MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

"Regulating cybersecurity in the financial sector: on the prospects of legal harmonisation"

verfasst von / submitted by

Alina Vasilevska, LL.B.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Dr. iur. Roland Vogl

Abstract

While in the first half of 2020, the number of cyberattacks worldwide targeting financial institutions increased by 238% in comparison with previous years[1], and it is estimated that the average cost of a single cyberattack in the financial sector could reach USD 5 million in 2023[2], legally regulating cybersecurity in the financial sector remains a challenging area of international law. The rapid growth of cybercrime and, at the same time, the lack of a unified approach to regulate cybersecurity in the financial sector and the lack of proper amount of scientific research highlight this research's topicality. The study addresses the issues of creating a unified framework for European cybersecurity regulation in the financial sector and establishes the perspectives on eliminating present legal grey areas in European cybersecurity regulation in the financial sector. By analysing the existing theoretical and legal framework of regulating cybersecurity in the European Union and the United States financial sector, the study aims to formulate recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation. The results indicate that it is possible to establish a unified and harmonised cybersecurity regulatory framework for the international financial sector by reforming financial sector cybersecurity regulation and eliminating existing legal grey zones.

Keywords: cybersecurity, cyberattack, financial sector, European cybersecurity regulation, NIS 2 Directive, DORA Regulation, 23 NYCRR 500.

[1] Edward Kost, "The 6 Biggest Cyber Threats for Financial Services in 2023," UpGuard (2023), available on: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services. Accessed January 27, 2023.
[2] Abi Tyas Tunggal, "What is the Cost of a Data Breach in 2023?" UpGuard (2023), available on: https://www.upguard.com/blog/cost-of-data-breach. Accessed May 15, 2023.

Abstract *(in German)*

Während in der ersten Hälfte des Jahres 2020 die Zahl der weltweiten Cyberangriffe auf Finanzinstitute im Vergleich zu den Vorjahren um 238% gestiegen ist[3] und Schätzungen zufolge der durchschnittlichen Kosten eines einzigen Cyberangriffs im Finanzsektor im Jahr 2023 5 Mio. USD erreichen könnten[4], bleibt die gesetzliche Regelung der Cybersicherheit im Finanzsektor ein schwieriger Bereich des internationalen Rechts. Die rasche Zunahme der Cyberkriminalität und das gleichzeitige Fehlen eines einheitlichen Ansatzes zur Regulierung der Cybersicherheit im Finanzsektor und eines angemessenen Umfangs der wissenschaftlichen Forschung unterstreichen die Aktualität dieser Untersuchung. Die Studie befasst sich mit der Schaffung eines einheitlichen Rahmens für die europäische Regulierung der Cybersicherheit im Finanzsektor und zeigt die Perspektiven zur Beseitigung der derzeitigen rechtlichen Grauzonen in der europäischen Regulierung der Cybersicherheit im Finanzsektor auf. Durch die Analyse des bestehenden theoretischen und rechtlichen Rahmens für die Regulierung der Cybersicherheit im Finanzsektor der Europäischen Union und der Vereinigten Staaten zielt die Studie darauf ab, Empfehlungen für Vertreter des europäischen Finanzsektors zur ordnungsgemäßen Anwendung der aktuellen Cybersicherheitsgesetzgebung zu formulieren. Die Ergebnisse zeigen, dass es möglich ist, einen einheitlichen und harmonisierten Regelungsrahmen für die Cybersicherheit im internationalen Finanzsektor zu schaffen, indem die Regulierung des Finanzsektors im Bereich der Cybersicherheit reformiert und bestehende rechtliche Grauzonen beseitigt werden.

Stichworte: Cybersicherheit, Cyberangriff, Finanzsektor, europäische Cybersicherheitsvorschriften, NIS 2-Richtlinie, DORA-Verordnung, 23 NYCRR 500.

[3] Kost, *supra* note 1.
[4] Tunggal, *supra* note 2.

Summary

This Master Thesis aims to assess the issues of creating a unified framework for European cybersecurity regulation in the financial sector, establishing the perspectives on the elimination of present legal grey areas in European cybersecurity regulation in the financial sector, as well as to formulate recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation. In order to achieve the research objectives, the study encompassed doctrinal research with interdisciplinary aspects and a comparative legal analysis with the aim of law harmonisation. The Thesis consists of three parts covering the topic's theoretical and practical aspects.

The first part of the Master Thesis provides a theoretical background of cybersecurity regulations in the financial sector, with a focus on the definition and categorisation of possible cyber threats. Furthermore, it identifies key factors that cause cyber threats in the financial sector, as well as establishes the main legal complications of regulating.

The second part analyses the current legal framework for regulating cybersecurity in the EU and the US financial sector. The analysis includes a detailed assessment of the EU legal framework, namely GDPR, SIPS Regulation, PSD2, CRD IV, CRR, NIS 2 Directive and DORA Regulation and the US legal framework, namely GLBA, SOX and NYSDFS Cybersecurity Regulation. The analysis included as well the assessment of international standards – ISO 27001, NIST CSF and PCI DSS. According to the aforementioned analysis, the limitations of states in harmonising regulation of cybersecurity in the financial sector within the existing legal frameworks are identified.

In the third part, the author proposes a possible means to eliminate present legal grey areas in European cybersecurity regulation in the financial sector, namely its reform by adopting the new legislation proposed by the author – Single European Cybersecurity Regulation for the financial sector (SECYR) prescribing the possible scope of its applicability, as well as substantive and enforcement provisions. In addition, recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation are provided.

Lastly, the conclusions on the existing legal and regulatory framework concerning cybersecurity regulation in the financial sector are drawn, as well as the actual legislative trends of the EU and the US regarding cybersecurity regulation in the financial sector are underlined. The author determines the uniqueness of the proposed reform by adopting the new legislation on the elimination of present legal grey areas in European cybersecurity regulation in the

financial sector and summarises the principal recommendations on the proper application of current cybersecurity legislation for representatives of the European financial sector. In addition, the author states possible further ways of researching cybersecurity regulation in the financial sector and confirms the hypothesis put forward.

Table of Contents

Abbreviations

CRD IV	Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms
CRR	Regulation No 575/2013 on prudential requirements for credit institutions and investment firms
DORA	Regulation 2022/2554 on digital operational resilience for the financial sector
EBA	European Banking Authority
EU	European Union
EUR	Euro
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
IBM	International Business Machines Corporation
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
NIS	Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
NIS 2	Directive 2022/2555 on measures for a high common level of cybersecurity across the Union
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NYDFS	New York State Department of Financial Services
PCI DSS	Payment Card Industry Data Security Standards
PSD2	Directive 2015/2366 on payment services in the internal market
SECYR	Single European Cybersecurity Regulation for the financial sector
SIPS	Systemically Important Payment Systems
SOX	Sarbanes Oxley Act
TLPT	Threat-Led Penetration Testing
US	United States
USD	United States Dollar

Introduction

The twenty-first century has been marked by the rapid development of information technology and the digital world. This progress has brought many changes not only to our everyday lives but also served to update business processes using new technologies. Thus a "digital" trend in the financial sector has emerged, where financial institutions see the provision of digital financial services as a critical factor in increasing access to their services and the corresponding business expansion.[5] It is almost impossible to imagine everyday reality without using e-commerce, cashless payments or online banking services since all this has become an integral part of the modern financial market.

However, where there is a high level of digitalisation, new technologies and money, there are also risks of a cyberattack by individuals who want to exploit cyberspace's unlimited possibilities for illegal enrichment. For this reason, the financial sector is one of the most vulnerable industries to cyberattacks. According to VMware, in the first half of 2020, at the start of the Covid-19 pandemic, the number of cyberattacks worldwide targeting financial institutions increased by 238%.[6] The technology company IBM and the Ponemon Institute found that the average cost of a single cyberattack in the financial sector in 2022 was USD 4.35 million, and it is estimated that the average cost of a single cyberattack could reach USD 5 million in 2023.[7] Overall, according to the European Commission, the annual damage from cybercrime in all industries for the global economy in 2020 amounted to EUR 5.5 trillion, which is twice as much as in 2015.[8]

Undoubtedly, cyber risks did not just emerge yesterday, and both financial institutions and regulators have long been trying to address them. However, until recently, cyber risk was treated as just one form of operational risk of a financial institution, thereby superficially regulating cybersecurity.[9] But, the attitude towards cybersecurity regulation in the financial sector has changed dramatically in the last three years. Several jurisdictions have adopted new legislation regulating cybersecurity, including one of the main subjects of this research, the NIS

---

[5] Anton N. Didenko, "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond," *Uniform Law Review*, Volume 25, Issue 1 (2020): p. 126, accessed March 24, 2023, doi: 10.1093/ulr/unaa006.
[6] Kost, *supra* note 1.
[7] Tunggal, *supra* note 2.
[8] European Parliament. Cybersecurity: why reducing the cost of cyberattacks matters (2022), available on: https://www.europarl.europa.eu/news/en/headlines/priorities/digital-transformation/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters. Accessed January 27, 2023.
[9] Didenko, *supra* note 1, p. 127.

2 Directive[10] and DORA Regulation[11], which entered into force on 16 January 2023 at the European Union level. Given that the development of cybersecurity regulation in the financial sector is in its infancy, there is a notable difference in cybersecurity regulation across jurisdictions, which currently leads to the lack of a harmonised international approach to cybersecurity regulation in the financial sector. Therefore, the rapid growth of cybercrime and, at the same time, the lack of a unified approach to regulate cybersecurity in the financial sector and the lack of proper amount of scientific research carried out highlight the topicality of this research.

The problem of the research is that based on the fact that in the last three years, there has been a rapid increase in cyberattacks in the financial sector, there is a lack of an effective and unified legal regulation approach to cybersecurity in the financial sector and insufficient scientific research as well. In order to find the reason for the lack of effective and unified legal regulation for cybersecurity in the financial sector in Europe, we need to conduct an in-depth study of the practical needs. The hypothesis underlying this research is: despite the different levels of cybersecurity development strategies in the financial sector in different countries and the technological complexities of the financial system and cyberspace, with the reform of the financial sector's cybersecurity regulation and the elimination of the present legal grey areas, it seems possible to establish a unified and harmonised cybersecurity regulatory framework for the international financial sector.

The aim of this project is to study the issues of creating a unified framework for European cybersecurity regulation in the financial sector, establishing the perspectives on the elimination of present legal grey areas in European cybersecurity regulation in the financial sector, as well as to formulate recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation. In order to achieve the aim of the research as well as to examine the hypothesis, the following tasks must be completed:

1. To study the theoretical framework of regulating cybersecurity in the financial sector.
2. Define the concept of cybersecurity in the financial sector, the main types of cyber threats and the factors causing such threats.

[10] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2), *OJ L* 333, 27.12.2022, available on: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Accessed June 13, 2023.

[11] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA), *OJ L* 333, 27.12.2022, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554. Accessed June 13, 2023.

3. To reveal the legal complications of regulating cybersecurity in the financial sector.
4. Analyse the legal framework for regulating cybersecurity in the European Union and the United States financial sector.
5. Examine the effectiveness of applying relevant standards for regulating cybersecurity in the financial sector.
6. To create possible ways of eliminating present legal grey areas in European cybersecurity regulation in the financial sector.
7. To establish practical measures for the proper application of current cybersecurity legislation.

This study includes doctrinal research. Information was obtained from available primary and secondary sources, such as legislation, as well as newsletters, legal articles, journals, and reports from scholars and institutions. A review of the scientific literature was conducted to establish a theoretical framework for this research. Legislative source analysis was used to become acquainted with the provisions contained in the laws and the established phenomena of the research. A comprehensive review was conducted of current problems of legal doctrinal concepts of cybersecurity regulation in the financial sector. Comparative legal analysis was performed, as attention was paid not only to continental legal systems, but common law systems were examined as well. These were ways of acquiring information that could not be obtained otherwise.

The scope of the research is limited to the analysis of legislative acts that are adopted, effective or most applicable to the regulation of cybersecurity in the financial sector. In addition, this research does not consider in detail aspects of criminal liability for cybercrimes or criminal law in general. When analysing the legislative framework, a lack of primary sources was encountered, namely, the absence of relevant judicial practice.

This Master Thesis consists of four parts. In the first part, the author analyses the available scientific literature and establishes a theoretical framework for regulating cybersecurity in the financial sector. In the second part, the author examines and analyses the available legal regulation of cybersecurity in the European Union and the United States financial sector. In the third part, the author proposes a possible means to eliminate present legal grey areas in European cybersecurity regulation in the financial sector and formulates recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation. And in the last fourth part of the research, the author summarises and highlights the main conclusions of the research.

1. Research theoretical framework

Cyberspace is one of the five dimensions along with land, sea, air and space. Cyber is a new global virtual world, a separate dimension without classical external and internal boundaries. A cybercriminal can be located in one country, aim at a target in another country, and cause damage in a third country; however, the actual cyberattack will not come from the first state in which the cybercriminal is physically located but from cyberspace, a separate dimension that does not have a geographic location. Such cyberspace capabilities gave rise to the need for cybersecurity. According to the Cambridge Dictionary, the term "cybersecurity" refers to

> things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet.[12]

As can be seen, cybersecurity has a broad definition and covers a wide range of activities, measures and controls. Within the framework of this research, cybersecurity can be divided into three categories: information security (protecting data integrity and confidentiality), combating cybercrime, and general institutional cybersecurity. Also, within the framework of this study, all attention will be paid to cybersecurity in the financial sector as one of the most vulnerable industries to cyberattacks. The financial sector, under Article 2(1)(a)-(u) of the DORA Regulation, refers to the following financial institutions and their counterparties:

> credit institutions; payment institutions […]; account information service providers; electronic money institutions […]; investment firms; crypto-asset service providers […] and issuers of asset-referenced tokens; central securities depositories; central counterparties; trading venues; trade repositories; managers of alternative investment funds; management companies; data reporting service providers; insurance and reinsurance undertakings; insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; institutions for occupational retirement provision; credit rating agencies; administrators of critical benchmarks; crowdfunding service providers; securitisation repositories; ICT third-party service providers.[13]

Based on the foregoing, the author proposes the following definition of cybersecurity in the financial sector for this research: measures and controls implemented by the financial institution and regulatory bodies to protect the financial institution, its data and financial market integrity in general from cyber threats. Hence, the question of legal regulation of the cybersecurity of the financial sector arises. In order to answer this question, it is necessary to understand what categories of cyberattacks exist, what factors cause them, and what legal complications of cybersecurity regulation currently exist.

---

[12] *Cambridge Advanced Learner's Dictionary & Thesaurus* (Cambridge: Cambridge University Press), s.v. "Cybersecurity," available on: https://dictionary.cambridge.org/dictionary/english/cybersecurity. Accessed February 22, 2023.

[13] Regulation (EU) 2022/2554 (DORA), *supra* note 11.

1.1. Categories of cyber threats

With the development of new technologies, the types of cyberattacks have also acquired a new scale and sophistication. Today's cyberattacks can originate from and affect all ecosystems – states, businesses and individuals, thereby jeopardising the security of all dichotomies of these ecosystems – civil/military, public/private, and external/internal.[14] Cyberattack is one of the so-called "hybrid threats", and according to North Atlantic Treaty Organization (NATO), it is on a par with disinformation, economic pressure, the deployment of irregular armed forces and the use of regular forces.[15] The European Commission explains that

> Hybrid threats refer to when, state or non-state, actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (*i.e.* diplomatic, military, economic, technological) while remaining below the threshold of formal warfare.[16]

Cyberattacks can be attributed to five interrelated types of threats – cyberwar, cyber espionage, cyber terrorism, cyber vandalism, and, finally, cybercrime. This division of cyberattacks into separate categories contributes to understanding and determining the degree of responsibility under national and international law and also allows responsible persons to take the necessary cybersecurity measures concerning each category.

1.1.1. Cyberwar

Cyberwar can be attributed to the first category of cyber threat. At the moment, there is no formal definition of the term "cyberwar" that would clearly define an act of war in the actions of any subject. From the examples of cyberwar assumed in history, it is possible to define cyberwar as a state-sponsored fight carried out through electronic networks directed against an enemy country.[17] Cyberwar is rarely a separate action on the part of the state, most often, it is a continuation of an already existing interstate conflict or political confrontation. The main goal of cyberwar is to disable, disrupt, destroy or prevent the use of government and military networks and the country's critical infrastructures to weaken the enemy country. Experts distinguish several types of attacks by which states carry out cyberwar – propaganda, cyber espionage, cyber vandalism, direct attacks on specific computer systems and servers, and

[14] Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?" *JCMS: Journal of Common Market Studies*, Volume 55, Issue 6 (2017): p. 1255.
[15] North Atlantic Treaty Organization (NATO). NATO's response to hybrid threats (2023), available on: https://www.nato.int/cps/en/natohq/topics_156338.htm. Accessed March 2, 2023.
[16] European Commission. Hybrid Threats, available on: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en. Accessed March 2, 2023.
[17] Imperva. Cyber Warfare, available on: https://www.imperva.com/learn/application-security/cyber-warfare/. Accessed March 2, 2023.

attacks on critical infrastructures.[18] One of the most high-profile cyberattacks equated to cyberwar on its scale to this day is the invasion of the Stuxnet spyware virus or computer worm, developed jointly by the US and Israel and used in 2010 against Iran in order to disable centrifuges on which the Iranians enriched uranium, thereby damaging and slowing down Iran's nuclear program.[19] It should be noted that the results of this cyberwar were very positive – the countries reached the Joint Comprehensive Plan of Action to limit Iran's nuclear program.[20] The most recent cyberwars include the ongoing war between Russia and Ukraine, during which such types of cyberattacks were discovered as mass propaganda from both parties of the military conflict, attempts to gain access to critical infrastructures of Ukraine from Russia, namely, interruptions in water supply, transport communications and power supply networks of Ukrainian cities.[21]

1.1.2. Cyber espionage

The second category of cyber threat is cyber espionage. This act is an unauthorised and often illegal way of gaining access to protected information for use in one's own interests.[22] Cyber espionage is inextricably linked with the concepts of cyberwar and cyber vandalism. Cyber espionage is carried out by circumventing the enemy's cybersecurity system using spyware and is most often carried out by intelligence agencies or hacker groups at their request. Establishing the degree of legal responsibility for cyber espionage is carried out on an individual basis since cyber espionage can be considered a crime in the victim state but may not be considered a crime in the aggressor country which initiated the cyber espionage. Cyber espionage can be classified according to three parameters: 1) direction – economic, political, military or mixed cyber espionage; 2) level – regional, state, or international cyber espionage; 3) object – a high-ranking private person, corporation, or state structure.[23] If the last two parameters are pretty simple in their definition – they classify the scale and victim of cyber espionage, then the directions of cyber espionage need to be analysed in more detail.

---

[18] Imperva, *supra* note 17.
[19] Ben Schaefer, "The Iran Nuclear Agreement as a Deterrent for Cyberattack," Georgetown Security Studies Review (2018), available on: https://georgetownsecuritystudiesreview.org/2018/08/18/the-iran-nuclear-agreement-as-a-deterrent-for-cyberattacks/. Accessed March 2, 2023.
[20] *Ibid.*
[21] Yurii Shchyhol, "Russia's cyberwar against Ukraine offers vital lessons for the West," Atlantic Council (2023), available on: https://www.atlanticcouncil.org/blogs/ukrainealert/russias-cyberwar-against-ukraine-offers-vital-lessons-for-the-west/. Accessed March 2, 2023.
[22] Robert Grimmick, "What is Cyber Espionage? Complete Guide with Protection Tips," Varonis (2022), available on: https://www.varonis.com/blog/what-is-cyber-espionage. Accessed March 3, 2023.
[23] *Ibid.*

Economic cyber espionage is always understood as a criminal offence, the purpose of which can be not only the theft of financial information or the infliction of material damage but also the violation of trade secrets, theft of intellectual property, including the desire to steal innovative developments, the so-called know-how. Concerning political cyber espionage, this act will not always qualify as a criminal offence; this fact will depend on the cyber spy's status and the goals pursued. So, for example, if political cyber espionage is one of the methods of cyberwar, then this act will not be related to a criminal offence and will be regarded as an accepted cybersecurity measure. Cyber espionage is often carried out by opponents of well-known politicians and parties in order to discriminate, destabilise and undermine their authority. In turn, military cyber espionage is mainly aimed at reconnaissance purposes, namely, in order to obtain information about the military preparation of the enemy country, for example, its number and readiness of military forces, the geographical location of strategic military facilities, and the offensive plan (if any). Finally, mixed cyber espionage includes several or often, for example, during a war, all areas of cyber espionage – economic, political and military.[24] One of the most notorious cyber-espionage cases was that of Edward Snowden, a former Central Intelligence Agency and National Security Agency officer who, according to the Pentagon, stole more than 1.7 million classified files relating to the US military in 2013, thereby committing a so-called insider attack.[25]

1.1.3. Cyber terrorism

The third category of cyber threat is cyber terrorism. Cyber terrorism is understood as illegal actions in cyberspace involving an attack on the life, health or property of an indefinite number of persons with the aim of violating public security, intimidating the population or provoking a military conflict and subsequently gaining influence over political, economic, social or ideological objectives.[26] It must be emphasised that in order to classify illegal activities as cyber terrorism, the activities must pose a threat to national security, society and individuals and must result in violence against people or property, or at least cause sufficient harm to cause fear that such a threat exists and can be implemented. Cyber terrorism, just like cyberwar, can manifest itself as an attack on critical infrastructure in order to limit their work or to completely stop life support systems, gain illegal access to state and military archives with classified information, spread false threats of attacks to destabilise the economic or social-political situation, and other

[24] Grimmick, *supra* note 22.
[25] *Ibid*.
[26] Robert Sheldon and Katie Terrell Hanna, "cyberterrorism," TechTarget (2022), available on: https://www.techtarget.com/searchsecurity/definition/cyberterrorism. Accessed March 4, 2023.

actions endangering the life and health of people or have other grave consequences. Unlike cyberwar and cyber espionage, in which states are most often the actors, cyber terrorists are mainly members of terrorist organisations, ideologically inclined individuals, and people who seek to harm others. Although there are not many examples of cyber terrorism in history, one of them is the cyberterrorist act of Ardit Ferizi, who in 2015 hacked into the US military system and stole the personal information of approximately 1,300 representatives of US government and military personnel and then sold it to the foreign terrorist organisation the Islamic State of Iraq and the Levant (ISIL), which added victims to its so-called "hit list".[27]

1.1.4. Cyber vandalism

The fourth category of cyber threat is the previously mentioned cyber vandalism. This type of cyberattack is the deliberate act of damaging, disrupting, or destroying the digital property of another person or company without any overt criminal, political, or ideological motive.[28] Unlike all previously considered cyber threats, cyber vandalism can be classified as one of the most harmless, yet, the consequences for the injured party can be pretty impressive – financial and reputational losses, as well as restricted access for customers if, for example, the company website providing a service is compromised. Cyber vandalism mainly takes the form of hacking or defacing a website, damaging or destroying a digital object, posting false or harmful information or feedback, or placing viruses or other malware to be downloaded unknowingly by others. On the other hand, cyber vandals are most often people who seek to harm others, wish to avenge an offender, are trolls and harming is their pastime, who wish to draw attention to themselves or their targets, as well as people who feel superior by committing acts of cyber vandalism.[29] The most famous case of cyber vandalism is the digital attack on the Wikipedia website, namely the web page of Donald Trump, then the Republican presidential candidate in the US, in 2016 at the height of the presidential campaign.[30] Initially, Donald Trump's Wikipedia web page was completely removed, and later, after restoration, the entire content was changed to the single phrase, "Let's be fair, nobody cares about him."[31]

---

[27] The United States Department of Justice. ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison (2016), available on: https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison. Accessed March 4, 2023.
[28] Beth Hendricks, "Vandalism in Digital Crime: Types & Evidence," Study.com (2022), available on: https://study.com/academy/lesson/vandalism-in-digital-crime-types-evidence.html. Accessed March 4, 2023.
[29] Computer Hope. Vandalism (2021), available on: https://www.computerhope.com/jargon/v/vandalism.htm. Accessed March 4, 2023.
[30] Hendricks, *supra* note 28.
[31] *Ibid.*

1.1.5. Cybercrime

Finally, the fifth and most common category of cyber threat is cybercrime. This category of cyberattack combines all criminal actions that do not fall under the categories of cyberwar, cyber espionage, cyber terrorism, and cyber vandalism, but cybercrime can be an integral part of them. According to Teplinsky (2013), the term cybercrime refers to both traditional crimes committed using electronic networks, such as extortion, fraud or identity theft, as well as crimes specific only to electronic networks and cyberspace, such as phishing, ransomware and malware, and distributed denial-of-service attacks.[32] What distinguishes cybercrime from other categories of cyberattacks is its purpose – most cybercrime is committed for financial gain. As previously stated, financial services rank second among the most affected sectors by cybercrime after the healthcare industry. In 2022, the average cost of a data breach worldwide for the financial sector was USD 5.97 million.[33] So far, the most significant data breach in the financial sector worldwide is the September 2017 hack attack on Equifax, a US-based multinational consumer credit reporting agency.[34] During the company's security breach, 147 million customers, or potentially more than 40% of the US population, were affected, and highly sensitive data such as customer names, dates of birth, social security numbers, driver's license numbers and credit card numbers were compromised.[35]

1.2. Factors causing cyber threats

In order to understand what exactly causes cyberattacks in the financial sector and prevent them in time, it is not enough to classify cyberattacks into categories. As discussed above, the majority of cyberattacks in the financial sector are carried out by hackers whose goal is to obtain financial profit. However, in order for a cyberattack to occur and for the hacker to accomplish his goal, the financial institution must "allow" him to do so. Various experts in the field of cybersecurity and legal scholars identify many factors causing cyber threats, ranging from ordinary human inattention to the inability of the state to use the precautionary principle

[32] Melanie J. Teplinsky, "Fiddling on the Roof: Recent Developments in Cybersecurity," *American University Business Law Review*, Volume 2, Issue 2 (2013): p. 249.
[33] IBM Security. Cost of a Data Breach Report 2022 (2022): p. 7, available on: https://www.ibm.com/downloads/cas/3R8N1DZJ. Accessed March 5, 2023.
[34] Edward Kost, "10 Biggest Data Breaches in Finance," UpGuard (2023), available on: https://www.upguard.com/blog/biggest-data-breaches-financial-services. Accessed March 5, 2023.
[35] *Ibid.*

concerning cyber risks threatening the financial system's stability[36]. Let us take a closer look at the main factors that can make financial industry representatives vulnerable to cyberattacks.

1.2.1. Lack of preparation

According to legal scholars such as Calliess and Baumgarten (2020), the main factor in causing cyber threats is the lack of preparation by the financial industry representatives, by citizens using financial instruments and by governments that regulate national cyberspace.[37] Many companies, especially new start-ups or fintechs, deliberately do not develop cybersecurity or give it the least attention, as they prefer to spend their resources on developing new technologies and are solely focused on financial growth. According to citizens, all cyberspace is free, and any attempts to secure it will only lead to restrictions and a corresponding slowdown in the development of new technologies.[38] As for the lack of preparedness of states, the European Union Agency for Cybersecurity (ENISA) cyber experts (2021) argue that, as a rule, as long as the malicious activity is at an acceptable level and makes up less than 2% of national income, governments are tolerant of cyber threats.[39] Thus, worldwide there is a growing recognition that cyberspace and new technologies carry certain risks, and this fact must be simply accepted.

1.2.2. Human element

The second factor in causing cyber threats can be humans, which includes such threats as the skills gap[40], human error[41] and remote work[42]. Companies focusing exclusively on technological and software security neglect employees and corporate processes. So according to IBM data for 2022, 62% of companies worldwide do not have a staffed team responsible for cybersecurity.[43] This lack of cybersecurity personnel or their skills certainly affects a company's cost of a cyberattack. Statistically, organisations with understaffed cybersecurity

---

[36] Christian Calliess and Ansgar Baumgarten, "Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective," *German Law Journal*, Volume 21, Issue 6 (2020): p. 1156, accessed March 7, 2023, doi: 10.1017/glj.2020.67.
[37] *Ibid*., p. 1153.
[38] *Ibid*.
[39] Rossen Naydenov and Marianthi Theocharidou, "EU Cybersecurity Initiatives in the Finance Sector," European Union Agency for Cybersecurity (ENISA) (2021): p. 5, accessed March 8, 2023, doi: 10.2824/15644.
[40] IBM Security, *supra* note 33, p. 45.
[41] Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans and Andrea Renda, "Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force," Centre for European Policy Studies (CEPS) (2018): pp. 8-9, available on https://www.ceps.eu/wp-content/uploads/2018/11/CEPS_TFR%20on%20Cyber%20Defence_1.pdf. Accessed March 10, 2023.
[42] IBM Security, *supra* note 33, p. 44.
[43] *Ibid*., p. 45.

teams that experienced a cyberattack had a 12% or USD 0.55 million higher average data breach cost than organisations with full cybersecurity personnel.[44]

According to scientists Pupillo, Griffith, Blockmans and Renda (2018), the weakest link in cybersecurity is human vulnerability and errors.[45] Vulnerabilities arise in any process performed by people on a regular basis, whether it is a bank employee opening his work email or a bank client entering his password in an Internet banking platform. For example, the previously mentioned subcategory of cybercrime, phishing, is a clear example of human vulnerability. Phishing attacks are carried out by sending emails, text messages or calls with fraudulent but convincing content and various false links.[46] A common example is a call from a hacker who claims to be a bank employee and states that an unknown person transferred a large amount of money from the client's account, and in order to stop the transaction, he needs to obtain personal data and information about the PIN code from the client. However, not only clients of financial institutions but also their employees become victims of phishing, which often leads to significant data leaks and financial losses. So, in 2021, at the height of the Covid-19 pandemic, the X-Force Threat Intelligence Index named the phishing cyberattack the most common for the financial sector; this cyberattack accounted for 46% of all types of cyberattacks committed.[47]

Another threat that has also emerged during the Covid-19 pandemic is remote work, which means that company employees have access to confidential databases directly from their homes. The most common threat when working remotely is connecting to insecure networks, such as public or even often home Wi-Fi, which allows hackers to gain access to computer credentials.[48] According to IBM data for 2022, the average global cost of a data breach in companies with 81% to 100% of employees working remotely was USD 5.10 million, whereas in those with less than 20% of employees working remotely the average cost was USD 3.99 million, a reduction of 24.4%.[49]

---

[44] IBM Security, *supra* note 33, p. 45.
[45] Pupillo, Griffith, Blockmans and Renda, *supra* note 41.
[46] Sangfor Technologies. Cyber-attacks on Banks Devastate the Financial Sector (2022), available on: https://www.sangfor.com/blog/cybersecurity/cyber-attacks-on-banks-devastate-financial-sector. Accessed March 10, 2023.
[47] *Ibid*.
[48] Mary K. Pratt, "Remote work cybersecurity: 12 risks and how to prevent them," TechTarget (2022), available on: https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them. Accessed March 10, 2023.
[49] IBM Security, *supra* note 33, p. 44.

1.2.3. Technological complexity

The third factor in causing cyber threats is the technological component of the financial system since the system itself is a complex network of participants from different environments but using common technologies.[50] European Supervisory Authorities (2019) note that the financial sector consists not only of financial institutions but also of third-party service providers, for example, cloud service providers.[51] Due to the high device specificity of cloud models, the number of prominent players in the market is limited, which leads to concentration risks. This fact is also confirmed by IBM statistics for 2022, according to which 45% of cyberattacks and data leaks worldwide occur in the cloud.[52] In addition to cloud services, European Supervisory Authorities also note that with the development of new technologies such as new information systems, the Internet of Things and 5G technologies, financial institutions have become entirely reliant on them in their daily activities, which has led to a wide range of entry for cybercriminals.[53]

1.2.4. Interconnectedness of the financial sector

The fourth factor arising from the technological component of the financial system is the interconnectedness of the entire financial market. As was clarified earlier, the financial system consists not only of financial institutions but also of various other actors and infrastructures. According to the European Central Bank (2018), in the event of a failure in the work of one of the participants in the financial system providing non-critical financial services, there is as well a high risk of failure of a significant participant supplying critical financial services; this phenomenon has even been called Single Point of Failure.[54] Cyber expert Bouveret (2018) explains that the critical infrastructures of the financial market are "payment and settlement systems, trading platforms, central securities depositories, and central counterparties.[55]" For

[50] IBM Security, *supra* note 33, p. 39.
[51] *Ibid*.
[52] *Ibid*.
[53] European Supervisory Authorities, "Joint Advice of the European Supervisory Authorities: To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector" (2019): p. 4, available on: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf. Accessed March 11, 2023.
[54] European Central Bank, "Cyber resilience oversight expectations for financial market infrastructures" (2018): p. 2, available on: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. Accessed March 14, 2023.
[55] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," International Monetary Fund (IMF) Working Paper (2018): p. 12, available on: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924. Accessed March 14, 2023.

example, suppose the payment and settlement system provided by one of the participants in the national financial sector ceases to function. In that case, critical participants in the financial market (*e.g.* large banks) will not be able to process transactions, which will lead to an increased risk of liquidity and solvency of these critical participants. A similar scenario will be observed in reverse; if critical financial market participants (*e.g.* large banks) are unable to process transactions, then this will lead their counterparties (*e.g.* a participant providing a payment and settlement system) to increased liquidity and solvency risk.[56]

1.2.5. Regulatory complexity

Finally, the factor causing cyber threat, which deserves special attention due to its practical complexity, is regulatory complexity, applicable both to regulatory bodies and to the representatives of the financial industries themselves. According to legal scholars such as Calliess and Baumgarten (2020), special attention on the part of regulatory bodies should be given to the principle that the European Commission and the European Court of Justice consider as a general legal principle of EU law – the precautionary principle, but in this case in relation to cybersecurity.[57] Due to the rapid development of new technologies, the rapidly changing nature of cyber risks, and the impossibility of identifying all threat scenarios for the financial sector, preventive government action is needed at the earliest stages of ascertaining cyber risks that can undermine the stability of the financial system.[58] Unfortunately, as explained earlier in the lack of preparation factor, governments generally tolerate cyber threats as long as the malicious activity is at an acceptable level and is less than 2% of national income.[59] Moreover, according to the International Monetary Fund data for 2021-2022, 56% of all central banks and national supervisory authorities worldwide did not have a national cyber strategy for the financial sector, while 48% of states did not have any cybercrime regulations at all.[60] As for the representatives of financial industries, the regulatory factor causing the cybersecurity threat manifests itself in practice, most often in the form of general inability, inability to timely implement or unwillingness to implement existing cybersecurity regulations and better

[56] Bouveret, *supra* note 55.
[57] Calliess and Baumgarten, *supra* note 36.
[58] *Ibid*.
[59] Dan Tofan, Theodoros Nikolakopoulos and Eleni Darra, "The cost of incidents affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)," European Union Agency for Network and Information Security (ENISA) (2016): p. 5, accessed March 16, 2023, doi: 10.2824/475621.
[60] Tobias Adrian and Caio Ferreira, "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards," International Monetary Fund (IMF) Blog (2023), available on: https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards. Accessed March 16, 2023.

practices into the internal policies of their financial institutions. So, for example, according to a study conducted by the American Bank Policy Institute in 2022, financial institutions' chief information security officers spend 40% of their working time on the solution and implementation of numerous requirements of regulatory bodies in their internal cybersecurity regulations.[61]

1.3. Legal complications of cybersecurity regulation

Legal authors highlight three main legal issues in the legal regulation of cybersecurity in the financial sector. These problems can be described as jurisdictional fragmentation, difficulty determining responsibility for malicious behaviour, and who should be responsible for regulatory action in cyberspace. The following is a summary of the legal reasoning behind each issue.

1.3.1. Jurisdictional fragmentation

The problem of jurisdictional fragmentation of cyberspace is related to its main characteristic – globality or, in other words, the inability to establish clear geographical boundaries of cyberspace. According to existing legal norms, the usual concept of jurisdiction is inextricably linked with state sovereignty, which clearly imposes a sovereign state's exclusive responsibility over its territory and population, thereby excluding any jurisdictional interference from other states.[62] Also, according to the United Nations, since customary public international law rules safeguard states' sovereign equality, this makes it impossible for any state to claim sovereignty over cyberspace and, hence, exercise its effective regulation alone.[63] Thus, according to Clough (2010), it is not difficult to enact legislation governing behaviour in cyberspace; it is difficult to assert jurisdiction over this behaviour because possible illegal activities can occur from anywhere in the world, which makes traditional rules based on geographic location inapplicable.[64]

---

[61] Suleyman Ozarslan, "Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022," Picus Security (2022), available on: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022. Accessed March 16, 2023.

[62] Artur Appazov, "Legal Aspects of Cybersecurity," University of Copenhagen (2014): p. 10, available on: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf. Accessed March 18, 2023.

[63] United Nations Office on Drugs and Crime (UNODC). "Comprehensive Study on Cybercrime" (2013): p. 184, available on: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed March 18, 2023.

[64] Jonathan Clough, "Jurisdiction," chapter, in *Principles of Cybercrime*, 2nd ed. (Cambridge: Cambridge University Press, 2015): p. 475, accessed March 18, 2023, doi:10.1017/CBO9781139540803.015.

The problem of jurisdictional fragmentation of cyberspace mainly arises when it is necessary to determine whether this or that behaviour entails legal liability. Given the ease with which cybercrimes can be committed affecting different states and their jurisdictions, according to the legal scholar Weber (2003), national law enforcement systems need to use all available cross-border cooperation mechanisms among themselves – mutual legal assistance, extradition and others.[65] However, according to legal scholars Urbas (2012) and Brenner (2012), these mechanisms are not always available or be implemented by countries due to the different legal qualifications of cybercrime in different jurisdictions[66], as well as the initial difficulty in determining the origin of a cyber threat – whether it comes from outside or inside the state[67]. An example of the different legal qualifications of cybercrime in different jurisdictions in the financial sector is the previously analysed phenomenon of economic cyber espionage since this act can be considered a crime in the victim state but will not be such in the aggressor country.

However, the problem of jurisdictional fragmentation of cyberspace is not intractable in highly integrated societies such as the EU, where the national laws of each Member State substantially conform to one another and coherently govern comparable conduct. [68] Nevertheless, as for the rest of the world, particularly developing countries, the problem of jurisdictional fragmentation of cyberspace destroys not only the effectiveness of their own legal system but also threatens the effectiveness of the legal systems of developed countries. Since many developing countries do not have relevant cybersecurity laws that could regulate and provide liability for one or the other behaviour in cyberspace[69], this factor can become decisive when a hacker chooses his geographic location when committing a cybercrime because of the opportunity to go unpunished. One of the most controversial examples is the 2001 cyberattack with malware created in the Philippines called the Love Bug.[70] According to available data, the software has infected millions of computers, including government departments in various countries and companies such as Microsoft, Siemens, and Ford, resulting in a crash and loss of

[65] Amalie M. Weber, "The Council of Europe's Convention on Cybercrime," *Berkeley Technology Law Journal*, Volume 18, Issue 1 (2003): p. 433.
[66] Gregor Urbas, "Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement," *Journal of Internet Law*, Volume 16, Issue 1 (2012): p. 8.
[67] Susan W. Brenner, "Cybercrime and the Law: Challenges, Issues, and Outcomes" (Boston: Northeastern University Press, 2012): p. 211.
[68] Appazov, *supra* note 62, p. 11.
[69] *Ibid*.
[70] James Griffiths, "'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on," CNN Business (2020), available on: https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html. Accessed March 18, 2023.

work time worth about USD 10 billion.[71] However, the suspected hacker who ran the malware was never prosecuted because, at the time, there were no similar precedents or relevant cybersecurity laws in the Philippines, which made a cyberattack unprosecutable and prevented the suspected hacker from being extradited to countries that were harmed and had relevant cybersecurity laws[72], since extradition requires the crimes to be prosecutable in both countries.

1.3.2. Establishing responsibility for behaviour

Another legal problem in regulating cybersecurity in the financial sector is the attribution or definition of the entity responsible for a particular behaviour.[73] According to generally accepted legal norms, in order to establish the legal consequences of behaviour in cyberspace, it is first necessary to determine the source and nature of the cyberattack. Legal scholars single out two main perpetrators of cyberattacks in the financial sector – the individual and the state.[74] A cyberattack committed by an individual will most often be qualified as a criminal act for the purpose of, for example, obtaining financial gain and will be regulated by the relevant national legislation, *i.e.* criminal, administrative and others. In turn, a cyberattack committed by the state will most often be qualified as an act of aggression, for example, with the aim of destabilising the victim state and will be regulated by international law. However, the nature of cyberspace does not make it easy to distinguish who exactly is behind a cyberattack – an individual acting independently or an individual acting as an agent of the state.[75]

As countermeasures can only be legal if the attacker is correctly identified, the problem of attribution in cybersecurity regulation is evidentiary. That is where the main difficulties highlighted by Appazov (2014) arise.[76] Firstly, cybercriminals can use computers, servers and other technology belonging to innocent parties, including state computers, to carry out a cyberattack, which will make it possible to simulate an attack allegedly coming from the state, which will not be true. Secondly, as it was clarified above, the geographic location from which the cyberattack was supposedly carried out will also be ambiguous evidence since the Internet servers, for example, with the help of which the cyberattack was carried out, can be located anywhere due to the anonymity and global nature of cyberspace. Thirdly, if the evidence is in a foreign jurisdiction, then access to it may be denied, or it may even be destroyed as evidence.

---

[71] Griffiths, *supra* note 70.
[72] *Ibid.*
[73] Appazov, *supra* note 62, p. 11.
[74] *Ibid.*
[75] *Ibid.*
[76] *Ibid.*

Fourth, if a cyberattack is committed by a state, then the victim state must prove that its consequences pose a severe threat to the national security of the country and that a cyberattack can qualify as an "armed attack" in the context of international law.[77]

1.3.3. Establishing responsibility for regulatory action

In the context of cybersecurity regulation in the financial sector, cyber experts and legal scholars have also long argued about who exactly should be responsible for taking regulatory action for financial cyberspace – the private sector, government agencies, or together in close cooperation with each other.[78] Proponents of the private sector believe that public authorities are less advanced in implementing cybersecurity than the private sector since only the private sector has the necessary amount of knowledge and experience to regulate financial cyberspace effectively. According to Sales (2018), the private sector holds the most valuable information on which cybersecurity depends – threat data, namely which types of cyber threat exist and which new types have recently been discovered, as well as information on cyber threat countermeasures, *i.e.* what actions need to be taken to reflect a specific cyber threat or eliminate a possible vulnerability.[79] In turn, those advocating that public authorities should be responsible for taking regulatory measures for financial cyberspace are convinced that the market approach of the private sector cannot be applied to the public and national security of the state.[80] Supporters of state regulation also believe it is unacceptable for the state to depend on the private market.[81] In turn, according to Calliess and Baumgarten (2020), only through the process of division of labour between the private sector and public authorities, otherwise called "private-public engagement", can the stability of the financial system and cyber resilience be achieved, although this is not easy to implement in practice.[82]

---

[77] William M. Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity," *Georgia Journal of International and Comparative Law*, Volume 40, Issue 1 (2011): pp. 261-262.
[78] Nathan Alexander Sales, "Privatizing Cybersecurity," *UCLA Law Review*, Volume 65, Issue 3 (2018): p. 628.
[79] *Ibid.*
[80] *Ibid.*
[81] *Ibid.*
[82] Calliess and Baumgarten, *supra* note 36, p. 1157.

2. Analysis of legal regulation regarding cybersecurity in the financial sector

Currently, work is ongoing on the creation of a legislative framework for regulating cybersecurity in the financial sector around the world. Since the nature of cyberspace and new technologies is very volatile and rapidly changing, and new and more sophisticated cyber threats emerge daily, the cybersecurity legislative framework must always be up-to-date and flexible in its application. However, the fact that cybersecurity legislative acts need to be always relevant also gives rise to significant difficulties in the legal regulation of cybersecurity in the financial sector, namely, a large number of different security standards, new laws, guidelines and others are created, which are either significantly similar to each other and so-called legislative overlaps occur, or *vice versa*, legal provisions contradict each other, both of which lead to confusion and additional risks for financial sector participants.[83]

The legislative framework for regulating cybersecurity in the financial sector in the EU is a multi-level structure, with different rule-makers and a large number of legal sources. In general, legal provisions for regulating cybersecurity in the financial sector exist at the international, European and national levels. They are developed by various international organisations, transnational forums, international and national standards bodies, national legislative and regulatory bodies, as well as regional, non-governmental and independent private organisations.[84] Also, the legal provisions on the regulation of cybersecurity in the financial sector considerably differ in legal nature and effect, namely, legislative acts can be divided into mandatory, for example, the source of secondary law – regulations; voluntary, for example, standards; and also legislative acts combining both mandatory and voluntary provisions.

Since different jurisdictions and countries have different attitudes towards regulating cybersecurity in the financial sector, it is necessary to find out whether the current legislative framework is comprehensive and practical and to determine why the US, according to the National Cyber Power Index 2022, is the most powerful nation in the field of cybersecurity regulation in the world[85]. Thus, what legal approaches and challenges do the EU and the US have in regulating cybersecurity in the financial sector, remains to be seen in this Section.

---

[83] Edward Kost, "Top 8 Cybersecurity Regulations for Financial Services," UpGuard (2023), available on: https://www.upguard.com/blog/cybersecurity-regulations-financial-industry#toc-7. Accessed April 10, 2023.
[84] Calliess and Baumgarten, *supra* note 36, p. 1158.
[85] Julia Voo, Irfan Hemani and Daniel Cassidy, "National Cyber Power Index 2022," Belfer Center for Science and International Affairs, Harvard Kennedy School (2022): p. 9.

2.1. The European Union legal framework

Although the current binding EU legislation regarding the regulation of cybersecurity in the financial sector is limited, there are provisions at the EU level, in particular regulations and directives, establishing specific cybersecurity mandatory requirements for representatives of the financial sector. This section will analyse all relevant EU-binding legislation related to cybersecurity in the financial sector, including the NIS 2 Directive and DORA Regulation that entered into force on January 16, 2023.[86]

2.1.1. GDPR

The main legislative act directly related to the regulation of cybersecurity in the financial sector is the General Data Protection Regulation (GDPR), which focuses on the protection of the personal data of EU citizens.[87] In the context of the financial sector, personal data is any information capable of identifying an individual: name, address, identification numbers and other information provided by the client when, for example, opening a bank account. The GDPR imposes an obligation on financial service providers to obtain the express consent of an EU citizen to use his personal data and subsequently allowing him to exercise his rights over them, for example, the right to access, manage, restrict and delete his personal data.[88] Also, Articles 32-34 of GDPR impose upon financial service providers the obligation to take appropriate technical and organisational measures to prevent possible cyber threats, notify the supervisory authority about the leakage of personal data, as well as report the leakage of personal data to the data owner.[89]

The GDPR applies to any operation of a financial institution involving the personal data of a client, whether it is the collection of data when opening a bank account, storage of data, use of data in the processing of transactions or exchange with a counterparty providing a payment and settlement system, alteration or data deletion. It should be noted that compliance with the GDPR is mandatory not only for EU financial institutions but also for international representatives of the financial sector who collect or process any personal data of EU residents.

---

[86] Natallia Karniyevich, Fabian Niemann, Marjolein Geus and Feyo Sickinghe, "NIS 2 Directive, RCE Directive and DORA: Important EU cybersecurity-related legislative acts come into force," Bird&Bird (2023): p. 2, available on: https://www.twobirds.com/-/media/new-website-content/pdfs/2023/germany/nis-2_rce_dora_germany_newsflash.pdf. Accessed April 13, 2023.

[87] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), *OJ L* 119, 04.05.2016, available on: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed April 13, 2023.

[88] *Ibid.*

[89] *Ibid.*

Thus, a financial institution headquartered in the US, but operating in the EU and owning the personal data of EU citizens, will be required to comply with the GDPR. According to Article 83(5) of the GDPR, non-compliance with the Regulation can result in financial institutions being fined up to EUR 20 million or 4% of annual turnover, whichever is greater.[90]

2.1.2. SIPS Regulation

One of the few EU binding legislation that has precise requirements for cybersecurity in the financial sector is the Regulation of the European Central Bank No 795/2014 on oversight requirements for a systematically important payment system[91] (SIPS Regulation). Systemically important payment systems (SIPS) are payment systems that facilitate the clearing, settlement, and accounting of cash and other financial transactions such as payments, securities and derivatives contracts, whose failure threatens to shut down the entire domestic and international economy.[92] SIPS contribute to maintaining financial stability and promoting economic growth but simultaneously concentrates risks due to their high significance and indispensability.[93] Thus, Article 15(4)(a) of the SIPS Regulation dated May 25, 2021, entitled "operational risk", clearly sets out the requirements for SIPS operators and their cybersecurity regulation, namely

> A SIPS operator shall establish an effective cyber resilience framework with appropriate governance measures in place to manage cyber risk. The SIPS operator shall identify its critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyber attacks. These measures shall be regularly tested. The SIPS operator shall ensure it has a sound level of situational awareness of cyber threats. The SIPS operator shall ensure that there is a process of continuous learning and evolving to enable it to adapt its cyber resilience framework to the dynamic nature of cyber risks, in a timely manner, whenever needed.[94]

These provisions set out necessary measures to prevent cyber risks that could threaten SIPS. Thus, the Article requires SIPS operators to regularly test their measures designed to protect, detect, respond to and recover from cyberattacks, thereby taking into account the crucial cyber risk to the financial sector as outdated policies and procedures. The requirement for continuous learning also considers such cyber risk as the human factor. The requirement for creating a business continuity plan prevents the risk of undermining the stability of the national and international economy. The Article also touches upon the critical risks of cooperation with third

---

[90] Regulation (EU) 2016/679 (GDPR), *supra* note 87.
[91] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (SIPS Regulation), *OJ L* 217, 23.07.2014, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0795. Accessed April 14, 2023.
[92] Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO), "Principles for financial market infrastructures" (2012): p. 5, available on: https://www.bis.org/cpmi/publ/d101a.pdf. Accessed April 14, 2023.
[93] *Ibid*.
[94] Regulation of the European Central Bank (EU) No 795/2014 (SIPS Regulation), *supra* note 91.

parties. In addition, the use of general terminology in the Article, such as "appropriate measures" and "to adapt its cyber resilience framework to the dynamic nature of cyber risks", allows the SIPS Regulation to be as flexible as possible and easily adaptable to the regulation of any SIPS. Moreover, recognising the nature of cyber risks as dynamic and using common terminology does not limit SIPS in creating new and innovative approaches to cybersecurity regulation. Thus, it can be concluded that except for incident notification and reporting requirements, the SIPS Regulation addresses all vital elements of an effective cybersecurity regulatory framework in the financial sector.

2.1.3. PSD2

An important piece of legislation is also Directive 2015/2366 on payment services in the internal market[95] (PSD2). This Directive was created for representatives of the financial sector in order to facilitate their integration, secure exchange of financial data, and establish a high level of security for payment systems. Although the Directive does not contain clear provisions regarding the regulation of cybersecurity, some articles prescribe requirements for the so-called IT systems of a financial institution, which can be related to the implementation of cybersecurity. So, Article 5(1) of PSD2 states that

> The security control and mitigation measures […] shall indicate how they ensure a high level of technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations.[96]

To supplement PSD2 and make it more effective, Article 95 of the Directive imposes an obligation on the European Banking Authority (EBA), a regulatory agency of the EU, to develop at the request of the European Commission the necessary EBA guidelines regarding various security measures.[97] It should also be noted that similar to the GDPR, the PSD2 directive imposes obligations not only on EU financial institutions but also on international representatives of the financial sector serving EU consumers whose payments originate, pass through or end in the EU. Also, according to Article 103 of PSD2, when transposing this Directive to the Member State's national law, appropriate penalties for non-compliance with

[95] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2), *OJ L* 337, 23.12.2015, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366. Accessed April 16, 2023.
[96] *Ibid.*
[97] *Ibid.*

PSD2 should be established, although the specific types or amount of penalties are not established in the Directive.[98]

2.1.4. CRD IV and CRR

Next, a package of capital requirements should be considered, consisting of Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms[99] (CRD IV) and Regulation No 575/2013 on prudential requirements for credit institutions and investment firms[100] (CRR). The CRD IV/CRR requirements package has been developed for banking institutions and investment firms, mainly relating to their capital and liquidity.[101] According to Article 74(1) of CRD IV, financial institutions must have "robust governance arrangements, which include […] effective processes to identify, manage, monitor and report the risks, […] adequate internal control mechanisms[102]"; according to Article 85(1) must "implement policies and processes to evaluate and manage the exposure to operational risk[103]"; and according to Article 85(2) must have "contingency and business continuity plans.[104]" Similar provisions regarding the operational risk assessment system, including criteria for a standardised approach and qualitative and quantitative standards for measuring operational risks, are also contained in articles 288, 320-322, and 368 of CRR.[105] Thus, after analysing the package of requirements CRD IV/CRR, it can be concluded that the provisions contained in it only relate to general operational risks, which may also imply cyber risk management, but not a single article directly relates to financial institutions' cybersecurity.

[98] Directive (EU) 2015/2366 (PSD2), *supra* note 95.
[99] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (CRD IV), *OJ L* 176, 27.06.2013, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0036. Accessed April 17, 2023.
[100] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (CRR), *OJ L* 176, 27.06.2013, available on: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32013R0575. Accessed April 17, 2023.
[101] Europex (Association of European Energy Exchanges). Capital Requirements Directive (CRD) IV and Capital Requirements Regulation (CRR), available on: https://www.europex.org/eulegislation/crd-iv-and-crr/. Accessed April 17, 2023.
[102] Directive 2013/36/EU (CRD IV), *supra* note 99.
[103] *Ibid*.
[104] *Ibid*.
[105] Regulation (EU) No 575/2013 (CRR), *supra* note 100.

2.1.5. NIS 2 Directive and DORA Regulation

Finally, it is necessary to move on to the most recent legislative acts regulating cybersecurity in the financial sector, namely, those that entered into force on January 16, 2023 – Directive 2022/2555 on measures for a high common level of cybersecurity across the Union[106] (NIS 2) and Regulation 2022/2554 on digital operational resilience for the financial sector[107] (DORA). Since these pieces of legislation are closely interrelated, they should be analysed together.

Concerning the NIS 2 Directive, its predecessor was the first cybersecurity legislation in the EU – Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS), the aim of which was to achieve a high level of cybersecurity in the Member States.[108] Unfortunately, the implementation of this Directive proved to be difficult because, together with the enhanced cybersecurity capabilities in the Member States that gave the general provisions of the NIS Directive, it also led to legal fragmentation in the internal markets of the Member States. Therefore, the European Commission decided to replace the current Directive with the NIS 2 Directive, which entered into force on January 16, 2023, with a transitional period for Member States until October 17, 2024.[109]

The NIS 2 Directive applies to all companies providing essential and important services to the European economy and is, therefore, fully applicable to the financial sector. Articles 20-21 of the NIS 2 Directive offer a reasonably comprehensive framework for regulating cybersecurity in the financial sector. So, the first paragraph of Article 20 of the NIS 2 Directive, for the first time, introduces a requirement for the approval of cybersecurity risk management measures by the management bodies of companies and obliges management bodies to monitor implementation and be held liable for violations of their own cybersecurity measures.[110] In turn, the second paragraph of Article 20 of the NIS 2 Directive obliges Member States to provide training to companies' management bodies in order to give them the necessary knowledge and skills to identify and manage cybersecurity risks, and must also offer similar training on an ongoing basis to other company employees.[111] As can be seen, Article 20 of the NIS 2 Directive

[106] Directive (EU) 2022/2555 (NIS 2), *supra* note 10.
[107] Regulation (EU) 2022/2554 (DORA), *supra* note 11.
[108] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS), *OJ L* 194, 19.07.2016, available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148. Accessed April 20, 2023.
[109] Directive (EU) 2022/2555 (NIS 2), *supra* note 10.
[110] *Ibid*.
[111] *Ibid*.

clearly addresses a cyberthreat-causing factor such as a human one. In addition to the fact that the Article, for the first time, defined the management bodies of a financial institution as liable in the event of cybersecurity failures, it also requires financial institutions to conduct training for management bodies and personnel on an ongoing basis.

Article 21 of the NIS 2 Directive, in turn, obliges companies to take appropriate technical, operational and organisational measures to manage cybersecurity risks, in particular regarding the introduction of appropriate policies and procedures, incident handling, business continuity and supply chain security, basic cyber hygiene practices and cybersecurity training, human resource security, and access control.[112] Article 23 of the NIS 2 Directive also requires Member States to be prepared to respond to possible cybersecurity risks and to comply with notification obligations when they occur, for example, through the Computer Security Incident Response Team (CSIRT) and, where applicable competent national network and information systems authorities.[113] Moreover, this Article establishes clear deadlines for the fulfilment by essential and important entities of their reporting obligation. The Directive also allows Member States to require essential and important service providers to certify their cybersecurity products and processes to European standards, national authorities or any other body authorised to certify cybersecurity products and processes. In turn, according to Article 34 of the NIS 2 Directive, in case of non-compliance with the Directive, essential entities can be fined up to EUR 10 million or 2% of the annual turnover, whichever is greater and important entities can be fined as well up to EUR 7 million or 1.4% of annual turnover, whichever is greater.[114]

In addition to the NIS 2 Directive, Regulation 2022/2554 on digital operational resilience for the financial sector (DORA) has become a real breakthrough in regulating cybersecurity in the financial sector, which Member States must implement before January 17, 2025.[115] According to Article 2(1)(a)-(u), DORA is applicable to all regulated financial institutions and their counterparties, which means a relatively comprehensive coverage –

> credit institutions; payment institutions […]; account information service providers; electronic money institutions […]; investment firms; crypto-asset service providers […] and issuers of asset-referenced tokens; central securities depositories; central counterparties; trading venues; trade repositories; managers of alternative investment funds; management companies; data reporting service providers; insurance and reinsurance undertakings; insurance intermediaries, reinsurance intermediaries and

[112] Directive (EU) 2022/2555 (NIS 2), *supra* note 10.
[113] European Commission. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (2023), available on: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Accessed April 21, 2023.
[114] Directive (EU) 2022/2555 (NIS 2), *supra* note 10.
[115] Regulation (EU) 2022/2554 (DORA), *supra* note 11.

> ancillary insurance intermediaries; institutions for occupational retirement provision; credit rating agencies; administrators of critical benchmarks; crowdfunding service providers; securitisation repositories; ICT third-party service providers.[116]

The purpose of this Regulation is to harmonise the regulatory framework for regulating the security of ICT of financial institutions and their counterparties and to ensure that financial institutions, through the implementation of best practices in cyber risk management, will be able to resist, respond and recover from any cyberattacks. DORA requirements can be divided into four main pillars: ICT risk management, incident reporting, digital operational resilience testing and third-party risk management.

The second chapter of the DORA Regulation sets out requirements for ICT risk management. So, Article 5 of DORA states that

> 1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, […] in order to achieve a high level of digital operational resilience.
>
> 2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).[117]

As can be seen, similar to the NIS 2 Directive, DORA requires the financial institution's management body to take responsibility for developing and approving a digital operational resilience strategy, as well as approving, overseeing and periodically reviewing the implementation of the business continuity policy, and response and recovery plans in the event of a cyberattack. Another requirement put forward by DORA is the establishment of acceptable risk levels for cyber failures by the financial institution, which must satisfy the increased level of ICT security established by DORA.[118]

The third chapter of the DORA Regulation sets out the requirements for managing ICT-related incidents. Article 17 of DORA reads as follows

> 1. Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.
>
> 2. Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.[119]

---

[116] Regulation (EU) 2022/2554 (DORA), *supra* note 11.
[117] *Ibid*.
[118] *Ibid*.
[119] *Ibid*.

With these requirements, DORA imposes a relatively large amount of work on financial institutions since they are not only required to have an appropriate ICT-related incident management process but also have to classify the impact of cyber incidents, analyse their root causes, and maintain a clear reporting system for reporting cyber incidents to national and European competent authorities.

The fourth chapter of the DORA Regulation deals with digital operational resilience testing; it imposes an obligation on financial institutions to have a policy, appropriate processes and controls for testing the operational resilience of cyber systems. In particular, DORA obliges financial institutions to conduct security tests of their cyber systems at least once a year while completely eliminating any identified cyberattack vulnerabilities. However, in the case of financial institutions that are considered systemically important and mature, Article 26 of DORA also imposes an obligation on them to conduct "at least every 3 years advanced testing by means of TLPT."[120] For financial institutions, this means that through threat-led penetration testing (TLPT), they must make a controlled attempt to compromise the cyber resilience of their institution by simulating a real cyberattack.

Finally, the fifth chapter of the DORA Regulation establishes requirements for third-party risk management. In particular, DORA places an obligation on financial institutions to treat third-party risk management as an integral part of their own cyber risk management. DORA also establishes certain conditions and minimum requirements for the composition of outsourcing contracts that contribute to the maintenance of the critical functions of financial institutions, which will need to be implemented during the transition period. It should also be noted that Article 31(1) of DORA establishes specific oversight of all third-party cyber service providers that are critical to financial institutions, namely by establishing a "Lead Overseer" that will oversee them, among other tasks, thereby forcing third-party providers of critical cyber services to improve their operational resilience and cybersecurity processes.[121] In turn, concerning non-compliance with the Regulation, Article 50 of DORA, unlike the NIS 2 Directive, does not establish specific fines but only empowers the competent authorities with supervisory, investigative and sanctioning powers.[122]

As can be seen from the joint legislative analysis, both the NIS 2 Directive and the DORA Regulation are aimed at improving cybersecurity in the EU, due to which they have

[120] Regulation (EU) 2022/2554 (DORA), *supra* note 11.
[121] *Ibid*.
[122] *Ibid*.

many similarities and even overlapping provisions. Nevertheless, it should be noted that DORA clearly distinguishes the relationship between these two pieces of legislation; namely, it indicates that the NIS 2 Directive is still applicable to financial institutions, but DORA "constitutes *lex specialis* with regard to Directive (EU) 2022/ 2555 [NIS 2 Directive],[123]" thereby establishing its priority over the NIS 2 Directive.

2.2. The United States legal framework

While at the EU level, the first directive regulating cybersecurity, namely the NIS Directive, appeared only in 2016, in the US, the legislative framework for regulating cybersecurity in financial services has been actively developing already since the 1990s. Thus, the main legislative acts regulating cybersecurity in the financial sector in the US are the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA) and the NYDFS Cybersecurity Regulation. Further, the main provisions of the previously listed US legislative acts will be analysed in detail, and the main distinguishing features of the legislative framework for regulating cybersecurity in the financial services of the EU and the US will be identified.

2.2.1. GLBA

Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernisation Act of 1999 with a sufficient number of amendments, is an analogue of the European GDPR legislation but aimed exclusively at financial sector representatives.[124] Thus, the goal of GLBA is to ensure the protection of financial sector clients' data from any events that threaten their integrity and security, including cyberattacks, and to require representatives of financial institutions to disclose and explain to their clients the data exchange methods used.

The GLBA requirements can be divided into three main sections. The first section of the GLBA, which can be defined as the financial privacy rule, governs the collection and disclosure of sensitive customer financial data. The second section establishes the safeguards rule that representatives of financial institutions must implement to ensure the security of the sensitive financial data of their clients. And finally, the third section is responsible for strict control of access to sensitive financial data of clients in order to reduce the likelihood of

[123] Regulation (EU) 2022/2554 (DORA), *supra* note 11.
[124] Garry Kranz, "Gramm-Leach-Bliley Act (GLBA)," TechTarget (2021), available on: https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act#:~:text=The%20Act%20consists%20of%20three,the%20Pretexting%20provisions%2C%20which%20prohibit. Accessed April 25, 2023.

unauthorised access.[125] In turn, with respect to the applicability of the GLBA, compliance with it is mandatory for all US financial institutions, and failure to properly comply will subject financial institutions to sanctions for non-compliance. For example, if a financial institution fails to comply with GLBA, the civil penalty could be up to USD 100,000 per violation. However, if the failure to comply was solely by or through the fault of financial institution officials, the civil penalty could be up to USD 10,000 per violation and/or up to five years in prison.[126]

2.2.2. SOX

The following important piece of legislation is the Sarbanes Oxley Act (SOX), passed by the US Congress in 2002 to protect investors from financial fraud, including those occurring in a cyber environment, through a system of internal audits.[127] SOX is mandatory by law and applies to all public companies, including foreign companies and subsidiaries that trade shares in the US. In particular, the SOX cybersecurity method is to implement strict internal control processes in the IT infrastructures of financial institutions to protect the financial information and records they contain.[128]

It should be noted that the SOX provisions do not explicitly mention cybersecurity, however, some sections of the statute may be applicable to the regulation of cybersecurity in the financial sector. For example, Section 302 of SOX, which establishes corporate responsibility for financial reports, requires financial institutions to have internal controls to ensure financial information's accuracy and secrecy until disclosure is required.[129] In turn, Section 404 of SOX imposes obligations on the officers of a financial institution, most often on the chief executive officer (CEO) and chief financial officer (CFO), namely requiring them to be accurate, provide complete documentation and be responsible for evaluating the previously mentioned internal controls in compiling reports that must be regularly submitted to the Securities and Exchange Commission (SEC) to prove their compliance with SOX regulatory requirements.[130] SOX also requires financial institutions to have data security policies that

[125] Kranz, *supra* note 124.
[126] *Ibid*.
[127] Fortinet. What Is the Sarbanes Oxley Act (SOX)? Available on: https://www.fortinet.com/resources/cyberglossary/sox-sarbanes-oxley-act. Accessed April 26, 2023.
[128] Ryan Branagan, "What is SOX Compliance in the Cybersecurity World?" Securiwiser, Just Get Visible Ltd (2022), available on: https://www.securiwiser.com/blog/what-is-sox-compliance-in-the-cybersecurity-world/. Accessed April 26, 2023.
[129] United States. Sarbanes-Oxley Act of 2002 (SOX), Public Law 107-204, 116 Stat. 745 (2002): p. 35, available on: https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf. Accessed April 26, 2023.
[130] *Ibid*.

clearly spell out how data is protected. Since SOX compliance is mandatory for all public financial institutions in the US, Section 906 of SOX sets out the applicable penalties for non-compliance. For example, if a public financial institution fails to comply with the SOX requirements, the penalty could be in the form of exclusion from the listing of the public stock exchange. However, if the non-compliance was solely by or through the fault of public financial institution officials, the fine could be up to USD 5 million and/or up to twenty years in prison, depending on whether the non-compliance with the law is intentional.[131]

2.2.3. NYDFS 23 NYCRR 500

Finally, the New York State Department of Financial Services 23 NYCRR 500 Cybersecurity Regulation (NYDFS Cybersecurity Regulation), which came into force in 2019, became a breakthrough in cybersecurity regulation in the financial sector in the US.[132] This Regulation aims to protect the customer data of financial institutions operating in New York from cyber threats. Section 500.01(c) of NYDFS Cybersecurity Regulation specifies that the Regulation refers to

> any Person [any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association] operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.[133]

It is important to note that since the NYDFS Cybersecurity Regulation applies to all financial institutions operating or conducting any other financial activity in New York, this also means that in practice, the Regulation applies to almost all financial institutions in the US since it is almost impossible to find a US financial institution that does not operate in New York.

The following main requirements of the NYDFS Cybersecurity Regulation can be distinguished. Financial institutions must implement and maintain a cybersecurity program and policy covering risk assessment, data management, access control, and customer privacy.[134] They must also appoint a Chief Information Security Officer responsible for overseeing and implementing the financial institution's cybersecurity

---

[131] Kezia Farnham, "SOX Penalties: What They Are, How to Avoid Them & Who Is Protected," Diligent (2022), available on: https://www.diligent.com/insights/grc/sox-penalties/. Accessed April 26, 2023.
[132] Ryan Rowcliffe, "NYDFS Strengthens MFA Requirement: What You Need to Know," HYPR (2022), available on: https://blog.hypr.com/the-nydfs-multi-factor-authentication-requirement. Accessed April 29, 2023.
[133] New York State. New York State Department of Financial Services 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies (2017) (NYDFS Cybersecurity Regulation): pp. 2-3, available on: https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf. Accessed April 29, 2023.
[134] *Ibid*., pp. 3-5.

policy.[135] Furthermore, financial institutions must have policies and procedures in place to ensure the security of data available to third-party service providers or any other third parties, as well as to carry out penetration testing and have an Incident Response Plan in place in order to respond and mitigate the consequences of a cyberattack quickly.[136] To protect against unauthorised access to secure information, the NYDFS Cybersecurity Regulation also requires financial institutions to use effective controls, which may include Multi-Factor Authentication.[137] Financial institutions personnel must receive appropriate cybersecurity training, and cybersecurity incidents must be notified to the superintendent, supervisory and regulatory authority of Financial Services in New York, within 72 hours.[138]

It should be noted that the NYDFS Cybersecurity Regulation does not contain provisions regarding penalties for non-compliance by a financial institution with the requirements of the Regulation since the penalties are separately prescribed by the relevant laws – Banking Law, Insurance Law and Financial Services Law, as well as penalties may be additionally imposed by the superintendent. In practice, fines for non-compliance with the NYDFS Cybersecurity Regulation by financial institutions range from USD 1.5 million to USD 5 million; however, there are record-breaking exceptions, namely Robinhood Crypto LLC was fined a record USD 30 million in 2022.[139]

2.2.4. Critical assessment

After analysing the most important and relevant US legislation regulating cybersecurity in the financial sector, several conclusions can be drawn compared to regulation in the EU. Firstly, it should be noted that one of the main differences between the European and American approaches to regulating cybersecurity in the financial sector is the lack of clear provisions in European legislation regarding fines and their amounts. The EU often leaves on Member States an obligation to set sanctions and their range for non-compliance with European law, thus often creating misunderstanding and disproportionate punishment for violations in European cyberspace. While the US, consisting of 50 states, in almost every piece of legislation relating to cybersecurity in the financial sector clearly sets out fines and their amounts for non-compliance with laws that will be applicable throughout the US. Secondly, another important

[135] NYDFS 23 NYCRR 500 (NYDFS Cybersecurity Regulation), *supra* note 133, p. 5.
[136] *Ibid*., pp. 5-10.
[137] *Ibid*., p. 8.
[138] *Ibid*., pp. 9-10.
[139] Compliance Manager GRC. Understanding the NYDFS Cybersecurity Regulation (23 NYCRR 500) and Its Implications on Financial Institutions (2022), available on: https://www.compliancemanagergrc.com/blog/nydfs-cybersecurity-regulation/. Accessed April 29, 2023.

difference between the European and American approaches to regulating cybersecurity in the financial sector, while complementing the difference about penalties, is the criminalisation of non-compliance with cybersecurity legislation in the US. As an analysis of US legislation has shown, regardless of whether the cybercrime was intentional or not, the management body responsible for implementing the cybersecurity of a financial institution can be prosecuted and imprisoned for up to 20 years. The third difference between the European and American approaches to regulating cybersecurity in the financial sector is the detailing of the provisions of legislative acts. The European DORA Regulation has 79 pages for comparison, while the US NYDFS Cybersecurity Regulation contains only 14 pages.

2.3. International standards

In addition to binding legislative acts, the worldwide cybersecurity legislative framework also provides a large number of standards relating to the regulation of cybersecurity, both in general and specifically in the financial sector. Cybersecurity standards are general provisions, of various forms and legal status, for cyber risk management, developed internationally by various private self-regulatory organisations and specialised administrative bodies. Due to the nature of cyberspace and new technologies, which are volatile and changing rapidly, and newer and more sophisticated cyber threats emerging day by day, representatives of financial institutions need up-to-date practical provisions that can "replace" the long and expensive process of creating hard law. The uniqueness of cybersecurity implementation standards lies in their high level of applicability, as they are based on practice and developed exclusively by experienced cyber professionals.[140]

According to their specifics, cybersecurity standards in the context of the financial sector can be divided into three types – good principles, practices and guidelines. The principles are general provisions covering broad areas of cybersecurity, providing flexibility in implementation according to countries' national circumstances. Practices are approaches and actions whose applicability in the course of research has been effective and has led to a high level of cybersecurity. Finally, guidelines are step-by-step instructions or cybersecurity requirements for the financial sector to undertake or comply with.[141] Concerning the legal status of standards, they are soft law instruments and do not have binding nature. However, national authorities responsible for cybersecurity regulation at the national level can voluntarily

[140] Calliess and Baumgarten, *supra* note 36, pp. 1159-1160.
[141] *Ibid*., p. 1160.

introduce cybersecurity standards into national legislation, which *de facto* makes them binding in nature.[142] Moreover, as explained earlier, binding legislative acts often stipulate or refer to standards in their provisions. Thus, the main international standards relating to cybersecurity regulation in the financial sector, which apply to the EU, the US and other countries, will be analysed further.

2.3.1. ISO/IEC 27001:2022 and NIST CSF

The main international standard for cybersecurity in the financial sector is ISO/IEC 27001:2022, better known as ISO 27001. This standard was created by the International Organization for Standardization (ISO) and is a set of policies, processes and recommendations aimed at creating, implementing and managing an information security management system (ISMS) and reducing cybersecurity risks.[143] The application of the standard is not mandatory for financial institutions, although if a company decides to publicly demonstrate its compliance, then it will be necessary for it to undergo ISO 27001 certification and prove that the necessary controls and protection of confidential information about its customers have been implemented,[144] namely the following provisions

> risk treatment plan; risk assessment report; information security policy and objectives; information risk treatment process; internal audit programme; results of internal audits; records of skills, qualifications, training, and experience; results of the management review; results of corrective actions; monitoring and measurement of results.[145]

Compliance with ISO 27001 provides a financial institution with many benefits. Firstly, when implementing the Standard, a financial institution will automatically comply with such binding legislation as GDPR and PSD2, on the regulatory requirements of which ISO 27001 is built, thereby demonstrating the security of its customers' confidential data. Secondly, the fact that the confidential information of the clients of a financial institution is highly cyber-secured inspires confidence directly from the clients and the relevant cybersecurity regulatory authorities. Thirdly, the systematic approach of ISO 27001 to risk management helps to promptly identify and eliminate potential cyber threats.[146]

---

[142] Calliess and Baumgarten, *supra* note 36, p. 1160.
[143] ZCyberSecurity. 12 Cyber security Regulations for Financial Services, available on: https://zcybersecurity.com/cyber-security-regulations-financial-industry-sector/. Accessed May 3, 2023.
[144] *Ibid*.
[145] Subho Halder, "Top 7 Cybersecurity Regulations in the Financial Industry that you Need to Know," Appknox (2021), available on: https://www.appknox.com/blog/cybersecurity-regulations-in-the-financial-industry. Accessed May 4, 2023.
[146] *Ibid*.

It should be noted that in the US there is a government organisation similar to ISO called the National Institute of Standards and Technology (NIST), which has a structure similar to, but not interchangeable with ISO 27001, called the NIST cybersecurity framework (NIST CSF).[147] This framework is a set of recommendations for minimising cybersecurity risks, which includes five main functions – identification, protection, detection, response and recovery. ISO 27001 and NIST CSF have overlapping and completely different provisions, so it is recommended to carefully apply the frameworks based on one's security needs. If the application of ISO 27001 is optional for all representatives of the financial sector, then NIST CSF is voluntary only for representatives of the private financial sector and for all US federal entities and their counterparties, compliance with NIST CSF requirements is mandatory. Another difference between ISO 27001 and NIST CSF is the process of compliance, namely, in the case of ISO 27001, in order for a financial institution to prove its compliance with the standard, it will need to be certified, while in the case of NIST CSF, no certification is needed.[148]

2.3.2. PCI DSS

The next important standard is PCI DSS or Payment Card Industry (PCI) Data Security Standards (DSS), which has a binding nature.[149] Developed by Payment Card Industry, the Standard applies to all financial institutions issuing credit cards and processing credit card transactions, and all their counterparties receiving and processing credit card information, such as payment solution providers. The goal of creating the PCI DSS is to ensure the security of credit card transactions, protect the identity of cardholders and reduce fraud. Generally, the Standard consists solely of technical and operational requirements that ensure security at the three major stages of the confidential credit card data lifecycle – storage, transmission and processing.[150] Because PCI DSS is a mandatory standard in its application, non-compliance will cost financial institutions USD 5,000 to USD 100,000 per month.[151]

2.3.3. Other standards

In general, based on the study of the World Bank Group, at the international level, about 50 different mandatory and optional standards, guidances, notices, strategies, working papers and

[147] Vanta. NIST CSF vs. ISO 27001: What's the difference? Available on: https://www.vanta.com/resources/nist-csf-vs-iso-27001-whats-the-difference. Accessed May 4, 2023.
[148] *Ibid*.
[149] Halder, *supra* note 145.
[150] *Ibid*.
[151] Ekran System. 7 Best Practices for Banking and Financial Cybersecurity Compliance (2022), available on: https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance. Accessed May 5, 2023.

other documents can be counted, which can also be attributed to the regulation of cybersecurity in the financial sector.[152] In addition to the frameworks discussed earlier, one can also note the G7 Cyber Expert Group's (G7 CEG) Fundamental Elements of Cybersecurity for the Financial Sector,[153] binding Society for Worldwide Interbank Financial Telecommunication (SWIFT) Customer Security Program[154] and Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO) Guidance on cybersecurity[155]. To one extent or another, all of them are trying to improve cybersecurity, bring legal clarity and provide guidance to financial sector representatives in need of cybersecurity.

[152] World Bank Group. "Financial Sector's Cybersecurity: A Regulatory Digest, 6th edition" (2021): p. 4, available on: https://thedocs.worldbank.org/en/doc/3c28bd048d78efd27744987253e2c44a-0430012021/related/CybersecDigest-v6-FINAL-vs.pdf. Accessed May 6, 2023.
[153] *Ibid*., p. 96.
[154] *Ibid*., p. 93.
[155] *Ibid*., pp. 123-124.

3. Elimination of present legal grey areas in European cybersecurity regulation in the financial sector

As shown by the legislative analysis of the current EU regulations governing cybersecurity in the financial sector, Europe is actively reviewing and reforming its cybersecurity legislation; this is clearly seen in the recently adopted NIS 2 Directive and DORA Regulation. Nevertheless, even with these reasonably successful attempts to improve and harmonise cybersecurity regulation in the financial sector, there remain a few legal grey areas that could potentially threaten the stability of the European financial market. Thus, some of the legal challenges of regulating cybersecurity in the financial sector at the moment are the use of the "one-size-fits-all" principle regarding the applicability of cybersecurity legislation to financial institutions, making an exception only for systematically important financial institutions, the lack of uniform standards for the cyber reporting procedure, the lack of provisions that clearly prescribe the type and amount of penalties for non-compliance with cybersecurity requirements and other legal challenges. In this regard, it remains to be seen whether there is a unified solution on the part of EU legislators to eliminate the current legal grey areas in the regulation of cybersecurity in the financial sector and also to find out what practical actions representatives of the financial sector need to take to create and maintain an effective cybersecurity strategy for their financial institution and comply with current legislation and existing best practices in the field of cybersecurity regulation in the financial sector.

3.1. Creation of the Single European Cybersecurity Regulation for the financial sector (SECYR)

A potential unified solution by EU legislators to eliminate the current legal grey areas in the regulation of cybersecurity in the financial sector will be reform at the EU level by adopting the Single European Cybersecurity Regulation for the financial sector (SECYR). EU legislators, for example, the European Commission, have the right to determine the type of potential legislative act, whether it will be a Regulation or a Directive. Although in order to achieve complete harmonisation at both European and national levels and create a level playing field, it is assumed that the only appropriate form for this piece of legislation is binding in its entirety and directly applicable in all Member States – Regulation. The main goals of SECYR will be to eliminate the existing fragmentation of the legal framework for regulating cybersecurity in the financial sector, provide legal certainty, create a level playing field for the implementation of cybersecurity for financial institutions and comparability of cybersecurity

requirements with the level of maturity of the representative of the financial sector and its cybersecurity strategy.

3.1.1. Scope of applicability

In order to create effective regulation of cybersecurity in the financial sector in the form of the adoption of SECYR, its provisions should clearly state its scope of applicability. Thus, the provisions of SECYR, determining to whom it will apply and to what extent it will need to be implemented, will be considered below.

(a) International

The level of development and application of SECYR should ideally be international or even, to some extent, global, covering as many countries as possible. Since the nature of cyberspace is transnational, regulation of cybersecurity in the financial sector can only be effective and equal if there is coordination and cooperation from all states participating in cyberspace. But certainly, in today's political realities and due to the different levels of development of countries and their cybersecurity strategies, the possibility of global cooperation and the creation of a single response to cyber threats in the form of a single binding on all parties Regulation is seen as something impossible. Nevertheless, in highly integrated societies such as the EU and the US, creating a single effective cybersecurity system in the financial sector seems possible. Examples of international applications that SECYR should follow are the previously analysed GDPR and PSD2 legislation, which apply not only to EU financial institutions but also to international representatives of the financial sector conducting financial activities in the EU or serving EU consumers, thereby also covering representatives of the US financial sector. As part of the creation of SECYR, such cooperation between the EU and the US in the form of an exchange of experience, practices, resources, capabilities and responsibilities regarding the regulation of cybersecurity in the financial sector can lead to harmonisation and effective regulation of cybersecurity at the international level, as well as initiate other countries to join the common EU-US strategy to regulate cybersecurity in the financial sector thereby contributing to the globalisation of SECYR.

(b) Cross-sectoral

The next aspect of the SECYR application is the cybersecurity regulation sector. SECYR should not apply exclusively to the financial sector, but at the same time, it should not apply to cybersecurity regulation in general since the absence of a financial specification in the provisions of SECYR carries the risk of creating abstract provisions and minimising legal

clarity. Thus, SECYR should be a cross-sectoral piece of legislation aimed at regulating cybersecurity in the financial sector while also covering and being applicable to sectors in which third-parties to financial institutions operate. These are all sectors in which third-party services critical to the financial institution operate, *i.e.*, for example, SECYR should also apply to the sector of cloud services, payment and settlement systems, software, marketplace and insurance.

(c) Covered entities

When establishing the specific individuals to whom SECYR will apply, Section 500.01(c),(i) of NYDFS Cybersecurity Regulation gives an excellent example for formulating what is meant by the concept of Covered Entity under the SECYR legislation

> Covered Entity means any Person [any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association] operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorisation under the Banking Law, the Insurance Law or the Financial Services Law.[156]

Although it should be noted that as discussed earlier in the legislative analysis, Article 2(1)(a)-(u) of DORA Regulation provides relatively comprehensive coverage of regulated financial institutions and their counterparties, such prescribing of all persons to whom the Regulation may apply, puts the representatives of the financial sector in an unequal position and significantly increases the chance that out of scope financial entities will be at increased risk of cyberattacks and can potentially destabilise the European financial market.

(d) Determination of the level of complexity of a financial institution's cybersecurity strategy based on three criteria – size, importance and maturity of the financial institution

Existing laws governing cybersecurity in the financial sector often use the "one-size-fits-all" principle concerning the applicability of cybersecurity laws to financial institutions, making only occasional exceptions in the application based on the size of the financial institution – small, medium or large financial entity or its importance, as seen, for example, in the previously discussed DORA Regulation. Focusing only on the size of a financial institution and its importance and not taking into account its maturity and the development of an internal cybersecurity strategy potentially leads to unequal regulatory treatment and, accordingly, to the impossibility of implementing legal provisions by all financial institutions, which ultimately leads to inefficiency of cybersecurity regulation in the financial sector in general. Thus, SECYR needs to lay down the following three criteria – the size, importance and maturity of the

[156] NYDFS 23 NYCRR 500 (NYDFS Cybersecurity Regulation), *supra* note 133, p. 2.

financial institution; once determined, the appropriate level of cybersecurity requirements for the financial institution can be established.

The first criterion for establishing the proper application of the SECYR requirements will be based on the size of the financial institution and the following provisions of the DORA Regulation and its legal wording can be used as an example:

> '[M]icroenterprise' means a financial entity […] [that] employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million. […]
>
> '[S]mall enterprise' means a financial entity that employs 10 or more persons, but fewer than 50 persons, and has an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but does not exceed EUR 10 million.
>
> '[M]edium-sized enterprise' means a financial entity that is not a small enterprise and employs fewer than 250 persons and has an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million.[157]

And accordingly, it is possible to formulate the definition for Large enterprise', which is absent in the DORA Regulation, namely

> 'Large enterprise' means a financial entity that is not a medium-sized enterprise and employs more than 250 persons and has an annual turnover that exceed EUR 50 million and/or an annual balance sheet that exceed EUR 43 million.[158]

The second criterion for establishing the proper application of the SECYR requirements will be based on the determination of the importance of the financial institution. Here it is necessary to clearly establish that the division is possible only into two degrees of importance – SIPS and all other financial institutions. In the above-conducted analysis of European legislation regulating cybersecurity in the financial sector, the wording "essential and important entities" was repeatedly encountered, which potentially narrows the scope of applicability of legislation and imposes additional obligations on Member States in the form of establishing and updating the list of essential and important financial entities, which will be pretty subjective. Moreover, also in the above-conducted theoretical analysis, it was revealed that in the event of a failure in the work of one of the participants in the financial system providing non-critical financial services, there is as well a high risk of failure of an essential or important participant supplying critical financial services and *vice versa*; this phenomenon was called Single Point of Failure.[159] Thus, it is impossible to determine the importance of one financial institution in comparison with another, except for SIPS, whose failure due to their indispensability and high concentration, threatens to shut down the entire domestic and international economy and,

---

[157] Regulation (EU) 2022/2554 (DORA), *supra* note 11.
[158] *Ibid*.
[159] European Central Bank, *supra* note 54.

accordingly, the cybersecurity requirements for SIPS should be prescribed separately and be more specific and strict.

The third criterion for establishing the proper application of the SECYR requirements will be based on determining the maturity of the financial institution and its cybersecurity strategy. The need for such an approach is associated with the rapid evolution of the financial sector and the entry into the financial market of such new players as fintechs (most often in the form of startups) – small financial technology firms. It is impossible to compare the development level of fintech cybersecurity strategy, which has neither the necessary experience nor sufficient resources to implement cybersecurity at a high level, with the development of the cybersecurity strategy of a large bank operating in the financial market for more than 20 years. It follows that it is impossible to apply the exact cybersecurity requirements to a newly created fintech and a bank that has existed for 20 years since this creates an uneven playing field and the apparent impossibility for newly created financial institutions to comply with cybersecurity regulation.

Thus, once the three SECYR criteria of size, importance and maturity of a financial institution are determined, the required level of its cybersecurity can be clearly established. To achieve maximum equality of cybersecurity conditions among representatives of the financial sector, it is proposed to introduce three levels of complexity of the cybersecurity strategy: 1) evolved, 2) advanced and 3) innovated; the higher the level of complexity, the more cybersecurity requirements SECYR imposes on a financial institution. A small, newly established fintech company is required to meet the first level (evolved) complexity of the cybersecurity strategy and strive to reach the next level; in turn, SIPS are required to meet the second level (advanced) complexity of the cybersecurity strategy and also strive to reach the next level. Subsequently, a timeframe can be proposed for financial institutions to move to the next level of cybersecurity strategy complexity, but at the initial stage of SECYR development, such a requirement is not necessary.

3.1.2. Substantive provisions

Having set the scope of applicability of SECYR, it is necessary to go directly to the substantive provisions of the Regulation. The SECYR requirements will cover all vital elements of an effective cybersecurity regulatory framework, namely the following five areas: cybersecurity risk management, cyber incident reporting, cyber-intelligence sharing, cybersecurity resilience testing and third-party cybersecurity risk management. The main goal of all SECYR provisions will be to support the cybersecurity of a financial institution at the stages of prevention,

detection, response and recovery from a cyberattack. It should be noted that in order to create the most practically applicable cybersecurity requirements for the financial sector, all of the following requirements are minimum requirements, which means they are mandatory for all financial institutions, regardless of the applicable level of complexity of the cybersecurity strategy – 1) evolved, 2) advanced or 3) innovated. However, it should be clarified that all financial institutions with the first level (evolved) of the complexity of cybersecurity strategies are allowed to implement the minimum requirements using simplified SECYR provisions, for example, a lower level of detail in their Cybersecurity Strategy and Policy, less frequent training and internal and external cybersecurity audits and so on. In turn, financial institutions with the third level (innovated) of the complexity of cybersecurity strategies will be required to implement the minimum requirements using the more demanding provisions of SECYR, such as a higher degree of detail in their Cybersecurity Strategy and Policy, frequent training and internal and external cybersecurity audits and more. All simplified and complex provisions should be clearly established in the SECYR, but in this research, due to its limited scope, simplified and complex provisions are spelled out only in some aspects of the Regulation.

(a) Cybersecurity risk management

The first area of SECYR regulation is cybersecurity risk management, and a reasonable basis for its substantive provisions is provided by the second chapter of the DORA Regulation and Sections 500.02-500.04, 500.08-500.10, 500.12-500.16 of the NYDFS Cybersecurity Regulation. Thus, the following potential SECYR requirements regarding the cybersecurity risk management of a financial institution can be identified:

- Financial institutions must implement and maintain a Cybersecurity Strategy and Policy covering its application security, risk assessment, data management including limitations on data retention, access controls including multi-factor authentication, monitoring and encryption of non-public information, and customer privacy;
- Financial institution’s management body must take responsibility for developing and approving its Cybersecurity Strategy and Policy;
- Financial institutions must implement and maintain a Business Continuity Policy;
- Financial institution’s management body must approve, oversee and periodically review the implementation of the Business Continuity Policy;
- Financial institutions must have an Incident Response and Recovery Plan in order to respond and mitigate the consequences of a cyberattack quickly;

- Financial institution's management body must approve, oversee and periodically review the implementation of the Incident Response and Recovery Plan in the event of a cyberattack;
- Financial institutions must establish acceptable risk levels for cyber failures;
- Financial institutions must appoint a Chief Information Security Officer responsible for overseeing and implementing the financial institution's cybersecurity strategy and enforcing its cybersecurity policy;
- Financial institutions must implement and maintain Internal and External Cybersecurity Audit Programs;
- Financial institutions must conduct cybersecurity training for personnel on an ongoing basis.

(b) Cyber incident reporting

The second area of SECYR regulation is cyber incident reporting. Since the basis for maintaining effective cybersecurity regulation, *i.e.*, reviewing and changing existing cybersecurity requirements, is reliable statistics on cyber incidents, legislators need access to them. As shown by the above-conducted legislative analysis of the current regulation of cybersecurity in the financial sector, at the moment, there are no uniform and harmonised requirements for financial institutions regarding cyber incident reporting; most of the legislation does not prescribe provisions related to cyber incident reporting at all or only mention the time during which a supervisory authority must be notified of a cyber incident, as is done in Section 500.17(a) of the NYDFS Cybersecurity Regulation, setting a time period of 72 hours[160]. Thus, in order to obtain reliable and sufficient data on cyber incidents and their root causes, it is necessary to implement the following SECYR harmonised requirements for the cyber incident reporting procedure:

- Financial institutions must independently establish the materiality criterion of a cyber incident. Since a financial institution will not physically be able to report on every cyber incident, and the governing body will not be physically able to process such a volume of data, financial institutions need to establish clear criteria for determining the significance of a cyber incident that has occurred, for example, by its size, the cost of losses, the time it takes for a complete recovery of a financial institution after a cyber incident and other factors;

[160] NYDFS 23 NYCRR 500 (NYDFS Cybersecurity Regulation), *supra* note 133, p. 10.

- SECYR must identify the principal cybersecurity regulator in each Member State, to whom the financial institution should report first. SECYR does not restrict financial institutions from cyber incident reporting to other bodies, such as other regulators, peer financial institutions or customers, provided that all requirements of the GDPR are met;
- SECYR shall provide a sample of a uniform and standardised basic cyber incident reporting format for financial institutions;
- SECYR should establish specific deadlines for financial institutions for *ex-post* notification of their cyber incidents, in particular establishing three tiers of reporting: (1) initial notification (within three hours of a cyber incident), (2) interim notification (within three days of the cyber incident) and (3) final notification (within two weeks after the financial institution has fully recovered from the cyber incident and returned to the previous quality and volume of work); also, within a day after the occurrence of a cyber incident, information about a violation of obligations to ensure cybersecurity of data must be published on the official website of the financial institution;
- SECYR should establish a requirement for financial institutions to produce an annual (preceding calendar year) report on the status of their cybersecurity strategy, including analysed statistics on cyber incidents.

(c) Cyber-intelligence sharing

The third area of SECYR regulation is cyber-intelligence sharing between private-sector financial institutions and between the private sector and public authorities. Some of the previously discussed legislation regulating cybersecurity in the financial sector casually mentioned the desirability of cyber-intelligence sharing among financial sector participants, but left the implementation of this requirement on a voluntary basis. In turn, the provisions of SECYR should oblige financial institutions to cooperate effectively and share important information related to cybersecurity with other financial institutions and government bodies. Such cooperation between the private sector, as well as the private and public sectors, will allow combining the resources of all participants, thereby significantly increasing the effectiveness of cybersecurity regulation and the fight against cybercrime in the financial sector.

An example of important cyber information that should be shared is operational, tactical and strategic cyber threat data. However, there are several barriers to sharing such information. These obstacles include competition and lack of trust between financial institutions, commercial and banking secrecy, confidentiality and data protection under the GDPR, and national security risks in the case of the exchange of information between countries. Nevertheless, some measures can solve these obstacles if financial institutions and government

bodies move towards mutual trust. One such measure could be the creation by regulators of a secure platform for cyber-intelligence sharing, which guarantees confidentiality by anonymising the information transmitted by financial institutions.

(d) Cybersecurity resilience testing

The fourth area of SECYR regulation is cybersecurity resilience testing. Although DORA provides a sound basis for SECYR provisions regarding cybersecurity testing, namely, it obliges financial institutions to conduct general security tests of their cyber systems at least once a year and in the case of financial institutions that are considered systemically important and mature, Article 26 of DORA also imposes an obligation on them to conduct "at least every 3 years advanced testing by means of TLPT,"[161] SECYR's requirements should be stricter. As threat-led penetration testing (TLPT), a controlled attempt to compromise the cyber resilience of an institution by simulating a real cyberattack, is one of the most effective methods for measuring a financial institution's current level of cybersecurity preparedness, requiring TLPT as part of SECYR should be mandatory for all financial institutions, regardless of their importance and maturity. So, for example, financial institutions with the first level (evolved) of the complexity of cybersecurity strategies will be required to conduct general security tests of their cyber systems and advanced testing through TLPT at least once a year. In turn, financial institutions with the second (advanced) and third (innovated) levels of the complexity of cybersecurity strategies will be required to conduct general security tests of their cyber systems and advanced testing through TLPT at least once every six months.

(e) Third-party cybersecurity risk management

Finally, the fifth area of SECYR regulation is third-party cybersecurity risk management. The current legislation perfectly prescribes all the requirements regarding third-party risk management, so it remains only to duplicate them in SECYR. Thus, the SECYR requirements should include Section 500.11 of the NYDFS Cybersecurity Regulation and the fifth chapter of the DORA Regulation, including an obligation on financial institutions to treat third-party risk management as an integral part of their own cyber risk management, to have policies and procedures in place to ensure the security of data available to third-party service providers or any other parties, establishing certain conditions and minimum requirements for the composition of outsourcing contracts that contribute to the maintenance of the critical functions of financial institution and establishing a "Lead Overseer", a specific oversight body for all

[161] Regulation (EU) 2022/2554 (DORA), *supra* note 11.

third-party cyber service providers that are critical to financial institutions, thereby forcing third-party providers of critical cyber services to improve their operational resilience and cybersecurity processes.[162]

3.1.3. Enforcement

Having established the scope of applicability and substantive provisions of SECYR, it is finally necessary to proceed directly to the enforcement provisions of the Regulation. Therefore, the following SECYR enforcement mechanisms will be discussed below: penalties, establishing a national cybersecurity body for the financial sector, licensing and certification, and keeping regulations up to date.

(a) Penalties

Indeed, one of the most essential enforcement mechanisms is appropriate and adequate punishment. As the US experience has shown, including through criminalisation and the presence in their legislation of clear provisions regarding fines and their amounts applicable in case of non-compliance, the US has become the most powerful nation in the field of cybersecurity in the world. At the initial stage of SECYR development, it will be most effective and rational to combine the already existing Article 34 of the NIS 2 Directive and Section 906 of SOX, thereby establishing that in case of non-compliance with the SECYR, financial institutions with the second (advanced) and third (innovated) levels of the complexity of cybersecurity strategies can be fined up to EUR 10 million or 2% of the annual turnover, whichever is greater and financial institutions with the first level (evolved) of the complexity of cybersecurity strategies can as well be fined up to EUR 7 million or 1.4% of annual turnover, whichever is greater; also if the public financial institution fails to comply with the SECYR requirements, the penalty could be in the form of exclusion from the listing of the public stock exchange; finally, if the non-compliance was solely by or through the fault of public financial institution officials, the fine could be up to EUR 4 million and/or up to twenty years in prison, depending on whether the non-compliance with the law is intentional. However, in addition to explicit provisions regarding fines and their amounts, SECYR should also establish a straightforward process for determining liability for a breach of cybersecurity and the proportionality of punishment for it since the ability of a financial institution to prevent a cyberattack is not always determined by its own actions or inactions; for example, in the event

[162] Regulation (EU) 2022/2554 (DORA), *supra* note 11.

of a cyberattack on the state financial system, punishing one or another financial institution would not make any sense.

(b) Establishing a national cybersecurity body for the financial sector

The following important enforcement mechanism is the mandatory creation of a national cybersecurity body for the financial sector. Based on the specifics of cybersecurity regulation in the financial sector, having a general national cybersecurity body responsible for cybersecurity regulation in all sectors is not enough. The primary responsibilities that the national cybersecurity body will perform for the financial sector will be to supervise the enforcement by financial institutions of mandatory laws governing cybersecurity, determine responsibility for violations of cybersecurity and establish proportional punishment for it, promptly respond to cyber incidents, support financial and government institutions in the investigation of cyber incidents (coordination and assistance in the development of operational actions), the exchange of important cyber information with financial institutions and authorities, the analysis of existing and forecasting future cyber threats, the provision of strategic reports on cybersecurity, the implementation of close cooperation with the private and public sectors, and the implementation of close cooperation with the national cybersecurity body for the financial sector of other Member States that have adopted SECYR.

(c) Licensing and certification

Another important enforcement mechanism that SECYR must establish is the licensing and certification of the financial institution's cybersecurity, which will serve as evidence of the financial institution's compliance with all SECYR requirements on an ongoing basis. Thus, within the framework of SECYR, a single agreed-upon cybersecurity certification scheme for a financial institution should be created. At the initial stage of SECYR development, such a scheme can be based on the existing ISO 27001 certification process analogy. For example, financial institutions with the first level (evolved) of the complexity of cybersecurity strategies will be required to undergo cybersecurity certification every two years. In turn, financial institutions with the second (advanced) and third (innovated) levels of the complexity of cybersecurity strategies will be required to undergo cybersecurity certification once a year.

(d) Keeping regulations up to date

Finally, SECYR can only be enforceable if its requirements are relevant and up to date, so an important enforcement mechanism, but one that will already be imposed on the legislature issuing SECYR, is to ensure that SECYR is always up to date. Because the nature of cyberspace is volatile – new technological breakthroughs arise together with new cyber threats, the SECYR

regulations need periodic review by competent personnel with a high level of knowledge and best practices in the field of cybersecurity in the financial sector. Such periodic reviews of the SECYR provisions should take place at least every two years, considering the strategic cybersecurity reports received from each participating state and its national cybersecurity body for the financial sector. In addition to periodic reviews, another tool for keeping SECYR up to date is the presence in the Regulation of "sunset clauses" – legal clauses that the legislator can cancel after the expiration of the established period unless a decision has been made to extend the validity of the clause.[163] Such a temporary legislative measure will allow the legislator to quickly respond to changes in cyberspace in the financial sector, "test" new approaches to cybersecurity regulation and eliminate the need for frequent revision of SECYR.

3.2. Recommendations on the proper application of current cybersecurity legislation for representatives of the European financial sector

Based on the fact that Member States must implement the NIS 2 Directive by October 17, 2024, and the DORA Regulation by January 17, 2025, financial institutions can no longer postpone taking the necessary steps to comply with the new legislation. The following recommendations are examples of practical actions that financial sector representatives need to take to create and maintain an effective cybersecurity strategy for their financial institution and comply with current legislation and existing best practices in the field of cybersecurity regulation in the financial sector. These recommendations are addressed to all financial sector representatives, including their third parties, IT and cybersecurity developers, consulting firms and the general public interested in cybersecurity regulation in the financial sector.

1. Assess the current state of the financial institution's cybersecurity and its resilience to cyberattacks and other external influences.
2. Identify if the financial institution is or could potentially be subject to new legislation in the form of the NIS 2 Directive and DORA Regulation.
3. Establish the requirements of the new legislation that the financial institution will need to implement, including whether all of the procedures and processes described below are implemented in the financial institution's cybersecurity strategy:
   (a) Existence of an organisational structure and establishment of a clear division of responsibility regarding the implementation of cybersecurity in a financial institution

[163] Calliess and Baumgarten, *supra* note 36, p. 1176.

between the Chief Executive Officer (CEO), Chief Operations Officer (COO), Chief Risk Officer (CRO), Chief Information Officer (CIO) and Chief Information Security Officer (CISO); including a high-level involvement of the financial institution's board in cybersecurity matters.

(b) Availability of a digital operational resilience strategy and policy.

(c) Assumption of responsibility by the financial institution's management body for developing and approving a digital operational resilience strategy and policy.

(d) Availability of basic cyber hygiene practices.

(e) Presence of a business continuity policy that ensures the continuity of the critical operations of a financial institution during any possible technical failures and cyberattacks.

(f) Existence of a response and recovery plan that includes a detailed description of what constitutes a cyberattack and cybersecurity failure, how employees should respond, what internal and external resources are needed, and how the financial institution's critical operations will be recovered in the event of a cyberattack or any other breach of cybersecurity integrity.

(g) Assumption of responsibility by the financial institution's management body for approving, overseeing and periodically reviewing the implementation of the business continuity policy and response and recovery plan.

(h) Establishment by a financial institution of acceptable risk levels for cyber failures, which must satisfy the increased level of ICT security established by DORA Regulation.

(i) Maintenance of a cybersecurity programme by the financial institution that includes regular risk assessment for cyber failures and an action plan to mitigate these.

(j) Existence of an appropriate cyber and ICT-related incident management process, including the ability of the financial institution to classify the impact of cyber incidents and analyse their root causes.

(k) Maintenance of a clear cybersecurity reporting system for reporting cyber incidents to national and European competent authorities, including the existence of procedures and processes to facilitate the rapid exchange of information about cyber incidents with third parties, *i.e.* financial institution customers and service providers.

(l) Availability of highly qualified personnel with innovative thinking, relevant education, in-depth expertise in technology and compliance with regulatory requirements for cybersecurity in the financial sector.

(m) Availability and implementation of cybersecurity training for financial institution personnel that will give them the necessary knowledge and skills to identify and manage cybersecurity risk.

(n) Maintenance of adequate security controls for the financial institution's digital infrastructure, including, but not limited to, encryption, authentication, access control, audit trails, monitoring systems, incident management systems, and incident response plans.

(o) Existence and ability of the financial institution to implement a digital operational resilience testing policy; for systematically important and mature financial institutions, it is also the existence and ability to implement a threat-led penetration testing policy.

(p) Treatment of third-party risk management as an integral part of financial institutions' own cyber risk management.

(q) Presence of certain conditions and minimum requirements in financial institutions' outsourcing contracts, as set out in the DORA Regulation that contribute to the maintenance of the critical functions of financial institutions and ensure an uninterrupted supply chain that meets cybersecurity requirements.

(r) Existence of an oversight system for all third-party cyber service providers that are critical to financial institutions.

4. Identify whether there are any related or additional national cybersecurity requirements in the financial sector; if so, pursue a coordinated implementation approach with the above requirements.
5. Cooperate effectively within the private sector, *i.e.* share important information related to cybersecurity in the financial sector, lessons learned from cyber incidents and cyber testing exercises with other financial institutions.
6. Collaborate effectively with financial institution regulators to gain a comprehensive understanding of regulatory and supervisory requirements for cybersecurity in the financial sector and ensure alignment with the financial institution's commercial priorities; particularly important for financial institutions operating in multiple jurisdictions to identify gaps and overlaps in regulatory and supervisory requirements regarding cybersecurity in the financial sector.
7. Checking by third parties that provide products, services or processes for financial institutions, even if they are not directly subject to new legislation, whether the Member States in which they operate will require financial institutions to use certified products, services or processes; if so, national legislation governing cybersecurity in the financial

sector imposes an obligation on third parties to undergo certification of the products, services or processes provided.

4. Conclusions

The subject area examined in this Master Thesis is of considerable relevance, given the ongoing initiatives to regulate cybersecurity in the financial sector in the EU and US legislation frameworks. The main aim of the research was to study the issues of creating a unified framework for European cybersecurity regulation in the financial sector, establishing the perspectives on the elimination of present legal grey areas in European cybersecurity regulation in the financial sector, as well as to formulate recommendations for representatives of the European financial sector on the proper application of current cybersecurity legislation. Various considerations, legal requirements and perspectives have been assessed, and the following conclusions are drawn from this research's analysis.

Recently regulation of cybersecurity in the financial sector has started to attract significant attention from legislators and legal scholars due to the high vulnerability of the industry to cyberattacks. The main focus of the analysis of outstanding academic research is skewed to the technological complexities of cyberspace and financial systems, rather than on the legal aspect of cybersecurity regulation in the financial sector. Despite the lack of a common definition, it is established that cybersecurity in the financial sector refers to measures and controls implemented by the financial institution and regulatory bodies to protect the financial institution, its data and financial market integrity in general from cyber threats.

The categorisation of possible cyber threats in the financial sector divided them into cyberwar, cyber espionage, cyber terrorism, cyber vandalism and the most common cybercrime for financial gain. The key identified factors as causing cyber threats in the financial sector are lack of preparation by the financial industry representatives, citizens using financial instruments and governments that regulate national cyberspace; human element including skills gap, human error and remote work; technological complexity of the financial system; the interconnectedness of financial institutions, various actors and infrastructures within the financial sector and regulatory complexity when dealing with the volatility of cyberspace. The main legal complications of regulating cybersecurity in the financial sector are identified in the form of jurisdictional fragmentation arising from the inability to establish clear geographical boundaries of cyberspace, establishing responsibility for behaviour due to the anonymity of cyberspace and establishing responsibility for regulatory action due to the difficulty of determining who has more knowledge and experience, the private sector or government agencies.

Legislative analysis revealed that countries are still limited in harmonising regulation of cybersecurity in the financial sector within the current EU and the US legal frameworks. Lack of a clear division of responsibility for overlapping requirements of various legislative acts regulating cybersecurity in the financial sector; not taking into account, when regulating, the maturity and development of cybersecurity of the financial institution; the use of different sectoral approaches, some legislative acts regulate cybersecurity exclusively in the financial sector, in some cases even regulating only subsectors (*e.g.* payment systems), while some regulate cybersecurity in general; the lack of uniform standards for the cyber reporting procedure; not binding cyber-intelligence sharing between the private sector and public authorities and lack of provisions that clearly prescribe the type and amount of penalties applicable for non-compliance with legislation were recognised as the major limiting factors. Nevertheless, recent changes in the EU and the US legal frameworks have significantly increased the level of cybersecurity regulation in the financial sector.

The principal changes in cybersecurity regulation in the European financial sector were the recently adopted NIS 2 Directive and DORA Regulation by the European Commission on January 16, 2023. While NIS 2 Directive applies to all companies providing essential and important services to the European economy, DORA Regulation applies exclusively to all regulated financial institutions and their counterparties. Both legal acts establish requirements regarding cybersecurity risk management, incident reporting, digital operational resilience testing and third-party risk management and, for the first time, establish liability of the management bodies of a financial institution in the event of cybersecurity failure. Despite many similarities and even overlapping provisions of the NIS 2 Directive and DORA Regulation, the latter constitutes *lex specialis* with regard to NIS 2 Directive. Within US legal framework, a real breakthrough was the Cybersecurity Regulation adopted by the New York State Department of Financial Services in 2019, which is almost identical in scope to the DORA Regulation, except that the NYSDFS Cybersecurity Regulation does not prescribe as detailed covered entities as the DORA Regulation, thereby expanding and regulating a larger number of financial sector entities. Apart from binding legislation, the framework for regulating cybersecurity in the financial sector also includes a large number of international standards, among which ISO 27001, NIST CSF and PCI DSS can be singled out, even though their requirements are highly technical. Thus, it is possible to highlight the positiveness of legislative trends in regulating cybersecurity in the financial sector.

A practical analysis revealed that all the previously established limiting factors and legal grey areas in the current legislation regulating cybersecurity in the financial sector could be

eliminated with the help of reform by adopting the new legislation proposed by the author – Single European Cybersecurity Regulation for the financial sector (SECYR). The uniqueness of this legislation derives from its international character; cross-sectoriality; covering a large number of representatives of the financial sector; establishing the required level of complexity of a financial institution's cybersecurity based on three criteria – size, importance and maturity of the financial institution; setting uniform and harmonised requirements for cyber incident reporting; imposing the obligation of cyber-intelligence sharing between private-sector financial institutions and between the private sector and public authorities; establishing clear penalties and criminalisation for non-compliance with Regulation; imposing the obligation of establishing a national cybersecurity body for the financial sector; requiring the licensing and certification of a financial institution's cybersecurity and having sunset provisions for keeping regulations up to date.

In order for the representatives of the European financial sector to be compliant with the soon to be implemented by Member States NIS 2 Directive and DORA Regulation, they need to immediately assess the current state of the financial institution's cybersecurity and its resilience to cyberattacks. The principal recommendations on the proper application of current cybersecurity legislation for representatives of the European financial sector can be the creation of a digital operational resilience strategy and policy, basic cyber hygiene practices, a business continuity policy, a response and recovery plan in the event of a cyberattack and a digital operational resilience testing policy; regular risk assessment for cyber failures; establishment of a clear organisational structure; enactment of a cyber and ICT-related incident management process including cybersecurity reporting system; hiring highly qualified personnel and conducting cybersecurity training for them; implementation of adequate security controls; establishment of third-party risk management including implementation of certain conditions and minimum requirements in financial institutions' outsourcing contracts and the creation of a third-party oversight system.

In the future, the author intends to research in more detail the EU and the US cybersecurity governance structures – institutions, bodies and agencies and their possible assistance to existing legislation in regulating cybersecurity in the financial sector. In addition, the author also plans to conduct expert interviews with regulators adopting cyber security requirements at the national level and cyber security professionals to establish the legal prospects for cyber security regulation in the financial sector in the next couple of years.

Summing up the entire research, the hypothesis put forward earlier was fully confirmed. Establishing a unified and harmonised cybersecurity regulatory framework for the international

financial sector by reforming financial sector cybersecurity regulation and eliminating existing legal grey zones is indeed possible, even despite the different levels of cybersecurity development in the financial sector in different countries and the technological complexities of the financial system and cyberspace. Hence, if legislators allow, the proposed reform by adopting a new SECYR Regulation could become an effective mechanism for regulating cybersecurity in the financial sector and the future of international law.

5. Bibliography

Primary sources:

Legislation:

1. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2), *OJ L* 337, 23.12.2015, pp. 35-127. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366. Accessed April 16, 2023.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS), *OJ L* 194, 19.07.2016, pp. 1-30. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148. Accessed April 20, 2023.
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2), *OJ L* 333, 27.12.2022, pp. 80-152. Available on: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Accessed June 13, 2023.
4. Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (CRD IV), *OJ L* 176, 27.06.2013, pp. 338-436. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013L0036. Accessed April 17, 2023.
5. New York State. New York State Department of Financial Services 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies (2017) (NYDFS Cybersecurity Regulation): pp. 2-10. Available on: https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf. Accessed April 29, 2023.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), *OJ L* 119, 04.05.2016, pp. 1-88. Available on: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed April 13, 2023.

7. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA), *OJ L* 333, 27.12.2022, pp. 1-79. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554. Accessed June 13, 2023.
8. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (CRR), *OJ L* 176, 27.06.2013, pp. 1-337. Available on: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32013R0575. Accessed April 17, 2023.
9. Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (SIPS Regulation), *OJ L* 217, 23.07.2014, pp. 16-30. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0795. Accessed April 14, 2023.
10. United States. Sarbanes-Oxley Act of 2002 (SOX), Public Law 107-204, 116 Stat. 745 (2002): p. 35. Available on: https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf. Accessed April 26, 2023.

Secondary sources:

Books:

1. Brenner, Susan W. "Cybercrime and the Law: Challenges, Issues, and Outcomes." Boston: Northeastern University Press, 2012.
2. Clough, Jonathan. "Jurisdiction." Chapter. In *Principles of Cybercrime*, 2nd ed. Cambridge: Cambridge University Press, 2015. Accessed March 18, 2023. doi:10.1017/CBO9781139540803.015.

Journal articles:

1. Calliess, Christian, and Ansgar Baumgarten. "Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective." *German Law Journal*, Volume 21, Issue 6 (2020): pp. 1153-1176. Accessed March 7, 2023. doi: 10.1017/glj.2020.67.
2. Carrapico, Helena, and André Barrinha. "The EU as a Coherent (Cyber)Security Actor?" *JCMS: Journal of Common Market Studies*, Volume 55, Issue 6 (2017): p. 1255.
3. Didenko, Anton N. "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond." *Uniform Law Review*, Volume 25, Issue 1 (2020): pp. 126-127. Accessed March 24, 2023. doi: 10.1093/ulr/unaa006.
4. Sales, Nathan Alexander. "Privatizing Cybersecurity." *UCLA Law Review*, Volume 65, Issue 3 (2018): p. 628.
5. Stahl, William M. "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity." *Georgia Journal of International and Comparative Law*, Volume 40, Issue 1 (2011): pp. 261-262.
6. Teplinsky, Melanie J. "Fiddling on the Roof: Recent Developments in Cybersecurity." *American University Business Law Review*, Volume 2, Issue 2 (2013): p. 249.
7. Urbas, Gregor. "Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement." *Journal of Internet Law*, Volume 16, Issue 1 (2012): p. 8.
8. Weber, Amalie M. "The Council of Europe's Convention on Cybercrime." *Berkeley Technology Law Journal*, Volume 18, Issue 1 (2003): p. 433.

Official working papers:

1. Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO). "Principles for financial market infrastructures" (2012): p. 5. Available on: https://www.bis.org/cpmi/publ/d101a.pdf. Accessed April 14, 2023.
2. Bouveret, Antoine. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." International Monetary Fund (IMF) Working Paper (2018): p. 12. Available on: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924. Accessed March 14, 2023.
3. European Central Bank. "Cyber resilience oversight expectations for financial market infrastructures" (2018): p. 2. Available on:

https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. Accessed March 14, 2023.

4. European Supervisory Authorities. "Joint Advice of the European Supervisory Authorities: To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector" (2019): p. 4. Available on: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf. Accessed March 11, 2023.
5. Naydenov, Rossen, and Marianthi Theocharidou. "EU Cybersecurity Initiatives in the Finance Sector." European Union Agency for Cybersecurity (ENISA) (2021): p. 5. Accessed March 8, 2023. doi: 10.2824/15644.
6. Pupillo, Lorenzo, Melissa K. Griffith, Steven Blockmans and Andrea Renda. "Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force." Centre for European Policy Studies (CEPS) (2018): pp. 8-9. Available on: https://www.ceps.eu/wp-content/uploads/2018/11/CEPS_TFR%20on%20Cyber%20Defence_1.pdf. Accessed March 10, 2023.
7. Tofan, Dan, Theodoros Nikolakopoulos and Eleni Darra. "The cost of incidents affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)." European Union Agency for Network and Information Security (ENISA) (2016): p. 5. Accessed March 16, 2023. doi: 10.2824/475621.
8. United Nations Office on Drugs and Crime (UNODC). "Comprehensive Study on Cybercrime" (2013): p. 184. Available on: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed March 18, 2023.
9. Voo, Julia, Irfan Hemani and Daniel Cassidy. "National Cyber Power Index 2022." Belfer Center for Science and International Affairs, Harvard Kennedy School (2022): p. 9.
10. World Bank Group. "Financial Sector's Cybersecurity: A Regulatory Digest, 6th edition" (2021): pp. 4-124. Available on: https://thedocs.worldbank.org/en/doc/3c28bd048d78efd27744987253e2c44a-0430012021/related/CybersecDigest-v6-FINAL-vs.pdf. Accessed May 6, 2023.

Websites:

1. Adrian, Tobias and Caio Ferreira. "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards." International Monetary Fund (IMF) Blog (2023). Available on: https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards. Accessed March 16, 2023.
2. Appazov, Artur. "Legal Aspects of Cybersecurity." University of Copenhagen (2014): pp. 10-11. Available on: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf. Accessed March 18, 2023.
3. Branagan, Ryan. "What is SOX Compliance in the Cybersecurity World?" Securiwiser, Just Get Visible Ltd (2022). Available on: https://www.securiwiser.com/blog/what-is-sox-compliance-in-the-cybersecurity-world/. Accessed April 26, 2023.
4. Compliance Manager GRC. Understanding the NYDFS Cybersecurity Regulation (23 NYCRR 500) and Its Implications on Financial Institutions (2022). Available on: https://www.compliancemanagergrc.com/blog/nydfs-cybersecurity-regulation/. Accessed April 29, 2023.
5. Computer Hope. Vandalism (2021). Available on: https://www.computerhope.com/jargon/v/vandalism.htm. Accessed March 4, 2023.
6. Ekran System. 7 Best Practices for Banking and Financial Cybersecurity Compliance (2022). Available on: https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance. Accessed May 5, 2023.
7. European Commission. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (2023). Available on: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. Accessed April 21, 2023.
8. European Commission. Hybrid Threats. Available on: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en. Accessed March 2, 2023.
9. European Parliament. Cybersecurity: why reducing the cost of cyberattacks matters (2022). Available on: https://www.europarl.europa.eu/news/en/headlines/priorities/digital-transformation/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters. Accessed January 27, 2023.

10. Europex (Association of European Energy Exchanges). Capital Requirements Directive (CRD) IV and Capital Requirements Regulation (CRR). Available on: https://www.europex.org/eulegislation/crd-iv-and-crr/. Accessed April 17, 2023.
11. Farnham, Kezia. "SOX Penalties: What They Are, How to Avoid Them & Who Is Protected." Diligent (2022). Available on: https://www.diligent.com/insights/grc/sox-penalties/. Accessed April 26, 2023.
12. Fortinet. What Is the Sarbanes Oxley Act (SOX)? Available on: https://www.fortinet.com/resources/cyberglossary/sox-sarbanes-oxley-act. Accessed April 26, 2023.
13. Griffiths, James. "'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on." CNN Business (2020). Available on: https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html. Accessed March 18, 2023.
14. Grimmick, Robert. "What is Cyber Espionage? Complete Guide with Protection Tips." Varonis (2022). Available on: https://www.varonis.com/blog/what-is-cyber-espionage. Accessed March 3, 2023.
15. Halder, Subho. "Top 7 Cybersecurity Regulations in the Financial Industry that you Need to Know." Appknox (2021). Available on: https://www.appknox.com/blog/cybersecurity-regulations-in-the-financial-industry. Accessed May 4, 2023.
16. Hendricks, Beth. "Vandalism in Digital Crime: Types & Evidence." Study.com (2022). Available on: https://study.com/academy/lesson/vandalism-in-digital-crime-types-evidence.html. Accessed March 4, 2023.
17. IBM Security. Cost of a Data Breach Report 2022 (2022): pp. 7-45. Available on: https://www.ibm.com/downloads/cas/3R8N1DZJ. Accessed March 5, 2023.
18. Imperva. Cyber Warfare. Available on: https://www.imperva.com/learn/application-security/cyber-warfare/. Accessed March 2, 2023.
19. Karniyevich, Natallia, Fabian Niemann, Marjolein Geus and Feyo Sickinghe. "NIS 2 Directive, RCE Directive and DORA: Important EU cybersecurity-related legislative acts come into force." Bird&Bird (2023): p. 2. Available on: https://www.twobirds.com/-/media/new-website-content/pdfs/2023/germany/nis-2_rce_dora_germany_newsflash.pdf. Accessed April 13, 2023.

20. Kost, Edward. “The 6 Biggest Cyber Threats for Financial Services in 2023.” UpGuard (2023). Available on: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services. Accessed January 27, 2023.
21. Kost, Edward. “10 Biggest Data Breaches in Finance.” UpGuard (2023). Available on: https://www.upguard.com/blog/biggest-data-breaches-financial-services. Accessed March 5, 2023.
22. Kost, Edward. “Top 8 Cybersecurity Regulations for Financial Services.” UpGuard (2023). Available on: https://www.upguard.com/blog/cybersecurity-regulations-financial-industry#toc-7. Accessed April 10, 2023.
23. Kranz, Garry. “Gramm-Leach-Bliley Act (GLBA).” TechTarget (2021). Available on: https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act#:~:text=The%20Act%20consists%20of%20three,the%20Pretexting%20provisions%2C%20which%20prohibit. Accessed April 25, 2023.
24. North Atlantic Treaty Organization (NATO). NATO’s response to hybrid threats (2023). Available on: https://www.nato.int/cps/en/natohq/topics_156338.htm. Accessed March 2, 2023.
25. Ozarslan, Suleyman. “Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022.” Picus Security (2022). Available on: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022. Accessed March 16, 2023.
26. Pratt, Mary K. “Remote work cybersecurity: 12 risks and how to prevent them.” TechTarget (2022). Available on: https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them. Accessed March 10, 2023.
27. Rowcliffe, Ryan. “NYDFS Strengthens MFA Requirement: What You Need to Know.” HYPR (2022). Available on: https://blog.hypr.com/the-nydfs-multi-factor-authentication-requirement. Accessed April 29, 2023.
28. Sangfor Technologies. Cyber-attacks on Banks Devastate the Financial Sector (2022). Available on: https://www.sangfor.com/blog/cybersecurity/cyber-attacks-on-banks-devastate-financial-sector. Accessed March 10, 2023.
29. Schaefer, Ben. “The Iran Nuclear Agreement as a Deterrent for Cyberattack.” Georgetown Security Studies Review (2018). Available on https://georgetownsecuritystudiesreview.org/2018/08/18/the-iran-nuclear-agreement-as-a-deterrent-for-cyberattacks/. Accessed March 2, 2023.

30. Shchyhol, Yurii. “Russia’s cyberwar against Ukraine offers vital lessons for the West.” Atlantic Council (2023). Available on: https://www.atlanticcouncil.org/blogs/ukrainealert/russias-cyberwar-against-ukraine-offers-vital-lessons-for-the-west/. Accessed March 2, 2023.
31. Sheldon, Robert and Katie Terrell Hanna. “cyberterrorism.” TechTarget (2022). Available on: https://www.techtarget.com/searchsecurity/definition/cyberterrorism. Accessed March 4, 2023.
32. The United States Department of Justice. ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison (2016). Available on: https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison. Accessed March 4, 2023.
33. Tunggal, Abi Tyas. “What is the Cost of a Data Breach in 2023?” UpGuard (2023). Available on: https://www.upguard.com/blog/cost-of-data-breach. Accessed May 15, 2023.
34. Vanta. NIST CSF vs. ISO 27001: What’s the difference? Available on: https://www.vanta.com/resources/nist-csf-vs-iso-27001-whats-the-difference. Accessed May 4, 2023.
35. ZCyberSecurity. 12 Cyber security Regulations for Financial Services. Available on: https://zcybersecurity.com/cyber-security-regulations-financial-industry-sector/. Accessed May 3, 2023.