International Cybersecurity Law Review (2024) 5:169–212
https://doi.org/10.1365/s43439-024-00111-7

ORIGINAL PAPER

More than malware: unmasking the hidden risk of cybersecurity regulations

Mazaher Kianpour · Shahid Raza

Received: 5 December 2023 / Accepted: 4 January 2024 / Published online: 2 February 2024

Abstract Cybersecurity investments are made within a complex and ever-evolving environment, where regulatory changes represent a significant risk factor. While cybersecurity regulations aim to minimize cyber risks and enhance protection, the uncertainty arising from frequent changes or new regulations can significantly impact organizational response strategies. This paper explores the determinants and implications of regulatory risks associated with cybersecurity, aiming to provide a deeper understanding of how these risks influence strategic decision-making. The study delves into the suggestion of preventive and mitigative controls that enable businesses to adapt to and mitigate potential disruptions caused by regulatory changes, thereby preserving their established cybersecurity practices. Another key contribution of this study is the introduction of a stochastic econometric model that illustrates how regulatory risks and uncertainties can affect investment behaviors, often prompting a "wait-and-see" stance. This model synthesizes the complex relationship among investment choices, regulatory changes, and cybersecurity risks, providing insights into the dynamic nature of cybersecurity investment strategies. The research findings offer valuable guidance for risk management and strategic planning in cybersecurity investments. By comprehensively understanding the drivers and impacts of regulatory risks, businesses and policymakers can develop more effective risk evaluation and management approaches. This is essential for sustaining a strong cybersecurity posture while navigating the changing regulatory environment.

✉ Mazaher Kianpour · Shahid Raza
Cybersecurity Unit, RISE Research Institutes of Sweden, Stockholm, Sweden
E-Mail: mazaher.kianpour@ri.se

Shahid Raza
E-Mail: shahid.raza@ri.se

Shahid Raza
The School of Innovation Design and Engineering (IDT), Mälardalen University, Västerås, Sweden

Keywords Cybersecurity regulations · Regulatory risks · Cybersecurity investment · Regulatory uncertainty · Cybersecurity economics

1 Introduction

Today, the term "cybersecurity" often evokes images of malicious hackers, intricate malware, and sophisticated cyberattacks. These threats, while significant and on the rise [120], are just one aspect of broader challenges in cybersecurity. Beneath the surface lies a complex and, at times, overlooked challenge: the evolving landscape of cybersecurity regulations. As governments and businesses strive to secure cyber-physical assets, they are concurrently tasked with navigating a complex web of rules, guidelines, and standards designed to support this very purpose.

While these regulations play a crucial role in creating a secure digital environment, they can also have unintended consequences [30] and introduce complexities that hinder innovation, place burdens on businesses, and even potentially create new vulnerabilities [51]. This intricate balance between their intended protective role and the potential challenges they introduce highlights the need for an in-depth understanding of how changes in cybersecurity regulations and uncertainty about the future regulatory environment can impact business performance and investment in cybersecurity measures.

The discourse on cybersecurity investment has become critically important, heightened by rapid technological advancements and an evolving regulatory environment [43, 69, 99]. Investments in cybersecurity are essential not only for the protection of data and infrastructure but also for the compliance with stringent data protection laws. Noncompliance risks severe penalties, financial liabilities, and loss of customer trust. Regulators face the challenge of incentivizing necessary cybersecurity investments [55, 116]. Translating these regulations into clear investment directives is complex, especially as regulatory landscapes shift to address emerging threats and vulnerabilities [65]. Such changes, while enhancing security, introduce uncertainty about their future stability, posing regulatory risks for organizations.

Regulatory risks reflect the uncertainty behind new or changing regulations over time [128]. The uncertain, and sometimes ambiguous and unpredictable nature of regulatory schemes about cybersecurity introduces a high level of risks, regarding the economic performance of businesses when evaluating the return on their cybersecurity investments. They must consider the costs of implementing regulatory requirements and the risks of noncompliance. Consequently, decision-makers facing a high level of uncertainty may alter their strategies, leading to lower or delayed investments and lost opportunities [65, 138] and potentially rendering those policies less effective [42]. For instance, IBM reported that 56% of CEOs are currently delaying at least one major investment due to a lack of consistent regulations and standards in emerging areas such as data and privacy.[1]

Building on this foundation and recognizing the importance of this category of risks, this paper poses two research questions. First, what are the key determinants

[1] https://www.ibm.com/thought-leadership/institute-business-value/en-us/c-suite-study/ceo.

and implications of regulatory risks associated with cybersecurity, and what controls can be employed to effectively navigate and mitigate these risks? Second, how does uncertainty about the future cybersecurity regulatory environment influence cybersecurity investment decisions in organizations? To address these questions, our research employs a mixed-methods approach. It begins with a review of academic literature and practitioner-oriented reports, supplemented by case study analysis to understand the drivers and repercussions of regulatory risks associated with cybersecurity. This qualitative analysis is further enriched by a quantitative investigation using a stochastic econometric model, designed to quantify the effects of regulatory uncertainties on cybersecurity investment behaviors. The contributions of this study are twofold:

- Through a detailed examination of the determinants and implications of regulatory risks in cybersecurity, the study broadens both an academic and a practical understanding of this risk type. The responses to the first research question lay the groundwork for the development of an effective risk management framework to integrate the interplay between regulatory and cybersecurity risks, thereby fortifying organizational cybersecurity postures. Additionally, the study proposes a comprehensive list of preventive and mitigative measures. While this list may not be exhaustive, it offers invaluable insights for formulating robust risk management strategies tailored to the cybersecurity context.
- The development of the econometric model offers a tool for quantitatively assessing the impact of regulatory changes on investment strategies. This research contributes to the theoretical understanding of cybersecurity investment under regulatory risks and provides insights for organizations, regulators, and researchers.

The paper is organized as follows: Section 2 provides a foundational understanding of the subject by defining and discussing the importance of regulatory risks in cybersecurity. Section 3 employs the bowtie method to systematically explore the determinants and implications of regulatory risks, as well as outline various preventive and mitigative controls. The development and findings of the econometric model are detailed in Section 4. Section 5 synthesizes the key insights of the paper and provides a conclusion. Finally, Section 6 recognizes the study's limitations and proposes directions for future research.

2 Definition and significance of regulatory risks associated with cybersecurity

This section presents the definition and significance of cybersecurity-related regulatory risks. In general, regulatory risks refer to potential consequences that businesses may encounter due to changes in laws or regulations[2] enacted by various govern-

[2] In this study, we use the terms "laws" and "regulations" interchangeably. Both terms refer to mandatory rules or requirements established and enforced by governmental entities, regulatory authorities, or legislative bodies. While laws typically provide a broad legal framework and are enacted by legislative bodies, regulations offer specific rules or standards based on those overarching laws. Nonetheless, for our discussion, both signify binding obligations imposed by authoritative entities.

mental entities at the international, national, or local levels, as well as by industry regulators and international organizations [16, 128]. These risks are inherently connected to the application and enforcement of diverse regulations governing business activities, encompassing areas such as environmental protection, labor standards, data privacy, and financial reporting, operating both at the broader economic level and within specific industries or projects [123].

In the context of cybersecurity, regulatory risks stand distinct from other risk categories frequently discussed in the literature, such as cybersecurity risks and compliance risks. While each type of risk originates from unique sources, they can intersect in their impact on organizations. Regulatory risks stem from potential or actual changes in legal frameworks and regulations that might affect business operations or strategies. On the other hand, cybersecurity risks are centered on the threats and vulnerabilities linked to digital infrastructure, networks, and data[3] [103]. Compliance risks involve potential legal penalties for failing to adhere to laws or regulations, whereas governance risks arise from inadequate or ineffective leadership structures and decision-making processes [83]. It is crucial to understand and differentiate between these risks, as each demands specific mitigation strategies and management approaches.

The regulatory requirements that businesses must comply with can be complex and continuously evolving, making it challenging for them to keep up with changing regulations. According to Gartner's survey on enterprise risk perception, regulatory risks rank as the highest source of concern, slightly edging out cybersecurity risks [45]. Supporting this finding, previous surveys conducted by the Economist Intelligence Unit [38] and Ernst & Young [41] have consistently highlighted that firms consider regulatory risks as one of the most critical types of business risks.

In light of the increasing importance of regulatory risks, local and international businesses are paying more attention to changes in cybersecurity regulations in various countries or regions that can significantly impact their operations, data protection measures, and overall risk management strategies. To highlight this, we analyzed the Google search trends for the keywords "NIS Directive" and "NIS 2 Directive" 6 months before and after their respective implementations in August 2016 and January 2023. Figure 1 demonstrates the level of interest and engagement surrounding these two regulatory frameworks. As it reveals, the interest in NIS 2 Directive (EU) 2022/2555 is more substantial compared to NIS Directive (EU) 2016/1148 during the observed period surrounding the introduction of these regulations. Several factors may contribute to this disparity in search interest.

First, the passage of time between the implementation of the initial NIS Directive and the subsequent NIS 2 Directive may have contributed to increased recognition of regulatory risks and the need for more proactive understanding and adapting to regulatory changes that can affect business operations. Consequently, businesses are actively seeking to understand and adhere to the stipulations of the updated NIS 2 Directive to ensure that their operations remain uninterrupted, safeguard their reputation, and avoid stringent penalties. This has generated more interest in understanding the details of this directive.

[3] Table 3 presents a more detailed comparison between regulatory risks and cybersecurity risks.

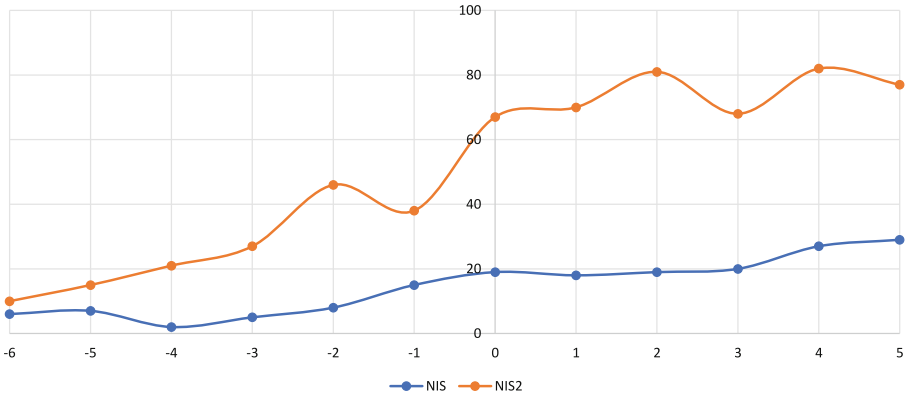


Fig. 1 The comparative Google search trends for the keywords "NIS Directive" and "NIS 2 Directive" over 6 months before and after their implementations. The horizontal axis is centered at 0, representing the implementation months of August 2016 for NIS Directive and January 2023 for NIS 2 Directive, with the months leading up to and following these dates plotted along the axis. The vertical axis quantifies the search interest

Second, the global business landscape has evolved with companies now having more cross-border operations than ever before. Therefore, international regulations like the NIS 2 Directive hold significant relevance for a larger pool of businesses, leading to a broader interest in its stipulations. Third, lessons learned from the initial implementation of the NIS Directive might have stimulated businesses to seek more information and be better prepared for the NIS 2 Directive. They may have experienced challenges or setbacks due to a lack of understanding or compliance with the initial directive and were keen to avoid similar pitfalls with the subsequent one.

Overall, the surge in Google search trends for the "NIS 2 Directive" compared to the "NIS Directive" provides a clear indication of the growing emphasis businesses are placing on cybersecurity regulations. It underscores the growing awareness among businesses and governments of the crucial role that cybersecurity regulations play in safeguarding their operations, data, and reputation. However, businesses are subject to varying degrees of regulatory risk exposure, which is influenced by factors such as the industry in which they operate, the geographical locations of their operations, the nature of their products or services, their compliance with applicable regulations, and the stringency of cybersecurity regulations enforced by regulators overseeing their operations.

To highlight this variation, Fig. 2 visually depicts the search trends associated with "GDPR", "NIS Directive", and "NIS 2 Directive" from 2016 onward. The illustration shows a marked contrast in the search popularity of these three regulations. Notably, while GDPR (Fig. 2a) has drawn significant attention not only from EU member states but also from non-EU countries, the search interest for the NIS Directives remains relatively localized. The widespread interest in GDPR underscores its global resonance, extraterritoriality, and far-reaching implications. The Cisco 2019 Data

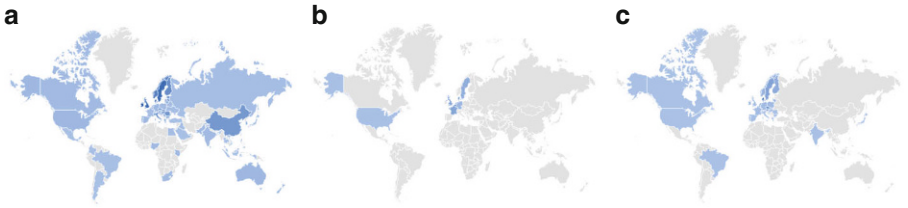


Fig. 2 Geographical distribution of Google search trends from 2016 onward for **a** "GDPR", **b** "NIS Directive", and **c** "NIS 2 Directive". The maps illustrate the global prominence of GDPR compared to the more localized interest in the NIS Directives. The intensity of the color indicates the level of interest, with stronger colors representing higher interest. Regions with interest levels below 20 are not considered

Privacy Benchmark Study[4] reports that organizations worldwide have sought clarity on GDPR to ensure compliance, recognizing its potential impact even outside the EU's jurisdiction. Another reason for this universal attention is that the GDPR has served as a regulatory blueprint for several countries, including Brazil [57]. Furthermore, economic powers like China and the US, given their extensive trade and business dealings with the EU, have shown substantial interest in understanding and adhering to GDPR.

In contrast, the NIS Directive and NIS 2 Directive, due to their specific focus on European networks and information systems, have attracted interest predominantly from countries within the European domain. However, as the figure indicates, there has been an increase in the number of countries showing interest in the NIS 2 Directive compared to the NIS Directive. This increase in attention can potentially be attributed to the same factors that we outlined earlier.

This analysis highlights a rising focus on shifts in cybersecurity regulations over time. Such growing attention underscores the evolving landscape of cybersecurity and its associated implications. While the significance of cybersecurity regulations is well acknowledged in the existing literature [55, 77, 95], the consequences of their alterations, coupled with the risks stemming from change and uncertainty, remain relatively unexplored. Specifically, the influence of these regulatory risks on aspects like cybersecurity investments and related domains warrants further examination. In this study, we address this gap by first identifying the drivers and implications of these changes in a broader context. Subsequently, we investigate how the perception of such risks influences investment behavior within the context of cybersecurity.

3 Determinants and implications of regulatory risks

In this section, we explore the determinants and implications of regulatory risks associated with cybersecurity.[5] To visualize the causal relationships between the determinants and implications and structure of our discussion, we utilize the bowtie

[4] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.

[5] It is essential to understand that these determinants can often be interconnected, amplifying, or mitigating their individual effects. For example, new technologies and innovations can potentially be a source of

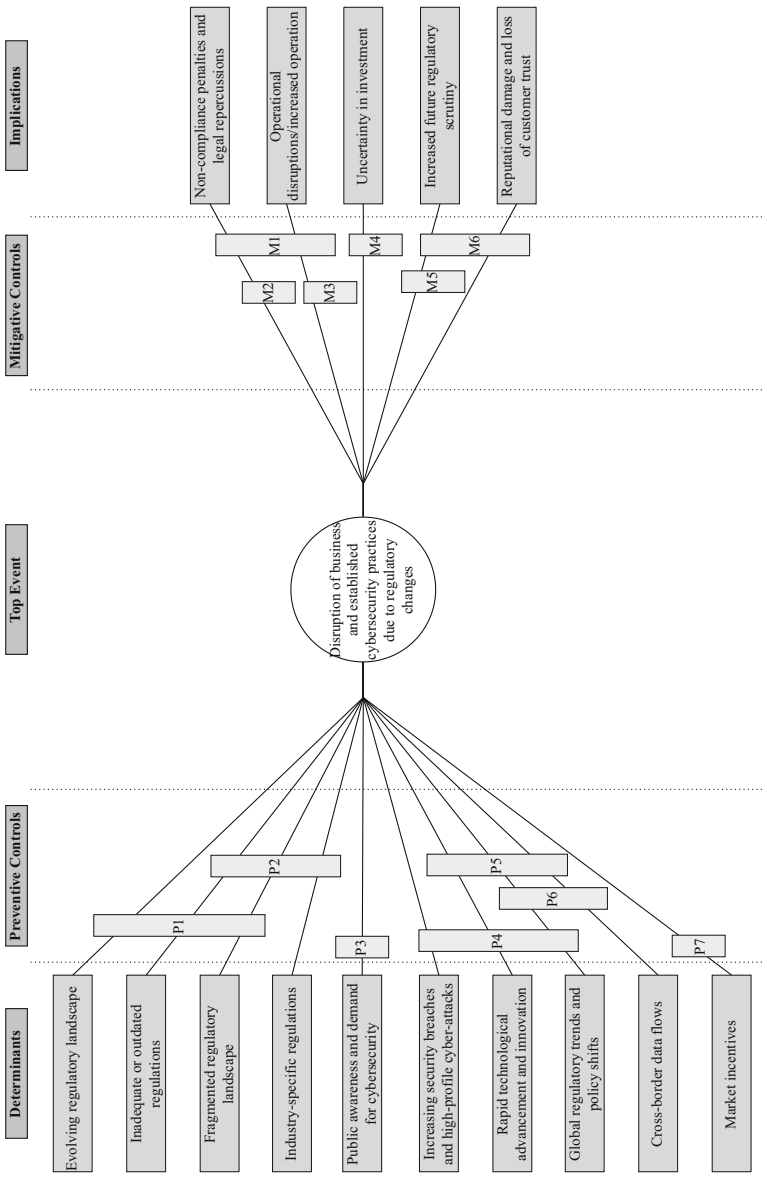


Fig. 3 The bowtie diagram of the determinants and implications of regulatory risks associated with cybersecurity. The suggested preventive (P) and mitigative (M) controls are explained in Sect. 3.3

diagram. This tool effectively showcases determinants on the one side and consequences on the other, with preventive controls that can change the likelihood of the event, and mitigative controls reducing the impact should an event occur. Bowtie analysis is a common approach to map the risks associated with undesired events [11]. In our context, the undesired event that we focus on is termed the "top event",

regulatory fragmentation [137]. Therefore, considering potential interactions is crucial to getting a comprehensive picture of such risks.

which represents *the disruption of established cybersecurity practices due to regulatory changes*. Figure 3 provides a comprehensive view of this bowtie diagram. In the following sections, we discuss each element in more detail.

3.1 Determinants

The left-hand side of a bowtie diagram represents the causes or determinants leading up to the top event. These can include various factors, triggers, or conditions that, if left uncontrolled, might increase the likelihood of the top event happening. In this section, we identify the determinants of changes in cybersecurity regulations. By highlighting the interplay and interconnectedness of these determinants, we underscore the potential synergies among them and demonstrate how they can intensify the risk of disruption of established cybersecurity practices due to regulatory changes.

3.1.1 Evolving cybersecurity regulatory landscape

As governments, international bodies, and regulatory agencies respond to the dynamic challenges of the digital age, cybersecurity regulations are continually evolving, primarily due to factors such as emerging threats [17], technological advancements [131], increasing reliance on digital systems in various industries [85], and growing awareness of privacy concerns [15]. While this evolution is necessary to ensure robust protection mechanisms, uphold data integrity, and instill public trust in digital platforms, it also introduces challenges such as uncertainty and complexity in compliance for businesses [86].

The uncertainty becomes particularly evident as new regulations are introduced in different regions and sectors. In the United States, for instance, the pace and number of cybersecurity legislative efforts vary widely among states. As our data in Table 1 presents, over 2019–2022, the number of cybersecurity legislation (whether enacted, failed, vetoed, or pending) has been substantial. New York spearheads the movement with an impressive 116 legislative attempts in the last 4 years, while New Jersey and Maryland are not far behind with 107 and 87 efforts, respectively. On the opposite end of the spectrum, Wyoming and South Dakota have shown minimal activity, with, respectively, only one and two legislative efforts over the same period. Furthermore, states such as Texas and Vermont have exhibited significant year-to-year variations, suggesting that external factors or shifts in regional priorities may influence legislative outputs. The reasons behind these fluctuations might be influenced by incidents, shifts in state leadership priorities, or reactions to national trends. Regardless, such variances in regional cybersecurity efforts highlight the challenge businesses face in predicting the future state of the regulatory environment.

Hoffmann et al. [65] characterize this situation as *regulatory uncertainty.* This uncertainty is not solely derived from the fluctuating count or status of regulations – ranging from those that are enacted to those still pending or those that have failed. Another significant source of uncertainty stems from the constantly changing group of stakeholders engaged in regulatory regimes [72, 80]. The way in which these actors perceive, interpret, and define issues such as privacy and security can introduce additional layers of unpredictability to the regulatory landscape. For instance,

Table 1 Number of new legislations in US states from 2019–2022. Data extracted from National Conference of State Legislatures (NCSL)

State	2022	2021	2020	2019	Total
Alabama	0	2	0	3	5
Alaska	1	1	1	0	3
Arizona	7	1	0	3	11
Arkansas	0	3	1	3	7
California	16	9	12	12	49
Colorado	1	1	0	0	2
Connecticut	0	7	3	7	17
Delaware	0	0	1	2	3
District of Columbia	0	0	1	0	1
Florida	14	8	7	17	46
Georgia	3	5	10	6	24
Hawaii	5	7	5	1	18
Idaho	2	1	0	0	3
Illinois	20	13	21	9	63
Indiana	1	1	8	4	14
Iowa	18	6	17	8	49
Kansas	2	3	1	1	7
Kentucky	3	0	0	3	6
Louisiana	1	7	13	8	29
Maine	0	6	1	0	7
Maryland	27	23	26	11	87
Massachusetts	14	13	10	10	47
Michigan	3	3	6	2	14
Minnesota	6	9	25	18	58
Mississippi	1	3	4	5	13
Missouri	4	3	3	1	11
Montana	0	4	0	3	7
Nebraska	1	0	1	1	3
Nevada	0	1	0	8	9
New Hampshire	2	6	5	6	19
New Jersey	24	37	15	31	107
New Mexico	3	1	2	1	7
New York	34	23	33	26	116
North Carolina	2	3	4	5	14
North Dakota	0	5	0	6	11
Ohio	3	3	1	2	9
Oklahoma	3	1	7	5	16
Oregon	3	1	0	5	9
Pennsylvania	9	7	9	4	29
Puerto Rico	2	2	4	6	14
Rhode Island	13	4	6	3	26
South Carolina	1	0	3	2	6
South Dakota	1	0	1	0	2

Table 1 (Continued)

State	2022	2021	2020	2019	Total
Tennessee	1	5	1	0	7
Texas	0	37	0	23	60
Utah	3	1	2	0	6
Vermont	1	17	5	3	26
Virginia	5	0	11	12	28
Washington	5	4	10	6	25
West Virginia	2	2	1	2	7
Wisconsin	3	2	2	0	7
Wyoming	0	1	0	0	1

within the EU, there are 22 interconnected actors responsible for delivering 18 distinct cybersecurity functions, as delineated in an institutional map by the European Union Agency for Network and Information Security (ENISA)[6]. While not all of these actors play a direct role in regulatory settings and enactment, the institutional path-dependencies and fragmentation of authority resulting from the diversity and heterogeneity of these actors contribute significantly to regulatory uncertainty [37]. Moreover, the varying degrees of influence and jurisdiction each actor holds lead to overlapping responsibilities and potential conflicts in enforcement [105].[7]

To complement the qualitative insights provided by the literature regarding the conceptual understanding of regulatory uncertainty, we empirically measured the fluctuations in regulatory sentiment and uncertainty in cybersecurity. Figure 4 illustrates the fluctuations in the daily index of regulatory sentiment and uncertainty surrounding cybersecurity from October 25, 2012, to October 17, 2023. To quantify this index, we employed the text-based measurement methodology suggested by [122][8]. Our analysis encompasses 3930 articles sourced from Infosecurity Magazine. The magazine's acclaimed editorial content offers in-depth features that delve into the strategy, insights, and technological facets of cybersecurity. We specifically focused on articles under the *"Compliance"* category, given their direct relevance to regulations. As depicted in the figure, there is a noticeable sense of uncertainty concerning cybersecurity regulations. Notably, on November 25, 2016, the uncertainty index peaked at 1. Below, we have highlighted a segment from an article published on that very day, which encapsulates the prevailing uncertainty of the time.

[6] https://www.enisa.europa.eu/cybersecurity-institutional-map/results.

[7] The EU Cybersecurity Strategy outlined the need for a Joint Cyber Unit as a platform to strengthen cooperation among authorities in the EU cybersecurity ecosystem. This unit can facilitate coordination among these disparate entities and align their different agendas, strategies, and operational frameworks to avoid further exacerbating the regulatory uncertainty.

[8] The list of uncertainty keywords in our measurement includes: "regulation", "law", "ban", "restrict", "change", "uncertain", "ban", "change", "evolve", "require", "update", "introduce", "uncertainty", "modify", "new policies", "legal implications", "regulatory change". (Note: The list includes all conjugated forms of the verbs, such as past, present, future, conditional, subjunctive, and imperative.) For sentiment analysis (intensity and polarity), we used VADER (Valence Aware Dictionary and Sentiment Reasoner), a lexicon and rule-based sentiment analysis tool [66].

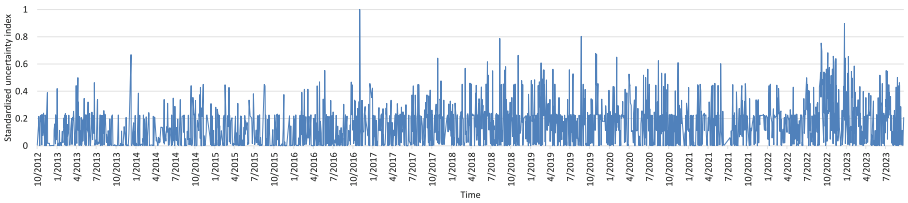


Fig. 4 Measuring regulatory uncertainty through news analysis from Infosecurity Magazine (from October 25, 2012, to October 17, 2023)

> The EC and the European Union (EU) are dealing with a number of cyber-related issues at the moment. Top of the agenda is the potential impact of Brexit on cybersecurity across the region, as well as incoming data protection laws. The European General Data Protection Regulation (GDPR) comes into force in May 2018, but there is plenty of work ahead for businesses and governments before that deadline.[9]

This integration of empirical data with theoretical insights allows for a deeper understanding of the complexities involved in navigating decision-making processes in the face of evolving regulatory environments. The existing body of literature on decision-making under regulatory uncertainty presents dichotomous outcomes. On one hand, evidence suggests that when decision-makers are confronted with a high level of uncertainty, they tend to adopt a wait-and-see approach, holding off on investments until a clearer, more reliable forecast emerges [14, 138]. Conversely, other studies indicate that this high uncertainty does not invariably lead to delayed decisions or investments. Instead, some decision-makers might proceed with investments and even benefit from investments if they gain a first-mover advantage [6].

In addition to regulatory uncertainty, another challenge that is posed by the evolving regulatory landscape is the increasing complexity. Such complexity can arise from the proliferation of regulations, their interconnectedness, or even the shifting nuances within them. An illustration of increasing complexity can be observed in the transition from the NIS Directive to the NIS 2 Directive. Table 2 displays the directives and regulations cited within both Directive 2016/1148 (NIS) and Directive 2022/2555 (NIS 2), along with their respective frequencies. In the NIS Directive, references to other directives and regulations were limited, but in NIS 2 Directive, the references had expanded considerably. This demonstrates that the updated directive is situated within a more intricate web of legislation and highlights the expanding interconnectivity and scope of cybersecurity considerations across various areas of regulation and incorporating more facets of societal, technological, and economic activities. It is also worth noting that Regulation (EU) 2016/679, known as GDPR, is referenced 17 times in the NIS 2 Directive. The GDPR is a cornerstone regulation that focuses on personal data protection. Its frequent mention underlines the confluence of cybersecurity and data protection regulations and stresses the imperative of aligning cyber practices with privacy obligations.

[9] https://www.infosecurity-magazine.com/news/european-commission-hit-by-ddos/.

Table 2 The references cited in NIS Directive and NIS 2 Directive. The list excludes the directives and regulations that have been repealed or amended.

Directive 2016/1148 (NIS Directive)		Directive 2022/2555 (NIS 2 Directive)	
Directives	Regulations	Directives	Regulations
Directive 2015/1535	Regulation 300/2008	Directive 2022/2557	Regulation 910/2014
Directive 2013/11/EU	Regulation (1315/2013	Directive 2018/1972	Regulation 2016/679
Directive 2009/22/EC	Regulation 725/2004	Directive 2015/1535	Regulation 2022/2554
Directive 2009/72/EC	Regulation 526/2013	Directive 2019/944	Regulation 300/2008
Directive 2009/73/EC	Regulation 1025/2012	Directive 2018/2001	Regulation 2018/1139
Directive 2009/12/EC	Regulation 182/2011	Directive 2020/2184	Regulation 2021/696
Directive 2012/34/EU	Regulation 45/2001	Directive 2002/58/EC	Regulation 2019/881
Directive 2005/65/EC	Regulation 1049/2001	Directive 2011/93/EU	Regulation 182/2011
Directive 2002/59/EC	Regulation 910/2014	Directive 2013/40/EU	Regulation 2022/2065
Directive 2010/40/EU	Regulation (549/2004	Directive 2005/29/EC	Regulation 2018/1725
Directive 2014/65/EU	Regulation 2015/962	Directive 2009/119/EC	Regulation 1025/2012
Directive 2011/24/EU	Regulation 575/2013	Directive 2009/73/EC	Regulation 2019/1150
	Regulation 648/2012	Directive 2009/12/EC	Regulation 2019/943
	Regulation 2320/2002	Directive 2012/34/EU	Regulation 1315/2013
		Directive 2005/65/EC	Regulation 549/2004
		Directive 2002/59/EC	Regulation 725/2004
		Directive 2010/40/EU	Regulation 2015/962
		Directive 2014/65/EU	Regulation 575/2013
		Directive 2011/24/EU	Regulation 648/2012
		Directive 2001/83/EC	Regulation 2022/2371
		Directive 2008/98/EC	Regulation 2022/123
			Regulation 1907/2006
			Regulation 178/2002
			Regulation 2017/745
			Regulation 2017/746

3.1.2 Inadequate or outdated cybersecurity regulations

As a natural response to the constantly evolving cyber threat landscape and rapid technological advancements, regulations that are seen as inadequate or outdated inevitably become primary candidates for, sometimes abrupt, updates or revisions [86, 98]. The uncertainty introduced by such swift regulatory changes can disrupt long-term planning, strain resources, and potentially place businesses at a competitive disadvantage, especially if they are unprepared.

Many pre-existing regulations may not be tailored sufficiently to counter the increasing sophistication of attack vectors and the evolving cyber threat landscape [34]. Take supply chain attacks, for instance. ENISA, in its 2018 assessment, identified supply chain attacks as a significant threat. This view was further cemented in their 2021 report, where such attacks were highlighted as a prime threat. While the NIS directive of 2016 and preceding regulations and directives overlooked this essential aspect, the NIS2 directive took a more proactive stance. Article 21(2) of

NIS2 designates supply chain cybersecurity as an integral part of cybersecurity risk management.

Parallelly, as our societies are undergoing rapid digital transformations, regulators have been pivoting to ensure their regulatory responses remain contemporary and agile. This adaptability is especially vital when facing security challenges posed by emergent technologies, which are often unanticipated by regulations before the widespread adoption of these technologies.[10] For example, the use of generative AI across businesses will be affected by AI regulations, particularly concerning bias, discrimination, misinformation, and unethical uses. Recent directives including the Blueprint for AI Bill of Rights[11] from the White House, China's proposed measures for the management of GenAI serviced[12], and the draft European Union AI Act[13] emphasize ethical and secure AI services. Reflecting these concerns, the results of a survey by PwC[14] shows that 95% of the respondents expect that the costs of compliance will be moderate to significant. Furthermore, 39% of them responded that they will need to make major changes in their business to comply with regulatory changes within the context of AI.

Finally, deficient frameworks and approaches for crafting regulations can act as a determinant for regulatory risks. Although all the states in the US have legislated cybersecurity, Kuhn [75] and Hyla [67] argue that the piecemeal approach adopted by the states is inadequate and can lead to a patchwork of regulations that is challenging for businesses operating across multiple states. This approach not only complicates compliance but also elevates the risks associated with potential noncompliance penalties. Several scholars have called for an integrated, harmonized approach, endorsed at a federal level, to mitigate such risks and provide a stable and transparent regulatory environment for businesses [21, 80, 129]. Should such a shift in strategy be realized, businesses would confront a new set of regulatory challenges and risks.

3.1.3 Fragmented cybersecurity regulatory landscape

Foundational cultural and regional differences, varying levels of cybersecurity capabilities and preparedness, diverse economic and political incentives, and discrepancies in the methods used to devise and enforce regulations give rise to a fragmented cybersecurity-related regulatory environment [87, 24, 84, 87]. Consequently, businesses find themselves navigating a myriad of regulations across different jurisdictions. Such scenarios lead to compliance efforts that might not necessarily translate into enhanced security. This not only burdens businesses with inefficient compliance tasks but also poses challenges in ensuring sustainable cybersecurity measures across the ecosystem.

[10] https://www.oecd.org/sti/inno/2102514.pdf.

[11] https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[12] https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023/.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[14] https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.

In the European Union, the introduction of the General Data Protection Regulation (GDPR) was a significant step towards achieving harmonization of data protection laws[119]. Nevertheless, this attempt at unification has introduced its own set of regulatory risks stemming from ambiguities in implementation [108, 136], operational overheads (i.e., the need for businesses to hire Data Protection Officers, conduct regular impact assessments, and ensure constant compliance)[134], interplay with other regulations [3], data transfer challenges [88], and unanticipated business model impacts [81]. An example of the latter is the GDPR's stringent consent requirements, which affected sectors like online marketing, where the traditional models of targeted advertising are now under scrutiny [118].

Building upon this harmonizing strategy, the EU introduced the Cybersecurity Act, aiming to avoid the fragmentation of the internal market concerning cybersecurity certification schemes, and the Joint Cyber Unit, to strengthen cooperation among EU institutions, agencies, bodies, and the authorities in the Member States. Moreover, different public–private or sector-specific partnerships have been established to harmonize the regulations across certain domains. For example, in the ICT sector, G5 collaborative regulation[15] is a human-centered regulatory framework that is based on significant cooperation of regulators and numerous stakeholders in developing harmonized regulations across sectors that rely on ICT [59]. While a comparative study of many partnerships in the area of cybersecurity by [20] shows that these forms of cooperation often remain at the rhetorical level because they have little to offer to the private side, observing the potential advantages of such harmonizations, other regions are similarly advancing towards unification through different partnerships [19, 112, 117]. Although this process is beneficial, it inadvertently introduces its own set of regulatory risks and uncertainties.

3.1.4 Industry-specific cybersecurity regulations

Certain sectors, including healthcare, finance, telecommunications, and aviation, are subject to specialized cybersecurity regulations. These industry-specific requirements can be more stringent and complex, reflecting the unique vulnerabilities and critical nature of services in these domains. For instance, in the healthcare sector, the availability of medical services and protection of patient data is paramount; in aviation, ensuring the security of navigation and communication systems is vital.[16] Consequently, these regulations are tailored to address the distinct challenges posed by each sector.

Furthermore, the imposition of cybersecurity regulations can lead to a profound transformation within industries. As discussed by [93], such regulations have the potential to reconfigure the governance structure of certain sectors, like the water industry. By introducing new regulatory requirements, traditional industry priorities can be realigned, prompting a shift in strategic focuses. This can result in industries emphasizing cybersecurity concerns even over their conventional operational challenges. In the long run, while such a shift enhances the security posture of an

[15] https://gen5.digital/explainers/why-do-we-need-g5-collaborative-regulation-four-fundamentals-2/.

[16] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0373.

industry, it also necessitates continuous adaptation against an evolving regulatory landscape.

3.1.5 Public awareness and demand for cybersecurity

The implications of cyberattacks extend beyond the immediate boundaries of businesses and permeate into the broader society. These incidents can lead to detrimental consequences such as the compromise of sensitive personal information, resulting in potential identity theft, financial losses, and a breach of privacy. Such breaches can inflict emotional distress on individuals, manifesting as embarrassment, anxiety, or a reduced trust in digital systems [2, 28, 125]. Consequently, cybersecurity is not just about protecting business interests or infrastructure; it is about safeguarding human rights and personal and societal well-being.

Although there are rights-based dilemmas concerning the extent of government interference in civic life, the results of a survey by Cisco[17] reveals that consumers value government's role in regulating the use of data, and they view the EU's GDPR very favorably. Moreover, the findings of an experiment by [124] suggest that exposure to different types of cyberattacks heightens cyber threat perceptions and shifts towards favoring stricter regulations. Therefore, increasing sensitivity to the importance of privacy and security, and public demand for government intervention in cybersecurity has led to a more proactive regulatory environment. The pace at which these regulatory changes are implemented to respond to this demand and their scope and level of granularity can significantly challenge businesses and heighten regulatory risks.

3.1.6 Increasing security breaches and high-profile cyberattacks

Target Data Breach in 2013, Sony Pictures hack in 2014, Equifax data breach and WannaCry ransomware attack in 2017, Cambridge Analytica Scandal in 2018, SolarWinds hack in 2019, among numerous other significant cyberattacks, not to mention the multitude of smaller, daily cyber incidents, have stimulated regulators worldwide into action, working to draft and implement resilient cybersecurity regulations, strengthen their breach notification laws, and mandating stringent compliance requirements for businesses [64, 73, 115, 121, 124, 139]. Furthermore, according to a report by ENISA, the ChoicePoint case in 2005 and some other high-profile security breaches led to the California Consumer Privacy Act (CCPA) being followed by further laws in at least 34 other states [5]. These regulatory shifts underscore the critical role that past cyber incidents play in shaping the future landscape of cybersecurity regulations [51].

Within the European context, a review of the EU Cybersecurity Strategy and regulations such as the NIS and NIS 2 Directives, Cybersecurity Act, and Cyber Resilience Act reveals a consistent theme of concern regarding the increasing number, magnitude, sophistication, frequency, and repercussions of cyber incidents. The

[17] https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf.

preamble of these documents underscores the view that such threats pose significant risks to the smooth functioning of networks and information systems. By explicitly highlighting these challenges, regulators demonstrate their awareness and recognition of the rapidly transforming cyber threat environment. The emergence of these regulations reflects a proactive attempt by regulators to anticipate and counteract these threats, ensuring the safety, security, and reliability of digital infrastructures across sectors and geographies. However, the agility of cyber threats, which often advance faster than current regulatory measures, means that this proactive stance amplifies regulatory risks emerging from the potential for overregulation, the complexities of harmonizing across jurisdictions, and the inadvertent stifling of innovation due to stringent compliance requirements. Consequently, businesses face the challenge of adapting to these regulations, often at significant costs, both in terms of financial investment and operational adjustments.

3.1.7 Rapid technological advancement and innovation

The technological landscape has experienced unprecedented growth and change in recent decades. Among different types of risk (e.g., market risk, technological, organizational, financial, and societal) that are present in the adoption of innovative technologies, an important question arises: How will regulators respond to the latest technologies? As per data from the ITU DataHub, the percentage of countries with established cybersecurity legislation/regulation surged from 24.1% in 2009 to 57.1% in 2021.[18] Delving deeper into the datasets provided by this organization[19], we observed a marked uptick in the number of countries formulating strategies, policies, or initiatives centered on emerging technologies.

As illustrated in Fig. 5, in 2022 compared to 2019, there was a marked rise in policies focusing on AI, IoT, Blockchain, and 5G/6G. This proliferation in policy formulation is indicative of global recognition of the implications and potential risks of these technologies. However, the challenge lies in the evolving nature of the regulatory landscape. The anticipation, volatility, and unpredictability of how regulators will engage, be it the introduction of new regulations, amendments to existing ones, or repealing outdated ones, can significantly affect the operational dynamics for businesses and the experiences of their clients.

Regulatory change and technological dynamics are intertwined, with regulations influencing technological directions and technological innovations necessitating regulatory adaptations [9, 12, 46, 114]. Advances in artificial intelligence, IoT, and big data analytics, for instance, have intensified the debate on how to ensure proper balance in regulatory frameworks [58]. Concurrently, as technology and novel business models evolve, they tend to outpace regulation controls [32]. To maintain relevance in this changing landscape, regulators are shifting towards more flexible approaches like regulatory sandboxes, outcome-based regulation, risk-weighted regulation, and adaptive regulation [91]. While this evolving regulatory paradigm offers organizations the opportunity to influence regulations and align their compli-

[18] https://datahub.itu.int/data/?e=701&c=&i=100103&s=8428.

[19] https://datahub.itu.int/data/?e=701&c=&i=100062&s=31428.

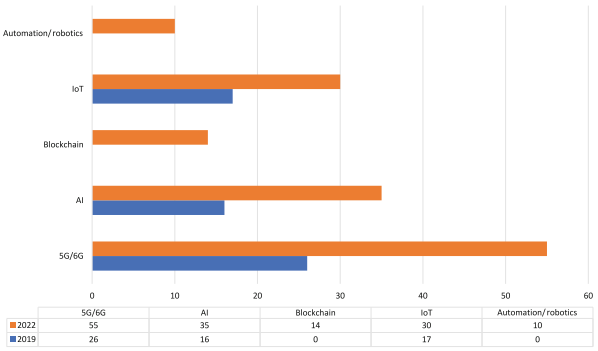


Fig. 5 The growth in focus on emerging technologies such as AI, IoT, Blockchain, and 5G/6G

ance mechanisms, it also introduces multifaceted regulatory risks that can jeopardize their operational stability, strategic objectives, and economic growth.

3.1.8 Global regulatory trends and policy shifts

In the 1990s and early 2000s, the EU adopted a more reserved approach towards cybersecurity regulation. Rather than leveraging robust regulatory instruments or placing emphasis on centralized, union-driven governance, the strategy centered on non-legally binding instruments at the national level [63]. The primary aim was to instill a sense of cybersecurity autonomy and responsibility within Member States. However, as the digital era progressed, coupled with an increase in high-profile cyberattacks and the evolving nature of threats[20], the EU began to recognize the need for a more assertive and unified stance. This shift in the EU's policy not only led to the introduction of more stringent regulations and proactive measures to strengthen its cybersecurity posture but also signaled a broader global trend, emphasizing the importance of holistic and cooperative cybersecurity strategies across regions [20, 26].

Additionally, macroeconomic factors have emerged as significant influencers in shaping these regulatory paths. For instance, global economic downturns can make nations more protective and cautious, leading to tightened regulations to guard domestic businesses[21]. Conversely, periods of economic growth and globalization might promote more open policies, but with an emphasis on standardized cybersecurity practices to facilitate cross-border digital trade [1, 113]. Geopolitical tensions, such as those arising from international cyber-espionage or state-backed cyberattacks, further underscore the need for robust, agile, and responsive regulatory frameworks [61]. Given the interplay and complexity of these factors, it becomes paramount for regulations to remain dynamic, adapting to the multifaceted challenges and opportunities that lie ahead. However, such adaptability can introduce regulatory risks such as misalignment with global standards, barriers to emerging

[20] https://www.enisa.europa.eu/news/enisa-news/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1.

[21] https://www.imf.org/en/Blogs/Articles/2023/01/30/global-economy-to-slow-further-amid-signs-of-resilience-and-china-re-opening.

industries like fintech [79] or biotech [94] due to overcaution, or even the unintended consequence of creating regulatory loopholes that can be exploited [25]. It is equally possible that rapid policy shifts could lead to confusion, with businesses struggling to stay compliant, thereby affecting their competitive landscape.

3.1.9 Cross-border data flows

Over the past few years, data has become the most valuable asset for businesses[22]. To maintain a competitive edge, businesses have delved deep into data collection, storage, analysis, utilization, monetization, and sharing. While these practices facilitate the creation of personalized products and services, more efficient business processes, and new revenue streams, they also raise concerns surrounding data usage, transparency, control, accuracy, ethics, security, reliability, and privacy. This point of view resonates with national and global regulators, reaching the institution of data protection regulations in over 160 countries, along with regional frameworks like the EU's GDPR and collaborative initiatives such as the APEC CBPR System[23].

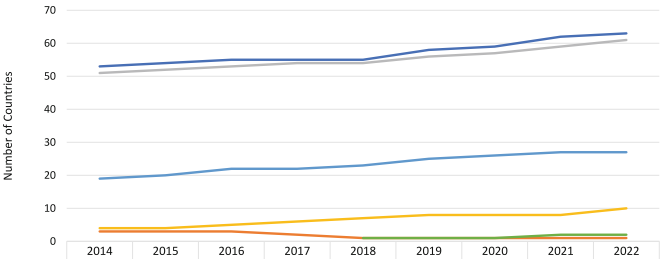
Figure 6 provides a comprehensive overview of how countries have adjusted their data transfer regulations from 2014 to 2022. The information presented is extracted from the OECD Regulatory Database[24], which covers the Digital Services Trade Restrictiveness Index of 85 countries. At a glance, the most dominant policy adopted by countries pertains to permitting cross-border transfers of personal data when certain private sector safeguards are in place, with an upward trend observed over the years. In contrast, there is a declining trend for countries allowing free cross-border transfers based on the accountability principle. Furthermore, a growing number of countries are mandating that certain data be stored locally, and a few have adopted policies where data transfers are subject to approval on a case-by-case basis. However, the number of countries like Eswatini and Saudi Arabia where data transfer is completely prohibited, though small, has shown a slight increase in recent years. The chart indicates the evolving nature of data privacy and protection norms globally, reflecting the complexities businesses face in an ever-changing digital world.

To gain the trust of consumers, regulators are revisiting their conventional strategies to effectively address emerging data risks. However, to support innovation, regulators must seek the right balance between free-market development and regulation. [10] characterize the cross-border data flow regulations by the inconsistency of laws among countries, different levels of social responsibility, and business competition. Such characterization introduces several challenges including increased regulatory scrutiny over data handling practices, challenging strategic choices like potentially backing away from data monetization opportunities to maintain stakeholder trust, and obligatory requirements driven by regulations to build a risk-aware organizational culture to respect the privacy of customers [101].

[22] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[23] https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[24] https://qdd.oecd.org/subject.aspx?Subject=STRI_DIGITAL.



	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cross-border transfer of personal data is possible when certain private sector safeguards are in place	53	54	55	55	55	58	59	62	63
Free cross-border transfer of personal data or application of the accountability principle	3	3	3	2	1	1	1	1	1
Cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws	51	52	53	54	54	56	57	59	61
Cross-border transfer is subject to approval on a case-by-case basis	4	4	5	6	7	8	8	8	10
Certain data must be stored locally	19	20	22	22	23	25	26	27	27
Transfer of data is prohibited	0	0	0	0	1	1	1	2	2

Fig. 6 A comparative analysis of regulatory stances of cross-border data transfer, emphasizing private safeguards, accountability principles, and stricter controls across 85 countries (2014–2022). Data extracted from OECD Regulatory Database

3.1.10 Market incentives

Businesses may prioritize time-to-market and cost-effectiveness over implementing robust security measures, which necessitates increased regulatory oversight. This profit-driven focus risks bypassing the "security by design" principle, potentially leaving vulnerabilities unaddressed. This issue is explicitly highlighted in the US National Cybersecurity Strategy 2023:

> Markets impose inadequate costs on–and often reward–those entities that introduce vulnerable products or services into our digital ecosystem. Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance. Software makers can leverage their market position to fully disclaim liability by contract, further reducing their incentive to follow secure-by-design principles or perform pre-release testing.

Additionally, the role of market incentives has been investigated in real-world cyber incidents. According to [111], it was short-term profit motives and cost-cutting measures that contributed to the vulnerabilities leading up to the SolarWinds cyberattack in 2020. In the aftermath of this breach, the Biden administration issued two executive orders aimed at improving cybersecurity practices across industries[25]. Furthermore, other global regulatory bodies initiated reviews and proposed tighter regulations to ensure that companies prioritize security at every stage of product and software development [100]. The highlighted case emphasizes that neglecting

[25] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

cybersecurity, often due to market-driven motivations, exposes businesses not only to cyber threats but also to unexpected and possibly severe regulatory risks.

3.2 Implications

This section delineates the implications of regulatory risks associated with cybersecurity once the determinants surpass the preventive and mitigative barriers, as depicted in Fig. 3. It is essential to note that the implications associated with regulatory risks in cybersecurity are not unique. They often overlap with issues stemming from other risk categories, such as cyber risks and compliance risks. This interconnectedness not only underscores the complexity of navigating the regulatory and cybersecurity landscape but also emphasizes the need for a holistic approach to assessing and managing these risks and formulating cybersecurity policies and strategies. Businesses and regulators alike must recognize these overlapping domains and collaboratively develop frameworks that address multifaceted challenges [68].

3.2.1 Noncompliance penalties

Within the context of regulatory risks associated with cybersecurity, noncompliance penalties stand as one of the most immediate and tangible repercussions faced by businesses. These penalties, caused by not adhering to changing cybersecurity regulations, encompass both financial and legal implications. Financially, companies can incur substantial fines. For instance, immediately after GDPR came into effect on May 25, 2018, the Austrian organization "None Of Your Business" and the French NGO "La Quadrature du Net" filed complaints against Google. These complaints cited various GDPR violations, including lack of transparency (Article 5), insufficient information (Articles 13/14), lack of legal basis (Article 6), and obtaining "unambiguous" rather than "specific" consents (Article 4, number 11). In 2019, France's data protection authority, CNIL, imposed a 50 million euro fine on Google as a result of these complaints.

On the legal front, organizations might find themselves entangled in prolonged lawsuits, further escalating their costs. These lawsuits can lead to operational consequences, such as service restrictions, business suspensions, or even the revocation of operational licenses. For instance, Zoom faced legal action for allegedly collecting data when users installed or launched the application, then purportedly sharing this data without adequate disclosure with third parties, including Facebook Inc. This practice was challenged as a violation of the California Consumer Privacy Act (CCPA), a few weeks after it took effect on January 1, 2020.

3.2.2 Operational disruptions/increased operation cost

Adapting to new or evolving regulations often necessitates considerable changes in systems, leading to both disruptions and increased expenses. For instance, the advent of GDPR demanded businesses across various sectors to rethink their data storage and processing paradigms. Such a shift was substantial, with compliance

costs for Fortune 500 companies approximated at around $7.8 billion[26]. Moreover, the financial and operational impact of GDPR forced some businesses to either modify or entirely discontinue specific services. A notable example includes Uber Entertainment, an online gaming company, choosing to shut down a multiplayer video game to bypass GDPR compliance costs[27]. On a broader scale, industry giants like Facebook have been struggling with regulators regarding their facial recognition features in the EU for more than 6 years[28], while Google prompted Google Analytics users to amend their data retention configurations.

The evolving regulatory environment not only amplifies operational costs but also reshapes market dynamics. Regulatory demands can inadvertently set high barriers to entry[50], which is particularly challenging for startups and smaller entities lacking ample resources for compliance. This could lead to reduced market competition, favoring larger or more financially equipped organizations. For instance, the fallout of GDPR echoed in the Merge and Acquisition (M&A) space, with a Euromoney survey revealing that 55% of over 500 M&A practitioners across Europe, the Middle East and Africa (EMEA) aborted transactions due to concerns regarding data protection and GDPR compliance.[29] This apprehension was even more pronounced in regions like Germany, the Nordics, and the UK.

In the broader picture, the continuous need to adapt to regulations can impede companies from fully utilizing data, potentially limiting technology adoption, stifling productivity growth, and placing businesses at a competitive disadvantage. The synthesis of these challenges underscores the delicate balance businesses must maintain between compliance and competitiveness in a dynamic regulatory landscape.

3.2.3 Uncertainty in investment decisions

In the cybersecurity context, at its core, each firm aims to minimize the risk associated with cyberattacks. Regulations can be an effective instrument to achieve this goal by incentivizing businesses to invest in cybersecurity [49, 95, 96]. [55] developed an economic-based analytical framework for assessing the impact of regulations designed to offset the tendency to underinvest in cybersecurity by the private sector. They found that success depends on the firms' (i) ability to determine the optimal mix of inputs to cybersecurity and (ii) ability and willingness to increase their cybersecurity investments.

However, [78] points out that rapidly evolving cybersecurity regulations complicate cybersecurity management and significantly increase cybersecurity investment costs. This situation directly impacts businesses' ability to determine the optimal levels of cybersecurity investment and, in some cases, affects their ability and willingness to increase their cybersecurity investments. According to the Cisco 2023 Data Privacy Benchmark Study, investment in privacy at larger organizations re-

[26] https://www.cpomagazine.com/data-protection/global-500-faces-gdpr-compliance-costs-of-7-8-billion/.

[27] https://variety.com/2018/gaming/news/super-monday-night-combat-shuts-down-1202790517/.

[28] https://www.cnbc.com/2018/04/19/facebooks-facial-recognition-may-not-meet-gdpr-rules.html.

[29] https://m-a-worldwide.com/gdpr-and-the-effects-on-the-ma-process/.

mained relatively unchanged after steep increases from 2019 to 2020. While the reasons are not clear in this study, it may suggest a plateau in investment growth due to regulatory uncertainties. After substantial investments to comply with GDPR and in response to the expanding cybersecurity legislation in the US since 2019 (see Table 1), many organizations are now grappling with the complexities and uncertainties brought about by the rapidly evolving regulatory landscape. This constant state of flux in regulations presents significant challenges for businesses in predicting future requirements and effectively measuring the returns on their current and future cybersecurity investments.

In such an uncertain environment, a wait-and-see approach often becomes an attractive option for businesses [13, 27, 56]. Hesitant to commit to substantial, irreversible investments that might soon become obsolete or misaligned with new regulations and convert into sunk costs, firms may opt to temporarily hold off on significant cybersecurity spending. This cautious stance allows them to more accurately gauge the direction of regulatory changes and adapt their cybersecurity strategies in a more informed manner. However, this approach is not without its risks, notably the potential vulnerability of their systems to emerging cyber threats during this period of observation and delayed action. Consequently, achieving a balance between the need for immediate, robust cybersecurity measures and the strategic foresight to adapt to future regulatory changes is a critical element of effective cybersecurity planning. Section 4 presents our model designed to delve into the interplay between regulatory risks and cybersecurity risks and investigate how various regulatory environments influence cybersecurity investment behavior.

3.2.4 Increased future regulatory scrutiny

Businesses that suffer data breaches are often subjected to heightened regulatory scrutiny in the aftermath. While this scrutiny is closely related, it should not be confused with routine compliance checks. The latter, typically carried out by regulatory enforcement agencies such as the Federal Trade Commission (FTC) or National Data Protection Authorities, focuses on ensuring that businesses adhere to set standards or regulations at a given point in time. On the other hand, regulatory scrutiny refers to the focused evaluation by regulators on the cybersecurity practices, standards, and behaviors, and assessing their impact on businesses and consumers[30]. It is worth noting that this intensified scrutiny is not just a repercussion of data breaches or using new technologies, but can also emerge as a direct consequence of shifts and evolutions in cybersecurity regulations.

When new cybersecurity regulations are introduced or when existing ones undergo significant changes, regulatory bodies might proactively scrutinize organizations to ensure their understanding and compliance with the new standards. Throughout this process, regulators are actively seeking information to understand and set parameters around the expanding number of ways that businesses can collect and use consumer data. Their focus also extends to confirming the robustness of safeguards designed

[30] https://commission.europa.eu/law/law-making-process/regulatory-scrutiny-board_en.

to maintain data privacy and security. As highlighted by a KPMG study[31], primary domains of regulatory scrutiny encompass data privacy and security, data collection and usage, transparency and consumer rights, and tackling model and algorithmic bias.

On October 16, 2023, the Division of Examinations (EXAMS) under the Securities and Exchange Commission (SEC) issued its 2024 Examination Priorities[32]. The 2024 Priorities reflect the Commission's continued scrutiny of information security and operational resiliency at registrants and the risks posed by third-party service providers, as well as new attention to emerging financial technology. In this issue, it is mentioned that:

> The Division will focus on registrants' policies and procedures, internal controls, oversight of third-party vendors (where applicable), governance practices, and responses to cyber-related incidents, including those related to ransomware attacks. Part of this review will consider whether registrants adequately train staff regarding their identity theft prevention program and their policies and procedures designed to protect customer records and information.

This signifies heightened regulatory scrutiny, emphasizing the importance of both proactive measures and responsive actions within the context of cybersecurity and data protection. Nevertheless, this uptick in oversight can also come with its own set of challenges and potential drawbacks for businesses. Such challenges may include increased operational costs, business delays, disproportionate resource allocations, and discouraging businesses from adopting novel technologies or business models for fear of potential noncompliance or regulatory backlash.

3.2.5 Reputational damage and loss of customer trust

Beyond the immediate legal and financial penalties, businesses face the profound risk of damaging their reputation and losing customer trust, especially when they fail to adapt to new regulations. This can lead to a serious long-term impact, with consumers likely to switch to competitors they perceive as more trustworthy in handling their data. The Forbes and PwC survey reveals this reality, showing that only 25% of consumers believe companies handle their personal information responsibly, leading 87% to consider moving to a competitor if they lose trust in a company's data handling abilities.[33]

Compounding this issue, the Cisco 2023 report emphasizes that since 2019, loyalty and trust have been at the forefront of consumer expectations from privacy investments. The fact that 92% of consumers expect companies to proactively protect data, according to the Forbes and PwC survey[34], instead of just reacting to

[31] https://kpmg.com/us/en/articles/2022/regulatory-scrutiny-technology-information.html.

[32] https://www.sec.gov/files/2024-exam-priorities.pdf.

[33] https://www.forbes.com/sites/forbestechcouncil/2017/12/08/mind-the-trust-gap-how-companies-can-retain-customers-after-a-security-breach/.

[34] https://www.forbes.com/sites/forbestechcouncil/2017/12/08/mind-the-trust-gap-how-companies-can-retain-customers-after-a-security-breach/.

government regulations, sets a high bar. Today, consumers are increasingly aware of privacy issues and expect stringent cybersecurity practices. Failure to adapt to new regulations can lead to public perception of negligence or disregard for customer data security. Regulatory risks further compound these challenges, making businesses more vulnerable to reputational harm and erosion of trust if they fail to navigate and adhere to the evolving cybersecurity regulations.

3.3 Preventive and mitigative controls

The third essential component of the bowtie methodology is the identification of barriers. As illustrated in Fig. 3, barriers are positioned on both sides of the top event, serving distinct yet complementary roles. On the left-hand side, the barriers are designed to either eliminate potential threats or prevent the escalation of such threats leading to the top event. These are proactive measures aimed at decreasing the likelihood of the occurrence of the top event in the first place. On the right-hand side of the top event, the barriers focus on recovery and mitigation. In case the top event does occur, these barriers are instrumental in lessening the severity of the consequences and aiding in the swift recovery from the incident. Sections 3.3.1 and 3.3.2 provide an exploration of the preventive and mitigative controls depicted in Fig. 3, respectively.

3.3.1 Preventive controls

Preventive controls are proactive measures aimed at preempting and mitigating potential regulatory risks before they arise. These controls are crucial for businesses striving to remain proactive, enabling them to adapt to changes in the regulatory landscape with informed foresight. Our study proposes seven such preventive controls, each designed to reduce the probability of the top event's occurrence. It is important to note that this list is not exhaustive, and the efficacy of each control may be subject to future debate. Moreover, while we have aligned each preventive control with one or more specific determinants as illustrated in Fig. 3, this alignment does not preclude their applicability to other determinants.

P1: Regulatory horizon scanning is a strategic process where businesses continuously monitor and analyze the current and upcoming regulatory landscape to identify potential changes that could impact their operations [110]. By doing so, organizations can adapt to regulatory changes proactively rather than reactively, which can serve as a preventive barrier against potential disruptions. Horizon scanning not only enhances time-to-compliance, facilitates the avoidance of penalties, and contributes to the reduction in compliance costs, but it also offers a strategic market advantage. Firms that are agile in adapting to new regulations can leverage this responsiveness as a competitive edge [132]. For example, companies that were early adopters of GDPR compliance were able to market their services in the EU more effectively [48, 82].

P2: Feedback loops with regulators and collaborative policy development are essential mechanisms for businesses to not only understand and adapt to regulatory changes but also to influence the creation and modification of regulations. By ac-

tively engaging with regulators and industry groups across multiple jurisdictions, businesses can advocate for the harmonization and modernization of regulations. Such engagement can lead to a reduction in the complexity of compliance and enable a more dynamic and cooperative approach to cybersecurity regulation. This is supported by literature such as [74] and [135], which highlight the benefits of collaborative regulatory development. Furthermore, [30] emphasizes the need for regulations that are adaptable and responsive to the fast-evolving nature of cyber threats and technologies. Engagement in policy development not only helps businesses stay ahead of regulatory changes but also allows them to contribute their expertise and practical insights, leading to more effective and implementable regulations. This collaborative approach can result in regulations that balance the need for security with the realities of business operations and technological innovation. Consequently, such a proactive stance can help mitigate the regulatory risks that businesses face and enhance their ability to respond effectively to the evolving cybersecurity landscape.

However, as noted by [4], regulatory actions are often subject to a myriad of political and lobbying influences, pulling in different directions. To counteract potential biases and ensure transparency, procedural instruments can be implemented to restrict attempts to influence decision-making through back-door lobbying. In the United States, for example, transparency is enforced by requiring that all communications between third parties and regulators concerning proposals are placed on official record [106]. Similarly, in the European Union, Article 11 of the Treaty on European Union provides a legal framework for interest representation, and there are stringent guidelines and mechanisms to ensure that the regulatory process is transparent and inclusive of various stakeholders' viewpoints [40].

P3: Public relations and communication strategies that anticipate and address public concerns about cybersecurity can preempt threats to business disruption by maintaining an informed and trusting customer base, positioning the company as a reliable entity amidst regulatory changes, and ensuring that the public demand for security is met with adequate and well-communicated measures. Well-designed public relations and communication strategies not only address the consequences of cybersecurity incidents [71] but also establish proactive preventive barriers against the adverse effects of regulatory uncertainties by fostering stakeholder trust, positively influencing market perception, enhancing customer retention, and minimizing the risk of noncompliance penalties.

P4: Adaptive governance and dynamic investment strategies enable businesses to proactively address the uncertainty of regulations that arise from the rapid pace of technological evolution, escalating cyber threats, and shifts in policy and global trends [7, 17]. This preventive control fosters an environment of resilience and agility, allowing businesses to stay ahead of regulatory changes that are often influenced by socio-technical factors [30]. Adaptive governance provides a framework for continuous policy review and adjustment, ensuring compliance with current and anticipated regulatory requirements. Meanwhile, dynamic investment strategies allocate resources effectively to areas most impacted by these changes, such as cybersecurity enhancements, technology updates, and compliance training programs. This comprehensive approach not only mitigates the risks associated with regulatory

uncertainties but also positions organizations to capitalize on new opportunities and navigate the complexities of a rapidly changing global landscape.

In addition to dynamic investment strategies, diversifying investments can be particularly effective as a preventive control. Regulatory risks belong to the category of unsystematic risks, meaning that these are specific risks unique to a sector, region, or firm [22]. By diversifying cybersecurity investments, businesses can spread their risk exposure across different areas that may be impacted differently by regulatory changes. This approach reduces the potential negative impact of regulatory changes on any single aspect of businesses' cybersecurity strategy. It allows for more flexible adaptation to regulatory environments that are often variable and unpredictable, enhancing the overall resilience of their cybersecurity infrastructure.

Utilizing an optimal mix of inputs to cybersecurity in the analytical framework developed by [55] suggests that a diversified approach to cybersecurity investments can be beneficial in adapting to various regulatory scenarios. This diversification can be implemented at different levels within an organization's cybersecurity strategy: (1) *technological solutions*, investing in a range of cybersecurity technologies, such as firewalls, intrusion detection systems, and encryption tools, ensures comprehensive protection against various types of cyber threats, (2) *geographical considerations*, diversifying cybersecurity practices to comply with regional regulatory frameworks can mitigate the risk of noncompliance in different jurisdictions, and (3) *operational areas*, diversification across different operational areas, including network security, data management, and staff training, ensures a holistic defense mechanism against cyber threats and regulatory changes. Diversification allows businesses to create and sustain value, not just protect it, helping them to adapt to evolving threats while enhancing cost management and revenue growth [104].

P5: Scenario planning involves envisioning various future regulatory landscapes and anticipating potential changes and their impacts on cybersecurity practices. This systematic approach requires businesses to construct detailed scenarios based on plausible regulatory changes, including stricter data protection laws, shifts in policies and trends, and compliance requirements for new technologies and innovations [8]. Through this method, businesses can evaluate their risk exposure levels under diverse regulatory scenarios, identifying potential weaknesses and areas for improvement in their cybersecurity frameworks [109].

Moreover, scenario planning facilitates the development of contingency plans, equipping businesses to respond effectively to regulatory changes [107]. It also encourages cross-functional collaboration, integrating insights from legal, IT, compliance, and risk management teams to ensure a holistic view of potential regulatory impacts. Consequently, businesses can strengthen their defenses against cybersecurity threats in alignment with changing regulations and gain strategic insights that drive informed decision-making and long-term resilience in a dynamic regulatory environment.

P6: Cross-jurisdictional regulatory mapping and engagement with local regulatory bodies function as preventive barriers, particularly in contexts where businesses operate across multiple regions or countries. In these scenarios, organizations must comply with a diverse range of legal and regulatory frameworks and manage the complexities that arise from being influenced by varying global and regional

trends, cultural norms, and enforcement practices [36]. This comprehensive mapping enables businesses to identify and understand each jurisdiction's regulatory environment. Hence, they can develop tailored strategies to ensure compliance in every region they operate. This approach is particularly effective in preempting legal issues and avoiding the penalties associated with noncompliance [44].

Additionally, cross-jurisdictional regulatory mapping is instrumental in strategic planning and decision-making [89]. It allows businesses to assess the regulatory implications of entering new markets, launching new products, or altering their operations. This level of insight is invaluable for mitigating risks and capitalizing on opportunities in a globally interconnected business landscape. Furthermore, this mapping aids in harmonizing organizational policies and practices across different jurisdictions. By identifying commonalities and differences in regulatory requirements, businesses can create streamlined, yet adaptable compliance frameworks. This not only optimizes resources but also ensures a consistent and coherent approach to compliance and corporate governance.

P7: Market incentive realignment refers to the strategic adjustment of market incentives to mitigate the regulatory uncertainties that can disrupt business operations and established cybersecurity practices. As we discussed before, market incentives might initially drive businesses towards cost cutting or rapid innovation, potentially at the expense of compliance or security. This can lead to vulnerabilities and misalignments with evolving regulatory standards, thereby motivating regulators to introduce new regulations or modify existing ones. To address this, market incentive realignment involves reshaping these incentives to prioritize regulatory compliance and robust cybersecurity practices. This realignment process aims to recalibrate these incentives, aligning them with long-term regulatory compliance and robust cybersecurity measures. It involves encouraging businesses to adopt a forward-thinking approach, where compliance and security are integral to their operational strategy, rather than seen as hindrances to innovation or cost efficiency.

3.3.2 Mitigative control

The second category of controls, on the right-hand side of Fig. 3, includes six mitigative controls that act as reactive mechanisms to counteract and manage the ramifications of sudden regulatory changes or oversights. They serve as contingency plans to address and rectify issues arising from sudden regulatory changes or compliance oversights. Together, these barriers form a comprehensive shield, fortifying businesses against the uncertainties and challenges of the ever-evolving cybersecurity regulatory domain.

M1: Accountability structures refer to the frameworks and systems put in place within an organization to ensure that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing risks [102]. Accountability structures establish a framework within which businesses can rapidly and effectively adapt to regulatory changes, minimizing disruptions and maintaining robust cybersecurity practices [47]. Well-implemented accountability structures can significantly reduce the risks and costs associated with noncompliance and operational disruptions in the face of regulatory changes. It can also create incentives

for businesses to adhere to existing regulations. For example, when data quality standards are not met, action needs to be taken to ensure that the root cause for the data quality issues is remediated and that sustainable data stewardship programs are in place at the data owner level. This can be accomplished by utilizing effective accountability policies [33].

M2: Legal expertise and counsel in the context of regulatory risks is essential, particularly when considering the potential for regulatory chill. This term refers to the apprehension and restraint experienced by businesses due to the uncertainty or ambiguity of regulatory expectations and enforcement [133]. Governments and regions like the EU wield substantial power to implement various measures aimed at protecting their digital sovereignty and the rights of their citizens within their territorial boundaries. In such a dynamic and often intricate legal landscape, effective legal advice is indispensable for businesses [29]. It aids them in navigating these multifaceted regulatory environments, ensuring adherence to laws and regulations while minimizing the risk of unintentionally provoking regulatory actions. This kind of expertise is vital to maintain operational integrity and promote a forward-looking stance in anticipation of, and adaptation to, evolving regulatory demands and shifts. This proactive approach is not only about compliance but also involves understanding the broader implications of regulations on business strategy and long-term planning.

M3: Contingency funding and planning are critical strategies to ensure business continuity and minimize disruptions to established cybersecurity practices due to regulatory changes. Just as cybersecurity risks necessitate these measures, the same applies to the context of regulatory risks in cybersecurity [130]. Contingency funding ensures that an organization has allocated resources to address unexpected regulatory changes. For example, implementing GDPR was a significant undertaking for organizations, with the implementation time and costs being considerable. According to McKinsey[35], the cost could exceed €10 million depending on the company's starting position, and 45% of major European companies would need to make substantial investments in basic tools to comply with GDPR requirements. Strategically established contingency funds and plans act as critical financial and operational safety nets, safeguarding business continuity and resilience against rapid adaptation and unexpected costs, particularly those that are difficult to anticipate.

M4: Financial strategy adaptation enables businesses to respond to the dynamic regulatory environment, ensuring that their investment strategies remain robust and aligned with both current and future compliance requirements. Such adaptation can include various approaches such as portfolio rebalancing, strategic divestment, and resource reallocation. Portfolio rebalancing stands as a cornerstone of this approach. It involves careful analysis and adjustment of investment portfolios to mitigate risks and capitalize on opportunities arising from new regulations. This process is critical for maintaining an optimal balance between risk and return in the face of regulatory shifts. By regularly reviewing and adjusting their asset allocation, organizations can

[35] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency.

reduce exposure to areas negatively impacted by regulatory changes while increasing investments in more favorable or compliant areas.

Strategic divestment complements rebalancing by enabling organizations to exit investments that become untenable or less profitable due to regulatory shifts. This proactive step involves identifying and selling off assets or business segments that are likely to underperform or pose compliance risks under the new regulatory framework. For example, an organization chooses to divest from third-party vendors or partners that fail to comply with new privacy regulations like GDPR or CCPA. This measure not only minimizes the risk of noncompliance but also redirects capital towards partnerships with entities that demonstrate robust compliance and data security practices, thereby strengthening the organization's overall cybersecurity posture.

Finally, resource reallocation is about strategically directing investments toward emerging areas of growth that align with the new regulatory landscape. This can involve investing in new technologies, markets, or sectors that are expected to benefit from the regulatory changes. This could also extend to reallocating human resources, like hiring more cybersecurity professionals specialized in regulatory compliance or investing in employee training programs focused on understanding and implementing new cybersecurity regulations.

M5: Regulatory gap analysis equips businesses with the tools to pinpoint discrepancies between their current operational practices and the established or expected regulatory frameworks [31]. This proactive approach not only facilitates timely compliance adjustments but also circumvents potential pitfalls associated with regulatory noncompliance. By consistently conducting regulatory gap analysis, businesses can stay ahead of evolving regulations, effectively mitigating the risk of unforeseen regulatory challenges and the consequent negative repercussions such as heightened scrutiny, legal sanctions, or financial penalties.

Furthermore, regular implementation of regulatory gap analysis positions a business as a compliance-forward entity, enhancing its reputation among stakeholders, customers, and regulatory bodies. It also fosters a culture of continuous improvement and readiness within the organization [60], ensuring that regulatory compliance is not just a one-time endeavor but an ongoing commitment. This ongoing process aids in strategically aligning business operations with regulatory expectations, thereby reducing the likelihood of operational disruptions and fostering a stable, predictable environment for business growth and innovation.

M6: Transparency and disclosure protocols serve not only to comply with regulatory requirements but also to enhance investor confidence, guide corporate governance, and address reputational risks. Drawing from the economics perspective outlined by [95], transparency and disclosure play crucial roles in mitigating information asymmetry and adjusting misaligned incentives between businesses and their stakeholders, including investors, customers, and regulatory bodies. [95] argues that transparency gives credibility to the claim that improving cybersecurity is taken seriously at the entity (e.g., government) level.

Moreover, these protocols enable businesses to preemptively address potential regulatory changes by anticipating regulatory trends, building a compliance-ready culture, engaging proactively with regulators and stakeholders, facilitating thorough risk assessment and management, and ensuring detailed documentation and evidence

of compliance [77, 90]. By maintaining openness in their cybersecurity practices, businesses can adapt more swiftly and effectively to new regulations, thereby reducing the risk of penalties and maintaining stakeholder trust. As such protocols align with existing regulations like GDPR and SEC Rules and Disclosure Requirements[36], this strategic approach to transparency and disclosure is not merely a compliance measure but a critical element in managing cybersecurity risks and ensuring business resilience in a dynamic regulatory environment.

4 Cybersecurity investment under regulatory risks

Addressing our first research question, we identified the determinants and implications of regulatory risks in cybersecurity. Now, turning to our second question, we focus on how these risks influence cybersecurity investment behavior. This section presents a dynamic model that analyzes a firm's investment strategies, encompassing both regulatory and cybersecurity risks. While existing cybersecurity investment models primarily assess the likelihood of a breach and its related cybersecurity risks [43, 52], our study offers a new perspective by incorporating regulatory risks into these decisions. Studies like [55] and [54] have explored the impact of government regulations and incentives on cybersecurity investment, particularly addressing externalities and underinvestment. However, these studies primarily focus on the economic externalities of cybersecurity breaches, not directly on the regulatory landscape. Our model represents an advancement in directly integrating regulatory risks into the decision-making process for cybersecurity investments, addressing a critical gap in current research.

This model integrates stochastic processes to simulate regulatory changes and assesses the impact of these changes on the firm's perceived uncertainty. This perception is critical, as it directly impacts strategic decision-making related to investments [35, 65]. We consider both the likelihood of data breaches occurring and the severity of penalties associated with noncompliance, integrating these factors into the following multi-objective maximization problem:

$$\max_{I_t} \mathbb{E}\left[\int_0^T e^{-\delta t}\pi(I_t, R_t)dt\right], \tag{1}$$

where $t \in [0, T]$ represents the time horizon. Furthermore, we introduce δ as the discount factor, which plays a pivotal role in our analysis. The discount factor δ is used to translate future costs and benefits into present value terms, reflecting the time value of money and the preference for immediate benefits over future ones. In the context of cybersecurity investment, this means that costs and benefits occurring at a future time t are "discounted" back to the present value. Typically, δ is a value between 0 and 1, where a lower δ indicates a higher present value placed on future costs and benefits.

[36] https://www.sec.gov/news/press-release/2023-139.

The maximization problem in Eq. (1) seeks to balance several competing priorities: minimizing the risk of data breaches, optimizing compliance with dynamic regulations, and ensuring cost-effective allocation of resources towards cybersecurity measures. To achieve this, the model quantifies the trade-offs between increased investment in cybersecurity and the corresponding reduction in both regulatory risks and the potential damage from data breaches. To address this, we have formulated the payoff function of the problem as follows:

$$\pi(I_t, R_t) = S(I_t) - C(I_t, R_t) - \theta_t \eta - (P_b(t) \times L). \tag{2}$$

In this function:

- I_t denotes the level of investment in cybersecurity at time t.
- R_t is the level of regulatory requirements at time t.
- $P_b(t)$ denotes the firm's cybersecurity breach function at time t.
- θ_t represents the firm's perception of regulatory uncertainty at time t.
- η characterizes the penalties for misalignment between the firm's cybersecurity investment and the regulatory requirements.
- L represents the loss from a cybersecurity breach.

We incorporated $S(I_t)$ and $C(I_t, R_t)$ to capture the complex dynamics and trade-offs in cybersecurity investment decisions. $S(I_t)$ represents the positive outcomes of investment, both in terms of risk reduction and business benefits, while $C(I_t, R_t)$ represents the cost implications, taking into account both the investment and compliance aspects. $S(I_t)$ increases with I_t but at a decreasing rate, reflecting diminishing returns on investment ($S^{'} > 0$ and $S^{''} < 0$) [55]. A common form for this function is logarithmic [62]. For simplification, we implemented this function as $S(I_t) = \lambda.log(1 + I_t)$, where λ is a parameter that adjusts the scale of returns.

$C(I_t, R_t)$ encompasses all the direct expenditures associated with implementing and maintaining cybersecurity measures. This component also reflects costs related to compliance with cybersecurity regulations, such as costs incurred to align systems and processes with regulatory requirements. Given its dual focus, $C(I_t, R_t)$ is a function of both the level of investment in cybersecurity I_t and the prevailing regulatory requirements R_t. The interdependencies and externalities inherent in cybersecurity investments significantly influence this function [43, 52]. Moreover, the relationship between investment and costs is not always linear. Increased investment in cybersecurity can lead to economies of scale, where the cost per unit of security decreases as the scale of investment grows.

On the other hand, overly stringent regulatory requirements might lead to diminishing returns, where each additional unit of investment results in a disproportionately small reduction in compliance costs. However, in our implementation of the model, we have simplified the function $C(I_t, R_t)$ and chose to exclude interdependencies and non-linearity for ease of computation and to focus on the primary dynamics of cybersecurity investment and regulatory compliance. Therefore, we implemented this function as $C(I_t, R_t) = I_t + |R_t - I_t|$.

To accurately represent the dynamic nature of regulatory changes in the cybersecurity domain, our model incorporates the term

$$d R_t = \alpha(R^* - R_t)dt + \sigma d W_t, \tag{3}$$

where R^* represents the target level of regulations, which might be influenced by determinants identified in Sect. 3.1, the coefficient α represents the rate at which actual regulatory requirements adjust towards the target level R^*[37], the parameter σ captures the volatility or uncertainty in the regulatory changes, and $d W_t$ is a Wiener process[38].

A higher value of α indicates a faster adaptation of regulatory standards, reflecting a more responsive or agile regulatory environment. This could be indicative of sectors where rapid changes in technology or threat landscapes necessitate quicker regulatory responses. σ, however, represents the extent to which regulatory changes can deviate unexpectedly from the anticipated path due to unforeseen events, such as sudden technological breakthroughs, political shifts, or high-impact cyber incidents.

As regulations evolve, the firm updates its perception of regulatory risk $\theta_t = f(\Delta R, \sigma, |R_t - I_t|)$ where f is a function influenced by the rate and unpredictability of regulatory changes as well as the firm's alignment with these regulations. ΔR represents the average rate at which regulatory requirements are changing. A higher ΔR indicates a more rapidly evolving regulatory landscape, which could increase uncertainty. Another component of this function is the gap in current investment and regulatory requirements $|R_t - I_t|$. If a firm's investment closely aligns with the current regulatory requirements (I_t is close to R_t), this could reduce uncertainty from a compliance perspective [97, 128]. The firm is confident that it meets the regulatory standards, reducing the risk of noncompliance and any associated penalties or reputational damage. Conversely, a larger gap ($|R_t - I_t|$ is significant) could indicate that the firm is either underinvesting or overinvesting relative to regulatory standards [27]. While underinvesting increases the risk of noncompliance, overinvesting might lead to unnecessary expenditure and inefficiency. In both cases, the firm faces uncertainty, either about potential regulatory actions or about the cost-effectiveness of its investments.

The probability of breach $P_b(t)$ in Eq. (2) is influenced by the firm's investment in cybersecurity and the regulatory environment. $P_b(t) = g(I_t, R_t)$ decreases

[37] It should be noted that in real-world scenarios, the target level of regulations is not a known or fixed quantity. As we discussed in Sect. 3.1, this level is influenced by a complex interplay of factors including technological advancements, political decisions, social considerations, and evolving threat landscapes. In our implementation, we treated R^* as a stochastic variable. This could be improved by modeling this variable as a function of recent changes and events, or incorporated with feedback mechanisms.

[38] The Wiener process is a commonly used stochastic process in mathematical modeling due to its simplicity and well-understood properties. In the context of modeling the impact of regulatory risks on investment in cybersecurity, the Wiener process was chosen because (1) it operates in continuous time, which is suitable for modeling the ongoing and evolving nature of regulatory environments and firms' investment decisions, (2) it introduces randomness into the model, capturing the unpredictable nature of regulatory changes, and (3) for its simplicity and analytical tractability.

with higher investment in cybersecurity and increases with a larger gap between regulatory requirements and actual investment [55, 56]. Hence, g is a function that:

- $\frac{\partial g}{\partial I_t} < 0$: higher investment in cybersecurity reduces the probability of a breach.
- $\frac{\partial g}{\partial |R_t - I_t|} > 0$: a larger gap between regulatory requirements and actual investment increases the probability of a breach.

After a detailed explanation of the model, Fig. 7 illustrates the outcomes of implementing this model, particularly highlighting the effects of the rate of regulatory adaptation (Fig. 7a–c) and uncertainty in the regulatory changes (Fig. 7d–f) on cybersecurity investment level. The figure demonstrates the dynamic interplay between regulatory requirements and investment decisions over time. Initially, the firm's investment closely aligns with the regulatory requirements, indicating compliance and risk minimization efforts. However, as time progresses, there is a noticeable shift in behavior, with the gap between the investment level and regulatory requirements widening, and a subsequent decrease in the investment level.

Furthermore, as volatility or uncertainty in the regulatory increases (Fig. 7d–f), the firm exhibits volatile investment patterns more quickly compared to scenarios where the rate is lower (Fig. 7a–c). This trend indicates a direct impact of regulatory risks on investment behavior, potentially leading to underinvestment. This divergence from regulatory alignment can be attributed to a "wait-and-see" approach adopted by the firm. Firms may adopt a strategic delay in investment under high uncertainty [23, 53, 92]. Hence, as the regulatory environment becomes more dynamic and potentially unpredictable, firms adopt a more cautious investment stance. This is especially plausible if the firm anticipates future regulatory changes that could render current investments less relevant or even obsolete and thus influence its uncertainty perception.

We extended our analysis by modifying the variable η, indicative of misaligned penalties. Figure 7g–i reveals a trend: as the value of η increases, the firm tends to align its investment level more closely with regulatory requirements. This indicates a direct relationship between penalties and investment behavior. This pattern corroborates with studies like those by [34] and [70], which affirm the effectiveness of penalties as a deterrent. However, juxtaposing this trend with Fig. 7b reinforces both theoretical and empirical evidence [18, 76] suggesting that firms often exhibit a reactive approach in cybersecurity investment. This approach often results in investments aimed at meeting minimum required standards, rather than striving for the implementation of optimal, comprehensive security practices.

Finally, to delve deeper into the effects of perceived regulatory uncertainty, Fig. 8 provides a visual representation of the changes in the firm's perception of regulatory uncertainty over time. The peaks in the graph indicate moments of heightened uncertainty. As observed, these correspond to times when there are significant changes in regulatory requirements, increased volatility in the regulatory environment, or when the firm's investment substantially deviates from the regulatory requirements. The lower levels of uncertainty occur during periods when the firm aligns its investment with the regulatory requirements or when the regulatory environment is relatively stable. These periods signify successful adaptation and effective compliance efforts by the firm. The figure additionally shows that despite increases in regulatory re-

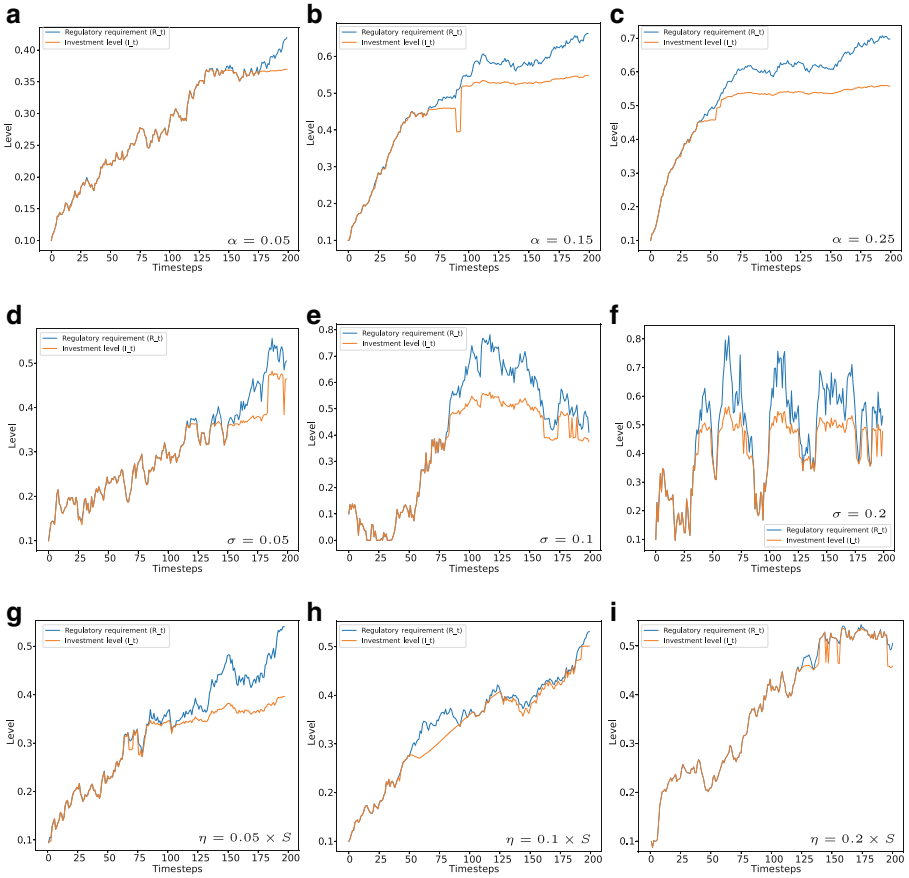


Fig. 7 Impact of regulatory adaptation rate (α), uncertainty (σ), and misalignment penalties (η) on cybersecurity investment. **a–c** focus on how varying adaptation rates influence investment alignment with regulatory requirements. **d–f** depict the firm's investment behavior under increasing levels of regulatory uncertainty, highlighting the transition from compliance-oriented to caution-dominated investment strategies. **g–i** demonstrate how changes in the magnitude of misaligned penalties (η) influence the firm's cybersecurity investment decisions. The value of α in these runs is 0.15

quirements, the investment level remains relatively constant (after $t > 400$). This observation aligns with our discussions in Sect. 3.2.3, where we explored the impact of regulatory uncertainty on investment behaviors.

5 Discussion and conclusion

This paper aimed to deepen our understanding of the regulatory risks associated with cybersecurity and to examine how perceived regulatory uncertainty and the risk of future regulatory changes affect the cybersecurity investment behavior of organizations. To this end, we identified a range of determinants and implications

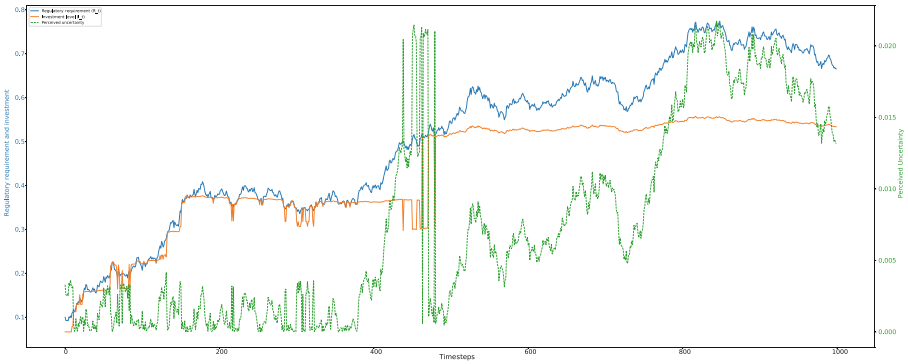


Fig. 8 The changes in the firm's perception of regulatory uncertainty over time. Peaks in the graph correspond to heightened uncertainty, often coinciding with significant regulatory shifts or deviations from regulatory compliance in investment. Troughs indicate periods of lower uncertainty, typically associated with stable regulatory environments or periods of high compliance. This figure aids in understanding the correlation between regulatory changes and the firm's adaptive investment strategies in the cybersecurity domain

associated with cybersecurity-related regulatory risks. While acknowledging that these sets are not exhaustive, they highlight the diverse factors that contribute to the regulatory risks faced by organizations and the potential consequences that could disrupt their business operations and established cybersecurity practices.

In exploring the determinants of regulatory risks, our research employed sentiment analysis to measure the levels of regulatory uncertainty in the cybersecurity domain. This analysis is important in quantifying the general sentiment and uncertainty surrounding current and potential future regulations. The findings from this analysis revealed a significant degree of uncertainty towards cybersecurity regulations. This uncertainty can be attributed to several factors, including the rapid pace of technological change, the emergence of new cybersecurity threats, and the evolving nature of global data protection and privacy laws. As a result, organizations often find themselves in a challenging position, trying to anticipate and prepare for potential regulatory shifts while maintaining compliance with current standards.

We expanded our study by identifying additional determinants that contribute to the complexity of regulatory risks in cybersecurity. Collectively, these determinants create a continuously evolving regulatory risk landscape in cybersecurity. Understanding and managing these risks necessitates not only a reactive compliance approach but also a proactive strategy that anticipates future changes and adapts accordingly. Organizations that fail to adequately address and adapt to these regulatory risks in cybersecurity are at a heightened risk of facing not only legal and financial repercussions but also significant damage to their reputation and operational integrity. In an environment where cybersecurity threats are continuously evolving, and regulatory landscapes are in flux, a passive or noncompliant stance can lead to severe vulnerabilities. These vulnerabilities can manifest in various forms, from data breaches and loss of customer trust to disruptions in business operations and costly penalties for noncompliance. Moreover, organizations that lag in adapting to

new regulations may find themselves struggling to catch up with industry standards, thereby losing competitive advantage and market trust.

Regulatory risks, as we have found, can be mitigated but not eliminated. Mitigation does not come from eliminating or weakening regulations. Rather, it requires a collaborative effort from both regulators and organizations. In line with the suggested preventive and mitigative controls in this paper, it should not be seen as paradoxical that regulation itself can be a remedy to regulatory risk. A well-crafted and competent regulatory framework provides stability and certainty, offering mechanisms that not only minimize this risk but also preserve vital functions while remaining adaptable to evolving conditions.

These mechanisms can range from clear guidelines and transparent compliance requirements to robust monitoring and enforcement protocols. They may also include flexible provisions to accommodate technological advancements and changing cybersecurity threats. Furthermore, these frameworks can implement feedback loops, where businesses can contribute their insights and experiences, thereby ensuring that regulations remain relevant and effective. On the procedural front, these frameworks should incorporate stringent measures to prevent undue influence on decision-making processes, such as back-door lobbying regulations and strict conflict-of-interest policies. This is vital to maintain the integrity of the regulatory process and ensure that decisions are made in the best interest of public safety and cybersecurity, rather than being swayed by private interests.

In parallel, businesses are tasked with developing adaptive strategies and establishing robust compliance systems. These systems must be agile enough to respond effectively to regulatory changes, ensuring compliance without stifling innovation or operational efficiency. This dual approach–where regulators provide clear, stable, and adaptable frameworks, and businesses respond with agile and comprehensive compliance strategies–creates a dynamic yet secure environment. This environment is conducive to managing and mitigating regulatory risks effectively, ensuring that cybersecurity practices remain robust and responsive in a constantly evolving digital landscape.

After identifying the determinants and implications of regulatory risks associated with cybersecurity, our study progressed to examine how uncertainty about future cybersecurity regulatory environments influences investment decisions in organizations. To address this, we developed a quantitative model that analyzes investment patterns in relation to regulatory risks. The results from our model indicated that regulatory uncertainty has a direct and significant impact on cybersecurity investment behavior. Specifically, the model revealed a trend where organizations tend to reduce or defer their investments in cybersecurity infrastructure when faced with regulatory uncertainty. This cautious approach, often characterized as a "wait-and-see" strategy, is typically adopted due to concerns that future regulatory changes might render current investments obsolete or noncompliant.

However, while this approach is understandable from a risk management perspective, it carries its own set of risks. Primarily, it can leave organizations more exposed to emerging cybersecurity threats. In an environment where cyber threats are evolving rapidly, delaying critical cybersecurity investments or underinvestment can result in vulnerabilities that might be exploited by cybercriminals. This trade-off

highlights the complex decision-making landscape that organizations must navigate when balancing the need to stay agile and compliant with the imperative to protect against cybersecurity threats.

In summary, our research underscores three critical needs:

- For organizations: to develop adaptable and forward-thinking cybersecurity investment strategies. This entails a balanced approach where investments are not just prudent, but also flexible enough to adapt to regulatory changes. Investments in scalable, modular cybersecurity solutions and strategies like divestment and diversification are essential to meet future regulatory and cyber threat challenges.
- For regulators: to understand the broader impact of the regulatory environment, beyond just the regulations themselves, on organizational cybersecurity investment. Our research highlights the need for creating regulatory frameworks that balance predictability with adaptability, ensuring they keep pace with evolving technological and societal changes.
- For researchers: to prioritize and rigorously integrate regulatory risks into cybersecurity investment models. Recognizing the profound impact of regulatory changes and uncertainties on investment strategies, this approach will enable researchers to offer more comprehensive and realistic guidance for organizations navigating the complex cybersecurity landscape

6 Limitations and future work

Our study acknowledges certain limitations, primarily stemming from its reliance on existing literature, which may not entirely reflect the rapidly changing landscape of cybersecurity threats and regulatory shifts. Furthermore, the stochastic econometric model employed, while providing valuable insights, is based on certain interpretations and assumptions that may not fully encompass the complexity and diversity of regulatory trends, especially across various industries and regions. Future research could enrich this field by incorporating empirical studies that integrate expert opinions and direct business engagements. This approach would broaden the scope of determinants and implications examined, enable a more quantitative assessment of their impacts on regulatory risks, and explore additional preventive and control measures.

Longitudinal studies would enhance our understanding by allowing the tracking and analysis of the evolution of regulatory changes and cybersecurity investments over time. These studies would offer a dynamic, temporal view of the interplay between these factors, uncovering trends not visible in cross-sectional analyses. Future research also presents an opportunity to develop more sophisticated models that more accurately reflect the complex interplay of regulatory and cybersecurity risks, incorporating a wider array of technological, organizational, and socio-economic factors. Such comprehensive and empirically grounded research will be key to deepening our understanding and effectively managing the intricate relationship between regulation, cybersecurity risks, and investment strategies.

7 Appendix

7.1 Difference between cybersecurity risks and regulatory risks

As illustrated in Table 3, regulatory risks arise from changes in laws and regulations that can impact businesses, sectors, or markets, while cybersecurity risks are related to unauthorized access, theft, or damage to digital assets, systems, or networks, ensuring the confidentiality, integrity, and availability of data and systems. The table also underscores the key differences and potential areas of overlap between these risk categories, emphasizing the importance of understanding and comprehensively addressing both types of risks. Regulatory risks often involve compliance requirements related to data protection and privacy, which are directly connected to the management of cybersecurity risks. Conversely, failure to address cybersecurity risks adequately can lead to noncompliance with relevant regulations, resulting in

Table 3 The difference between cybersecurity risks and regulatory risks

	Cybersecurity Risks [information extracted from (39, 103, 126, 127])]	Regulatory Risks (information extracted from [12, 38, 128])
Definition	The potential loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations.	The potential for changes in laws, regulations, or government policies that could negatively impact a firm's operations, reputation, or financial position.
Focus	Protecting information systems, devices, networks, and user information from malicious actors seeking to exploit vulnerabilities.	Complying with legal and regulatory requirements related to data privacy, consumer protection, and safety.
Consequences	Data breaches, loss of sensitive information, damage to critical infrastructure, loss of customer trust, financial losses, reputational damage, and intellectual property theft.	Fines, legal liabilities, increased costs of compliance, potential loss of business opportunities, significant changes in business model or operations, loss of customer trust, and damage to reputation.
Threat sources	Malicious actors, insider threats, and vulnerable devices or networks.	A complex, uncertain, and evolving regulatory landscape, compliance gaps, legal uncertainties, and failure to maintain industry standards.
Mitigation	Cybersecurity risk mitigation relies on the implementation of technical and organizational measures, such as firewalls, encryption, multifactor authentication, and incident response plans, as well as employee training and awareness programs.	Regulatory risk mitigation involves the establishment and monitoring of compliance programs, policies, and procedures that align with applicable laws, regulations, and industry standards. This may also include regular audits and reporting to regulatory authorities.
Challenges	Complexity and heterogeneity of digital ecosystems, constantly evolving nature of cyber threats, limited visibility and control over devices and networks, and lack of security standards and best practices.	Ambiguity and diversity of regulatory requirements, adapting operations to comply with new regulations, compliance costs and burdens, requiring organizations to invest significant resources in compliance testing, audits, and certification, and legal risks and uncertainties.

fines, reputational damage, and other consequences. By acknowledging the interplay between regulatory and cybersecurity risks, businesses can develop integrated risk management strategies that encompass the full spectrum of challenges they face, ultimately fostering a more resilient and secure operational environment in today's complex digital landscape.

Acknowledgements This research was funded by the European Union's H2020 ARCADIAN-IoT (Grant agreement No. 101020259), H2020 CONCORDIA (Grant agreement No. 830927), and H2020 VEDLIoT (Grant agreement No. 957197).

Funding Open access funding provided by RISE Research Institutes of Sweden.

Conflict of interest The authors declare no conflict of interest.

References

1. Aaronson SA (2019) Data is different, and that's why the world needs a new approach to governing cross-border data flows. Digit Policy Regul Gov 21(5):441–460
2. Agrafiotis I, Nurse JR, Goldsmith M, Creese S, Upton D (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecur 4(1):tyy6
3. Almeida Teixeira G, Silva da Mira M, Pereira R (2019) The critical success factors of GDPR implementation: a systematic literature review. Digit Policy Regul Gov 21(4):402–418
4. Anderson R, Böhme R, Clayton R, Moore T (2008) Security economics and the internal market. Study commissioned by ENISA
5. Andersson R, Böhme R, Clayton R, Moore T (2008) Security economics and the internal market. European Network and Information Security Agency (https://www.enisa.europa.eu/publications/archive/economics-sec.)
6. Aragón-Correa JA, Sharma S (2003) A contingent resource-based view of proactive corporate environmental strategy. Acad Manag Rev 28(1):71–88
7. Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer MF (2021) A dynamic simulation approach to support the evaluation of cyber risks and security investments in smes. Decis Support Syst 147:113580
8. Bechara FR, Schuch SB (2021) Cybersecurity and global regulatory challenges. J Financ Crime 28(2):359–374
9. Bentzen E, Freij Å, Varnes CJ (2021) The role of flexibility and complexity in response to regulatory change: a case study of innovation in a major Danish financial institution. Int J Entrep Innov 22(4):229–239
10. Berkowitz J, Mangold M, Sharon S (2016) Data flow maps-increasing data processing transparency and privacy compliance in the enterprise. Wash Lee Law Rev 73:802
11. Bernsmed K, Frøystad C, Meland PH, Nesheim DA, Rødseth ØJ (2018) Visualizing cyber security risks with bow-tie diagrams. In: Graphical Models for Security: 4th International Workshop, GraMSec 2017, Santa Barbara, CA, USA, August 21, 2017. Springer, pp 38–56 (revised selected papers 4)
12. Bezzina J, Terrab M (2005) Impacts of new technologies on regulatory regimes. Technological convergence and regulation, p 15
13. Bloom N, Bond S, Van Reenen J (2007) Uncertainty and investment dynamics. Rev Econ Stud 74(2):391–415

14. Bloom N, Floetotto M, Jaimovich N, Saporta-Eksten I, Terry SJ (2018) Really uncertain business cycles. Econometrica 86(3):1031–1065
15. Blythe JM, Sombatruang N, Johnson SD (2019) What security features and crime prevention advice is communicated in consumer iot device manuals and support pages? J Cybersecur 5(1):tyz5
16. Bond G, Carter L (1995) Financing energy projects: experience of the international finance corporation. Energy Policy 23(11):967–975
17. Brass I, Sowell JH (2021) Adaptive governance for the internet of things: coping with emerging security risks. Regul Gov 15(4):1092–1110
18. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 34(3):523–548. https://doi.org/10.2307/25750690
19. Calliess C, Baumgarten A (2020) Cybersecurity in the eu the example of the financial sector: a legal perspective. Ger Law J 21(6):1149–1179
20. Carrapico H, Barrinha A (2017) The EU as a coherent (cyber) security actor? J Common Mark Stud 55(6):1254–1272
21. Chaisse J, Bauer C (2018) Cybersecurity and the protection of digital assets: assessing the role of international investment law and arbitration. Vanderbilt J Entertain Technol Law 21:549
22. Chen J (2023) What is unsystematic risk? types and measurements explained. https://www.investopedia.com/terms/u/unsystematicrisk.asp. Accessed 21 Oct 2023
23. Chevalier-Roignant B, Flath CM, Huchzermeier A, Trigeorgis L (2011) Strategic investment under uncertainty: a synthesis. Eur J Oper Res 215(3):639–650
24. Chiara PG (2022) The IoT and the new EU cybersecurity regulatory landscape. Int Rev Law Comput Technol 36(2):118–137
25. Chollete L, Harrison SG (2021) Unintended consequences: ambiguity neglect and policy ineffectiveness. Eastern Econ J 47:206–226
26. Christou G (2019) The collective securitisation of cyberspace in the European Union. West Eur Polit 42(2):278–301
27. Chronopoulos M, Panaousis E, Grossklags J (2017) An options approach to cybersecurity investment. IEEE Access 6:12175–12186
28. Citron DK (2009) Law's expressive value in combating cyber gender harassment. Mich Law Rev 108:373
29. Ciuriak D (2018) The economics of data: implications for the data-driven economy. Data governance in the digital age
30. Clark-Ginsberg A, Slayton R (2019) Regulating risks within complex sociotechnical systems: evidence from critical infrastructure cybersecurity standards. Sci Public Policy 46(3):339–346
31. Daud M, Rasiah R, George M, Asirvatham D, Thangiah G (2018) Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations? Int J Bus Soc 19(1):161–180
32. De Smet D (2012) Exploring the influence of regulation on the innovation process. Int J Entrep Innov Manag 16(1-2):73–97
33. Deloitte (2018) A better governance structure and effective operating models for regulatory reporting | deloitte us. https://www2.deloitte.com/us/en/pages/regulatory/articles/2018-governance-structure-and-effective-operating-models-for-regulatory-reporting.html. Accessed 11 Jan 2023
34. Didenko AN (2020) Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Rev 25(1):125–167
35. Dixit AK, Pindyck RS (1994) Investment under uncertainty. Princeton University Press
36. Dodds S, Reynolds B, Donegan T, Mundheim R (2020) Regulatory challenges for financial institutions operating across multiple jurisdictions. https://www.shearman.com/perspectives/2020/05/regulatory-challenges-for-financial-institutions-operating-across-multiple-jurisdictions. Accessed 13 Nov 2023
37. Dunn Cavelty M, Smeets M (2023) Regulatory cybersecurity governance in the making: the formation of enisa and its struggle for epistemic authority. J Eur Public Policy 30(7):1330–1352
38. E. I. U. (2005) EIU. Regulatory risk: trends and strategies for the CRO. http://graphics.eiu.com/files/ad_pdfs/eiu_CRO_RISK_WP.pdf. Accessed 21 Oct 2023
39. Eling M, McShane M, Nguyen T (2021) Cyber risk management: history and future research directions. Risk Manage Insur Rev 24(1):93–125
40. EU (2012) Consolidated version of the treaty on European Union. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF. Accessed 23 Nov 2023

41. EY (2010) The Ernst & Young business risk report 2010: the top 10 risks for business–A sector-wide view of the risks facing businesses across the globe. https://www.globalnegotiator.com/files/Risks-in-International-Business.pdf. Accessed 15 Nov 2023
42. Fabrizio KR (2013) The effect of regulatory uncertainty on investment: evidence from renewable energy generation. J Law Econ Organ 29(4):765–798
43. Fedele A, Roner C (2022) Dangerous games: a literature review on cybersecurity investments. J Econ Surv 36(1):157–187
44. Feridun M (2023) Cross-jurisdictional financial crime risks: what can we learn from the uk regulatory data? J Financ Crime. https://doi.org/10.1108/JFC-03-2023-0044
45. Firstbrook P, Pirzada Z (2021) Top security and risk management trends. Gartner
46. Freij Å (2022) Regulatory change impact on technology and associated mitigation capabilities. Technol Anal Strateg Manag 34(12):1418–1431
47. Gale M, Bongiovanni I, Slapnicar S (2022) Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Comput Secur 121:102840
48. Garber J (2018) Gdpr–compliance nightmare or business opportunity? Comput Fraud Secur 2018(6):14–15
49. Garcia A, Horowitz B (2007) The potential for underinvestment in internet security: implications for regulatory policy. J Regul Econ 31:37–55
50. Geradin D (2015) Should Uber be allowed to compete in Europe? and if so how? George Mason legal studies research paper, vol LS 15-11, pp 15–11
51. Gisladottir V, Ganin AA, Keisler JM, Kepner J, Linkov I (2017) Resilience of cyber systems with over-and underregulation. Risk Anal 37(9):1644–1651
52. Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Trans Inform Syst Secur (TISSEC) 5(4):438–457
53. Gordon LA, Loeb MP, Lucyshyn W (2003) Information security expenditures and real options: a wait-and-see approach. Comput Secur J 19(2). Available at SSRN: https://ssrn.com/abstract=1375460
54. Gordon LA, Loeb MP, Lucyshyn W, Zhou L et al (2014) Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. J Inform Secur 6(01):24
55. Gordon LA, Loeb MP, Lucyshyn W, Zhou L (2015) Increasing cybersecurity investments in private sector firms. J Cybersecur 1(1):3–17
56. Gordon LA, Loeb MP, Lucyshyn W, Zhou L (2018) Empirical evidence on the determinants of cybersecurity investments in private sector firms. J Inform Secur 9(2):133–153
57. Greenleaf G (2022) Now 157 countries: twelve data privacy laws in 2021/22
58. Griffy-Brown C, Miller H, Zhao V, Lazarikos D, Chun M (2020) Making better risk decisions in a new technological environment. IEEE Eng Manag Rev 48(1):77–84
59. Hadzovic S, Mrdovic S, Radonjic M (2023) A path towards an internet of things and artificial intelligence regulatory framework. IEEE Commun Mag 61(7):90–96. https://doi.org/10.1109/MCOM.002.2200373
60. Hasan S, Ali M, Kurnia S, Thurasamy R (2021) Evaluating the cyber security readiness of organizations and its influence on performance. J Inf Secur Appl 58:102726
61. Hassib B, Shires J (2022) Cybersecurity in the gcc: from economic development to geopolitical controversy. Middle East Policy 29(1):90–103
62. Hausken K (2006) Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Inf Syst Front 8:338–349
63. Hiller JS, Russell RS (2013) The challenge and imperative of private sector cybersecurity: an international comparison. Comput Law Secur Rev 29(3):236–245
64. Hinds J, Williams EJ, Joinson AN (2020) "it wouldn't happen to me": privacy concerns and perspectives following the Cambridge Analytica scandal. Int J Hum Comput Stud 143:102498
65. Hoffmann VH, Trautmann T, Hamprecht J (2009) Regulatory uncertainty: a reason to postpone investments? not necessarily. J Manag Stud 46(7):1227–1253
66. Hutto C, Gilbert E (2014) Vader: a parsimonious rule-based model for sentiment analysis of social media text. In: Proceedings of the international AAAI conference on web and social media, vol 8, pp 216–225
67. Hyla EJ (2018) Corporate cybersecurity: the international threat to private networks and how regulations can mitigate it. Vanderbilt J Entertain Technol Law 21:309
68. Kianpour M (2020) Knowledge and skills needed to craft successful cybersecurity strategies. In: Norsk IKT-konferanse for forskning og utdanning, vol 3

69. Kianpour M, Kowalski SJ, Øverby H (2021) Systematically understanding cybersecurity economics: a survey. Sustainability 13(24):13677
70. Kianpour M, Kowalski SJ, Øverby H (2022) Advancing the concept of cybersecurity as a public good. Simul Model Pract Theory 116:102493
71. Knight R, Nurse JR (2020) A framework for effective corporate communication after cyber security incidents. Comput Secur 99:102036
72. Kołacz MK, Quintavalla A, Yalnazov O (2019) Who should regulate disruptive technology? Eur J Risk Regul 10(1):4–22
73. Kosseff J (2017) Defining cybersecurity law. Iowa Law Rev 103:985
74. Kosseff J (2018) Developing collaborative and cohesive cybersecurity legal principles. In: 2018 10th International Conference on Cyber Conflict (CyCon). IEEE, pp 283–298
75. Kuhn ML (2018) 147 million social security numbers for sale: developing data protection legislation after mass cybersecurity breaches. Iowa Law Rev 104:417
76. Kwon J, Johnson ME (2014) Proactive versus reactive security investments in the healthcare sector. MIS Q 38(2):451–A3
77. Laube S, Böhme R (2016) The economics of mandatory security breach reporting to authorities. J Cybersecur 2(1):29–41
78. Lee I (2021) Cybersecurity: risk management framework and investment cost analysis. Bus Horiz 64(5):659–671
79. Lee I, Shin YJ (2018) Fintech: ecosystem, business models, investment decisions, and challenges. Bus Horiz 61(1):35–46
80. Lewallen J (2021) Emerging technologies and problem definition uncertainty: the case of cybersecurity. Regul Gov 15(4):1035–1052
81. Lindgren P (2016) Gdpr regulation impact on different business models and businesses. J Multi Bus Model Innov Technol 4(3):241–254
82. Lopes IM, Oliveira P (2018) Implementation of the general data protection regulation: a survey in health clinics. In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, pp 1–6
83. Losiewicz-Dniestrzanska E (2015) Monitoring of compliance risk in the bank. Procedia Econ Financ 26:800–805
84. Makulilo AB (2012) Privacy and data protection in Africa: a state of the art. Int Data Priv Law 2(3):163–178
85. Maple C (2017) Security and privacy in the internet of things. J Cyber Policy 2(2):155–184
86. Marotta A, Madnick S (2021) Convergence and divergence of regulatory compliance and cybersecurity. Issues Inform Syst 22(1):10–50. https://doi.org/10.48009/1_iis_2021_10-50
87. Martin G, Martin P, Hankin C, Darzi A, Kinross J (2017) Cybersecurity and healthcare: how safe are we? BMJ 358:j3179. https://doi.org/10.1136/bmj.j3179
88. Martin Y-S, Kung A (2018) Methods and tools for gdpr compliance through privacy and data protection engineering. In: 2018 IEEE European symposium on security and privacy workshops (EuroS&PW). IEEE, pp 108–111
89. Martyniszyn M (2021) Competitive harm crossing borders: regulatory gaps and a way forward. J Compet Law Econ 17(3):686–707
90. Masur JS, Nash JR (2022) Promoting regulatory prediction. Indian Law J 97:203
91. McAslan D, Gabriele M, Miller TR (2021) Planning and policy directions for autonomous vehicles in metropolitan planning organizations (mpos) in the United States. J Urban Technol 28(3-4):175–201
92. McDonald R, Siegel D (1986) The value of waiting to invest. Q J Econ 101(4):707–727
93. Michalec O, Milyaeva S, Rashid A (2022) Reconfiguring governance: how cyber security regulations are reconfiguring water governance. Regul Gov 16(4):1325–1342
94. Millett K, Dos Santos E, Millett PD (2019) Cyber-biosecurity risk perceptions in the biotech sector. Front Bioeng Biotechnol 7:136
95. Moore T (2010) The economics of cybersecurity: Principles and policy options. Int J Crit Infrastruct Prot 3(3-4):103–117
96. Moore T, Anderson R (2012) Internet security. In: The Oxford handbook of the digital economy
97. Moore T, Dynes S, Chang FR (2016) Identifying how firms manage cybersecurity investment. In: Workshop on the Economics of Information Security (WEIS), pp 1–27
98. Mughal AA (2019) Cybersecurity hygiene in the era of internet of things (iot): best practices and challenges. Appl Res Artif Intell Cloud Comput 2(1):1–31
99. Nagurney A, Shukla S (2017) Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. Eur J Oper Res 260(2):588–600

100. Newman NF, Trautman LJ (2021) Securities law: overview and contemporary issues. Ohio State Bus Law J 16:149
101. Nguyen D, Paczos M (2020) Measuring the economic value of data and cross-border data flows: a business perspective
102. NIST (2023) Nist airc – ai rmf core. https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF/Core_And_Profiles/5-sec-core. Accessed 16 Oct 2023
103. NIST (2018) Framework for improving critical infrastructure cybersecurity version 1.1. https://www.nist.gov/cyberframework/framework. Accessed 19 Nov 2023
104. Nocera J (2022) Strategies for investing in cybersecurity: PwC. https://www.pwc.com/us/en/tech-effect/cybersecurity/cyber-investment-strategies.html. Accessed 21 Oct 2023
105. Obendiek AS, Seidl T (2023) The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. J Eur Public Policy 30(7):1305–1329
106. Ogus A (2004) Comparing regulatory systems: institutions, processes and legal forms in industrialised countries. Leading issues in competition, regulation and development, pp 146–164
107. Oliver JJ, Parrett E (2018) Managing future uncertainty: reevaluating the role of scenario planning. Bus Horiz 61(2):339–352
108. Padden M, Öjehag-Pettersson A (2021) Protected how? Problem representations of risk in the general data protection regulation (gdpr). Crit Policy Stud 15(4):486–503
109. Parkin S, Kuhn K, Shaikh SA (2023) Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. J Cybersecur 9(1):tyad18
110. Paulović T, Chartier O, Zingaretti MC, Bertolozzi D, Martino G, Krüger T, Pelsy F, Sioland L, Oulès L, Baker AC et al (2022) Horizon scanning exercise on preparedness for future risk assessment requirements and possible challenges in regulatory science. EFSA Support Publ 19(4):7297E
111. Peisert S, Schneier B, Okhravi H, Massacci F, Benzel T, Landwehr C, Mannan M, Mirkovic J, Prakash A, Michael JB (2021) Perspectives on the solarwinds incident. IEEE Secur Privacy 19(2):7–13
112. Peng S-Y (2018) Private cybersecurity standards: cyberspace governance, multistakeholderism, and the(ir) relevance of the tbt regime. Cornell Int Law J 51:445
113. Pepper R, Garrity J, LaSalle C (2016) Cross-border data flows, digital innovation, and economic growth. Glob Inf Technol Rep 2016:39–47
114. Pisjak P (1994) Interdependence between regulation and technological innovation in the telecommunications sector. Technol Anal Strateg Manag 6(3):289–304
115. Porcedda MG (2018) Patching the patchwork: appraising the eu regulatory framework on cyber security breaches. Comput Law Secur Rev 34(5):1077–1098
116. Pym D, Swierzbinski J, Williams J (2013) The need for public policy interventions in information security
117. Salami E (2022) Implementing the afcfta agreement: a case for the harmonization of data protection law in Africa. J Afr Law 66(2):281–291
118. Sartor G, Lagioia F, Galli F (2021) Regulating targeted and behavioural advertising in digital services. how to ensure users' informed consent
119. Seo J, Kim K, Park M, Park M, Lee K (2018) An analysis of economic impact on iot industry under gdpr. Mobile Information Systems, vol 2018, pp 1–6
120. Shandler R, Gomez MA (2023) The hidden threat of cyber-attacks–undermining public confidence in government. J Inf Technol Polit 20(4):359–374
121. Shu X, Tian K, Ciambrone A, Yao D (2017) Breaking the target: an analysis of target data breach and lessons learned. arXiv:1701.04940. arXiv preprint
122. Sinclair TM, Xie Z (2021) Sentiment and uncertainty about regulation
123. Smith W (1997) Covering political and regulatory risks: Issues and options for private infrastructure arrangements. World Bank Publications
124. Snider KL, Shandler R, Zandani S, Canetti D (2021) Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. J Cybersecur 7(1):tyab19
125. Solove DJ, Citron DK (2017) Risk and anxiety: a theory of data-breach harms. Tex Law Rev 96:737
126. Stine K, Kissel R, Baker W, Fahlsing J, Gulick J (2008) Guide for mapping types of information and information systems to security categories. NIST sp 800-60, vol 1. National Institute of Standards and Technology, Gaithersburg
127. Stine K, Quinn S, Witte G, Gardner R (2020) Integrating cybersecurity and enterprise risk management (erm). National Institute of Standards and Technology, vol 10
128. Strausz R (2011) Regulatory risk under optimal monopoly regulation. Econ J 121(553):740–762

129. Streich G (2022) (Re-)configuring federal cybersecurity regulation: from critical infrastructures to the whole-of-the-nation. Indian Law Rev 55:733
130. Tammineedi RL (2010) Business continuity management: a standards-based approach. Inf Secur J Glob Perspect 19(1):36–50
131. Tanczer LM, Brass I, Elsden M, Carr M, Blackstock J (2019) The United Kingdom's emerging Internet of Things (IoT) policy landscape. In: Ellis R, Mohan V (eds) Rewired: cybersecurity governance, pp 37–56
132. Teixeira GA, da Silva MM, Pereira R (2019) The critical success factors of gdpr implementation: a systematic literature review. Digit Policy Regul Gov 21(4):402–418
133. Tienhaara K (2011) Regulatory chill and the threat of arbitration: a view from political science. In: Brown C, Miles K (eds) Evolution in investment treaty law and arbitration. Cambridge University Press,
134. Tikkinen-Piri C, Rohunen A, Markkula J (2018) EU general data protection regulation: changes and implications for personal data collecting companies. Comput Law Secur Rev 34(1):134–153
135. Timmers P (2018) The European Union's cybersecurity industrial policy. J Cyber Policy 3(3):363–384
136. Tosoni L (2021) The right to object to automated individual decisions: resolving the ambiguity of article 22 (1) of the general data protection regulation. Int Data Priv Law 11(2):145–162
137. Vázquez J, Boer M (2018) Addressing regulatory fragmentation to support a cyber-resilient global financial services industry
138. Yang B, Burns ND, Backhouse CJ (2004) Management of uncertainty through postponement. Int J Prod Res 42(6):1049–1064
139. Yang J, Lee Y, McDonald AP (2022) Solarwinds software supply chain security: better protection with enforced policies and technologies. In: Software engineering, artificial intelligence, networking and parallel/distributed computing, vol 22, pp 43–58