Journal of Entrepreneurship, Management and Innovation (2026)
Volume 22 Issue 3: 130-162

DOI: https://doi.org/10.7341/20262237
JEL Codes: D22, F23, G32, L22

Patterns of cybersecurity performance in corporations: International evidence*

***Anna Doś*[1], *Elisa Flori*[2], *Piotr Łasak*[3], *Francesco Pattarin*[4]**

Abstract

PURPOSE: *The primary objective of this study is to identify institutional environments (institutional-level factors) and corporate characteristics (organizational-level factors) associated with cybersecurity performance, and to assess their importance in explaining differences in cybersecurity performance across organizations.* ***METHODOLOGY:*** *We apply binary logistic regression to firm-level data from the Orbis database to examine how institutional- and organizational-level factors are associated with cybersecurity performance. The dataset covers companies operating in the United States, Europe, and China in 2022, comprising 1,211 observations.* ***FINDINGS:*** *Companies in China, Northern Europe and Southern Europe underperform those in the United States in terms of cybersecurity performance. Firms in the financial and healthcare sectors exhibit stronger cybersecurity performance, while higher financial leverage, larger firm size, and greater profitability (ROE) are associated with lower cybersecurity performance levels.* ***IMPLICATIONS:*** *From a theoretical perspective, our study supports the usefulness of an institutional approach to cyber risk, complementing and extending the investment-oriented perspective that currently dominates the literature. Our findings also offer insights for investors seeking to reassess asset allocation strategies in light of cybersecurity-related risk exposure. They inform managers aiming to identify best practices for safeguarding corporate value against cyber threats, and support policymakers in identifying where voluntary business cybersecurity practices underperform and may require complementary regulatory or policy measures.* ***ORIGINALITY & VALUE:*** *This study is the first to analyze multi-level patterns of cybersecurity performance on an international scale. It contributes to the existing literature by revealing the regional and sectoral distribution of cybersecurity performance and demonstrating that firms with greater financial risk exposure may also be more susceptible to cyber risks, thereby amplifying potential adverse outcomes.*

Keywords: *cybersecurity performance, corporate cybersecurity, cyber risk, cyber risk management, cybersecurity ratings, institutional theory, institutional determinants, firm-level determinants, financial leverage, operational risk*

INTRODUCTION

Corporations around the world are facing the need to reconsider their production, investment, and innovation strategies due to the rapid advancement of technology. The evolution of traditional industrial and manufacturing methods, propelled by sophisticated digital technologies, connectivity, and automation, has led to a growing reliance on digital systems and networks within business operations. While these innovative solutions bring about opportunities, they also introduce new risks, with cyber threats emerging as a major concern for both managers and investors. Cyber risk commonly refers to the risk of financial loss, disruption or reputational damage to an organization resulting from the failure of its IT systems

1 Anna Doś, Ph.D. Hab., Associate Professor, Department of Financial Markets, Krakow University of Economics, ul. Rakowicka 27, 31-510 Kraków, Poland, e-mail: dosa@uek.krakow.pl (ORCID ID: 0000-0002-4749-4234). *Any views, interpretations, or conclusions expressed in this article are exclusively those of the authors and do not represent the official position of the journal, its editorial board, the publisher, or the authors' affiliated institutions.
2 Elisa Flori, Ph.D., Department of Economics and Management, University of Trento, Via Vigilio Inama, 5, 38122 Trento, Italy, e-mail: elisa.flori@unitn.it (ORCID ID: 0000-0003-1726-2245).
3 Piotr Łasak, Ph.D. Hab., Associate Professor, Institute of Economics, Finance and Management, Jagiellonian University, ul. Prof. S. Łojasiewicza 4, 30-348 Kraków, Poland, e-mail: piotr.lasak@uj.edu.pl (ORCID ID: 0000-0002-3726-3862), corresponding author.
4 Francesco Pattarin, Prof. Dr., 'Marco Biagi' Department of Economics via Jacopo Berengario, 51, 41121, Modena, Italy, e-mail: francesco.pattarin@unimore.it (ORCID ID: 0000-0002-6302-7900).

Received 22 August 2025; Revised 24 November 2025; 30 January 2026; Accepted 16 February 2026.

(Aldasoro et al. 2020; Biliavska et al., 2025; Ruan, 2017). Sometimes cyber risk is treated as a form of operational risk (Curti et al., 2023). A more detailed taxonomy of cyber risk is provided by Rabitti et al. (2025). As businesses become increasingly dependent on IT products and services, cyber risk becomes more widespread. Moreover, in today's landscape, organizations are increasingly vulnerable to cyber risks due to ongoing geopolitical tensions, particularly as these tensions affect supply chains, physical infrastructure, and external networks. The World Economic Forum ranks the prevalence of cybercrime and cyber insecurity as the eighth most severe global risk over a two-year horizon. (WEF, 2023). According to Cybersecurity Ventures, the global cost of cybercrime was estimated at USD 9.5 trillion in 2024 and could reach USD 10.5 trillion per year by 2025 (CV, 2023; Sharif & Mohammed, 2022). IBM estimates that the average cost of a data breach reached an all-time high of USD 4.45 million in 2023 (IBM, 2023). Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report. Kazim and Shanshul (2024) provide estimates indicating that the costs of cybercrime are increasing by 15% per year. According to them, the British companies lost an estimated $55 billion between 2018 and 2023 due to cyberattacks.

Unfortunately, organizations are failing to keep pace with the scope and scale of cyber risk (Accenture, 2023). The considerable expense of a cyber-attack includes reputational, legal, and cyber-protection costs to the firm. These costs can affect the evaluation of a firm's risk and value. Accordingly, there is extensive evidence that financial markets react negatively to announcements of cyber-attacks suffered by companies (Kammoun et al., 2019; Arcuri et al., 2020; Smith et al., 2023).

Interestingly, academic literature appears to lag behind the growing practical concerns surrounding cyber risk. Thus far, only a limited number of papers have been published to investigate the factors that differentiate the levels of cyber risk across business organizations. Nevertheless, it's been established that the effects of cyber risk exposure as well as the effects of cyber events are serious and diverse. Jamilov et al. (2021) show a sizable effect of cyber exposure on the return on assets of firms, cash flows, and equity option valuation. It is also confirmed that cybersecurity risk negatively affects corporate innovation and supply chains (Wang et al. 2024; Crosignani et al. 2023). Evans et al. (2023) and Huang and Wang (2021) show that severe data breaches increase the cost of debt. A few authors report negative equity market returns following cyber events (Kammoun et al., 2019; Arcuri et al., 2020; Smith et al., 2023). Overall, these consequences provide a compelling rationale for managers to seek methods to safeguard corporate value against cyber threats and for investors to reassess their asset allocation strategies. Investors have an interest in understanding patterns of cyber-risk exposure across asset classes. Policymakers likewise aim to understand where and why voluntary business practices to enhance cybersecurity performance fall short. These concerns necessitate both an in-depth understanding of an organization's cyber risk exposure and an understanding of the distribution of cyber risk across businesses.

This study focuses on the latter issue, which is of paramount importance for large-scale screening by global investors and policymakers. Knowledge of differences in cyber risk exposure across company categories is scarce. Aldasoro et al. (2022), focusing on USA evidence, found that larger firms and firms operating in the financial sector experience greater levels and numbers of cyber risk-related losses. Palsson et al. (2020) provide evidence that, in the USA, the number of cyber incidents is highest in the financial sector, followed by the Information Technology (IT) sector, healthcare, retail, and education. Concurrently, IBM (2023) has demonstrated that the average cost of a data breach in the USA is twice that in European countries. Despite these contributions, prior research has predominantly focused on U.S. firms, offering limited insight into how cyber risk levels in the United States compare with those in other regions or how industry-level sensitivity to cyber threats varies globally. Moreover, apart from firm size, other key organizational characteristics have rarely been examined as determinants of cyber risk exposure. Overall, the literature on the determinants of cyber risk remains at a nascent stage, providing only fragmented evidence on the firm-level and contextual factors associated with cyber risk. Moreover, a critical factor of cybersecurity problems is the response of corporations to cyber risk. Once cyber risk is recognized and assessed, a company can introduce diverse risk mitigation measures to improve its cybersecurity (Kosub, 2015). This aspect is presently gaining scholars' attention (Lee, 2020; Romanosky and Sayers, 2024). In particular, Li et al. (2019) call for including both the internal and external environments of organizations in cybersecurity research.

In response to the urgent need to enhance understanding of the patterns of distribution of cyber risk among businesses, this study focuses on a selected aspect of cyber risk exposure, which is companies' cybersecurity performance, combining two critical elements of cyber risk: level of external threat and organizational response to exposure. Rather than providing an in-depth explanation of the mechanisms underlying the level of corporate cybersecurity, this study aims to identify factors specific to the business environment (institutional-level factors) as well as company-specific factors (organizational-level factors) that are associated with patterns of corporate cybersecurity performance across companies.

This knowledge is crucial for investors and policymakers, as it helps them identify high- and low-risk companies and recognize the most vulnerable business organizations. It also provides a key insight for future studies exploring the complex processes involved in cyber risk management decision-making and assessing the effectiveness of corporate responses to cyber threats. We measure organizations' cybersecurity performance with a cyber risk rating by Bitsight. It is a well-established rating, as it is provided by one of the first external rating organizations and – importantly – it isn't a prescriptive security framework but an external rating that monitors cybersecurity performance (Choi et al. 2021). The rating encompasses the organization's security practices, compromised systems, and cyber incidents. It is developed based on monitoring external network activity worldwide to detect cyber events, such as communication with command-and-control servers, malware activity, and participation in DDoS attacks. It exhibits a data-driven, outside-in approach (with no required participation by the rated organization) to rate an organization's cybersecurity performance. Therefore, it is not exposed to self-reporting bias. In addition, Bitsight's rating provides cyber risk scores comparable to those of other cyber risk rating agencies (Keskin et al. 2021).

BitSight's rating classifies organizations into three categories: *basic* (low cybersecurity performance), *intermediate* (average performance), and *advanced* (superior performance). Given the very small number of firms classified as low performers in the regions we focus on, the analysis focuses on two categories—*advanced* and *intermediate*—to capture meaningful variation in cybersecurity performance across organizations. Consequently, we use binary logistic regression analysis to examine the determinants of achieving an advanced level of cybersecurity performance. Our dataset covers companies operating in the USA, Europe, or China in 2022, with 1,211 data points. The independent variables are derived from the Orbis database. They include corporate characteristics that indicate organization-level as well as institutional-level factors.

We show that both institutional- and organizational-level factors significantly influence cybersecurity performance and cyber risk exposure. Companies in China, Northern Europe, and Southern Europe underperform those in the United States in cybersecurity performance, suggesting potential structural gaps in these regulatory frameworks. Firms in the financial and healthcare sectors tend to perform better than those in the "other industries" category, with the financial sector emerging as a benchmark among vulnerable sectors. Moreover, higher financial leverage, stronger financial performance, and larger firm size are associated with weaker cybersecurity performance, suggesting that leverage may amplify overall risk exposure.

Our findings provide valuable insights for investors on potential screening criteria to help construct a portfolio that accounts for a firm's effectiveness in managing cyber risk. Furthermore, our results offer policymakers guidance for identifying concentrations of cyber risk and emphasize the urgent need to implement safety measures to enhance sectoral and market resilience.

The manuscript is structured as follows. It begins with a review of cybersecurity as a strategic issue for companies, followed by the development of a theoretical framework and hypotheses, first focusing on institutional-level factors and then on organizational-level factors influencing cybersecurity performance. The subsequent sections present the variables, research methodology (binary logistic regression), and sample characteristics. The paper then reports and discusses the empirical results, and concludes with key findings, implications, and directions for future research.

LITERATURE REVIEW

Cyber risk and cybersecurity

The rapid digitalization of current economies and financial markets presents significant opportunities on the one hand, but introduces new and serious threats on the other (Agosto & Giudici, 2023). As Romanosky and Sayers (2024) note, today's cyber risk is among the gravest facing organizations. Such risk encompasses a range of phenomena that damage or otherwise negatively affect a firm's IT-related assets (Oltramari & Kott, 2018). Moreover, risks related to IT, often referred to as cyber risk, overlap with and contribute to other business risks, creating a novel challenge for companies, investors, and policymakers. And although a precise understanding of cyber risk is key to designing security-enhancing measures, today's literature falls short of providing a clear, unified, and broadly accepted definition of this phenomenon (Cains et al., 2022; Strupczewski, 2021). As Cremer et al. (2022) argue, research on cyber risk is still in its infancy due to its dynamic, emerging nature.

Aldasoro et al. (2020) associate cyber risk with the risk of financial loss, disruption, or reputational damage to an organization resulting from failures in its IT systems. Cebula et al. (2014), Curti et al. (2023), and Romanosky and Sayers (2024) define cybersecurity risks as operational risks to information and technology assets that affect the confidentiality, availability, or integrity of information or information systems. Strupczewski (2021) defines cyber risk as an operational risk associated with the performance of activities in cyberspace, threatening information assets, ICT resources, and technological assets, and may cause material damage to an organization's tangible and intangible assets, business interruption, or reputational harm. More specifically, cyber risk encompasses non-financial operational risks arising from the use of advanced technologies in business activities (Ramakrishna, 2023). This definition also embraces physical threats to the ICT resources within the organization (Table 1). The above-mentioned definitions highlight diverse sources, occurrences, and consequences of cyber risk that deserve further discussion.

Eling and Wirfs (2019) propose a classification of cyber risk based on its sources. Following a well-established definition of operational risk, they divide cyber risk into four main categories: threats caused by people, threats caused by systems and technical failures, failed internal processes, and external events. A deeper insight into cyber risk occurrences across these four categories is presented in Table 1.

Table 1. Classification of cyber threats and their causes

Endangered area	Activity causing the threat	Description
Privacy	Unauthorized contact or disclosure	Personal information is used in an unauthorized manner to contact or publicize information about an individual or organization.
Privacy	Unauthorized data collection	Information about the users of electronic services, such as social media, cell phones, websites, etc. is captured and stored without their knowledge or consent, or when prohibited information is collected.
Data	Physically lost or stolen	Personal confidential information or digital assets have been stored on, or may have been stored on, computers, peripheral equipment, data storage, or printouts that have been lost, stolen, or improperly disposed of.
Data	Malicious breach	Personal confidential information or digital assets have been or may have been exposed or stolen by unauthorized internal or external actors whose intent appears to have been acquiring such information.
Data	Unintentional disclosure	Personal confidential information or digital assets have either been exposed or may have been exposed to unauthorized viewers due to an unintentional or inadvertent accident or error.
Identity	Fraudulent use/ account access	Identity theft is the fraudulent use of confidential personal information or account access to steal money, establish credit, or access account information.
Industrial	Industrial controls and operations	Losses involving disruption or attempted disruption to "connected" physical assets such as factories, automobiles, power plants, electrical grids, and similar.
Network/ website disruption	N/A	Unauthorized use of or access to a computer or network, or interference with the operation of the same, including viruses, worms, malware, digital denial of service (DDOS), system intrusions, and similar.
Phishing, spoofing, social engineering	N/A	Attempts to get individuals to voluntarily provide information which could then be used illicitly.
Skimming, physical tampering	N/A	Use of physical devices to illegally capture electronic information, such as bank account or credit card numbers, for individual transactions, or to install software on point-of-sale devices to accomplish the same goal.
IT	Configuration/ implementation errors	Losses resulting from errors or mistakes which are made in maintaining, upgrading, replacing, or operating the hardware and software IT infrastructure of an organization, typically resulting in system, network, or web outages or disruptions.
IT	Processing errors	Losses resulting from internal errors in electronically processing orders, purchases, registrations, and similar, usually due to a security or authorization inadequacy, software bug, hardware malfunction, or user error.
Cyber extortion	N/A	Threats to lock access to devices or files, fraudulently transfer funds, destroy data, interfere with the operation of a system/network/site, or disclose confidential digital information such as identities of customers/employees, unless payments are made.

Source: Own elaboration based on Malavasi et al. (2022).

It should be stressed that cyber risk can arise from more than one category of sources. Another distinctive aspect of cyber risk is that it primarily arises from criminal activities. Crotty and Daniel (2022) highlight that while cyber threat agents range from nation-states to script kiddies, by far the most active are cybercriminals accounting for over 80% of cyber incidents. Internet connection is a key channel for cybercrime (Radwan, 2023; Stevens, 2023). Significantly, new types of cybercrime are not always covered by existing law, which is one factor enabling their commission.

Cyber risk occurrence can have diverse results. Agrafiotis et al. (2018) note that the consequences of cyber risk can be suffered by businesses as well as their environments, and thus, negative externalities should be taken into consideration when identifying the consequences of cyber risk. Finally, Agrafiotis et al. (2018) distinguish five types of cyber risk consequences:

- physical/digital - harm related to physical or digital negative effects on someone or something (abuse, identity theft, reduced performance);
- economic - harm that relates to negative financial or economic consequences (reduced profits, investments, fall in stock price);
- psychological - harm which focuses on an individual and their mental well-being (discomfort, low satisfaction, negative changes in perception);
- reputational - harm pertaining to the general opinion held about an entity (damaged relationships with customers, reduced corporate goodwill, reduced credit scores);
- social/societal - capture of harms that may result in a social context or society more broadly (disruption in daily life activities, negative changes in public perception).

Focusing on economic harms, Jamilov et al. (2023) highlight that cyber risk consequences can be observed as:

- firms' balance sheet effects - it has negative and significant effects on future ROA, cash flow, and valuation;
- firms' stock market performance – negative and significant effect on stock returns, large and significant positive effect on realized volatility. An example is the negative market returns that follow announcements of cyber-attacks suffered by hospitality companies (Arcuri et al, 2020).

All of these categories of costs are financially material. The experts estimate that the cost of global losses from cybercrime amounted to USD 8.15 trillion in 2022, and predict that this figure will reach USD 13.82 trillion in 2028 (Fleck, 2024). The dynamics of losses from 2018 to 2028 are presented in Figure 1.

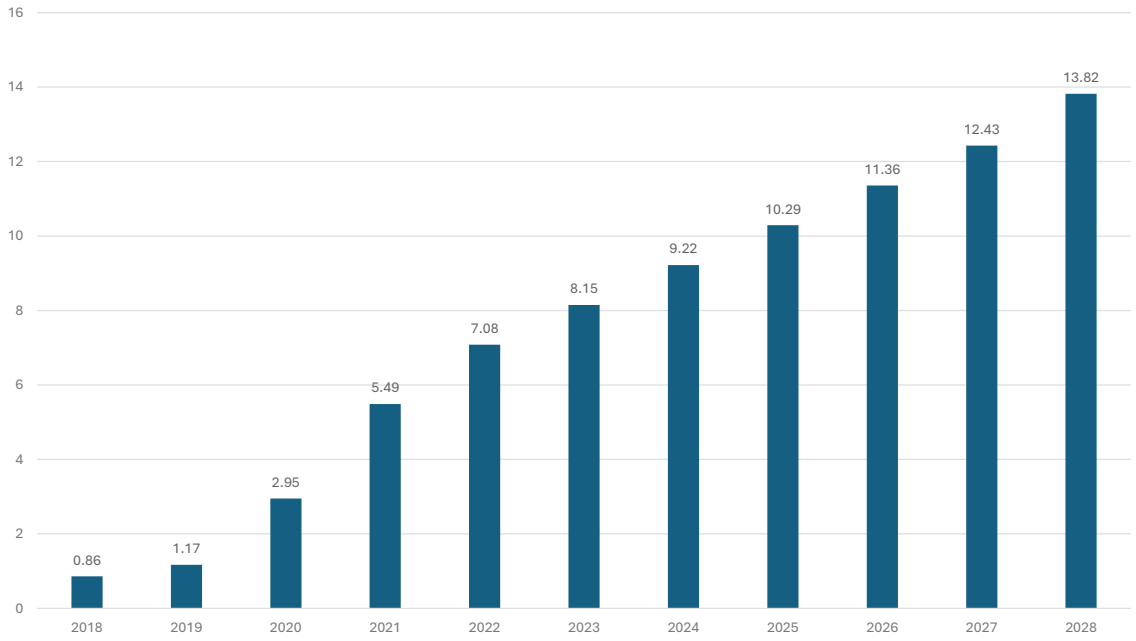

Figure 1. The estimated annual cost of cybercrime worldwide in the period of 2018-2028 (trillion USD)

Source: own elaboration based on Statista.

The most important category of cyber costs is data breach costs. According to Statista (2023), the global average cost of a data breach between March 2021 and March 2022 was USD 4.35 million. Notably, the most targeted are enterprises in finance, information, professional services, healthcare, manufacturing, public administration, education, and other branches (Kuzior et al., 2023).

Risk-averse decision-makers aim to decrease cyber risk exposure and attain cybersecurity. Craigen et al. (2014) propose that 'cybersecurity is the organization and collection of resources, processes, and structures, used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights'. Cains et al. (2022) argue that the term cybersecurity has a broader, interdisciplinary perspective and encompasses fields such as sociology, psychology, risk, decision science, and many others. They conclude, however, that because cybersecurity is multidisciplinary, no standardized terminology exists across disciplines. In this research, we adopt a broad definition of cybersecurity as the collection of tools, techniques, policies, security measures, security guidelines, risk mitigation strategies, actions, training, good practices, security reassurance, and latest technologies that may be used to protect cyberspace and the assets of users (Humayun et al. 2020). The main security objectives are confidentiality, integrity, and availability (Gunduz et al., 2020).

In the past, business cybersecurity efforts have predominantly focused on technical controls, such as firewalls, intrusion prevention/detection systems, and encryption mechanisms (Cremer et al., 2022; Haner & Knake, 2021; Kuzior et al., 2023; Valkenburg & Bongiovanni, 2024). Presently, more sophisticated approaches are used, including quantitative methods and models (Dacorogna & Cratz, 2023; Bentley et al., 2020) as well as practices focused on organizational, human, and governance dimensions (Savas & Caratas, 2022; Valkenburg & Bongiovanni, 2024; Zängerle et al., 2023). Although there is considerable variation in the approach and sophistication of practices related to the management of cyber risk (Romanosky & Sayers 2024), cybersecurity practices focus on the business's internal and external environment and its effect on cyber risk as well as on business financial performance and the connection between financial and operating outcomes (Orlando, 2021).

Cybersecurity can be improved by cyber risk management (Bentley et al., 2020; Dacorogna and Cratz, 2023; Giudici & Raffinetti, 2021; Orlando, 2021; Reanud et al., 2020). This process involves identifying and analyzing cyber risks, followed by decisions on risk avoidance, mitigation, and financing (Eling et al. 2021). Financing options may include transferring the risk, for example, through insurance, or retaining it. Cyber incidents trigger financial losses, but also reputational and trust losses. Thus, risk prevention and mitigation measures are of paramount importance (Valkenburg & Bongiovanni, 2024). Focal points of cyber risk management include (Orlando, 2021):

- pursuing research on the inclusion of cyber risk considerations in board and top management decision-making and overall corporate governance;
- implementing technical cybersecurity solutions;
- applying a suitable cyber risk policy, embracing risk transfer, risk mitigation, and risk retention to reach the desired level of residual risk.

Regardless of the type of cyber risk, the literature emphasizes that prevention and early detection are strategically significant for combating this category of risk (Kuzior et al., 2022; Hariharan, 2020). In addition, human factors and proper risk awareness and communication are key (Gatzeert and Schubert, 2020; Björck et al, 2024; Ulrich et al., 2021). While not all risks can be avoided, their negative consequences can be reduced through careful risk mitigation planning.

The complexity of cyber risk and its financial significance are paramount challenges from an investor's perspective. Global investors must understand the levels of risk across sectors, countries, and other categories of companies, primarily to efficiently diversify risk and assess which companies offer the most attractive returns for an acceptable level of risk. Additionally, investors need to identify systemic risks, such as regulatory changes or geopolitical events, that could impact entire sectors or other groups of companies. Therefore, it is essential for investors to recognize which observable characteristics can serve as signals for cyber risk. These characteristics can be used to screen the entire universe of companies raising funds, helping investors select those that align with their risk appetite and financial goals, as well as to plan risk management and hedging strategies.

Because cyber risk creates negative externalities and is closely linked to criminal activity, there's a strong rationale for government intervention in business cybersecurity practices. Policymakers adopt an international perspective on cyber risk, considering cyber espionage and industrial espionage (Agosto & Guidici, 2023; Demertzis & Wolff, 2020). A good example of the international complexity of cyber risk is the EU market, where there are significant gaps between national

regulatory and supervisory architectures designed to safeguard business activity and the international nature of cyber risk. One good example of such a mismatch is the financial sector, where the digitalization of financial services and the increasing use of third-party service providers trigger concerns about financial stability (Vucinić & Luburić, 2022). There is an urgent need for improved, integrated cybersecurity policies globally, as research indicates that the growth of cyber risk may lead to systemic risk (Głogowski, 2023; Jamilov, 2021). Knowledge of patterns in the distribution of cyber risk is crucial for understanding the collective risk of groups of companies. It is also essential for implementing regulations or interventions, ensuring fair and stable markets, and coordinating policy responses between countries. As a result, policymakers are another key stakeholder group that requires knowledge of corporate cyber risk distribution patterns.

Therefore, in the subsequent sections, this study develops a framework to identify factors associated with cyber risk performance across companies, and consequently, with corporate cyber risk exposure. It focuses on factors at both the institutional level (related to the business environment) and the organizational level (specific to a company), which are easily observable and can serve as an initial screen for large-scale screening purposes.

Institutional factors of cybersecurity

In this section of the paper, we explore the role of institutional-level factors in understanding cybersecurity distribution patterns. Institutional theory proposes that the primary goal of organizational decisions is to enhance legitimacy among stakeholders within its environment. This legitimacy is achieved by adopting processes, structures, and strategies that align with institutions, that is, the rules of the game within a specified environment (Dacin et al. 2007). To structure the analysis of institutions potentially relevant for cybersecurity, we follow Williamson (2000), who proposes four levels of institutions: (1) social embeddedness, (2) institutional environment, (3) governance, and (4) resource allocation and employment.

The first level represents informal institutions, customs, traditions, social norms, and behaviours. It can be used to study cybersecurity from a cultural and social-behavioural perspective. The second level represents the formal rules of the game. It embraces the executive, legislative, judicial, and bureaucratic powers. Here, the crucial aspect is domestic cybersecurity law. The third level represents the governance structures designed by partners to mediate economic relationships (Klein, 1998). The fourth level allows for framing the cybersecurity issue from the perspective of an individual entity – the possessed infrastructure, programmes, and internal policies related to cybersecurity, as well as the human factors (Björck et al., 2024).

The second level can be operationalized by focusing on countries/regions with diverse regulatory solutions that create unique institutional environments. Countries exhibit different levels of digitalisation encompassing (Digital Progress and Trends Report 2023, World Bank Group):

- digital adoption (individuals using the internet, fixed broadband, access to digital payments);
- digital sector (value added in ICT manufacturing and ICT services, ICT patent publications, etc.);
- digital infrastructure (broadband infrastructure and data infrastructure).

Three regions exhibit notably distinct differences in terms of cybersecurity: the United States, the European Union, and China. These are the markets with the most advanced technology. On the one hand, technology determines the level of cyber risk. On the other hand, the risk is influenced by regulations governing the use of information technologies. Each of these three markets has different regulations related to the development of new technology, which, in turn, affects the level of cyber risk. The US market is called a *market-driven regulatory model*, where the government is advocating for an open, unregulated, and private sector-led digital economy. It promotes "internet freedom agenda", according to which innovation is free from government regulation or censorship (Bradford, 2023). The EU market is called the *rights-driven regulatory model*, where tech companies must follow rules established by governments. The EU rules are drafted to specifically reflect European values that call for human dignity, data privacy, democratic discourse, or other core rights of European digital citizens. It is a human-centric and rights-driven approach to digital regulation. The Chinese *state-driven regulatory model* seeks to harness technology to strengthen government control as opposed to protecting individual freedom. It is a command-and-control system. The Chinese government seeks to leverage technology to fuel the country's economic growth and development while maintaining social harmony and control over its citizens' communications (Bradford, 2023). The features of the three markets lead to the conclusion that the US market is the most open, the Chinese one is the most closed and the EU market is featured by a middle level of freedom for private business activity in the high-tech sector. Greater openness seems more harmful to businesses in terms of cyber risk, as rapid technology adoption

creates vulnerabilities, system inconsistencies create weak points, cybercriminals can target less-regulated systems, and cyberattacks originating in one part of the world can quickly spread across open networks.

The three regulatory models are connected with the approaches to cybersecurity. The European Union initiated the regulation of cybersecurity in 2013 with the First European Union (EU) Cybersecurity Strategy. It was dedicated to three key areas: (1) network and information security measures dedicated to operators of essential services, and providers of critical and digital infrastructures; (2) electronic communications, including privacy and data protection issues; (3) cybercrime (Fuster and Jesmontaite, 2020). The strategy had five priorities: (1) achieving cyber resilience; (2) drastically reducing cybercrime; (3) developing cyber-de fence policy and capabilities related to the Common Security and Defence Policy (CSDP); (4) developing the industrial and technological resources for cybersecurity; and (5) establish a coherent international cyberspace policy (Bederna and Rajnai, 2022). The strategy was the starting point and triggered a regulatory wave. In consequence, the current European regulatory landscape for ICT and cyber risk for business activity is multilayered and complex. There is no single major European cybersecurity legislation; rather, there is a multitude of European and national regulations and sector-specific standards. Despite such a status quo, decision-makers continue their efforts to unify the legislation. In 2016, two of the most important and far-reaching pieces of legislation were implemented – the Directive on Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR). Moreover, until 2020, eight other legislations were introduced with ICT and cybersecurity relevance (Krüger & Brauchle, 2021). In 2020, the European Commission launched the Digital Europe Programme, which is part of the Multiannual Financial Framework (MFF), intended to shape the digital transformation of Europe's society and economy (Ghiretti, 2021). Apart from other goals, one is to enable widespread use of digital technologies across the economy and society and to improve cybersecurity (European Commission, 2021). Currently, the EU's approach to cybersecurity policy is based on three crucial pillars: (1) an institutional perspective, (2) as a values-based actor, (3) a realpolitik dimension (Hasmath & Berzina-Cerenkova, 2022). All three pillars play a significant role in defining the specific nature of EU cybersecurity policy.

In the Chinese case, the cybersecurity issues relate to the transformation of the economy. The last step in the transition of the Chinese economy began in 2015, when the CCP initiated the national strategic plan Made in China 2025 (MIC). It was oriented on transforming this country from a manufacturing giant into a world manufacturing power with a key focus on technological development. The development is strictly interconnected with the processes of digitalisation of the economy. Like other countries, the Chinese leadership treats cybersecurity as one of the most important security issues to address in the 21st century. China's approach to cybersecurity is driven by the central objective of establishing cyber sovereignty within China and ensuring that the respect of national sovereignty becomes one of the guiding principles governing global cyberspace. In the Chinese approach, security and control are prioritized over rights, openness, and freedom on the Internet. Moreover, the Chinese agenda on cybersecurity is divided into four main dimensions, which are not only oriented toward economic protection and technical aspects but also related to ideological and social issues, as well as military aspects. They embrace (Bersick et al., 2016): capability building (focused on the technical aspects of cybersecurity), stability and domestic security, with a special focus on content and public opinion, the military dimension, and the international governance of global cyberspace. These areas show that the Chinese approach implies China's "own control" over the enumerated processes. In such an approach, not only the common benefits, but also the conflictual nature and competitive partnership prevent far-reaching cooperation with other countries on cybersecurity issues. In addition, China implemented data protection law, consumer protection law, cybercrime law, and some other regulations (Jiang, 2020). It should be noted that while China, on the one hand, has strengthened its policies on personal data protection and consumer protection, it has also placed significant emphasis on and allocated resources to cybercrime, public order, and cyber defense.

The US market-driven regulatory model is characterized by greater tolerance for new technologies. Nevertheless, it quickly became apparent that control over IT infrastructure had deteriorated due to technological advances and increasingly sophisticated cyber-attacks. It caused concern for the White House administration. Its representatives also recognized that many other countries' governments were giving greater attention to cybersecurity issues. Consequently, the US began actively pursuing numerous actions and industrial policy initiatives. The time frames for cybersecurity policy in the US are similar to those in the EU. They were implemented since the beginning of the 21st century (Aggarwal & Reddie, 2018). Here might be included the creation of the Office of Homeland Security, the President's orders dedicated to cybersecurity issues, the Federal Information Security Management Act of 2002 (FISMA), the Comprehensive National Cybersecurity Initiative (CNCI), Commission on Cybersecurity for the 44th Presidency, Critical Infrastructure Security

and Resilience, and many more. In December 2014, the U.S. Congress passed five major legislative proposals aimed at enhancing U.S. cybersecurity. The authors of the law were convinced that the focus on cyber risk is crucial, as cybersecurity challenges constitute the greatest long-term threat to national security (Trautman, 2015). The key strategic plans in this area include National Strategy to Secure Cyberspace (2003), Cybersecurity Review (2009), the National Cyber Strategy (2018), and the National Cybersecurity Strategy published by the White House on March 2, 2023. All of these strategies were dedicated to the most significant dangers, and they consequently encompassed an increasing number of issues. Among others, there was the vulnerability of critical infrastructure and the importance of fighting cybercrime. There was also sharing information about breaches and security gaps, and engaging with the private sector.

Cybersecurity from the US perspective also has an international dimension. The concern about China's efforts to promote advanced technology through its Made in China 2025 policy has taken on a larger role in the policy addressing global competition in high technology. Together with other initiatives, the US government faces a delicate balancing act to create an effective and usable information-sharing regime, foster a duty of care toward cybersecurity by private actors, oversee the nascent cyber insurance system, devote public resources to cybersecurity education, and engage with the transnational aspects of cybersecurity. Despite many threats, the industrial policies favored by Washington are also likely to reflect existing power dynamics in the US domestic marketplace. The current 'winners' in the internet marketplace – IT companies – appear to have significant lobbying advantages with attendant consequences upon the US government's market facilitation and regulatory roles. This means that the cybersecurity policy remains in its infancy in the US (Aggarwal & Reddie, 2018). US-EU relations regarding cybersecurity issues are closer. The EU and the US share common threat perceptions and interests; they converge around several cybersecurity principles and norms, and they coordinate their actions in practice. It means that the EU-US cybersecurity relationship has taken the form of functional cooperation, aimed at safeguarding common interests and avoiding the costs and vulnerabilities arising from EU-US interdependencies in the cyber realm. At the same time, both markets have different priorities in cybersecurity areas (Anagnostakis, 2021).

The literature-based analysis of cybersecurity levels in the USA, the EU, and China indicates significant variation across these markets and their businesses. In areas such as online banking, identity theft, and encryption, the United States leads, whereas the European Union excels in data security, privacy, smart grids, and cybercrime policies. China, in turn, performs better in network policy. Mishra et al. (2022) suggest that the United States and the European Union are somewhat more effective in addressing emerging cybersecurity threats than China. It should be emphasized that the highest levels of cybersecurity are currently observed in the USA and leading EU countries, attributable to advanced regulations, infrastructure, and international cooperation (Fahey, 2024; Jacuch, 2021). Despite rapid technological development, China remains comparatively more exposed to digital threats and is often perceived as a source of risk. Nevertheless, the country is quickly advancing its cyber capabilities by investing in new technologies, developing its own regulatory framework, and dynamically building its cybersecurity industry. China is implementing testing and training solutions and introducing educational programs focused on cybersecurity (Creemers, 2023; Yang et al., 2025). The government is centralizing management and promoting "cyber sovereignty," which enhances system control and resilience. The literature emphasizes that China's cybersecurity level is still lower than in the USA or leading EU countries, though the gap is gradually narrowing. The rapid development of advanced digital technologies in China is contributing to the country's growing sophistication in digital security. The state of digital security in China continues to evolve rapidly (Putri et al., 2024). It is important to note, however, that comparative analyses of cybersecurity across these regions remain relatively underexplored. Given the significance of this issue and the highly dynamic processes of economic digitalization, further research in this area is warranted. Therefore, based on the previous literature, we hypothesize that:

H1: Corporations with headquarters located in China or Europe have lower levels of cybersecurity performance than corporations with headquarters located in the US.

The third level of institutions proposed by Williamson (2000) is governance. DiMaggio and Powell (1983, p. 143) delve deeper into this level and define "organizational field" as comprising a population of organizations operating in the same domain, defined by the similarity of their services or products. DiMaggio and Powell (1983) stress that organizations that, in the aggregate, constitute a recognized area of institutional life become increasingly similar due to institutional processes that take place in that field. Therefore, institutional factors can be attributed to organizational fields. Therefore, attention should be paid to sectors that are the primary organizational field.

Industry-specific dynamics largely shape the processes of digitalization. This mechanism is precisely explained by the dynamics of change in organizational fields, which are referred to as isomorphic processes. Isomorphic processes encompass coercive, mimetic, and normative isomorphism, with all three evidenced as affecting organizational cybersecurity (Jeyaraj & Zadeh, 2020; Hu et al., 2005). A coercive isomorphism of cybersecurity practices can be observed at the level of supply chain networks (Creazza et al., 2022). The participating entities implement uniform mechanisms for combating cyber risk. Mimetic isomorphism can be observed at the level of digital platforms. In this case, some platforms imitate the methods of operation of others, especially those that are perceived as successful. Normative isomorphism can be observed in cybersecurity standards, such as SANS Institute, the Information Systems Audit and Control Association (ISACA), and the Software Engineering Institute (SEI) are promoted by sectoral associations (Cavusoglu et al. 2015).

While there may be discrepancies among industry rankings of cyber risks, certain industries are believed to be particularly risky (Shevchenko et al., 2022). According to Statista (2023), the greatest cyberattack risks challenge industries that handle vast amounts of sensitive data, such as education, law firms, marketing agencies, consulting services, and the healthcare industry, which relies on interconnected medical devices and extensive health record databases. The financial sector has also become a battleground for cyberattacks due to the large volume of sensitive data it stores. Conversely, criminals target the energy and utility sector because it controls critical infrastructure essential for social resilience. The reports from the IBM 'Cost of a Data Breach Report' for 2019 and 2023 present the distribution of data breach costs across industries (Table 2). Still, there is a need to better understand the distribution of cyber risk across sectors. Our research focuses on four industries: energy and finance, which are significant for economies and businesses, and healthcare and education, which are important for society. All these industries are characterized by a high level of technology integration in their activities.

Table 2. Cost of data breach by industry in the period of 2019-2023 (in millions USD)

Industry	2019	2020	2021	2022	2023
Healthcare	6.45	7.13	9.23	10.10	10.93
Financial	5.86	5.85	5.72	5.97	5.90
Pharmaceuticals	5.20	5.06	5.04	5.01	4.82
Energy	5.60	6.39	NA	4.72	4.78
Industrial	5.20	4.99	4.24	4.47	4.73
Technology	5.05	5.04	4.88	4.97	4.66
Professional services	4.62	4.23	4.65	4.70	4.47
Transportation	3.77	3.58	3.75	3.59	4.18
Communications	3.45	3.01	3.63	3.62	3.90
Consumer	2.59	2.59	3.70	3.86	3.80
Education	4.77	3.90	3.79	3.86	3.65
Research	1.65	1.53	3.60	3.88	3.63
Entertainment	4.32	NA	3.80	3.83	3.62
Media	2.24	1.65	3.17	3.15	3.58
Hospitality	1.99	1.72	3.03	2.94	3.36
Retail	1.84	2.01	3.27	3.28	2.96
Public sector	1.29	1.08	1.93	2.07	2.60

Source: Cost of a Data Breach Reports (2019, 2023).

The energy sector is a cornerstone of every economy and is typically classified as part of the state's critical infrastructure. Many other industries rely on the delivery of energy services, heightening the importance of cybersecurity threats within this sector (Kelic, 2019; Venkatachary et al., 2017). Given its significance to society, a cyber-attack on the energy sector could have catastrophic consequences, potentially disrupting gas and electricity supplies for millions of individuals and businesses (Livingston et al., 2019). It is highlighted that the probability of cyberattacks in the energy sector increases tremendously due to the complex infrastructure involved in smart grids as well as new geopolitical conflicts (Priyadarshini et al., 2021; Simons et al., 2020; Willett, 2023).

Turning to the finance sector (encompassing banking, insurance, and capital markets), cyber risk assumes paramount importance for several reasons. Firstly, financial institutions hold sensitive data, rendering them prime targets for cyber threats (Gatzert & Shubert, 2022; Varga et al., 2021). Secondly, the finance sector heavily relies on cutting-edge technologies, making it an attractive target for cyber breaches compared to non-financial entities (Eling & Wirfs, 2019). Thirdly, the finance sector generates systemic risk, wherein cyber threats can have a disproportionately large impact on society due to the pivotal role of financial institutions as universal intermediaries. Moreover, financial institutions are interconnected internationally, meaning that local problems at one institution can threaten many others in the network, with far-reaching negative consequences (Corbet & Gurdgiev, 2017; Curran, 2020; Gatzert & Shubert, 2022). All these reasons, along with the growing scale and intensity of cyber threats and risks in the financial sector, led us to include the financial sector in our study.

Another sector where cybersecurity plays a crucial role is healthcare. Malavasi et al. (2022) point out that the financial and health sectors face similar risks related to privacy data, and these industries are more exposed to unintentional data disclosure than other business sectors. It stores a wealth of information with significant monetary and intelligence value to cyber criminals and nation-state actors (Cartwright, 2023; Coventry & Branley, 2018). Over the last decades, the sector has improved service capacity, efficiency, and overall performance by leveraging digital technologies such as AI, IoT, user response data, digitalization, machine learning, human psychology, augmented reality (AR), big data mining, etc. At the same time, the positive processes raise the level of cyber risk. As Wasserman and Wasserman (2022) highlight, cyberattacks in healthcare are growing exponentially. By 2019, 24% of cyberattacks were in the healthcare industry. In 2014, 90% of hospitals and clinics experienced at least one data breach, and 45% experienced at least 5. The number of healthcare breaches filed in the US per year has more than tripled in the past decade. Compared to other sectors, cyber risks in healthcare have many dimensions. There are threats to personal data security, as well as other threats associated with the application of advanced technology in medical treatment. Moreover, the expansion of portable devices such as smartphones and USB devices, as well as the enormous number of connected medical devices, is widening the attack surface (Anand & Leonova, 2023). As Paul et al. (2023) point out, the healthcare sector in 2021 faced the most ransomware attacks. The proliferation of portable devices like smartphones and USB devices, as well as the growing number of connected medical devices, is widening the attack surface. In recent years, especially after the COVID-19 pandemic, education has also been among the sectors most endangered by cyber threats. Nevertheless, practices in the sector seem to be advancing rapidly, with considerable investment in resources and governance of cyber risk (Javaid et al. 2023, Garcia-Perez et al. 2023).

The contemporary teaching process is based on online services that support teaching and learning activities. Higher education institutions make full use of ITC and the Internet in nearly all of their operations (Kilag et al., 2023; Rahim, 2021). At the same time, cyberspace in this sector remains insecure. Educational institutions encounter diverse cybersecurity threats, including data breaches, ransomware attacks, phishing, and others. Educational organizations hold immense amounts of personal data, which can ultimately cause serious damage to these entities. As Liluashvili (2021) highlights, the cyberattack damage to higher education can include reputational, financial, and even national security, as some higher education entities are involved in defense research projects. Cyber risk exposure in education is driven by the volume of data, the importance of trust, and universities' culture of openness (Li et al., 2023; Ulven & Wangen, 2021). It is reported that sector regulators lag in establishing minimum cybersecurity requirements for education providers (Chapman, 2019).

Overall, there can be sectoral variations in the probability of cyber events as well as in the level of losses that such events can trigger. Sector-specific cybersecurity vulnerabilities shape the experience as well as the approach to cybersecurity management practices prevalent in the sector. These include sector-specific regulations, collaboration among sector stakeholders, the role of various regulatory/supervisory bodies, the impact of industry associations and networks, and more (Calliess & Baumgarten, 2020; Hasan et al., 2023). Sometimes, country governments establish specialized agencies to address specific problems (Srinivas et al., 2019). This leads us to the formulation of the research hypothesis:

H2: Operating in the energy, financial, healthcare, and education sectors is associated with a higher likelihood of superior cybersecurity performance.

Organizational drivers of cybersecurity

In this section of the paper, we explore organizational-level factors (elements within a company) that may help to explain the distribution of cyber risk performance across organizations. Firms accept cyber risk as part of their overall operational risk

to leverage a competitive edge in technology, distribution, or information. The neo-classical finance theory postulates that any attempt to manage unsystematic risk is of no value to the firms. Nevertheless, industry practitioners routinely allocate resources to risk management activities, signaling the value and relevance of prudent risk management in a real business context where market imperfections exist (Lin et al., 2012; Bogodistov & Wohlgemuth, 2017). Still, the implementation of cyber risk management practices has been found to be diverse (Accenture, 2023), and thus, organizational factors associated with improvements in cybersecurity performance need to be explored. The literature predominantly views allocating resources to cybersecurity as an investment decision and consequently adopts investment-related theoretical frameworks, such as real options theory and learning models, to identify the factors driving cybersecurity investment levels (Xu et al. 2019; Weishäupl et al. 2018; Shaikh & Siponen, 2023). This study takes a risk management perspective. In this vein, committing resources to cybersecurity is perceived to reduce earnings and cash flow volatilities, facilitating evaluation and monitoring of firm performance by investors rather than another positive NPV project. Consequently, in this section, we build on the risk management literature to identify groups of organizational factors we expect to be associated with cybersecurity performance.

The role of firm size for cybersecurity performance appears to be a perplexing issue. The cyber risk literature provides extensive evidence that firm size predicts both cyber risk exposure and the level of cyber risk-related losses (Jamilov et al. 2023; Aldasoro et al. 2022; Kamiya et al. 2021; Biener et al. 2015; Jiang et al. 2024). Indeed, larger firms are often targeted for cyberattacks (Gatzert & Shubert, 2022). However, much less is known about the extent to which firm size influences overall corporate cybersecurity performance—a construct shaped by organizational processes and resource allocation dilemmas, and managerial priorities. The processes-related framing of the issue emphasizes that, while larger firms possess the resources needed to acquire and implement cybersecurity-enhancing measures, they also face organizational inertia (Audretsch & Elston, 2002; Colombo & Delmastro, 2002). Organizational inertia broadly refers to an established organization's inability to enact sufficient internal change in the face of environmental shifts (König et al. 2021). Larger organisations must rely on established hierarchies and routines, which lead to inertia (Ozawa, 2023). They must also coordinate across multiple units, so changes in one area often trigger costly adjustments elsewhere, resulting in slow, fragmented responses to new threats (Zhou et al. 2017). Overall, organisational inertia hampers the corporate agility required to adapt to a rapidly evolving digital environment (Zhen et al. 2021; Kaganer et al. 2023). Another mechanism underlying the relationship between firm size and cybersecurity performance is the resource-allocation dilemma, in which investments in cybersecurity must be carefully weighed against their expected benefits to the firm. While firm size is proportionally related to the costs of improving cybersecurity performance—such as expenditures on systems, software, and employee training—the benefits of such investments may not scale proportionally with size. Aldasoro et al. (2022) note that a significant proportion of losses resulting from cyber incidents are reputational in nature. Interestingly, the risk management literature suggests that for larger firms, declines in market valuation following reputational incidents tend to be relatively smaller (Murphy et al., 2009; Sturm, 2013; Carberry et al., 2018). The remediation of reputational incidents typically involves fixed costs that larger companies can more easily absorb (Zaby and Pohl, 2019). Moreover, firms with stronger brands may be better equipped to counter reputational damage, thereby reducing the overall impact of such incidents (Murphy et al., 2009; Greyser, 2009). In contrast, reputational risk imposes a greater burden on smaller firms, as it exacerbates information asymmetry and increases both the cost and difficulty of accessing equity and debt financing (Cao et al., 2012; 2015; Kölbel et al., 2017). Consequently, costly improvements in cybersecurity may yield diminishing marginal benefits for larger firms. Therefore, based on these process- and resource-allocation-related considerations, we hypothesize that:

H3: Larger companies are more likely to exhibit lower levels of cybersecurity performance than smaller companies.

Cyber risk constitutes an integral component of operational risk, and cyber-related losses can be regarded as fixed costs that contribute to a firm's operating leverage. Traditional financial literature has long examined the relationship between operating leverage and financial leverage (or gearing), generally suggesting that these two forms of leverage behave as substitutes (Li & Henderson, 1991; Trezevant, 1992). Within this framework, firms with higher financial leverage possess stronger incentives to mitigate operational risks to avoid amplifying overall earnings volatility (Purnanandam, 2008).

However, subsequent research in finance highlights that the interplay between financial and operational risks is complex. Empirical evidence indicates that the relationship between operating and financial leverage may at times be positive rather than substitutive (Ho et al., 2004; Chiou & Su, 2007; Sarkar, 2020). This complexity becomes particularly relevant when considering firms' decisions regarding cybersecurity investment and performance.

Improving cybersecurity performance is characterized by a high degree of investment specificity. Such improvements often require a considerable, intangible, multi-year investment with option-like payoffs. From a corporate finance perspective, this raises the issue of *debt overhang*—the well-documented phenomenon in which equity holders underinvest in positive net present value (NPV) projects when the expected gains primarily accrue to debtholders (Myers, 1977; Aivazian et al., 2005; Iqbal et al., 2022). Evidence shows that investment in cybersecurity performance reduces the benefits to equity holders by negatively affecting the firm's dividend policy (Hoang, 2025). Conversely, enhanced cybersecurity performance primarily benefits debtholders by reducing the firm's credit risk exposure (Sheneman, 2025). Consequently, equity holders bear the cost of enhanced cybersecurity, while the benefits accrue disproportionately to debt providers, weakening shareholders' incentives to finance such initiatives. Furthermore, the literature on corporate investment under financial constraints demonstrates that senior claims—such as mandatory debt-service payments—can crowd out otherwise positive-NPV investments (Rauh, 2006; Deng & Fang, 2022). The distortion is particularly severe for projects with long gestation periods or delayed payoffs, as these investments are typically financed through equity rather than debt (Hennessy, 2004; Grundy & Verwijmeren, 2020). Given that cybersecurity investments often possess long-term, intangible, and uncertain returns, they are especially vulnerable to such financing frictions. Therefore, after considering cybersecurity investment-specificity – capital structure link, we hypothesize that:

H4: Companies with higher financial leverage are more likely to exhibit lower levels of cybersecurity performance.

Cyber risk is frequently discussed in the context of financial performance. The prevailing view is that profitable companies possess greater capacity to allocate resources toward cybersecurity, thereby strengthening their digital resilience. In line with this argument, Makridis and Liu (2021) find that more productive firms tend to exhibit fewer cybersecurity vulnerabilities and have access to superior human capital, which enhances their ability to mitigate cyber threats. However, Anderson and Choobineh (2008) emphasize that decisions regarding the allocation of available budgets to cybersecurity are also shaped by a firm's risk tolerance. This insight introduces an important nuance: financial performance does not translate automatically into stronger cybersecurity, as firms' risk attitudes and managerial behaviors mediate how resources are deployed.

Two key mechanisms help explain the relationship between financial performance and cybersecurity investment decisions. The first pertains to the availability of slack resources and their usefulness in absorbing risk, while the second concerns the behavioral dynamics of managerial decision-making.

Firms with higher financial performance can build a resource cushion—commonly referred to as organizational slack—that allows discretionary allocation of funds to address emerging threats or pursue new opportunities (Bourgeois, 1981; Cyert & March, 2015). Slack serves as a buffer that enhances resilience by enabling the absorption of shocks during adverse events (Conz et al., 2023; Tognazzo et al., 2016). Yet, the availability of such resources can also encourage greater risk-taking. Empirical studies demonstrate that increases in slack are associated with the adoption of riskier strategies and practices (Voss et al., 2008; Moses, 1992). Moreover, this effect tends to be amplified in deregulated or high-uncertainty environments (Martinez & Artz, 2006), such as cybersecurity, where governance and risk standards are less formalized.

A complementary perspective arises from the managerial risk-taking literature, which focuses on decision-makers' behavior rather than organizational characteristics. From an agency theory standpoint, managers in well-performing firms are often subject to weaker shareholder scrutiny, thereby granting them greater discretion to pursue risky strategies (Jensen, 1986; Hoskisson et al., 2017). Empirical evidence suggests that monitoring intensity tends to concentrate on underperforming firms (Brav et al., 2022), implying that financially successful firms may neglect in certain domains—such as cybersecurity—where risks are less immediately visible.

A behavioral finance perspective further enriches this argument, showcasing that past financial performance can stimulate overconfidence (Puetz & Ruenzi, 2011; O'Connell & Teo, 2009). Financial success breeds overconfidence, as decision-makers take too much credit for good outcomes (Ben David et al., 2007; Gervais & Odean, 2001). Overconfidence, in turn, has been shown to negatively affect a wide range of corporate decisions, including mergers and acquisitions, financing policies, and risk management practices (Brahma et al., 2023; Malmendier et al., 2011; Adam et al., 2015). Within the context of digital transformation, overconfidence can undermine adaptive routines essential to organizational resilience (Kunz & Sonnenholzner, 2023) and lead to strategic errors in digital initiatives due to overly optimistic assessments of technological or market conditions (Qi et al., 2021).

Taken together, these strands of evidence suggest that high financial performance can have ambivalent implications for cybersecurity. On the one hand, greater resources could enable stronger protective investments; on the other hand, financial success may create slack and foster managerial overconfidence, both of which can reduce attention to cybersecurity risks. Accordingly, we hypothesize the following:

H5: Companies with higher financial performance are more likely to exhibit lower levels of cybersecurity performance than companies with lower financial performance.

METHODOLOGY

We developed a unique dataset, including data from the Orbis database, on corporate characteristics, industry and country of headquarters, and cyber risk performance. The sample size consists of 1,211 companies headquartered in the USA, China, or Europe. Our dataset covers one year: 2022. Aiming to uncover patterns of cybersecurity across organizations, we investigate the associations between institutional-level factors, organizational-level factors, and corporate cyber risk performance.

The information on cybersecurity performance is obtained from the Orbis database, based on the rating provided by BitSight, one of the first external cyber risk rating organizations. Importantly, it isn't a prescriptive security framework, but an external rating that monitors cybersecurity performance (Choi et al., 2021). Although it cannot capture all nuances of cybersecurity performance, BitSight's rating provides cyber risk scores similar to those of other cyber risk rating agencies (Keskin et al. 2021). This feature enhances the credibility of a rating (Berg et al., 2022). The rating is a measure of an organization's security performance and, accordingly, its level of cybersecurity risk. The cyber risk rating uses a data-driven, outside-in approach (with no required participation by the rated organization) to assess an organization's security effectiveness. This results in an objective assessment of an organization's security posture. Unlike other security ratings, BitSight's rating has been proven by third parties to correlate with the likelihood of a breach or ransomware attack. Four categories of risk vectors are included in the rating:

- Diligence: These risk vectors assess the steps an organisation has taken to prevent attacks, their best practice implementation, and risk mitigation (e.g., server configurations) to determine if their security practices are on par with industry-wide best practices;
- Compromised Systems: These risk vectors indicate the presence of malware or unwanted software, which is evidence of security controls failing to prevent malicious or unwanted software from running within an organization;
- User Behaviour: These risk vectors reflect employee activities, such as file sharing and password re-use, that can introduce malware to an organisation or result in a data breach;
- Public Disclosures: These risk vectors indicate publicly disclosed events of unauthorised access, often involving data loss or theft.

Risk vectors are weighted based on importance. According to the rating methodology, the rating ranges from 250 to 900. The provider proposes three categories of organizations based on their cyber risk ratings (Table 3).

Table 3. Categories of companies based on their level of cyber risk rating

Category	Rating Range	Description	Distribution
Advanced	740-900	Strong security performance and lower risk	50% of entities
Intermediate	640-730	Fair security performance and moderate risk	45% of entities
Basic	250-630	Poor security performance and high-risk	5% of entities

Source: Orbis database.

Given the very small number of companies in the "Basic" category in the database, we exclude this group from our analysis and focus instead on the "Intermediate" and "Advanced" categories, where meaningful differences can be observed. Accordingly, we treat our dependent variable as a binary variable, taking the value of 1 if a company exhibits an "Advanced" level of cybersecurity performance, and 0 otherwise (i.e., for companies classified as having an "Intermediate" level of cybersecurity performance).

Independent variables related to organizational-level factors are quantitative, and those related to institutional factors are qualitative: binary variables indicating whether a company operates in a given industry or is headquartered in a given country (the full country–region classification used to construct these dummies is provided in Table A1 in the Appendix). European countries were grouped into four regions—Northern, Southern, Western, and Eastern Europe (see Table A1 in the Appendix). This classification reflects well-documented differences across these regions in terms of digitalization, regulatory capacity, and corporate risk management practices. Northern Europe (Denmark, Finland, Ireland, Sweden) is characterized by advanced digital infrastructure and high levels of e-government adoption. Western Europe (Austria, Belgium, France, Germany, Luxembourg, Netherlands) comprises economies with strong regulatory capacity and long-standing traditions of corporate risk management. Southern Europe (Cyprus, Greece, Malta, Italy, Portugal, Spain) is distinguished by comparatively weaker enforcement capacity and lower average levels of digital maturity among firms. Eastern Europe (Bulgaria, Croatia, Hungary, Poland, Romania, Slovenia) consists largely of post-transition economies with more recent integration into EU regulatory and governance frameworks. In addition, we adopted control variables. Description of variables is provided in Table 4.

Table 4. Description of independent variables

Variables		**Explanation and measurement**
Dependent variable		
CyberRisk_AdvPerformance		• 1: Advanced security performance and lower risk • 0: Intermediate security performance and moderate risk
Independent variables		
Quantitative independent variables representing organisational-level factors	*Leverage*	An independent variable measuring the degree of financial leverage is calculated as the Debt to Equity (D/E) ratio, representing the relationship between debt and equity. Leverage was obtained from the Orbis database.
	ROE	An independent variable used to approximate a company's profitability. ROE (return on equity) is calculated as a relation of net profit to equity. ROE was obtained from the Orbis database.
	LogTA	An independent variable used to approximate a company's size. TA stands for Total assets. TA was obtained from the Orbis database. For modeling purposes, we used the natural logarithm of TA.
	Employees	An independent variable used to approximate a company's size. The number of employees was obtained from the Orbis database.
Qualitative variables representing institutional-level factors	*Region*	• China • North Europe • South Europe • West Europe • East Europe • United States
	Industry	• Education • Energy • Financial • Healthcare • Other

We encoded qualitative variables as binary, dropping the first level to avoid linear dependencies in the model matrix. Therefore, in interpreting regressions, coefficients for qualitative variables shall be interpreted as differential effects relative to the baseline reference.

Categorizing dependent variables into two groups allows the use of binary logistic regression models (Böhning, 1992). Logistic regression models a relationship between predictor variables and a categorical response variable. Binary logistic regression treats the outcome variable as a dichotomous variable. In our case, we compare the Intermediate categories to the Advanced category. We estimate three models. Model 1 includes only Leverage and its squared term, in order to capture potential nonlinear effects. Model 2 expands the specification by adding ROE, its squared term, and the number of Employees, thus incorporating all quantitative organizational-level factors. Model 3 further augments the model by adding Region and Industry, thereby including also qualitative institutional-level factors.

Model 1

$$CyberRisk\_AdvPerformance = \beta_0 + \beta_1 Leverage + \beta_2 Leverage^2 + \epsilon$$

Model 2

$$CyberRisk\_AdvPerformance = \beta_0 + \beta_1 Leverage + \beta_2 Leverage^2 + \beta_3 ROE + \beta_4 ROE^2 + \beta_5 Employees + \epsilon$$

Model 3

$$CyberRisk\_AdvPerformance = \beta_0 + \beta_1 Leverage + \beta_2 Leverage^2 + \beta_3 ROE + \beta_4 ROE^2 + \beta_5 Employees + \beta_6 Region + \beta_7 Industry + \epsilon$$

Sample characteristics

This section presents the descriptive statistics and correlation analysis for the variables included in the study. It provides an overview of the sample composition, detailing the number of companies observed across regions and industries, and examines the relationships among key firm-level and institutional-level variables used in the regression models. Descriptive statistics for dependent and independent variables are presented in Table 5.

Table 5. Descriptive statistics for dependent and independent variables

Variable	Min	Q1	Median	Mean	Q3	Max
Leverage	0	15.39	56.88	95.94	122.08	972.78
ROE (in %)	-906.9	-36.64	5.52	-23.84	21.76	311.42
N_employees	1	114	1034	9545	6575	440000
TA	663000	1.39E+08	7.02E+08	5.93E+09	3.51E+09	2.17E+11
CyberRisk_AdvPerformance	0	0	0	0.4443	1	1

This study focuses on developed economies with advanced levels of digitalization and economic complexity, specifically the United States, China, and European countries. While a country-level analysis was initially considered, the number of observable firms across several European countries proved too small to support reliable econometric inference. Consequently, we adopt a regional classification within Europe that reflects well-established institutional differences in regulatory traditions, approaches to risk, and innovation systems, and that represents a common approach in comparative institutional research. As shown in Table 6, companies are unevenly distributed across regions, reflecting differences in regional economic size and capacity. Nevertheless, the number of observations within each region remains sufficient to ensure the reliability and robustness of the regression analysis. Table 7 presents the distribution of companies by sector.

Table 6. Companies' distribution by region

Region	Intermediate cybersecurity performance	Share (%)	Advanced cybersecurity performance	Share (%)	Total	Share (%)
China	41	3.39	5	0.41	46	3.80
EastEU	14	1.16	4	0.33	18	1.49
NorthEU	54	4.46	38	3.14	92	7.60
SouthEU	42	3.47	11	0.91	53	4.38
UnitedStates	446	36.83	428	35.34	874	72.17
WestEU	76	6.28	52	4.29	128	10.57
Total	673	55.57	538	44.43	1,211	100.00

Table 7. Companies' distribution by industry

Region	Intermediate cybersecurity performance	Share (%)	Advanced cybersecurity performance	Share (%)	Total	Share (%)
Education	5	0.41	8	0.66	13	1.07
Energy	37	3.06	26	2.15	63	5.20
Financial	35	2.89	41	3.39	76	6.28
Healthcare	191	15.77	268	22.13	459	37.90
Other	405	33.44	195	16.10	600	49.55
Total	673	55.57	538	44.43	1,211	100.00

The distribution of companies across sectors reflects the sample's structural characteristics, with the financial and energy sectors dominated by large, well-established firms. Conversely, the relatively small representation of the education sector is consistent with its composition of predominantly small and private institutions, many of which are not covered by commercial databases.

The regional and sectoral composition of the sample is determined by data availability in the Orbis database and the coverage of external cybersecurity ratings; as a result, U.S.-based firms and highly digitalized sectors such as healthcare are overrepresented, a limitation that is explicitly accounted for through the inclusion of region and industry controls in the empirical models. While this uneven representation may limit the generalizability of the results, it does not affect the internal validity of the estimated relationships, which are identified through within-sample variation conditional on institutional and organizational controls.

To address the influence of outliers, Leverage was winsorized at the 5th and 95th percentile thresholds, while ROE and Employees were winsorized at the 2.5th and 97.5th percentile thresholds (Table A2 in the Appendix reports the pre-winsorization percentile cut-offs computed from the raw data). Total Assets (TA) were transformed using the natural logarithm and subsequently scaled. All continuous variables were mean-centered (but not standardized) to facilitate the interpretation of both main and squared effects. Table 8 presents the correlation matrix for variables after the transformations.

Table 8. Correlation matrix for variables after the transformations

Variable	Leverage	ROE	LogTA	Employees
Leverage	1.000			
ROE	0.060*	1.000		
LogTA	0.369***	0.500***	1.000	
Employees	0.272***	0.262***	0.566***	1.000

Note: The table reports pairwise Pearson correlation coefficients among continuous variables after transformations. Significance levels: $p < 0.1$, $p < 0.05$, $p < 0.01$.

Based on the correlation analysis, the transformed variable LogTA, representing company size, exhibited high correlations with several other independent variables. Consequently, it was excluded from the regression models to avoid multicollinearity, with Employees retained as the preferred proxy for firm size. We argue that the number of employees more accurately captures organizational inertia, as it directly reflects the scale and diversity of organizational structures, procedures, and routines, and thus better represents the overall complexity of the firm.

RESULTS AND DISCUSSION

Results from binary logistic regressions – including Model 1, 2, and 3 – are presented in Table 9. In the regression models, RegionChina, RegionEastEU, RegionNorthEU, RegionSouthEU, and RegionWestEU are interpreted relative to the omitted reference category RegionUSA, while IndustryEducation, IndustryEnergy, IndustryFinancial, and IndustryHealthcare are interpreted relative to the omitted reference category IndustryOther. Average Marginal Effects (AMEs) for all models are reported in Table A3 (see Appendix), providing a summary of the estimated effects in terms of changes in predicted probabilities. For Model 3, Table A4 presents a robustness check comparing standard logistic

estimates with Firth penalized estimates, showing that the results remain consistent in terms of coefficient signs, magnitudes, and significance levels. Predicted-probability plots and Generalized Variance Inflation Factors (GVIFs) for Model 3 are also provided in the Appendix (specifically, Figure A1 and Table A5), offering additional insights into model fit and potential multicollinearity.

Table 9. Results from the binary logistic regressions

Variable	(1)	(2)	(3)
Leverage	-0.007***	-0.004***	-0.004***
	(0.001)	(0.001)	(0.001)
Leverage²	0.00003***	0.00001	0.00001
	(0.00001)	(0.00001)	(0.00001)
ROE		-0.009***	-0.008***
		(0.002)	(0.002)
ROE²		-0.00002***	-0.00002***
		(0.00001)	(0.00001)
Employees		-0.00002***	-0.00002***
		(0.00001)	(0.00001)
RegionChina			-1.943***
			(0.500)
RegionEastEU			-0.815
			(0.555)
RegionNorthEU			-0.459**
			(0.232)
RegionSouthEU			-1.143***
			(0.369)
RegionWestEU			-0.151
			(0.217)
IndustryEducation			0.799
			(0.587)
IndustryEnergy			0.496
			(0.290)
IndustryFinancial			0.771***
			(0.261)
IndustryHealthcare			0.313*
			(0.162)
Constant	-0.439***	-0.205**	-0.248*
	(0.083)	(0.097)	(0.133)
Observations	1,211	1,211	1,211
Log Likelihood	-804.224	-758.992	-731.909
Akaike Information Criterion (AIC)	1,614.448	1,529.984	1,493.818
McFadden Pseudo R2	0.033	0.088	0.120
Adjusted McFadden Pseudo R2	0.030	0.080	0.102

Note: Robust standard errors (HC1) are reported in parentheses. Significance levels: $p < 0.1$, $p < 0.05$, $p < 0.01$.

Institutional- and organizational-level independent variables show a significant association with the dependent variable across both models. The steady improvement in model fit across models 1, 2, and 3 (lower AIC, higher log-likelihood) indicates that both firm-level and institutional-level factors improve the explanatory power of cybersecurity performance.

The main model demonstrates that being located in China or Southern Europe reduces the log-odds by more than 1, corresponding to a drop in the predicted probability of achieving an advanced level of cybersecurity of around 20–30 percentage points, depending on baseline probabilities. Thus, firms in China are significantly less likely to achieve an advanced level of cybersecurity performance than those in the United States. Within Europe, firms in Southern Europe also exhibit a substantially lower probability of achieving advanced cybersecurity performance than U.S. firms. Companies in Northern Europe perform moderately worse than their U.S. counterparts. At the same time, the coefficient for Western Europe and Eastern Europe is negative but statistically insignificant, indicating that cybersecurity performance in these

regions is broadly comparable to that observed in the United States. Although Western Europe is generally characterized by higher levels of economic and institutional development, the relatively strong performance observed in Eastern Europe (not different from that observed in the U.S.) may stem from specific characteristics of the sample composition.

Overall, these results indicate that U.S. firms outperform those in China and most European regions in terms of cybersecurity performance, with the weakest outcomes observed in China and Southern Europe. This evidence provides important insights for investors regarding geographic screening of cybersecurity risk exposure, which appears to be lowest in the United States. The findings also carry policy implications for Europe, suggesting that cybersecurity practices in Southern Europe should be urgently improved. The current "two-speed" model of cybersecurity performance risks undermining confidence in the European market as a whole. Similarly, policymakers in China may need to reconsider existing approaches, as current strategies appear insufficient to foster high levels of corporate cybersecurity resilience.

A coefficient of 0.771 for the Financial sector corresponds roughly to a 15–20 percentage point increase in the predicted probability of attaining advanced cybersecurity performance relative to firms in category "Other industries" for the total sample. This result is consistent with the sector's strict regulatory environment and its high exposure to cyber threats, both of which incentivize continuous investment in cyber resilience. Similarly, the Healthcare sector coefficient (0.313) implies an approximate 7–10 percentage point higher probability of achieving an advanced cybersecurity level. Healthcare firms demonstrate a significantly higher likelihood of advanced cybersecurity performance, potentially due to the sensitivity of personal data and stringent sector-specific compliance requirements.

Firms in the Energy sector are not significantly more likely to attain advanced cybersecurity performance. Therefore, although the sector is vulnerable to cybersecurity risks, its performance remains similar to that of the "Other industries" category. Although the coefficient for the education sector is positive, it is not statistically significant, suggesting no clear difference in cybersecurity performance relative to the "Other industries" category. Consequently, two industries emerge as leaders in cybersecurity performance: financial services and healthcare. This finding is particularly noteworthy as it contrasts with earlier evidence indicating that cyber losses were concentrated in the financial and healthcare sectors (Pálsson et al., 2020). Our results may suggest that the historically high exposure and accumulated experience with cyber incidents in these sectors have led to improved preparedness and more mature cyber-risk management practices. In other words, what was once a vulnerability has now become a source of comparative advantage.

From an investment perspective, this finding implies that cyber risk may now be more concentrated outside these two well-prepared sectors, offering valuable guidance for portfolio-level risk screening.

From a policy standpoint, regulators should investigate the factors underlying the superior cybersecurity performance observed in the financial and healthcare sectors. Understanding whether this advantage stems primarily from regulatory enforcement or economies of scale is crucial. If regulatory pressure has been the driving force, similar oversight should be extended to other sectors where data sensitivity and potential spillover effects pose systemic risks. Conversely, if economies of scale are the primary determinant, policymakers should design mechanisms that facilitate collaborative cybersecurity solutions and resource sharing among smaller firms and sectors. Moreover, the findings suggest that the energy sector—as a provider of critical infrastructure—may warrant greater regulatory oversight and enhanced technical support, given its exposure to cyber threats and a relatively moderate level of cybersecurity performance, which could lead to significant societal vulnerabilities. The results presented in Table 8 reveal several robust and statistically significant relationships between firm-level characteristics and the likelihood of achieving an advanced level of cybersecurity performance. Although the coefficients are modest in magnitude, their signs are consistently negative across model specifications.

Firm size, measured by the number of employees (*Employees*), is negatively associated with cybersecurity performance. The coefficient for *Employees* is consistently negative and significant, reinforcing the notion that firm size is inversely related to cybersecurity effectiveness. Despite the higher cyber-related losses typically observed among large companies (Aldasoro et al., 2020), our findings indicate that these firms also tend to underperform in terms of cybersecurity management relative to smaller firms. This suggests that greater organizational complexity and coordination costs may hinder the effective implementation of cybersecurity measures.

This finding carries important implications for both investors and managers. Investors often associate firm size with lower overall risk; however, our results provide novel evidence that investing in larger companies may actually entail greater exposure to cyber risk, which may not align with low-risk investment strategies. For managers of large corporations, the results highlight the disadvantages of organizational inertia. Although larger firms face heightened exposure due to their visibility and extensive use of IT systems (Dinkova et al., 2023), their structural rigidity may limit their capacity to adapt

to the increasingly dynamic cyber threat environment. Managers should therefore seek ways to enhance organizational agility by continuously updating systems, routines, and response mechanisms to strengthen cyber resilience.

From a policy perspective, these findings underscore the need for targeted initiatives aimed at improving cybersecurity performance among large firms. Given their systemic importance, cyberattacks in this segment can produce disproportionate, economy-wide consequences. Policymakers should therefore design incentives or regulatory mechanisms that promote greater cybersecurity preparedness and resilience among large organizations.

The inclusion of quadratic terms allows for potential nonlinearities in the relationship between financial characteristics and cybersecurity performance. However, for the variable leverage, the implied turning point lies at the extreme upper bound of the empirically observed data range (see Figure A1 in the Appendix). As a result, within the support of the data, the marginal effects of leverage on the probability of attaining advanced cybersecurity performance remain monotonic. Specifically, increases in financial leverage are consistently associated with a lower likelihood of achieving advanced cybersecurity performance across the vast majority of firms in the sample. Accordingly, the quadratic specification should not be interpreted as reflecting a substantively meaningful threshold or reversal in the effect of leverage, but rather as a flexible functional form that confirms the robustness of the negative marginal effects within the relevant range of observations.

Financial leverage exhibits a consistently negative and statistically significant association across all model specifications, indicating that firms with higher leverage are less likely to achieve advanced levels of cybersecurity performance. One plausible explanation is that equity holders may be reluctant to invest in projects where the benefits of improved risk management would accrue primarily to debt holders. This finding may also indicate that companies with a higher tolerance for financial risk are inclined to take on more operational risk associated with cyber events. It aligns with the leverage ratchet effect, as potential losses from cyber risks may prompt a further increase in the level of financial leverage in favour of shareholders. It is also possible that financial leverage reduces firms' financial flexibility, limiting the resources available for non-core investments such as cybersecurity enhancement. Resource constraints, therefore, may drive the lower likelihood of achieving advanced cybersecurity performance among leveraged firms. This finding serves as a crucial alert for corporate stakeholders, indicating that an easily observable proxy for risk (leverage) can signify a company's exposure to additional, less visible risks. Importantly, this finding potentially indicates a moral hazard problem, as there is an information asymmetry concerning cybersecurity performance between companies and their external stakeholders.

Profitability (ROE) also displays a strong negative relationship with cybersecurity performance. However, the plots (Figure A1 in the Appendix) reveal a clear nonlinear pattern. At low to moderate ROE levels, higher profitability is associated with a greater likelihood of advanced cybersecurity performance, suggesting that some degree of financial slack may support investments in cybersecurity capabilities. However, beyond a certain ROE threshold, further increases in profitability are associated with a declining probability of advanced cybersecurity performance. This downward slope at higher ROE levels implies that highly profitable firms either become complacent regarding cyber risk mitigation or prioritize short-term financial gains over long-term resilience investments. This suggests that high profitability, rather than being treated as a source of funding for cybersecurity measures, is associated with a higher cyber risk tolerance among highly profitable corporations across regions and sectors. This finding appears to confirm that companies with greater slack resources are more inclined to take on risks, as any resulting consequences can be readily absorbed by an abundance of resources (Moses, 1992). Another explanation is that some companies are highly focused on financial performance and may be willing to reduce or postpone cybersecurity investments to lower costs and thereby increase profitability. This finding carries important implications for shareholders, as it highlights a potential trade-off between their interests, such as receiving dividends and reinvesting profits, and utilizing profitability to offset any cyber losses that may occur. Thus, shareholders should be aware of the nonlinear relation between ROE and cybersecurity. Our result also aligns with studies indicating that decision-makers achieving higher financial performance tend to exhibit greater risk-taking behavior (Puetz & Ruenzi, 2011; O'Connell & Teo, 2009). Finally, the enhanced availability of affordable cybersecurity solutions could potentially reverse the relationship between Return on Equity (ROE) and cybersecurity performance.

In addition, we estimate binary logit models separately for five industry subsamples (Education, Energy, Financial, Healthcare, and "Other industries"), with **advanced cybersecurity performance** as the dependent variable. The results (Table 10) reveal substantial **heterogeneity across industries**, indicating that the correlates of cybersecurity performance are strongly sector-specific.

Table 10. Results from industry-specific binary logistic regressions

Variable	Education	Energy	Financial	Healthcare	Other
Leverage	-2.959***	0.002	-0.010*	-0.004*	-0.003
	(0.167)	(0.009)	(0.006)	(0.002)	(0.002)
Leverage²	0.031***	-0.00001	0.00005	0.00001	-0.00000
	(0.002)	(0.00004)	(0.00003)	(0.00002)	(0.00001)
ROE	-3.065***	-0.115**	-0.009	-0.008***	-0.007**
	(0.168)	(0.054)	(0.009)	(0.003)	(0.003)
ROE²	-0.011***	0.001**	0.0002	-0.00003**	0.00000
	(0.001)	(0.001)	(0.0002)	(0.00001)	(0.00002)
Employees	-0.051***	-0.0001	-0.00001	-0.0001	-0.00001*
	(0.002)	(0.0001)	(0.00002)	(0.00003)	(0.00001)
RegionChina			-15.340***	-1.007	-2.436***
			(1.351)	(0.800)	(0.742)
RegionEastEU		-14.933***		-0.341	-0.721*
		(1.450)		(0.341)	(0.414)
RegionNorthEU	-276.516***		-0.148	-0.629	-0.653
	(15.890)		(0.826)	(1.059)	(0.652)
RegionSouthEU		-0.138	-0.868	-1.903*	-1.007**
		(1.421)	(1.181)	(1.113)	(0.449)
RegionWestEU	-448.893***	18.224***	1.306*	-0.644	-0.193
	(23.659)	(1.194)	(0.764)	(0.491)	(0.272)
Constant	-263.851***	1.533	-0.366	-0.041	-0.246
	(12.587)	(1.137)	(0.615)	(0.235)	(0.171)
Observations	13	63	76	459	600
Log Likelihood	-0.000	-35.521	-44.637	-277.023	-351.849
Akaike Information Criterion (AIC)	16.000	89.043	109.274	576.045	725.698
McFadden Pseudo R^2	1.000	0.168	0.149	0.111	0.070
Adjusted McFadden Pseudo R^2	0.076	-0.043	-0.042	0.076	0.041

Note: Robust standard errors (HC1) are reported in parentheses.
Significance levels: $p < 0.1$, $p < 0.05$, $p < 0.01$.

Importantly, the results for subsamples show that regional coefficients vary strongly across sectors, underscoring the importance of industry–region interactions. In the Financial sector, firms headquartered in China are significantly less likely to exhibit advanced cybersecurity performance compared to U.S.-based financial firms. No statistically significant differences are observed between U.S. firms and those located in European regions, suggesting that regulatory and supervisory convergence in Financial sector may limit cross-regional variation within this sector. This suggests that the financial sector in China is more vulnerable to cyber threats than financial sector companies in the United States and Europe.

In the Energy sector, firms headquartered in Eastern Europe exhibit significantly lower cybersecurity performance than U.S. firms, whereas firms in Western Europe show significantly higher performance. This contrast highlights the uneven institutional and regulatory environments affecting cybersecurity preparedness within the same high-risk industry.

The Education sector shows extremely large and negative coefficients for European regions; however, given the very small sample size in this subsample (N=13), these estimates should be interpreted with caution.

Across most sectors, financial leverage is negatively associated with advanced cybersecurity performance. This relationship is particularly strong in the Education, Financial, and Healthcare sectors. No significant effect of financial leverage was found in Energy, suggesting that cybersecurity in Energy sector is a priority regardless of distribution of benefits between shareholders and debt providers.

Similarly, profitability (ROE) is negatively related to cybersecurity performance across all sectors, except the Financial sector, where higher profitability is correlated with improved cybersecurity performance.

Firm size, measured by the number of employees, shows a negative, statistically significant association with cybersecurity performance in Education and in the residual category "Other industries", whereas it is insignificant in Energy, Financial, and Healthcare. Given the small size of the Education subsample and the marginal significance of the coefficient for the "Other industries" category, the subsample analysis casts doubt on the robustness of the correlation between scale-related complexity and cybersecurity performance.

In addition, we conducted robustness checks by excluding U.S. firms from the sample and re-estimated three models using only non-U.S. companies. These results are now reported in Table A6 in the Appendix. The non-U.S. subsample analysis shows that, relative to firms headquartered in China, companies in Northern and Western Europe are significantly more likely to exhibit advanced cybersecurity performance, whereas differences in Eastern and Southern Europe are not statistically significant. Consistent with the full-sample results, higher ROE is associated with lower cybersecurity performance, whereas leverage and firm size do not exhibit robust effects within the non-U.S. subsample.

CONCLUSION

This study investigates patterns of cybersecurity performance across organizations, with a focus on institutional- and organizational-level factors that differentiate them. Using binary logistic regression, we analyzed a sample of 1,211 companies from the USA, Europe, and China in 2022.

Firms in China are significantly less likely to achieve an advanced level of cybersecurity performance than those in the United States. Within Europe, firms in Southern and Northern Europe also exhibit a substantially lower probability of achieving advanced cybersecurity performance than U.S. firms. Cybersecurity performance in Western Europe is broadly comparable to that observed in the United States. Overall, the non-U.S. robustness checks confirm that regional heterogeneity in cybersecurity performance persists beyond comparisons with U.S. firms, particularly highlighting the stronger performance of Northern and Western European companies relative to China. Next, we demonstrate that companies operating in the Financial and Healthcare sectors are significantly more likely to exhibit advanced cybersecurity performance than companies in the "Other industries" category, which are deemed less prepared to manage cyber risks. Consequently, our results highlight unequal progression and robustness of cybersecurity norms and regulations across sectors, including vulnerable sectors, and significant differences in sector exposure to cybersecurity.

Our findings reveal previously unidentified correlations between organizational factors and cybersecurity performance. Specifically, companies with higher Debt-to-Equity ratios exhibit lower cybersecurity performance. In addition, at low to moderate ROE levels, increases in profitability are associated with an improved cybersecurity performance, however, beyond a certain ROE threshold, further increases in profitability are associated with a declining probability of advanced cybersecurity performance. Overall, these findings suggest that businesses adjust their cybersecurity management to align with their overall risk tolerance, which is influenced by available resources and/or shareholders' risk preferences. Building on these results, we underscore the trade-offs between shareholder returns and the necessity to allocate resources for potential losses. Additionally, we draw attention to the potential moral hazard issue stemming from diminished cybersecurity performance among leveraged companies.

The subsample analyses reveal substantial heterogeneity across industries, highlighting the importance of industry–region interactions in explaining cybersecurity performance. Regional effects vary markedly by sector. Importantly, in finance, firms headquartered in China exhibit significantly weaker cybersecurity performance than U.S.-based firms, while no significant differences are observed between U.S. and European financial firms. Across most sectors, higher financial leverage is associated with lower cybersecurity performance; this relationship is not observed in energy. Profitability is generally negatively related to cybersecurity performance, except in the financial sector, where higher profitability is associated with stronger cybersecurity outcomes. Finally, firm size shows limited and inconsistent effects across subsamples, casting doubt on the robustness of a general relationship between scale-related complexity and cybersecurity performance.

Overall, our results support the identification of vulnerable groups using information easily accessible to managers, policymakers, and investors. Our models do not fully explain the variability in cybersecurity performance because numerous hidden factors (e.g., psychological propensities of decision-makers, complex network relationships, or organizational and governance deficiencies) can significantly contribute to the level of cybersecurity performance. However, these potential factors – although conceivably informative - cannot be directly observed by stakeholders.

The study carries both theoretical and practical implications. The primary theoretical implication is the establishment of the crucial role of country-level and industry-level institutions in shaping corporate cybersecurity performance, thereby supporting the notion that cyber risk management is institutionally anchored. Prior studies on cyber risk and cybersecurity have largely overlooked the institutional perspective. Our results highlight institutional theory as a promising approach for further investigating cybersecurity disparities across organizations. The second theoretical implication stems from the confirmation of all three hypotheses related to organizational factors. This confirms our assertion that cybersecurity practices are better understood through a risk management perspective rather than an investment decision perspective.

Our study holds significant practical implications for investors, managers, and policymakers alike. By elucidating the institutional and organizational factors that differentiate organizations' cybersecurity performance, we help investors understand variations in cyber risk exposure across entities. This understanding is crucial for constructing and managing global, multi-sector investment portfolios. Additionally, our findings can assist managers in benchmarking their organization's cybersecurity performance and identifying efficient cybersecurity practices beyond their sector.

The implications for policymakers are particularly noteworthy, given the substantial negative externalities associated with cyber risk. We highlight the superiority of Chinese and European norms over American ones, signaling to policymakers worldwide that, despite the USA's leading position in the tech sector and status as the most advanced economy, more effective cybersecurity solutions may be found in China or Europe. We alert policymakers and regulatory authorities focused on the education sector to the urgent need for intervention to ensure basic cyber safety. Based on our findings, regulators and policymakers in education should consider implementing measures already in place in healthcare and finance sectors.

Our study is subject to several limitations. Firstly, due to data constraints, we restrict our investigation to regions comprising China, Europe, and the USA. Consequently, there may be country-level solutions that surpass those identified in our study yet remain unexplored. Secondly, we did not have access to the continuous variable representing cybersecurity performance. As a result, our findings may lack some nuance that could be captured through more granular data. Nevertheless, we believe the results remain informative, as the study adopts the perspective of external stakeholders for whom categorical assessments are often more intuitive and actionable than continuous numerical scales. Thirdly, we do not incorporate human factors into our analysis of cybersecurity management. Given their recognized significance (Henshel et al. 2015; Corradini & Nardelli, 2019), our depiction of organizational-level factors in cybersecurity is thus incomplete. Fourthly: sectoral effects—particularly for Healthcare firms—may partly reflect sample composition and differences in the baseline category rather than purely underlying sectoral characteristics. Lastly, our study covers only a single year due to data availability, thereby failing to capture longitudinal patterns in the evolution of cybersecurity performance across diverse organizations.

We advocate that future research adopt an integrated behavioral and risk-management perspective to better understand the organizational-level factors that influence cybersecurity performance. We encourage researchers to disentangle cybersecurity performance by distinguishing between human resource preparedness, technical solutions, and procedural mechanisms to identify which components contribute most significantly to overall cybersecurity effectiveness. Future studies should also examine how cyber risk clusters with other forms of organizational risk, such as financial or operational risk, reveal potential interdependencies and compounding effects.

Acknowledgment

The article presents the results of Project No. 087/EFI/2024/POT, financed from the subsidy granted to the Krakow University of Economics.

References

Accenture. (2023). *How cybersecurity boosts enterprise reinvention to drive business resilience: State of cybersecurity resilience 2023*. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

Adam, T. R., Fernando, C. S., & Golubeva, E. (2015). Managerial overconfidence and corporate risk management. *Journal of Banking & Finance*, *60*, 195–208. https://doi.org/10.1016/j.jbankfin.2015.07.013

Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: The US case. *Journal of Cyber Policy*, *3*(3), 445–466. https://doi.org/10.1080/23738871.2018.1551910

Agosto, A., & Giudici, P. (2023). Cyber risk contagion. *Risks*, *11*(9), 165. https://doi.org/10.3390/risks11090165

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

Aivazian, V. A., Ge, Y., & Qiu, J. (2005). The impact of leverage on firm investment: Canadian evidence. *Journal of Corporate Finance*, *11*(1–2), 277–291. https://doi.org/10.1016/S0929-1199(03)00062-2
Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989
Anagnostakis, D. (2021). The European Union-United States cybersecurity relationship: A transatlantic functional cooperation. *Journal of Cyber Policy*, *6*(2), 243–261. https://doi.org/10.1080/23738871.2021.1916975
Anand, A., & Leonova, I. (2023). Cyber Risk and Mitigation Associated with Healthcare Industry. *Telecom Business Review*, *16*(1), 51–58.
Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security*, *27*(1–2), 22–29. https://doi.org/10.1016/j.cose.2008.03.002
Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080
Audretsch, D. B., & Elston, J. A. (2002). Does firm size matter? Evidence on the impact of liquidity constraints on firm investment behavior in Germany. *International Journal of Industrial Organization*, *20*(1), 1–17. https://doi.org/10.1016/S0167-7187(00)00072-2
Audretsch, D. B., Belitski, M., Caiazza, R., & Desai, S. (2022). The role of institutions in latent and emergent entrepreneurship. *Technological Forecasting and Social Change*, *174*, 121263. https://doi.org/10.1016/j.techfore.2021.121263
Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, *3*(1), 35–49. https://doi.org/10.1365/s43439-022-00048-9
Ben-David, I., Graham, J. R., & Harvey, C. R. (2007). *Managerial overconfidence and corporate policies.* National Bureau of Economic Research. https://doi.org/10.3386/w13711
Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A multivariate model to quantify and mitigate cybersecurity risk. *Risks*, *8*(2), 61. https://doi.org/10.3390/risks8020061
Bersick, S., Christou, G., & Yi, S. (2016). Cybersecurity and EU–China relations. In E. J. Kirchner, T. Christiansen, & H. Dorussen (Eds.), *Security relations between China and the European Union: From convergence to cooperation* (pp. 167–186). Cambridge University Press.
Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131–158. https://doi.org/10.1057/gpp.2014.19
Biliavska, Y., Biliavskyi, V., Shestak, Y., Dyeyeva, N., Kolesnyk, M., & Tryvailo, A. (2025). Monitoring of cyber risks in the financial sector of the economy. *Financial & Credit Activity: Problems of Theory & Practice, 3*(62), 355–369.
Björck, A., Pugnetti, C., & Casián, C. (2024). Communicating to mitigate behavioral cyber risks: The case of employee vulnerability. In T. L. Sellnow & D. D. Sellnow (Eds.), *Communicating risk and safety* (p. 585). De Gruyter Mouton. https://doi.org/10.1515/9783110752427
Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: a capability-based perspective. *The Journal of Risk Finance*, *18*(3), 234–251. https://doi.org/10.1108/JRF-10-2016-0131
Bourgeois, L. J., III. (1981). On the measurement of organizational slack. *Academy of Management Review, 6*(1), 29–39. https://doi.org/10.5465/amr.1981.4287985
Böhning, D. (1992). Multinomial logistic regression algorithm. Annals of The Institute of Statistical Mathematics, *44*(1), 197–200. https://doi.org/10.1007/BF00048682
Brahma, S., Boateng, A., & Ahmad, S. (2023). Board overconfidence and M&A performance: Evidence from the UK. *Review of Quantitative Finance and Accounting, 60*(4), 1363–1391.
Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press.
Brav, A., Jiang, W., & Li, R. (2022). *Governance by persuasion: Hedge fund activism and market-based shareholder influence* (ECGI Working Paper No. 797/2021). https://doi.org/10.2139/ssrn.3955116
Brockett, P. L., Golden, L. L., & Wolman, W. (2012). Enterprise cyber risk management. In J. Emblemsvåg (Ed.), *Risk management for the future—Theory and cases* (pp. 319–340). IntechOpen.
Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cybersecurity and cybersecurity risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/10.1111/risa.13687
Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, *21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67
Cao, Y., Myers, J. N., Myers, L. A., & Omer, T. C. (2015). Company reputation and the cost of equity capital. *Review of Accounting Studies*, *20*, 42–81. https://doi.org/10.1007/s11142-014-9292-9
Carberry, E. J., Engelen, P. J., & Van Essen, M. (2018). Which firms get punished for unethical behavior? Explaining variation in stock market reactions to corporate misconduct. *Business Ethics Quarterly*, *28*(2), 119–151. https://doi.org/10.1017/beq.2017.46
Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, *37*(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5
Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004
Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). *A taxonomy of operational cybersecurity risks* (Version 2) (Technical Note CMU/SEI-2014-TN-006). Carnegie Mellon University, Software Engineering Institute. http://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf
Chapman, J. (2019). *How safe is your data? Cyber-security in higher education* (Report No. 12, pp. 1–6). Higher Education Policy Institute.
Chiou, C. C., & Su, R. K. (2007). On the relation of systematic risk and accounting variables. *Managerial Finance*, *33*(8), 517–533. https://doi.org/10.1108/03074350710760278
Choi, S. J., & Johnson, M. E. (2021). The relationship between cybersecurity ratings and the risk of hospital data breaches. *Journal of the American Medical Informatics Association, 28*(10), 2085–2092. https://doi.org/10.1093/jamia/ocab127
Colombo, M. G., & Delmastro, M. (2002). The determinants of organizational change and structural inertia: Technological and organizational factors. *Journal of Economics & Management Strategy*, *11*(4), 595–635. https://doi.org/10.1111/j.1430-9134.2002.00595.x
Conz, E., Magnani, G., Zucchella, A., & De Massis, A. (2023). Responding to unexpected crises: The roles of slack resources and entrepreneurial attitude to build resilience. *Small Business Economics*, *61*(3), 957–981. https://doi.org/10.1007/s11187-022-00718-2
Corbet, S., & Gurdgiev, C. (2017). *Financial digital disruptors and cyber-security risks: Paired and systemic* (SSRN Working Paper). https://doi.org/10.2139/ssrn.2892842

Corradini, I., & Nardelli, E. (2019). Building organizational risk culture in cybersecurity: The role of human factors. In T. Ahram & W. Karwowski (Eds.), *Advances in human factors in cybersecurity* (pp. 193–202). Springer.
Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113,* 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008
Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21. https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf
Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073
Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145.
Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002
Crotty, J., & Daniel, E. (2022). Cyber threat: Its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. https://doi.org/10.1108/ACI-07-2022-0178
Curran, D. (2020). Connecting risk: Systemic risk from finance to the digital. *Economy and Society*, *49*(2), 239–264. https://doi.org/10.1080/03085147.2020.1718912
Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2023). *Cyber risk definition and classification for financial risk management. Journal of Operational Risk, 18*(2), 37–58. https://doi.org/10.21314/JOP.2022.036
Cybersecurity Ventures. (2023). *Cybercrime to cost the world $9.5 trillion USD annually in 2024.* https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024
Cyert, R., & March, J. (2015). Behavioral theory of the firm. In *Organizational behavior 2* (pp. 60–77). Routledge.
Dacin, M. T., Oliver, C., & Roy, J. P. (2007). The legitimacy of strategic alliances: An institutional perspective. *Strategic Management Journal*, *28*(2), 169–187. https://doi.org/10.1002/smj.577
Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, *2023*(10), 1000–1021. https://doi.org/10.1080/03461238.2023.2191869
Demertzis, M., & Wolff, G. (2020). Hybrid and cybersecurity threats and the EU's financial system. *Journal of Financial Regulation*, *6*(2), 306–316. https://doi.org/10.1093/jfr/fjaa006
Deng, M., & Fang, M. (2022). Debt maturity heterogeneity and investment responses to monetary policy. *European Economic Review*, *144*, 104095. https://doi.org/10.1016/j.euroecorev.2022.104095
DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101
Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics*, 1–30. https://doi.org/10.1007/s11187-023-00803-0
Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?. *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021
Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/rmir.12169
European Commission. (2021, March 23). *The Digital Europe Programme.* https://europa.eu
Evans, C. A., Beyer, B., Mason, T. W., & West, A. N. (2023). Data breach severity and debt market responses. *Accounting and the Public Interest, 23*(1), 76–109. https://doi.org/10.2308/API-2023-003
Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: On drivers of convergence. *Journal of European Integration, 46*(7), 1073–1088.
Fleck, A. (2024). *Cybercrime expected to skyrocket in coming years.* Statista. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 97–115). Springer.
Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cybersecurity and digital transformation. *Technovation*, *121*, 102583. https://doi.org/10.1016/j.technovation.2022.102583
Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725–763. https://doi.org/10.1111/jori.12381
Gervais, S., & Odean, T. (2001). Learning to be overconfident. *The Review of Financial Studies, 14*(1), 1–27. https://doi.org/10.1093/rfs/14.1.1
Ghiretti, F. (2022). *Technological competition: Can the EU compete with China?* Istituto Affari Internazionali. https://www.jstor.org/stable/resrep30941
Giudici, P., & Raffinetti, E. (2021). Cyber risk ordering with rank-based statistical models. *AStA Advances in Statistical Analysis*, *105*(3), 469–484. https://doi.org/10.1007/s10182-020-00387-0
Głogowski, A. (2022). Systemic and cyber risk: The two monsters of financial system. In L. Gąsiorkiewicz & J. Monkiewicz (Eds.), *Digital finance and the future of the global financial system: Disruption and innovation in financial services*. Routledge.
Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C., & Panaousis, E. (2021). Automated cyber and privacy risk management toolkit. *Sensors*, *21*(16), 5493. https://doi.org/10.3390/s21165493
Greyser, S. A. (2009). Corporate brand reputation and brand crisis management. *Management Decision*, *47*(4), 590–602. https://doi.org/10.1108/00251740910959431
Grundy, B. D., & Verwijmeren, P. (2020). The external financing of investment. *Journal of Corporate Finance*, *65*, 101745. https://doi.org/10.1016/j.jcorpfin.2020.101745
Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Haner, J. K., & Knake, R. K. (2021). Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. *Journal of Cybersecurity, 7*(1), 1–15. https://doi.org/10.1093/cybsec/tyab003
Hariharan, N. K. (2021). *Cyber-risk management: Identification, prevention, and mitigation techniques.* OSF Preprints. https://doi.org/10.31219/osf.io/skxec
Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications, 209*, 103540. https://doi.org/10.1016/j.jnca.2023.103540
Hasmath, R., & Berzina-Cerenkova, U. (2022). Cyber technology and the European Union's Gestaltian approach to China. *Stosunki Międzynarodowe – International Relations, 2*(10). https://doi.org/10.2139/ssrn.3865622
Hennessy, C. A. (2004). Tobin's Q, debt overhang, and investment. *The Journal of Finance, 59*(4), 1717–1742. https://doi.org/10.1111/j.1540-6261.2004.00677.x
Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cybersecurity risk assessment. *Procedia Manufacturing*, *3*, 1117–1124. https://doi.org/10.1016/j.promfg.2015.07.186
Ho, Y. K., Xu, Z., & Yap, C. M. (2004). R&D investment and systematic risk. *Accounting & Finance*, *44*(3), 393–418. https://doi.org/10.1111/j.1467-629x.2004.00116.x
Hoang, H. V. (2025). Who pays for cybersecurity? Corporate dividends in response to cybersecurity risk in US firms. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-025-02601-3
Hoskisson, R. E., Chirico, F., Zyung, J., & Gambeta, E. (2017). Managerial risk taking: A multitheoretical review and future research agenda. *Journal of Management, 43*(1), 137–169. https://doi.org/10.1177/0149206316671583
Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004
Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261–286. https://doi.org/10.2308/TAR-2018-0643
Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cybersecurity threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171–3189. https://doi.org/10.1007/s13369-019-04319-2
IBM. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/reports/data-breach
Iqbal, N., Xu, J. F., Fareed, Z., Wan, G., & Ma, L. (2022). Financial leverage and corporate innovation in Chinese public-listed firms. *European Journal of Innovation Management*, *25*(1), 299–323. https://doi.org/10.1108/EJIM-04-2020-0161
Jacuch, A. (2021). Comparative analysis of cybersecurity strategies: European Union strategy and policies, Polish and selected countries strategies. *Online Journal Modelling the New Europe, 37*, 102–120.
Jamilov, R., Rey, H., & Tahoun, A. (2021). The anatomy of cyber risk. *National Bureau of Economic Research Working Paper*, *28906*. https://doi.org/10.3386/w28906
Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cybersecurity and Applications, 1*, 100016. https://doi.org/10.1016/j.csa.2023.100016
Jensen, M. C. (1986). Agency costs of free cash flow, corporate finance, and takeovers. *The American Economic Review, 76*(2), 323–329.
Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361–380. https://doi.org/10.1080/10919392.2020.1776033
Jiang, M. (2021). Cybersecurity policies in China. In *CyberBRICS: Cybersecurity regulations in the BRICS countries* (pp. 183–226). Springer. https://doi.org/10.1007/978-3-030-56405-6_5
Jiang, H., Khanna, N., Yang, Q., & Zhou, J. (2024). The cyber risk premium. Management Science, 70(12), 8791–8817. https://doi.org/10.1287/mnsc.2022.02056
European Commission. (2013, February 7). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace* (JOIN(2013) 1 final). European Commission.
Kaganer, E., Gregory, R. W., & Sarker, S. (2023). A process for managing digital transformation: An organizational inertia perspective. *Journal of the Association for Information Systems*, *24*(4), 1005–1030. https://doi.org/10.17705/1jais.00819
Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
Kammoun, N., Bounfour, A., Özaygen, A., & Dieye, R. (2019). Financial market reaction to cyberattacks. *Cogent Economics & Finance*, *7*(1), 1645584. https://doi.org/10.1080/23322039.2019.1645584
Kassem, R. (2024). Spotlight on fraud risk in hospitality a systematic literature review. *International Journal of Hospitality Management*, *116*, 103630. https://doi.org/10.1016/j.ijhm.2023.103630
Kazim, A. K. D., & Shanshul, N. R. (2024). The impact of cyber-attacks on companies and organisations in developed countries. *Edelweiss Applied Science and Technology*, *8*(6), 9245–9252
Kelic, A. (2019). Cyber risk in critical infrastructure. *ACM SIGMETRICS Performance Evaluation Review, 46*(2), 72–75. https://doi.org/10.1145/3305218.3305243
Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics, 10*(10), 1168. https://doi.org/10.3390/electronics10101168
Kilag, O. K. T., Indino, N. V., Sabagala, A. M., Abendan, C. F. K., Arcillo, M. T., & Camangyan, G. A. (2023). Managing cybersecurity risks in educational technology environments: Strategies and best practices. *American Journal of Language, Literacy and Learning in STEM Education, 1*(5), 28–38. https://grnjournal.us/index.php/STEM/article/view/357
Klein, P. G. (1998). *New institutional economics* (SSRN Working Paper). https://doi.org/10.2139/ssrn.115811
Kölbel, J. F., Busch, T., & Jancso, L. M. (2017). How media coverage of corporate social irresponsibility increases financial risk. *Strategic Management Journal*, *38*(11), 2266–2284. https://doi.org/10.1002/smj.2647
König, A., Graf-Vlachy, L., & Schöberl, M. (2021). Opportunity/threat perception and inertia in response to discontinuous change: Replicating and extending Gilbert (2005). *Journal of Management*, *47*(3), 771–816. https://doi.org/10.1177/0149206320908630
Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, 615–634. https://doi.org/10.1007/s12297-015-0316-8

Krüger, P. S., & Brauchle, J. P. (2021). *The European Union, cybersecurity, and the financial sector: A primer.* Carnegie Endowment for International Peace. http://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf
Kunz, J., & Sonnenholzner, L. (2023). Managerial overconfidence: promoter of or obstacle to organizational resilience?. *Review of Managerial Science*, *17*(1), 67–128. https://doi.org/10.1007/s11846-022-00530-y
Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: Forecasting information trends. *Journal of Risk and Financial Management*, *15*(12), 613. https://doi.org/10.3390/jrfm15120613
Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). Company cybersecurity system: Assessment, risks and expectations. *Production Engineering Archives, 29*(4), 379–392. https://doi.org/10.30657/pea.2023.29.43
Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157
Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: Identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications, 10*(1), 1–18. https://doi.org/10.1057/s41599-023-01787-7
Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24.
https://doi.org/10.1016/j.ijinfomgt.2018.10.017
Li, R. J., & Henderson, G. V., Jr. (1991). Combined leverage and stock risk. *Quarterly Journal of Business and Economics, 30*(1), 18–39. https://www.jstor.org/stable/40473011
Liluashvili, G. B. (2021). Cyber risk mitigation in higher education. *Law & World, 17*, 15–XX. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lwwrld17&div=5&id=&page=
Lin, Y., Wen, M. M., & Yu, J. (2012). Enterprise risk management: Strategic antecedents, risk integration, and performance. *North American Actuarial Journal*, *16*(1), 1–28. https://doi.org/10.1080/10920277.2012.10590630
Liu, T., & Makridis, C. (2021). *Abnormal returns and dispersion in cybersecurity exposure* (SSRN Working Paper). https://doi.org/10.2139/ssrn.3746589
Livingston, S., Sanborn, S., Slaughter, A., & Zonneveld, P. (2019). *Managing cyber risk in the electric power sector.* Deloitte. https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf
Malavasi, M., Peters, G. W., Shevchenko, P. V., Trück, S., Jang, J., & Sofronov, G. (2022). Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics*, *106*, 90–114. https://doi.org/10.1016/j.insmatheco.2022.05.003
Malmendier, U., Tate, G., & Yan, J. (2011). Overconfidence and early-life experiences: The effect of managerial traits on corporate financial policies. *The Journal of Finance, 66*(5), 1687–1733. https://doi.org/10.1111/j.1540-6261.2011.01685.x
Martinez, R. J., & Artz, K. (2006). An examination of firm slack and risk-taking in regulated and deregulated airlines. *Journal of Managerial Issues, 18*(1), 11–31.
McFadden, D. (1974). Conditional logit analysis of qualitative choice behavior. In P. Zarembka (Ed.), *Frontiers in econometrics* (pp. 104–142). Academic Press.
McFadden, D. (2021). Quantitative methods for analysing travel behaviour of individuals: Some recent developments. In D. McFadden (Ed.), *Behavioural travel modelling* (pp. 279–318). Routledge. https://doi.org/10.4324/9781003156055-18
Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120*, 102820. https://doi.org/10.1016/j.cose.2022.102820
Moses, O. D. (1992). Organizational Slack and Risk-taking Behaviour: Tests of Product Pricing Strategy. *Journal of Organizational Change Management*, *5*(3), 38–54. https://doi.org/10.1108/09534819210018045
Murphy, D. L., Shrieves, R. E., & Tibbs, S. L. (2009). Determinants of the stock price reaction to allegations of corporate misconduct: Earnings, risk, and firm size effects. *Journal of Financial and Quantitative Analysis, 43*(3), 581–612. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b230b9a438a64d3cd84bcb7ffeed8ad413656ac1
Myers, S. C. (1977). Determinants of corporate borrowing. *Journal of Financial Economics, 5*(2), 147–175.
O'Connell, P. G., & Teo, M. (2009). Institutional investors, past performance, and dynamic loss aversion. *Journal of Financial and Quantitative Analysis*, *44*(1), 155–188. https://doi.org/10.1017/S0022109009090048
Oltramari, A., & Kott, A. (2018). Towards a reconceptualisation of cyber risk: an empirical and ontological study. *Journal of Information Warfare*, *17*(1), 49–73. https://www.jstor.org/stable/26504129
Orlando, A. (2021). Cyber risk quantification: Investigating the role of cyber value at risk. *Risks*, *9*(10), 184. https://doi.org/10.3390/risks9100184
Ozawa, K. (2023). Organisational inertia and the dynamics of multiple organisational routines. *Knowledge Management Research & Practice*, *21*(3), 667–676. https://doi.org/10.1080/14778238.2021.1983481
Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance—Issues and Practice, 45*, 564–579. https://doi.org/10.1057/s41288-020-00171-w
Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007
Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K., & Satapathy, S. C. (2021). Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering*, *93*, 107204. https://doi.org/10.1016/j.compeleceng.2021.107204
Puetz, A., & Ruenzi, S. (2011). Overconfidence among professional investors: Evidence from mutual fund managers. *Journal of Business Finance & Accounting*, *38*(5-6), 684–712. https://doi.org/10.1111/j.1468-5957.2010.02237.x
Purnanandam, A. (2008). Financial distress and corporate risk management: Theory and evidence. *Journal of Financial Economics*, *87*(3), 706–739. https://doi.org/10.1016/j.jfineco.2007.04.003
Putri, S. O., Rachman, D. F., Septiana, I. F., & Sihombing, J. Y. (2024). China's economic cyber strategy in facing economic cyber threats 2020–2023. In *Proceedings of the International Conference on Business, Economics, Social Sciences, and Humanities* (Vol. 7, pp. 517–527).
Qi, W., Li, B., Liu, Q., & Lv, J. (2023). Low-skill lock-in? Financial resource mismatch and low-skilled labor demand. *Finance Research Letters*, *55*, 104003. https://doi.org/10.1016/j.frl.2023.104003
Rabitti, G., Khorrami Chokami, A., Coyle, P., & Cohen, R. D. (2025). A taxonomy of cyber risk taxonomies. *Risk Analysis, 45*(2), 376–386. https://doi.org/10.1111/risa.14272
Radwan, A. (2023). *Cyber-enabled crimes vs cyber-dependent crimes.* Internet Safety Statistics. https://www.internetsafetystatistics.com/cyber-enabled-crimes-vs-cyber-dependent-crimes/

Rahim, N. (2021). Bibliometric analysis of cyber threat and cyber attack literature: Exploring the higher education context. In M. Sarfraz (Ed.), *Cybersecurity threats with new perspectives*. IntechOpen. https://doi.org/10.5772/intechopen.98038
Ramakrishna, S. P. (2023). *Climate change risk management in banks: The next paradigm*. De Gruyter. https://doi.org/10.1515/9783110757958
Rauh, J. D. (2006). Investment and financing constraints: Evidence from the funding of corporate pension plans. *The Journal of Finance*, *61*(1), 33–71.
Renaud, K., Orgeron, C., Warkentin, M., & French, P. E. (2020). Cybersecurity responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. *Public Administration Review*, *80*(4), 577-589.
https://doi.org/10.1111/puar.13210
Romanosky, S., & Sayers, E. L. P. (2024). Enterprise risk management: how do firms integrate cyber risk?. *Management Research Review*, *47*(1), 1–17. https://doi.org/10.1108/MRR-10-2021-0774
Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security, 65*, 77–89. https://doi.org/10.1016/j.cose.2016.10.006
Sarkar, S. (2020). The relationship between operating leverage and financial leverage. *Accounting & Finance*, *60*, 805–826. https://doi.org/10.1111/acfi.12374
Savas, S., & Karatas, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4
Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*, 1–12. https://doi.org/10.1007/s10796-023-10404-7
Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cybersecurity and future trend. *World Journal of Advanced Research and Reviews, 15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0713
Sheneman, A. G. (2025). Cybersecurity risk and bank loan contracting. *The Accounting Review*, 1–28. https://doi.org/10.2308/TAR-2024-0103
Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. *Journal of Cybersecurity*, *9*(1), 1–12. https://doi.org/10.1093/cybsec/tyac016
Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*, *32*(3), 337–342. https://doi.org/10.1080/14781158.2020.1732899
Smith, K. T., Smith, L. M., Burger, M., & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. *Information & Computer Security*, *31*(4), 385–403. https://doi.org/10.1108/ICS-09-2022-0147
Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063
Statista. (2023). *Average total cost per data breach worldwide 2020–2022, by industry*. https://www.statista.com/statistics/387861/cost-data-breach-by-industry/
Statista. (2023). *Threat of cyber attacks to global organisations 2023.* https://www.statista.com/statistics/1337538/threat-cyber-attacks-organisations-worldwide/
Stevens, T. (2023). *What is cybersecurity for?* Bristol University Press.
Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143
Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization*, *85*, 191–206. https://doi.org/10.1016/j.jebo.2012.04.005
Tognazzo, A., Gubitta, P., & Favaron, S. D. (2016). Does slack always affect resilience? A study of quasi-medium-sized Italian firms. *Entrepreneurship & Regional Development*, *28*(9–10), 768–790. https://doi.org/10.1080/08985626.2016.1250820
Trautman, L. J. (2015). *Cybersecurity: What about US policy?* SSRN. https://doi.org/10.2139/ssrn.2548561
Trezevant, R. (1992). Debt financing and tax status: Tests of the substitution effect and the tax exhaustion hypothesis using firms' responses to the Economic Recovery Tax Act of 1981. *The Journal of Finance, 47*(4), 1557–1568. https://doi.org/10.1111/j.1540-6261.1992.tb04670.x
Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimisation: A Small Business Case Study. *IEEE Access*, *11,* 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670
Ulrich, P. S., Timmermann, A., & Frank, V. (2022). Organizational aspects of cybersecurity in German family firms–Do opportunities or risks predominate? *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(1), 21–40.
https://doi.org/10.1108/OCJ-03-2021-0010
Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13(2)*, 39. https://doi.org/10.3390/fi13020039
Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: A systematic literature review. *Computers & Security, 142*, 103708. https://doi.org/10.1016/j.cose.2024.103708
Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239
Venkatachary, S. K., & Venkatachary, R. (2017). Economic impacts of cybersecurity in energy sector: A review. *International Journal of Energy Economics and Policy, 7*(5), 250–262. http://hdl.handle.net/11159/1315
Voss, G. B., Sirdeshmukh, D., & Voss, Z. G. (2008). The effects of slack resources and environmental threat on product exploration and exploitation. *Academy of Management Journal, 51*(1), 147–164. https://doi.org/10.5465/amj.2008.30767373
Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27–53. https://doi.org/10.2478/jcbtp-2022-0012
Wang, J., Ho, C. Y. C., & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities?. *International Review of Financial Analysis*, *91*, 103028. https://doi.org/10.1016/j.irfa.2023.103028
Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, 862221. https://doi.org/10.3389/fdgth.2022.862221
World Economic Forum. (2023). *Global risks report 2023.* https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, *77*, 807–823. https://doi.org/10.1016/j.cose.2018.02.001
Willett, M. (2023). The cyber dimension of the Russia–Ukraine War. In *Survival: October-November 2022*, (pp. 7-26). Routledge.

Williamson, O. E. (2000). The new institutional economics: Taking stock, looking ahead. *Journal of Economic Literature*, *38*(3), 595–613. https://doi.org/10.1257/jel.38.3.595
Yang, Y., Liu, J., & Yang, Y. (2025). Research on China's innovative cybersecurity education system oriented toward engineering education accreditation. *Information, 16*(8), 645. https://doi.org/10.3390/info16080645
Xu, F., Luo, X., Zhang, H., Liu, S., & Huang, W. (2019). Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect. *Information Systems Frontiers*, *21*, 1069–1083. https://doi.org/10.1007/s10796-017-9807-6
Zaby, S., & Pohl, M. (2019). The management of reputational risks in banks: Findings from Germany and Switzerland. *Sage Open*, *9*(3). https://doi.org/10.1177/2158244019861479
Zängerle, D., & Schiereck, D. (2023). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice, 48*(2), 434–462. https://doi.org/10.1057/s41288-022-00282-6
Zhen, J., Cao, C., Qiu, H., & Xie, Z. (2021). Impact of organizational inertia on organizational agility: The role of IT ambidexterity. *Information Technology and Management, 22*(1), 53–65.
Zhou, Y. M., & Wan, X. (2017). Product variety, sourcing complexity, and the bottleneck of coordination. *Strategic Management Journal*, *38*(8), 1569–1587. https://doi.org/10.1002/smj.2619

Appendix

Table A1. Classification of countries by region

Region	Countries
North Europe	Denmark, Finland, Ireland, Sweden
South Europe	Cyprus, Greece, Malta, Italy, Portugal, Spain
West Europe	Austria, Belgium, France, Germany, Luxembourg, Netherlands
East Europe	Bulgaria, Croatia, Hungary, Poland, Romania, Slovenia

Table A2. Raw-data percentiles used to define winsorization thresholds

Variable	Percentile	Value
Leverage	5^{th}	0.85
	95^{th}	320.28
ROE	2.5^{th}	-309.16
	97.5^{th}	73.30
Employees	2.5^{th}	7.00
	97.5^{th}	73,650.00

Table A3. Average Marginal Effects (AMEs) – All models

Model	Variable	AME	Std. Error	z	p-value
1	Leverage	-0.002	0.000	-7.416	0.000
	$Leverage^2$	0.000	0.000	3.737	0.000
2	Leverage	-0.001	0.000	-3.435	0.001
	$Leverage^2$	0.000	0.000	1.225	0.220
	Employees	0.000	0.000	-3.813	0.000
	ROE	-0.002	0.000	-6.475	0.000
	ROE^2	0.000	0.000	-3.318	0.001
3	IndustryEducation	0.171	0.124	1.378	0.168
	IndustryEnergy	0.106	0.062	1.705	0.088
	IndustryFinancial	0.165	0.055	2.983	0.003
	IndustryHealthcare	0.067	0.035	1.888	0.059
	Leverage	-0.001	0.000	-3.336	0.001
	$Leverage^2$	0.000	0.000	1.005	0.315
	Employees	0.000	0.000	-3.551	0.000
	RegionChina	-0.344	0.056	-6.118	0.000

Model	Variable	AME	Std. Error	z	p-value
	RegionEastEU	-0.171	0.113	-1.512	0.131
	RegionNorthEU	-0.099	0.050	-1.978	0.048
	RegionSouthEU	-0.231	0.062	-3.696	0.000
	RegionWestEU	-0.033	0.045	-0.733	0.463
	ROE	-0.002	0.000	-4.669	0.000
	ROE^2	0.000	0.000	-2.829	0.005

Table A4. Robustness check: Comparison of standard logit and Firth penalized estimates – Model 3

Model	Variable	Odds Ratio	95% CI Lower	95% CI Upper	p-value
Penalized logit (Firth)	(Intercept)	0.782	0.603	1.013	0.063
Standard logit (BL)	(Intercept)	0.780	0.600	1.013	0.063
Penalized logit (Firth)	IndustryEducation	2.138	0.718	6.902	0.172
Standard logit (BL)	IndustryEducation	2.224	0.716	7.597	0.174
Penalized logit (Firth)	IndustryEnergy	1.641	0.927	2.876	0.088
Standard logit (BL)	IndustryEnergy	1.642	0.923	2.895	0.088
Penalized logit (Firth)	IndustryFinancial	2.139	1.290	3.567	0.003
Standard logit (BL)	IndustryFinancial	2.162	1.297	3.624	0.003
Penalized logit (Firth)	IndustryHealthcare	1.369	0.997	1.877	0.052
Standard logit (BL)	IndustryHealthcare	1.368	0.994	1.879	0.054
Penalized logit (Firth)	Leverage	0.996	0.993	0.998	0.001
Standard logit (BL)	Leverage	0.996	0.993	0.998	0.001
Penalized logit (Firth)	$Leverage^2$	1.000	1.000	1.000	0.305
Standard logit (BL)	$Leverage^2$	1.000	1.000	1.000	0.316
Penalized logit (Firth)	Employees	1.000	1.000	1.000	0.000
Standard logit (BL)	Employees	1.000	1.000	1.000	0.000
Penalized logit (Firth)	ROE	0.992	0.989	0.996	0.000
Standard logit (BL)	ROE	0.992	0.989	0.996	0.000
Penalized logit (Firth)	ROE^2	1.000	1.000	1.000	0.005
Standard logit (BL)	ROE^2	1.000	1.000	1.000	0.005
Penalized logit (Firth)	RegionChina	0.156	0.056	0.359	0.000
Standard logit (BL)	RegionChina	0.143	0.049	0.339	0.000
Penalized logit (Firth)	RegionEastEU	0.481	0.143	1.338	0.167
Standard logit (BL)	RegionEastEU	0.443	0.122	1.286	0.163
Penalized logit (Firth)	RegionNorthEU	0.637	0.399	1.008	0.054
Standard logit (BL)	RegionNorthEU	0.632	0.394	1.004	0.054
Penalized logit (Firth)	RegionSouthEU	0.331	0.159	0.639	0.001
Standard logit (BL)	RegionSouthEU	0.319	0.151	0.622	0.001
Penalized logit (Firth)	RegionWestEU	0.862	0.574	1.287	0.469
Standard logit (BL)	RegionWestEU	0.859	0.571	1.287	0.464

Figure A1. Predicted-probability plots – Model 3

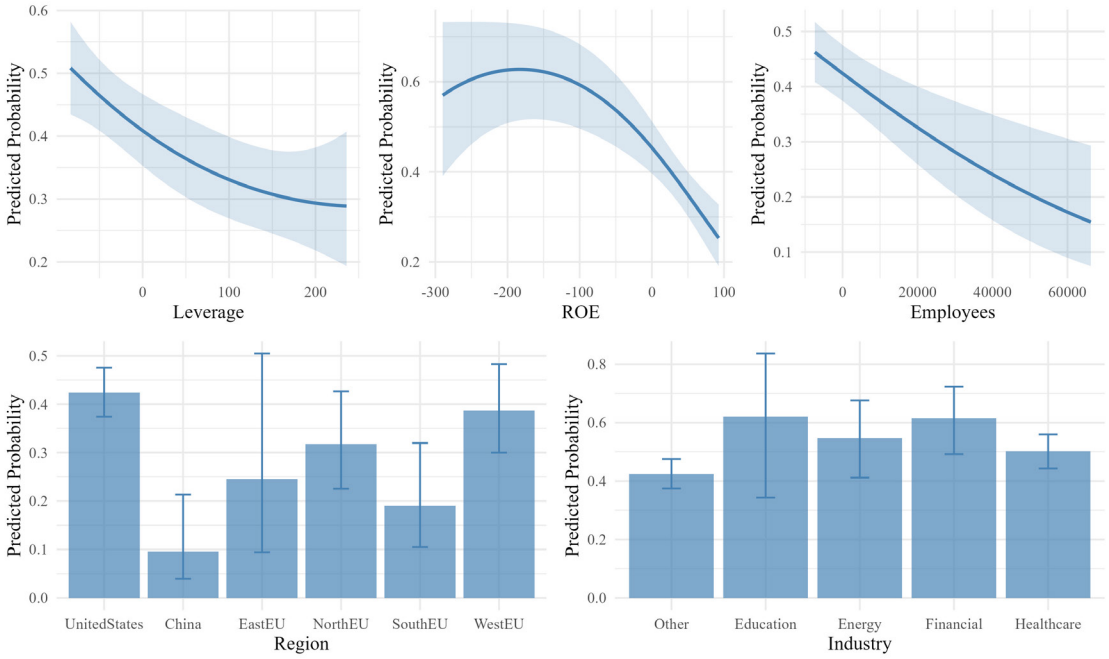

Table A5. Generalized Variance Inflation Factors (GVIFs) – Model 3

Variable	GVIF	Degrees of freedom (Df)	$GVIF^{1/(2*Df)}$
ROE	4.238	1	2.059
ROE^2	3.471	1	1.863
Leverage	2.947	1	1.717
$Leverage^2$	2.611	1	1.616
Employees	1.192	1	1.092
Industry	1.678	4	1.067
Region	1.122	5	1.012

Table A6. Results from the binary logistic regressions excluding U.S. firms

Variable	(1)	(2)	(3)
Leverage	-0.002	-0.001	-0.001
	(0.002)	(0.002)	(0.003)
$Leverage^2$	0.00001	0.00000	0.00001
	(0.00002)	(0.00002)	(0.00002)
ROE		-0.009**	-0.007*
		(0.004)	(0.004)
ROE^2		0.00003	-0.00003
		(0.00003)	(0.00003)
Employees		-0.00000	-0.00000
		(0.00001)	(0.00001)
RegionEastEU			0.898
			(0.804)
RegionNorthEU			1.267**
			(0.570)
RegionSouthEU			0.621
			(0.638)

Variable	(1)	(2)	(3)
RegionWestEU			1.597***
			(0.534)
IndustryEducation			1.864
			(1.267)
IndustryEnergy			0.620
			(0.856)
IndustryFinancial			1.313***
			(0.387)
IndustryHealthcare			0.315
			(0.327)
Constant	-0.810***	-0.665***	-2.135***
	(0.159)	(0.208)	(0.538)
Observations	337	337	337
Log Likelihood	-212.353	-204.326	-187.433
Akaike Information Criterion (AIC)	430.707	420.652	402.867
McFadden Pseudo R^2	0.002	0.040	0.119
Adjusted McFadden Pseudo R^2	-0.012	0.012	0.054

Biographical notes

Anna Doś (Ph.D., Hab.) is an Associate Professor at the Kraków University of Economics, within the Department of Financial Markets. Her research interests revolve around finance for sustainable development, with a particular emphasis on incorporating ESG factors into risk and profitability assessments in investments. Additionally, she explores strategies to enhance enterprise value aligned with sustainable development goals. Anna Doś has undertaken research internships at Sacred Heart University in Milan and the University of Modena and Reggio Emilia. Furthermore, she has collaborated on a scientific project with John Moores University in Liverpool.

Elisa Flori (Ph.D.) is a Postdoctoral Research Fellow at the University of Trento, where her research focuses on networks and the rule of law. She previously held a research fellowship at Luiss Guido Carli University. She earned her Ph.D. in Economics from the University of Modena and Reggio Emilia, during which she also collaborated with the University of Trento, the Technical University of Munich, and the University of Bologna. Her main interests include network analysis, supply chain relations, and sustainable finance.

Piotr Łasak (Ph.D., Hab.) is an Associate Professor at the Institute of Economics, Finance and Management, Jagiellonian University in Krakow, Poland. His research, publication and teaching activities focus on banking, corporate finance, and international finance. Among the main research topics are financial market development, regulation and supervision, mechanisms of financial and currency crises, and shadow banking system development. Among his particular research interests is the development of the Chinese financial market. The current main research area concerns financial technology (FinTech) and the banking sector's transformation as a consequence of digitalization and the influence of financial technologies. He is the author of several publications on this subject.

Francesco Pattarin (Prof., Dr.) is an Associate Professor of Banking & Finance at the University of Modena and Reggio Emilia. He holds a PhD in Economics from the University of Rome "La Sapienza" and an MSc in Finance from Birkbeck College, University of London. He is a member of the scientific board of AIRI (Artificial Intelligence Research and Innovation Center) and acts as a consultant for several Italian companies on data analytics projects for business and management. His current areas of interest include artificial intelligence for business applications, network analysis, corporate social responsibility and ESG, and innovative finance and financial markets.

Author contributions statement

Anna Doś: Conceptualization, Formal Analysis, Literature Investigation, Data Curation, Resources, Writing – Original Draft, Writing – Review & Editing. **Elisa Flori:** Conceptualization, Methodology, Formal Analysis, Validation, Data

Curation, Visualization, Literature Investigation, Writing – Review & Editing, Supervision. **Piotr Łasak:** Literature Investigation, Data Curation, Writing – Original Draft, Writing – Review & Editing. **Francesco Pattarin**: Conceptualization, Methodology, Formal Analysis, Data Curation, Writing – Original Draft.

Conflicts of interest

The authors declare no competing interests. Piotr Łasak serves as an Associate Editor of JEMI and was not involved in the peer review process, editorial handling, or decision-making for this manuscript.

Citation (APA Style)

Doś, A., Flori, E., Łasak, P., & Pattarin, F. (2026). Patterns of cybersecurity performance in corporations: International evidence. *Journal of Entrepreneurship, Management and Innovation, 22*(3), 130-162. https://doi.org/10.7341/20262237