013). Impact of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), 142-153. ISSN: 22316604, https://pdf4pro.com/view/impact-of-cyber-crime-issues-and-challenges-6ee450.html

Papanikolaou, A., Vlachos, V., Papathanasiou, A., Chaikalis, C., Dimou, M. & Karadimou, M. (2013). Cybercrime in Greece: How bad is it? 21st telecommunications Forum. *TELFOR*, 1-4. https://scindeks.ceon.rs/article.aspx?artid=1821-32511402086P

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incident. *Journal of Cybersecurity*, 2(2), 121-135, https://doi.org/10.1093/cybsec/tyw001

Stavrova, E., Zlateva, D. & Pinelova, E. (2021). Platform economy as an inevitable development of digital business. *Entrepreneurship*, 9 (1), 87-95. DOI: 10.37708/ep.swu.v9i1.8

Stavrova, E., Zlateva, D. & Pinelova L. (2021a). The digital transformation in the service of business. *Economics and management*, 18 (1), 128-136. DOI: 10.37708/em.swu.v18i1.11, https://em.swu.bg/images/SpisanieIkonomikaupload/SpisanieIkonomika2021/THE_DIGITAL_TRANSFORMATION_IN_THE_SERVICE_OF_BUSINESS.pdf

Strong, A., Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Welburn, W.J, & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk: Methodology and Examples. *RAND Corporation, Justice, Infrastructure and Environment.* DOI: https://doi.org/10.7249/RR2299

Todorov, I., Mirchova, S. & Krasteva, R. (2023/3). Relationships between sustainability dimensions in Greece. *Conference 93rd International Scientific Conference on Economic and Social Development – "Green Economy & Sustainable Development", Cakovec*, 17-31, https://www.esd-conference.com/upload/book_of_abstracts/Book_of_Abstracts_esdCakovec2023_Online.pdf, ISSN: 1849-753

Vagena, E. & Ntellis, P. (2020). Cybersecurity Legislation: Latest Evolutions in the EU and Their Implementation in the Greek Legal System. *EU Internet Law in the Digital Era. Springer, Cham*. https://www.springerprofessional.de/en/cybersecurity-legislation-latest-evolutions-in-the-eu-and-their-/17289522

Yuleva, R., (2019). Competitive advantages and competitive strategies of small and medium-sized enterprises. *Economics and Management,* 17(1), 71-81 https://em.swu.bg/images/SpisanieIkonomikaupload/Spisanieikonomika2019/COMPETITIVE%20ADVANTAGES%20AND%20COMPETITIVE%20STRATEGIES%20OF.pdf