

03.07.2024

The necessities and challenges of cybersecurity regulations

Mazaher Kianpour

SUMMER SCHOOL

CYBER IN
NORMANDY

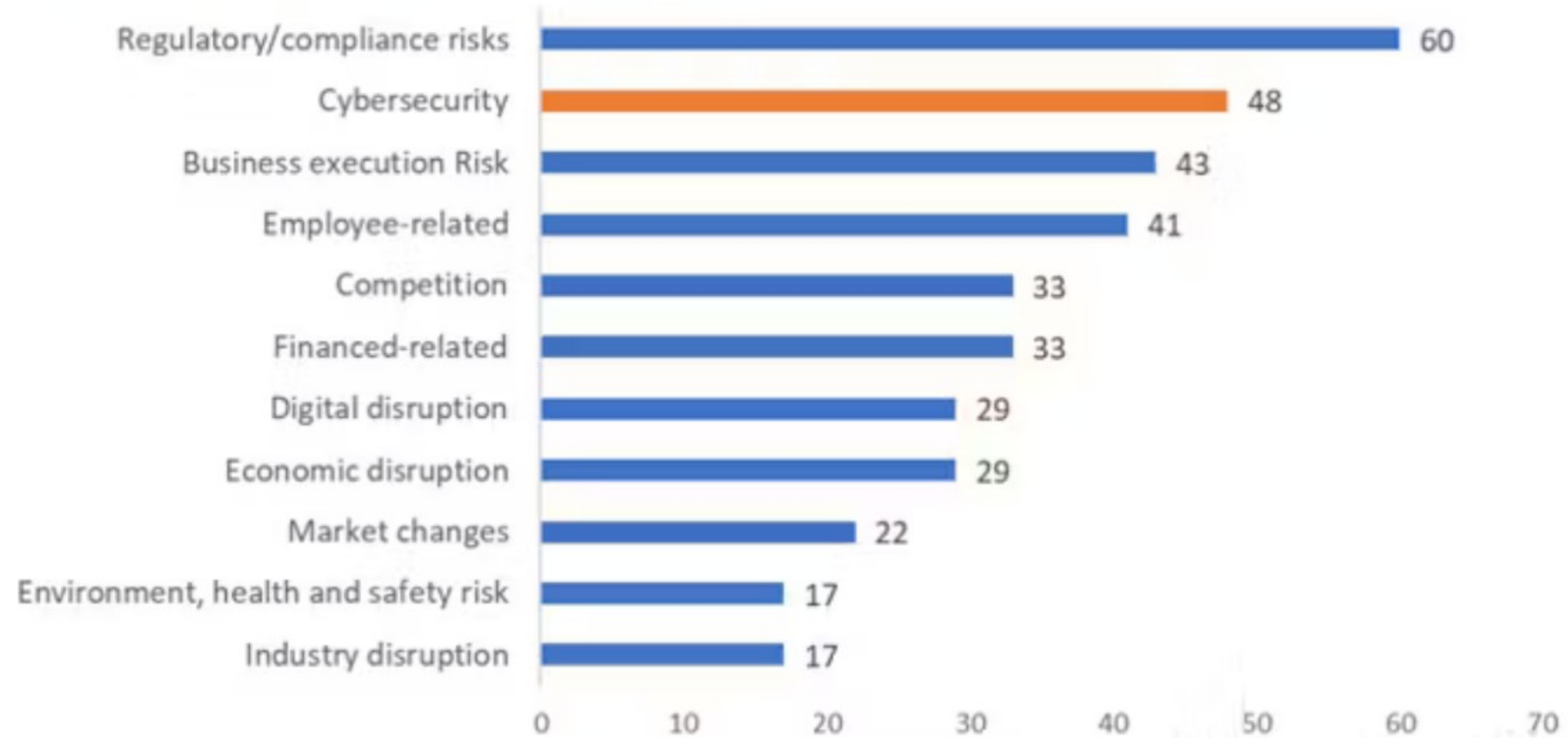




Mazaher Kianpour, Ph.D.

- Norwegian University of Science and Technology (NTNU)
- RISE Research Institutes of Sweden
- Field of Research: Cybersecurity Economics
- Work Experience as IT Manager and IS Associate
- Certified in Risks Analysis, Incident Response and Recovery, and Governance, Risk, and Compliance
- mazaher.kianpour@ntnu.no / ri.se

Figure 1: Top sources of risk to enterprises (%)



Source: Adapted by PwC from Gartner (2021). "Top security and risk management trends 2021."



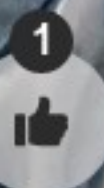


Agenda

- Part 1: Necessities of Cybersecurity Regulations
- Part 2: Threats Posed by Cybersecurity Regulations

Part 1: Necessities of Cybersecurity Regulations

- Introduction to the concept of regulations in cybersecurity
- Overview of global data protection laws, focusing on their impact on cybersecurity practices.
- A real-world cybersecurity breach and how it is relevant to cybersecurity regulations



What are regulations?



What are *Regulations*?

Regulations are legally binding rules or directives maintained by an authority.



TOPICS

Laws and Regulations



The **Laws and Regulations** category includes executive documents (e.g., Executive Orders, OMB memoranda, Presidential Directives), laws (acts of Congress and other statutes), regulations and other directives.

Types of legislation



The aims set out in the EU treaties are achieved by several types of legal act. Some are binding, others are not. Some apply to all EU countries, others to just a few.

Regulations

A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. For example, when the EU's regulation on ending roaming charges while travelling within the EU expired in 2022, the Parliament and the Council adopted a new regulation both to improve the clarity of the previous regulation and make sure a [common approach on roaming charges](#) is applied for another ten years.

Directives

A "directive" is a legislative act that sets out a goal that EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the [EU single-use plastics directive](#), which reduces the impact of certain single-use plastics on the environment, for example by reducing or even banning the use of single-use plastics such as plates, straws and cups for beverages.

Decisions

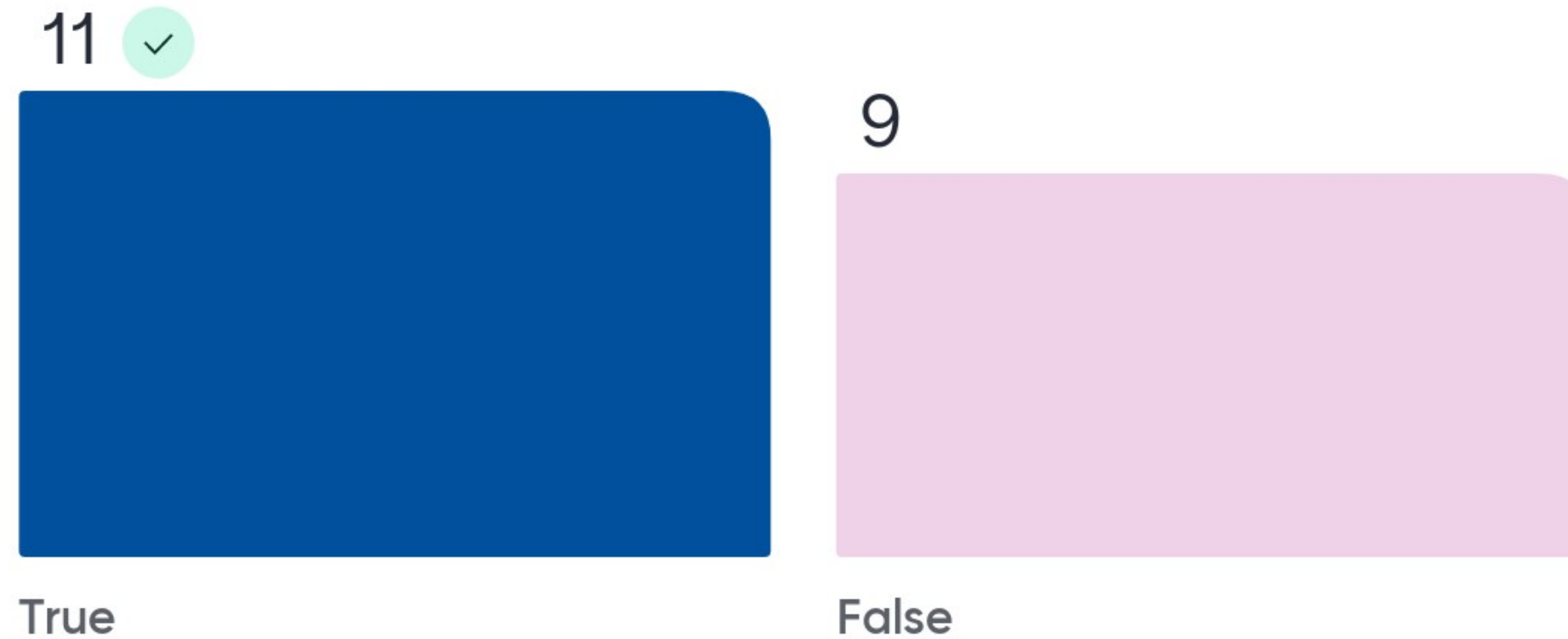
A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable. For example, the Council issued a [decision on allowing Croatia to adopt the euro](#) on 1 January 2023. The decision related to the country only.

Recommendations

A "recommendation" is not binding. When the Commission issued a recommendation that [EU countries' media service providers improve their ownership transparency and safeguard their editorial independence](#), this did not have any legal consequences. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.



National Institute of Standards and Technology (NIST) is not a regulatory agency.



NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

TOPICS

Laws and Regulations



The **Laws and Regulations** category includes executive documents (e.g., Executive Orders, OMB memoranda, Presidential Directives), laws (acts of Congress and other statutes), regulations and other directives. NIST, itself, is *not* a regulatory agency. However, many of NIST's cybersecurity efforts and publications have been created in response to various laws and regulations from other agencies, departments and branches of the U.S. Government.

Expand the term tree to display additional subtopics. Select a term for more details, including links to tagged CSRC content.

TOPICS

- + Security and Privacy
- + Technologies
- + Applications
- **Laws and Regulations**
 - + executive documents
 - + laws
 - + regulations
- + Activities and Products
- + Sectors

Created: 05/09/2016. Updated: 05/09/2020

- CSF 2.0 Resource Center +
- News and Events
- Related Programs
- Ways to Engage
- Cybersecurity @ NIST
- CSF 1.1 Archive +

CONNECT WITH US



History and Creation of the CSF 1.1

This online learning module provides readers with insight into how the NIST Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") was created, describes some of the major milestones during creation, and explains the goals for creating the Framework.

Improving Critical Infrastructure Cybersecurity

The Framework development process initiated with Executive Order 13636, which was released on February 12, 2013. The Executive Order introduced efforts on the sharing of cybersecurity threat information, and on building a set of current and successful approaches, a framework, for reducing risks to critical infrastructure. Through this Executive Order, NIST was tasked with the development of a "Cybersecurity Framework"



Executive Order 13636
February 12, 2013

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"



Frameworks and Standards influencing the regulations

NIST Risk Management Framework RMF



Overview

[+ expand all](#)

Recent Updates

October 17, 2023: NIST opens a 2-week expedited public comment period on draft controls for October 17–31, 2023, and plans to issue SP 800-53 Patch Release 5.1.1 in November 2023. Please review and submit comments on the proposed new control, control enhancements and corresponding assessment procedures using the [NIST SP 800-53 Public Comment Website](#). For more information, see: [CSRC News Article](#) and the [SP 800-53 Release 5.1.1 FAQ](#).

Please direct questions and comments to: 800-53comments@list.nist.gov.

The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA).

This site provides an [overview](#), explains each RMF step, and offers resources to support implementation, such as updated Quick Start Guides, and the [RMF Publication](#).

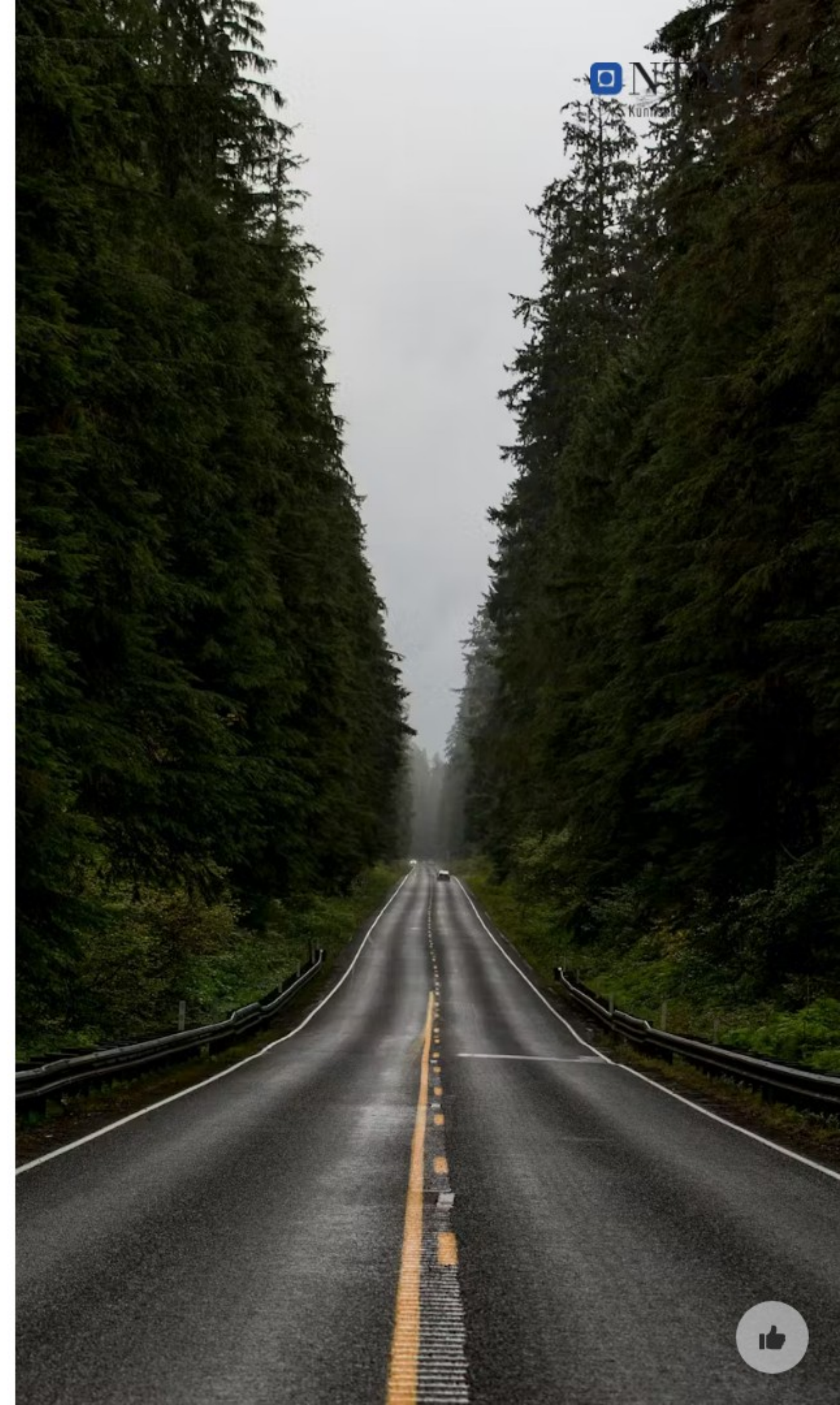
For IoT, ETSI's new EN 303 645 standard is influencing IoT regulations across the world, and for automotive, UNECE WP.29 regulation is leading the way globally.

These standards and regulations will play a vital role in transforming the security of IoT and automotive technology in years to come. Therefore, if OEMs wish to avoid the consequences of non-compliance, they must be aware of the legislation, and what is required of them.



Regulations as Guardrails

- Protection, Safety, and Resilience
- Guidance, Direction, and Support



UNITED STATES PATENT OFFICE

SAMUEL R. GARNER, OF MERCER, PENNSYLVANIA

HIGHWAY GUARD RAIL

Application filed April 12, 1932. Serial No. 604,825.

The present invention relates to a highway guard rail and has for one of its important objects to provide, in a manner as hereinafter set forth, a device of this character embodying resilient means for supporting the rail in position.

Another important object of the invention is to provide novel means for connecting the adjacent ends of the rail sections together and for slidably mounting said rails on the resilient supporting means.

Other objects of the invention are to provide a highway guard rail of the character described which will be simple in construction, strong, durable, efficient and reliable in use, attractive in appearance and which may be manufactured and installed at low cost.

designates vertical supporting posts provided in spaced relation and mounted in the ground.

The ability to rapidly respond, recover, adapt to, and transform in response to emerging risks and disasters.

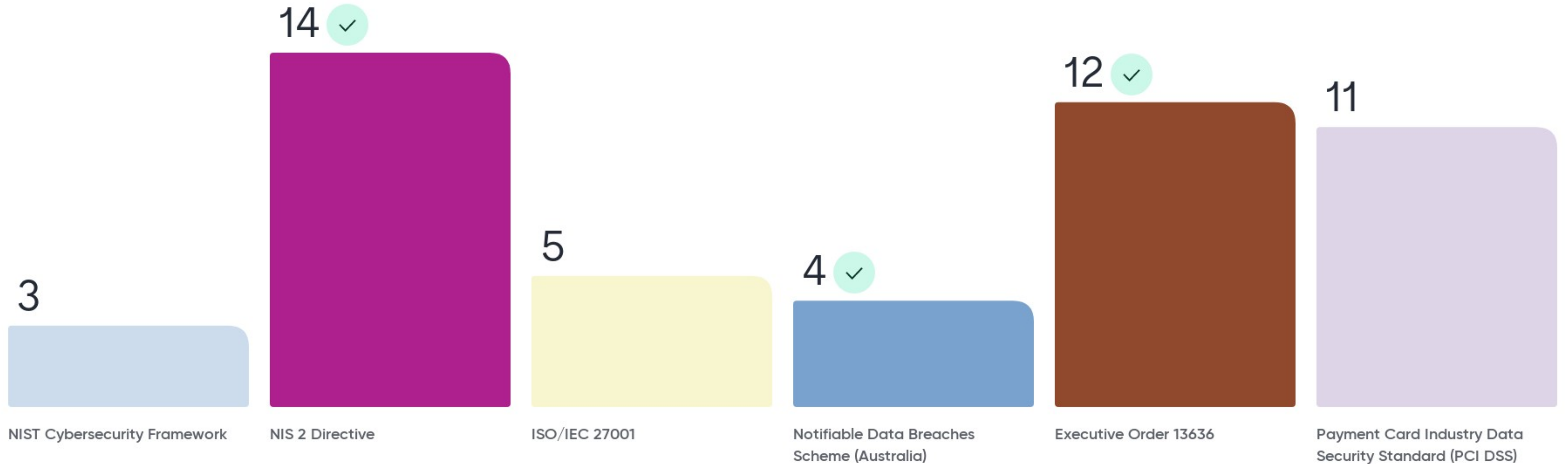
the rods 3 are connected to the plates 4 for yieldingly urging said plates outwardly. Wear plates 6 are mounted on the rods 3 between the posts 1 and the inner ends of the springs 5. Stop nuts 7 are threaded on the other end portions of the rods 3 and engageable with the posts for limiting actuation of said rods by the springs 5.

The reference numeral 8 designates guard rail sections having abutting ends located adjacent one of the posts 1. The rail sections 8 are secured together through the

Cybersecurity Regulations

Cybersecurity regulations are legally binding rules established by governments or regulatory bodies to ensure that organizations implement adequate measures to protect their information systems from cyber threats. These regulations are designed to ensure data protection, enhance national security, and promote trust and stability in the digital economy.

Which ones can be categorised as cybersecurity regulations?



Overview of Cybersecurity Regulations

Began with sector-specific regulations in areas like health and finance. The U.S. has driven many regional standards with acts like FISMA, and state-specific regulations, e.g., California's CCPA. Canada has PIPEDA, while Mexico has the Federal Law on Protection of Personal Data.



Initially lagged in terms of formalized cybersecurity legislation, but many countries began developing regulations in the late 2010s. Countries like Colombia and Chile have started to prioritize cybersecurity. Regional cooperation is ongoing.

Diverse due to the varied economic and technological development. Developed nations like Japan and South Korea had early cyber laws. ASEAN nations are collaboratively enhancing their cybersecurity stance.



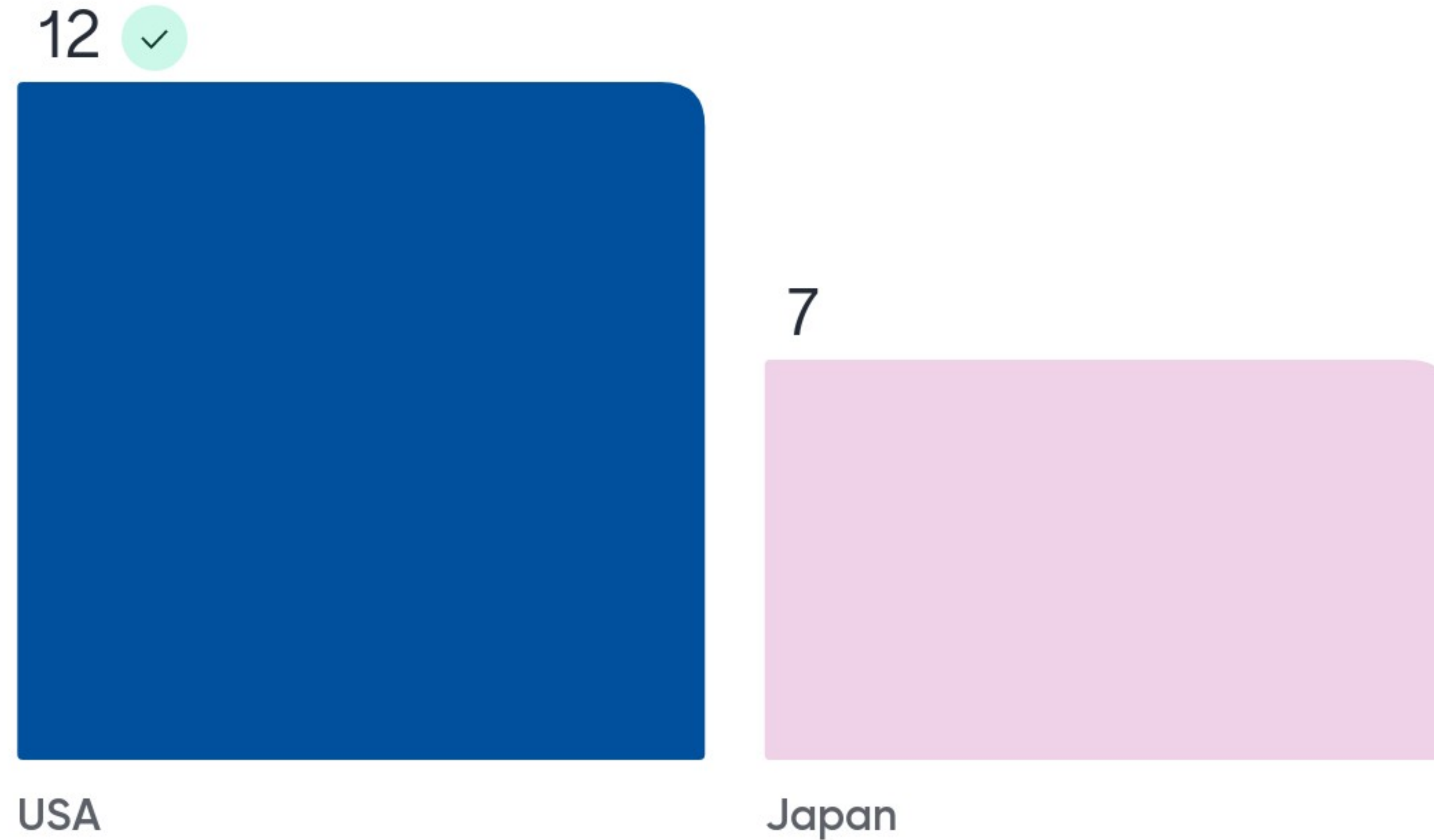
Australia has been proactive, introducing early cybercrime and privacy acts. New Zealand has its own Privacy Act. Smaller island nations are still developing their cybersecurity frameworks.

Steadily grew in prominence with the Data Protection Directive, which was later superseded by GDPR in 2018. The NIS Directive also focuses on cybersecurity for essential services. New versions of existing regulations and new regulations are continually being evaluated and introduced to address the evolving cybersecurity landscape.

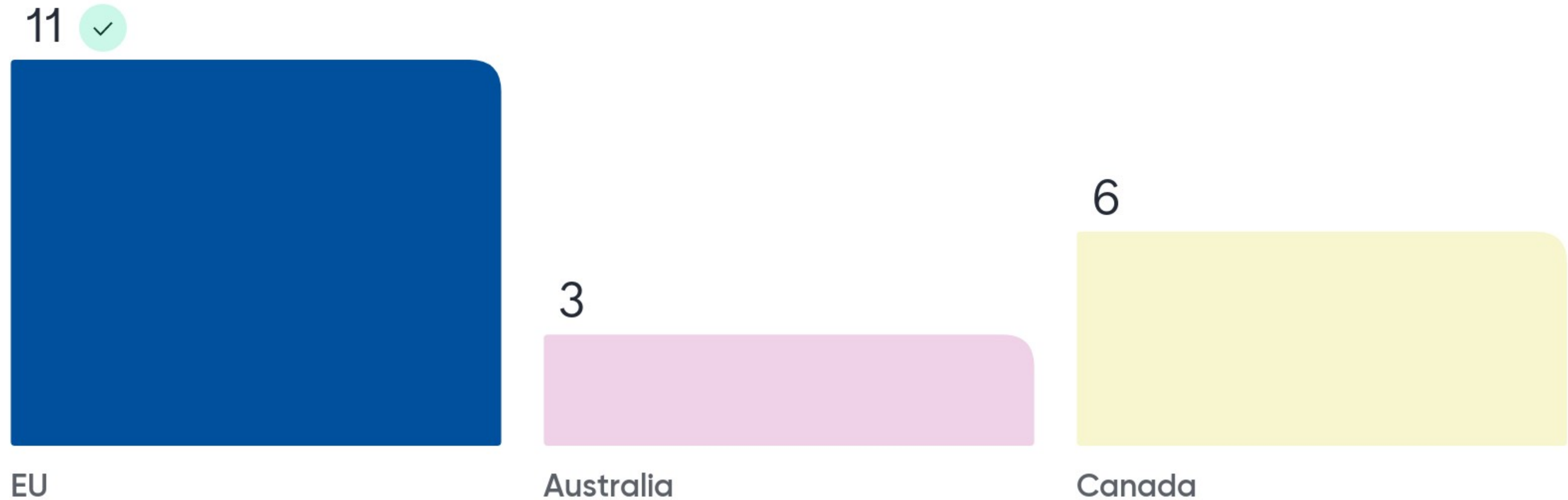


Widely varied, with some countries having almost no cybersecurity regulations and others slowly catching up. Regional bodies like the African Union are working to harmonize regulations.

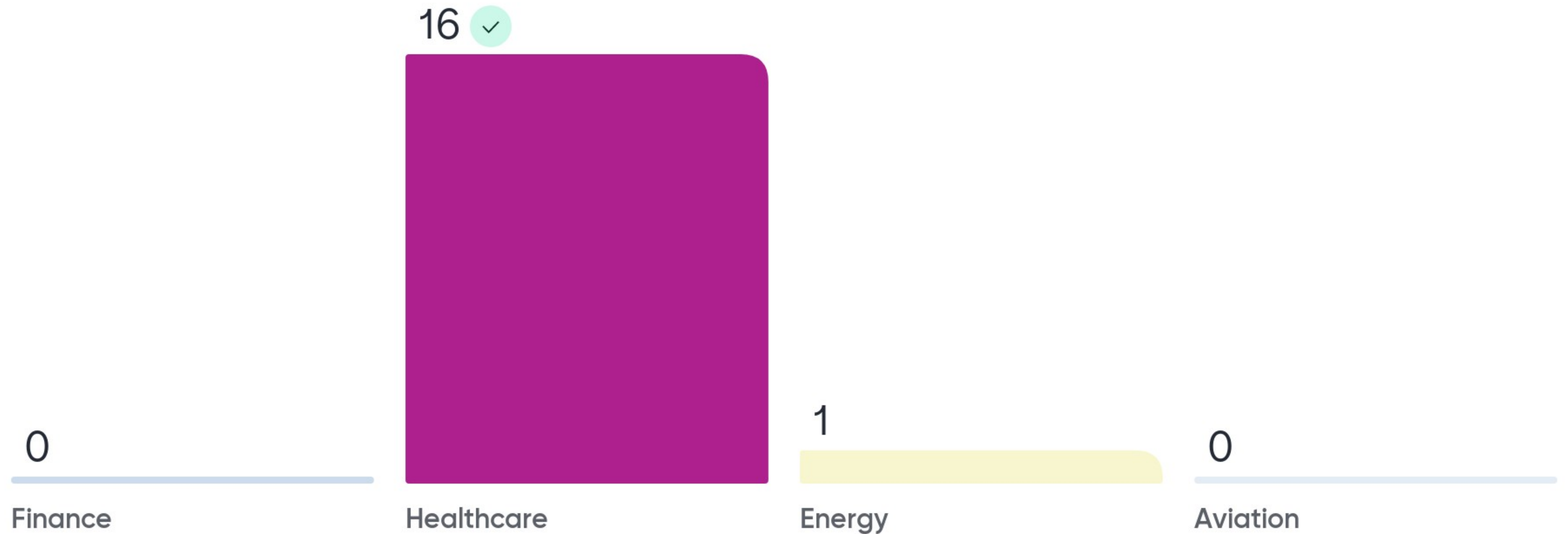
Sarbanes-Oxley Act (SOX)

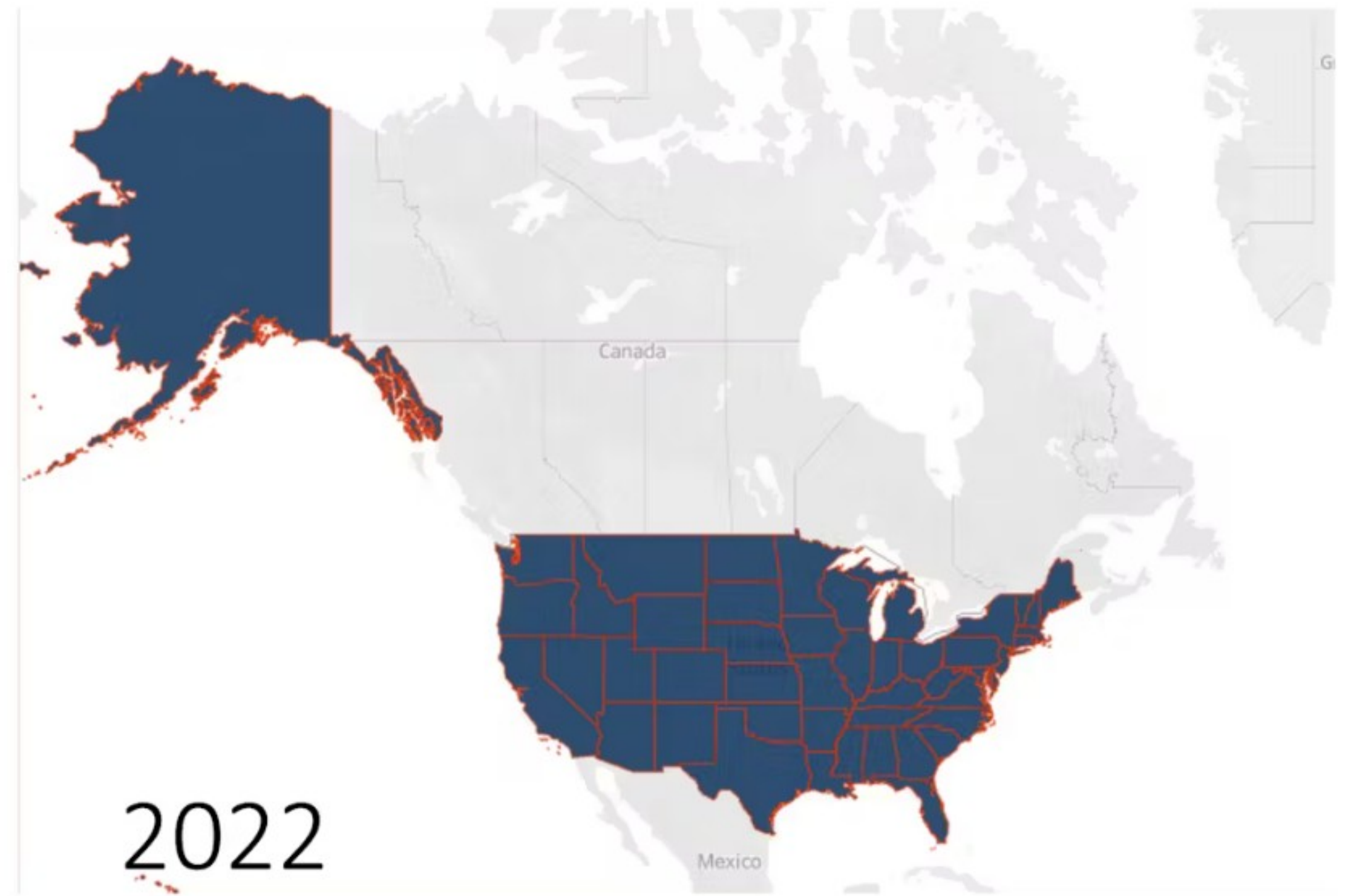
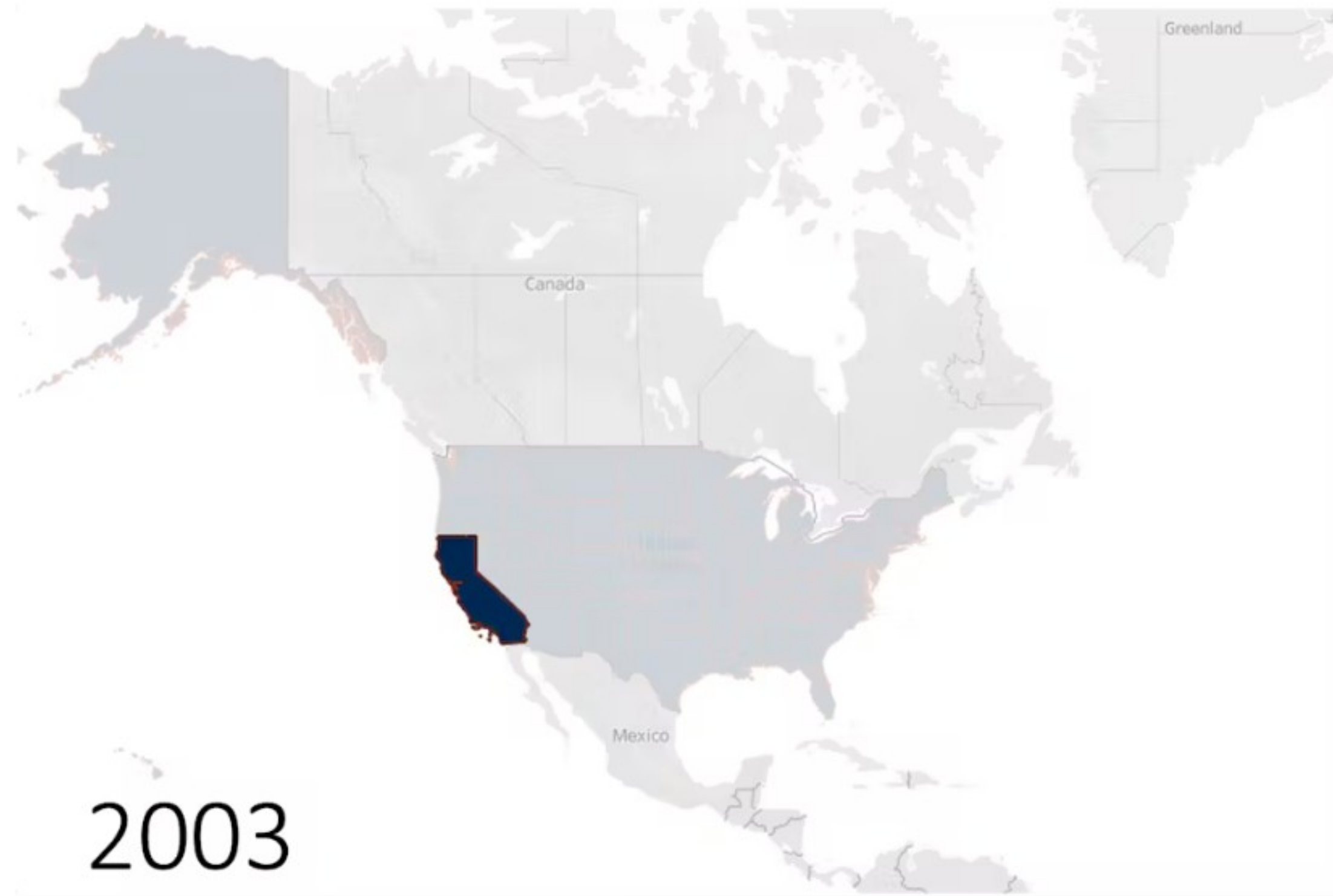


Digital Operational Resilience Act (DORA)



HIPAA applies to





Data Breach Notification Laws in the US



California Consumer Privacy Act (CCPA)

14 ✓



allows any California consumer to demand to see all the information a company has saved on them

9 ✓



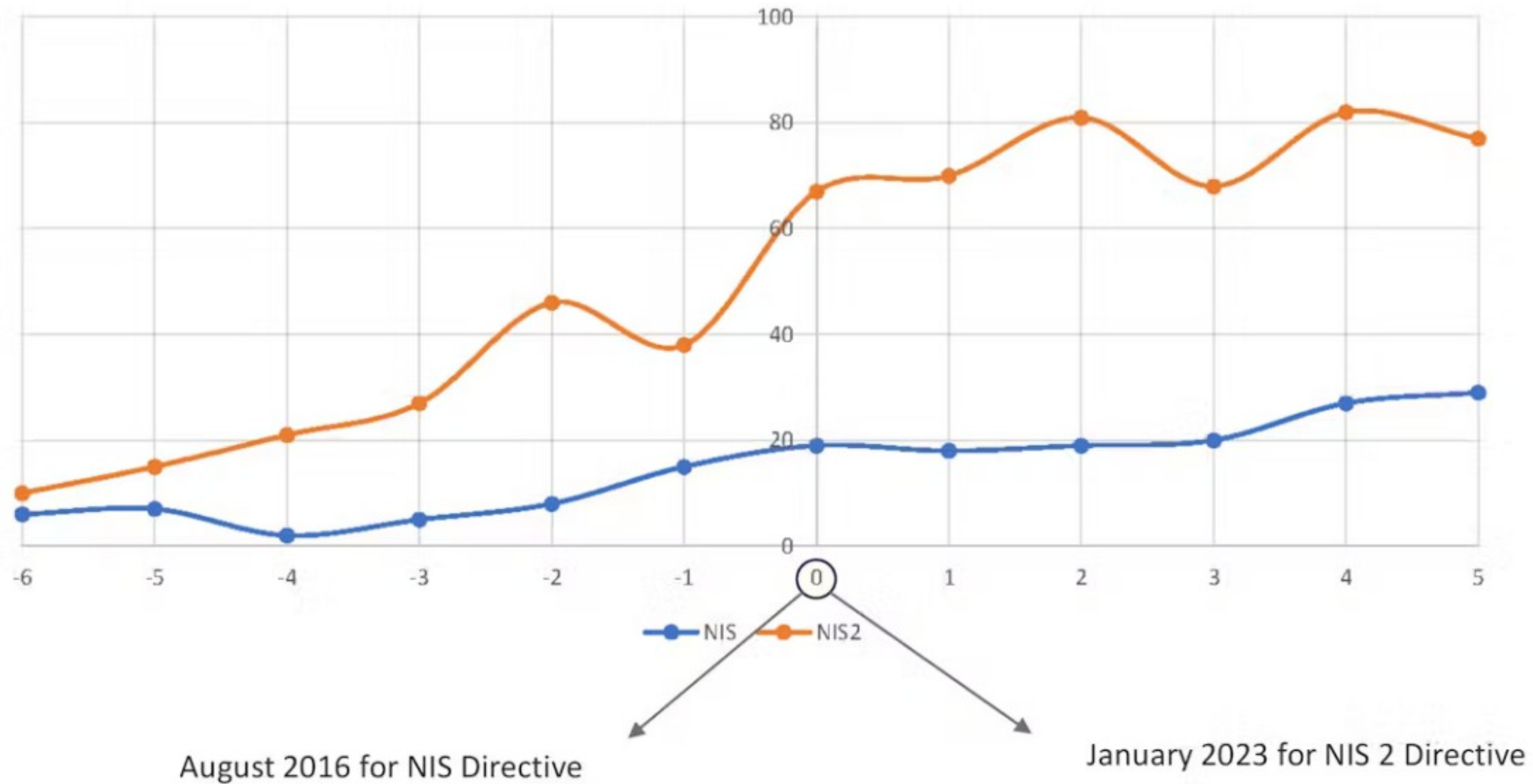
allows any California consumer to demand to see a full list of all the third parties that data is shared with

9 ✓



allows any California consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

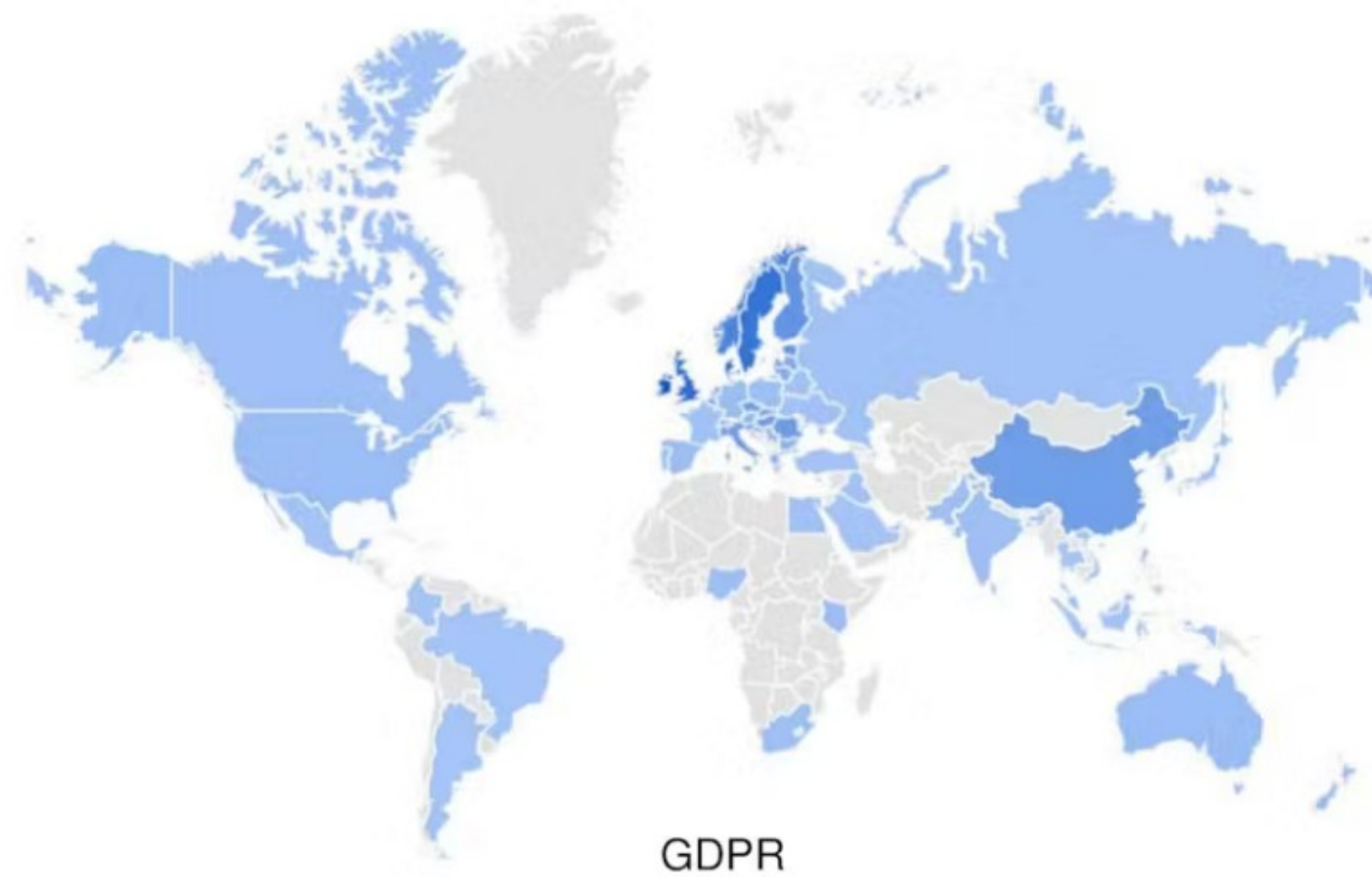
A Growing Regulatory Awareness



Google search trends for the keywords "NIS Directive" and "NIS 2 Directive" over 6 months before and after they entered into force.



A Growing Regulatory Awareness



Google Search Trend October 2023
(Regions with interest levels below 20 are not considered)



Figure 2 GDPR readiness by country
Percent of respondents, N=3206

Source: Cisco 2019 Data Privacy Benchmark Study, n=3206

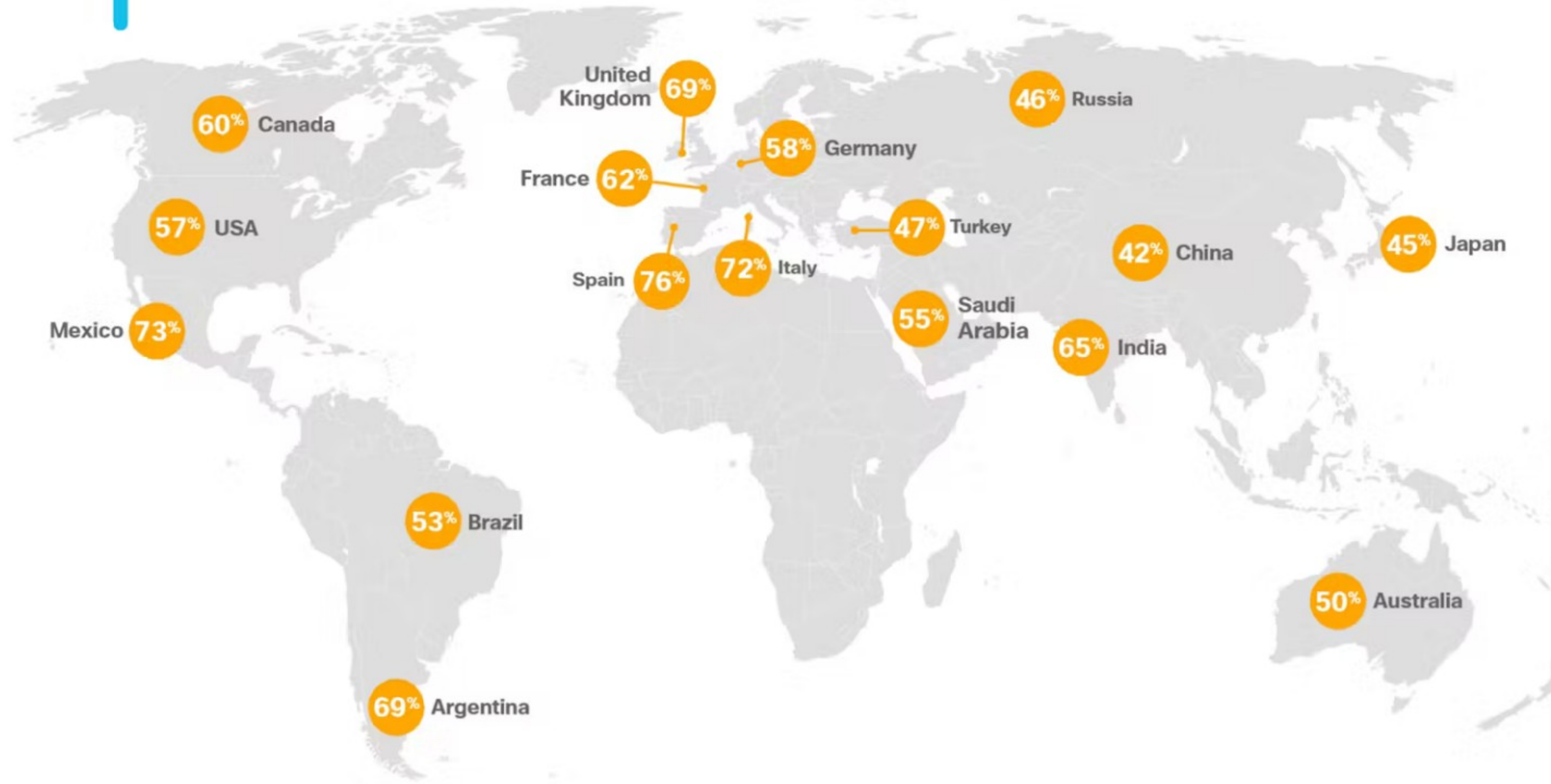
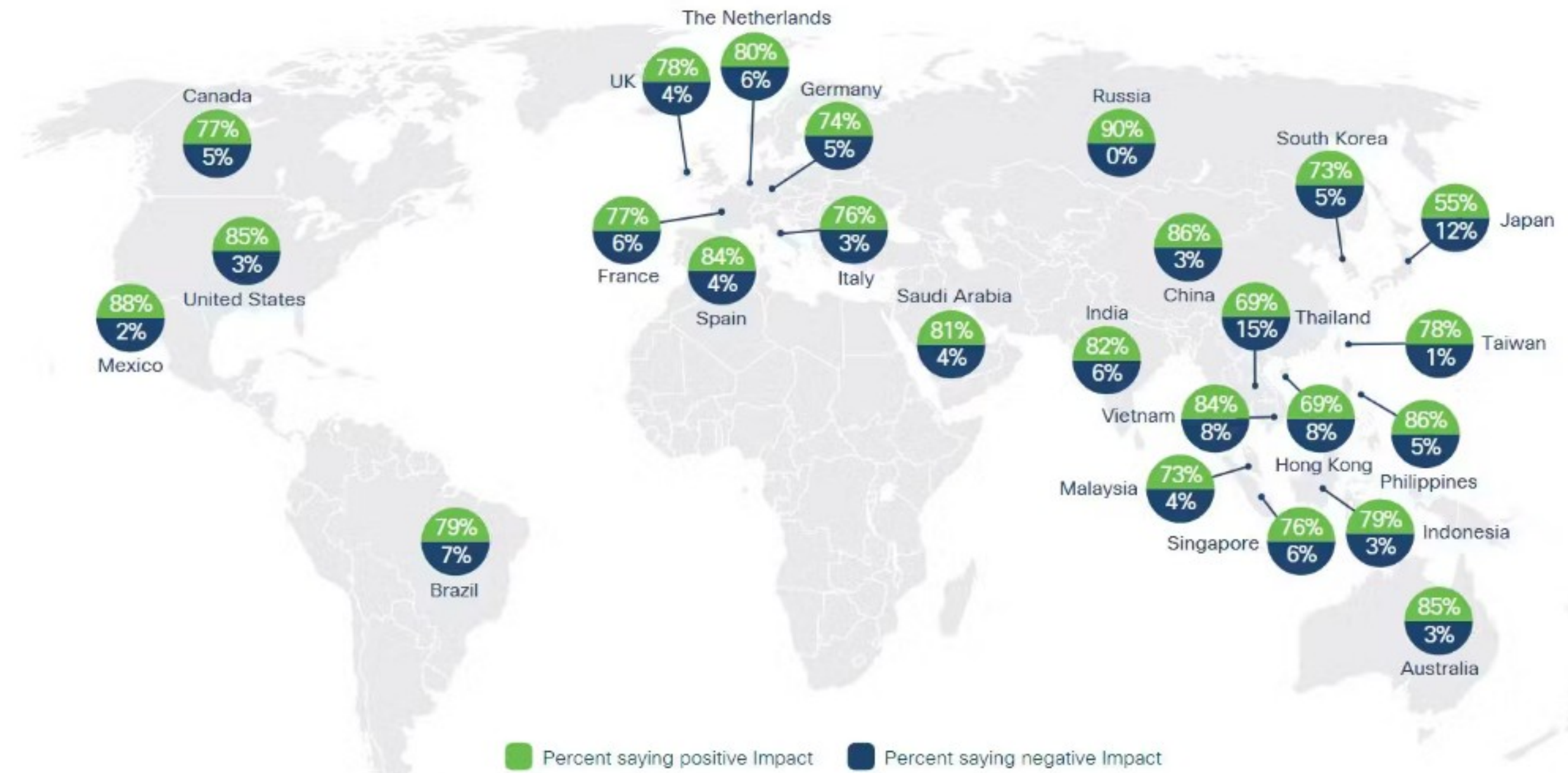


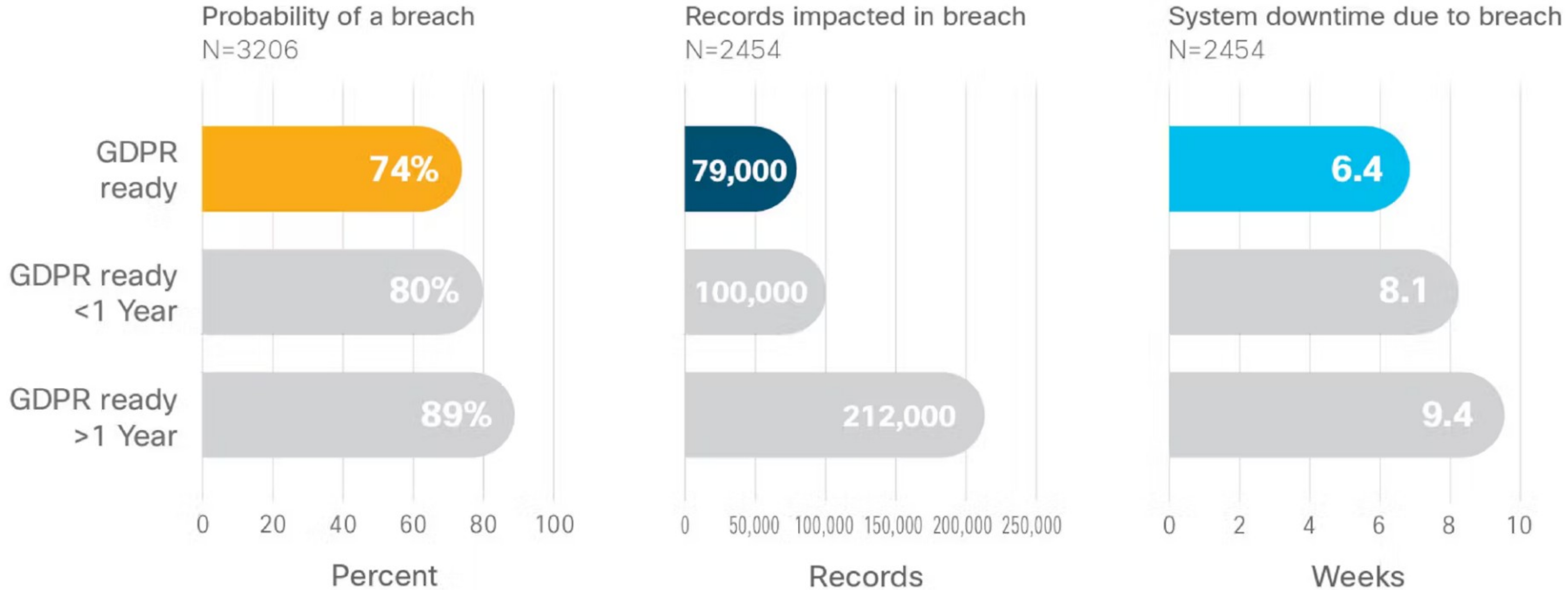
Figure 9. Perceived Impact of Privacy Regulations on Organizations, by Country (N=4446)



Source: Cisco Data Privacy Benchmark Study - 2021



Figure 9 Business benefits of privacy investments

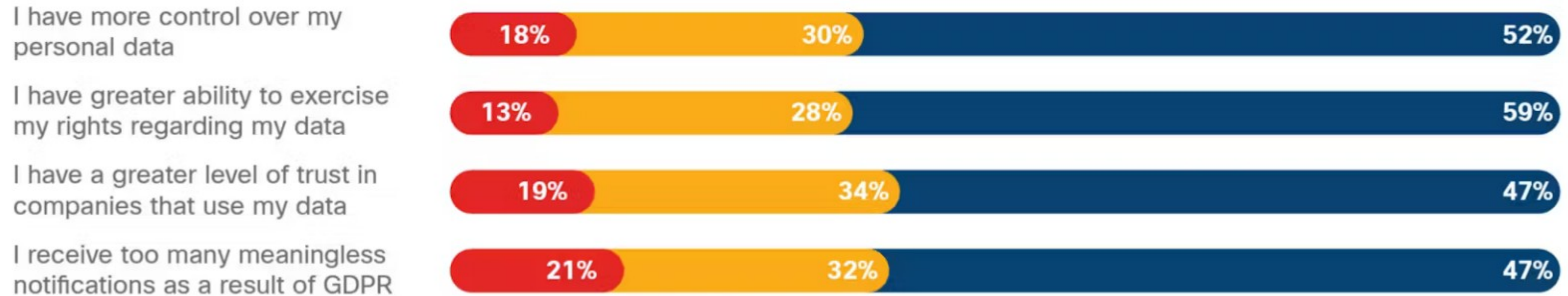


Source: Cisco 2019 Data Privacy Benchmark Study



Figure 10 Impact of GDPR on the individual.

N=941



Source: Cisco Consumer Privacy Study - 2019

● Disagree ● Neutral ● Agree



Why are regulations necessary?

Regulations mandate the security controls:

- Technical Controls (Encryption, MFA, etc.)
- Administrative Controls (Formal security policies, training and awareness, etc.)
- Physical Controls (Secure access to facilities, environmental controls)



Cybersecurity regulations necessitate the implementation of a combination of controls to ensure fulfilling their objectives.

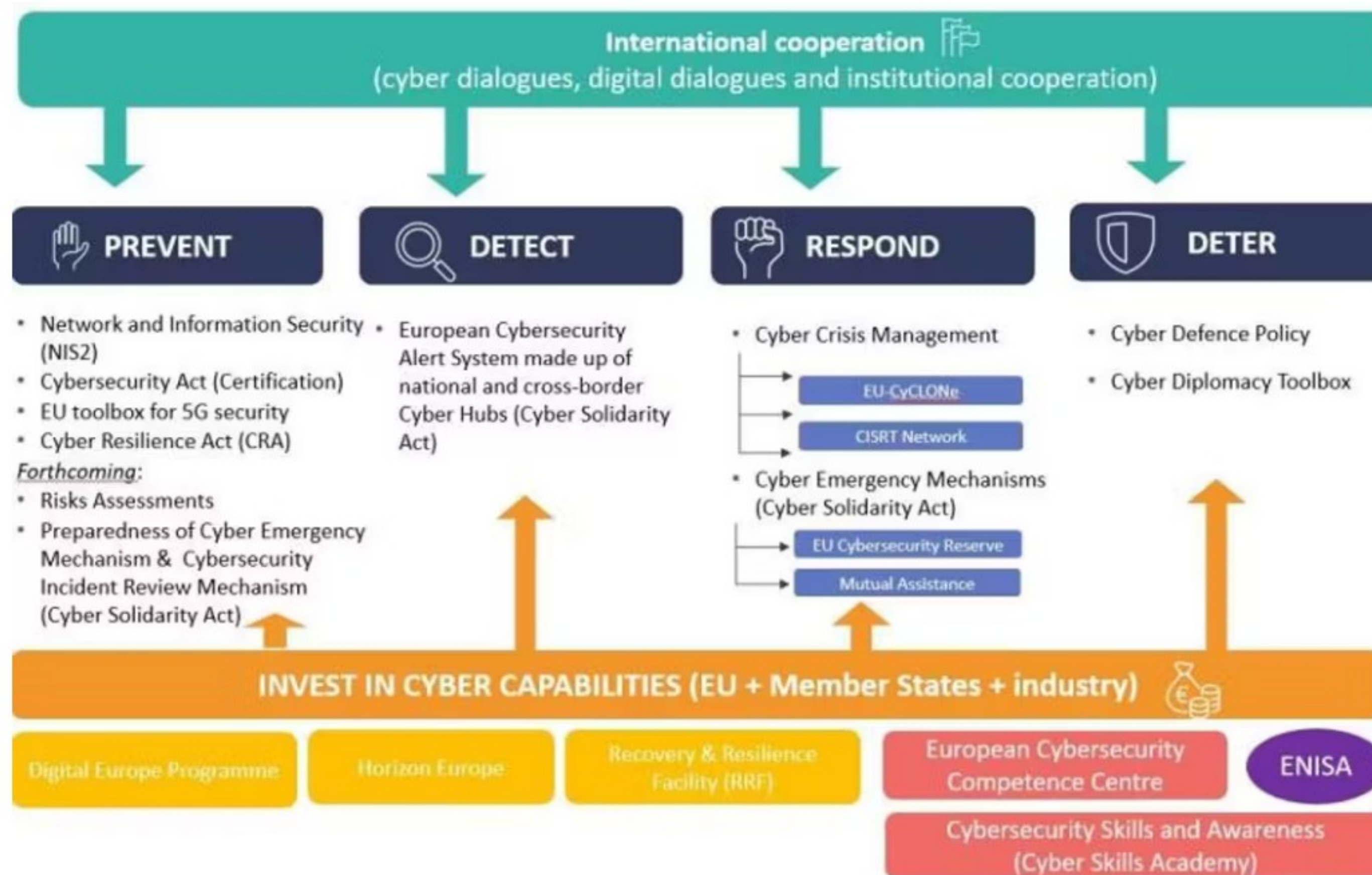
The General Data Protection Regulation (GDPR) mandates a comprehensive set of administrative, technical, and physical controls to protect personal data. This includes data encryption, access controls, regular data protection impact assessments, and incident response procedures.



Cybersecurity regulations necessitate the implementation of a combination of controls to ensure fulfilling their objectives.

The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to implement administrative controls (like training programs and policies), technical controls (like encryption and access controls), and physical controls (like secure facility access).





Source: ENISA



They also aim to

- Protect Sensitive Data and Mitigating Financial Loss
- Ensure National/Regional Security
- Standardize and Harmonize Regulatory Frameworks
- Promote Compliance, Trust, and Accountability
- Encourage Continuous Improvement



Externalities


Cybersecurity is a cost that the business itself does not fully bear, but that the rest of society does.



Externality

[,ek-,stər-'nɑ-lə-tē]

A cost or benefit caused by an economic actor that is not suffered or enjoyed by that same actor.

 Investopedia

SolarWinds certainly seems to have underspent on security. The company outsourced much of its software engineering to cheaper programmers overseas, even though that typically increases the risk of security vulnerabilities. For a while, in 2019, the update server's password for SolarWinds's network management software was reported to be "solarwinds123." Russian hackers were able to breach SolarWinds's own email system and lurk there for months. Chinese hackers appear to have exploited a separate vulnerability in the company's products to break into U.S. government computers. A cybersecurity adviser for the company said that he quit after his recommendations to strengthen security were ignored.

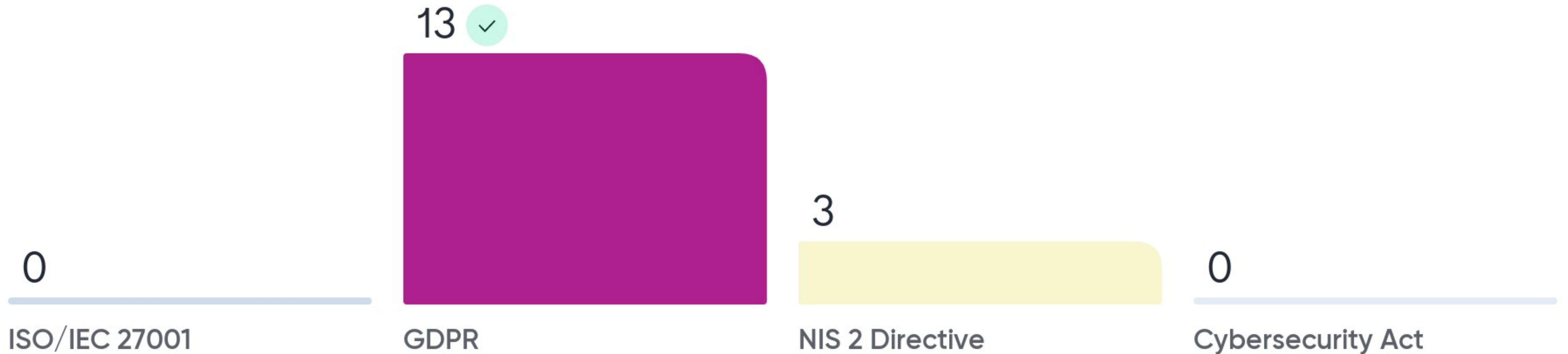
Misaligned incentives

People and organizations both tend to act in their own self-interest, which may not always be what was wanted, unless the rules incentivize them to do otherwise.



THIS STATEMENT IS VALID FOR

One of its primary objectives is to harmonize data protection laws across all EU Member States.



THIS STATEMENT IS VALID FOR

It is widely adopted across different sectors in the US, provides a standardized approach to managing and reducing cybersecurity risk



2

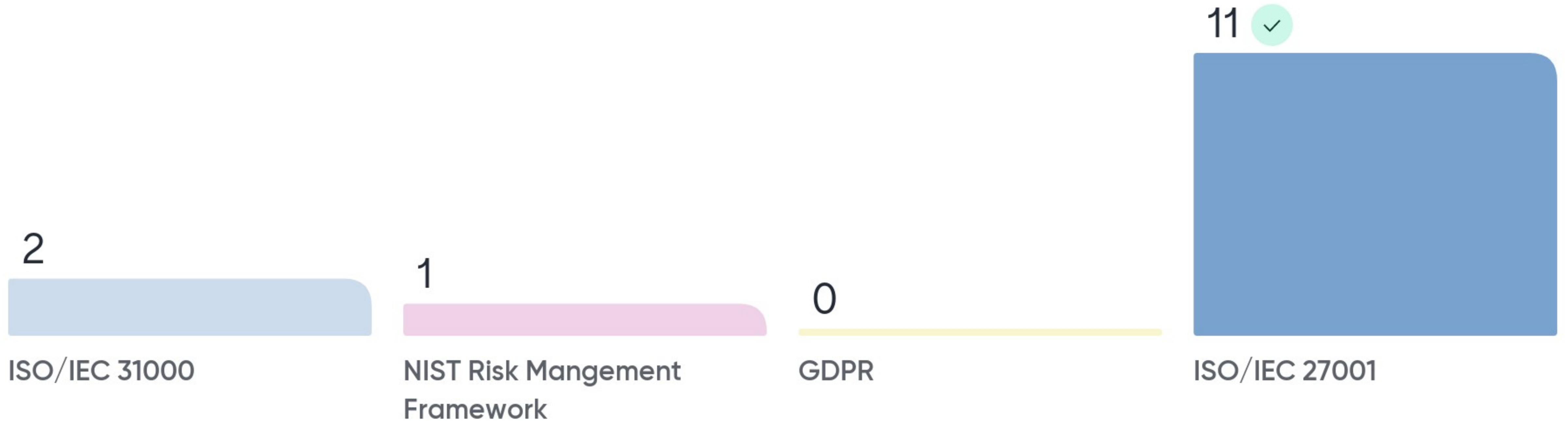


15



THIS STATEMENT IS VALID FOR

It provides a globally recognized framework that organizations can use to ensure their CS practices are consistent with intl. best practices.



THIS STATEMENT IS VALID FOR

It sets out measures for Member States to manage cybersecurity risks, ensuring a coordinated approach to cybersecurity across Europe.

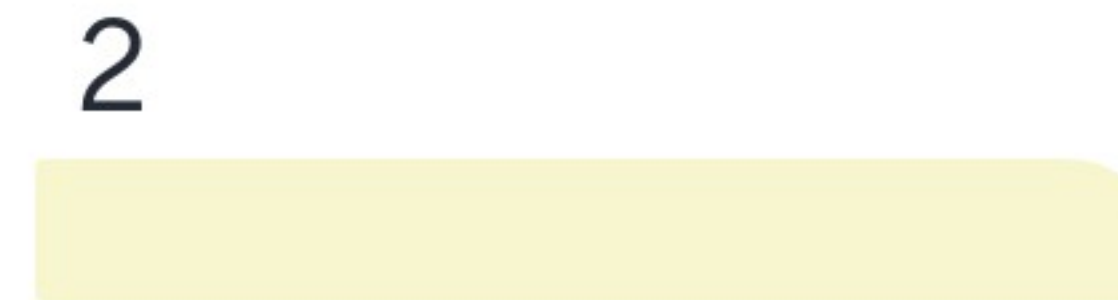
10 ✓



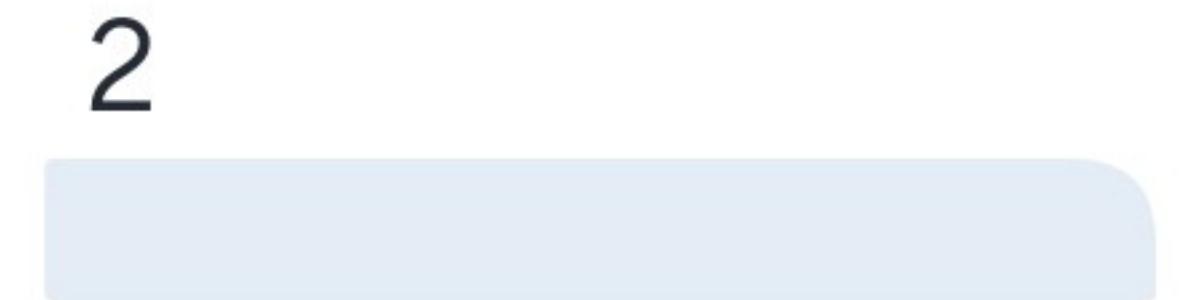
NIS 2 Directive



GDPR



Cyber Resilience Act



DORA

Which of the following reasons best explains why cybersecurity regulations are necessary in preventing such data breaches?

0

Regulations ensure that organizations install the latest antivirus software.

0



Regulations mandate comprehensive data protection policies and practices.

0

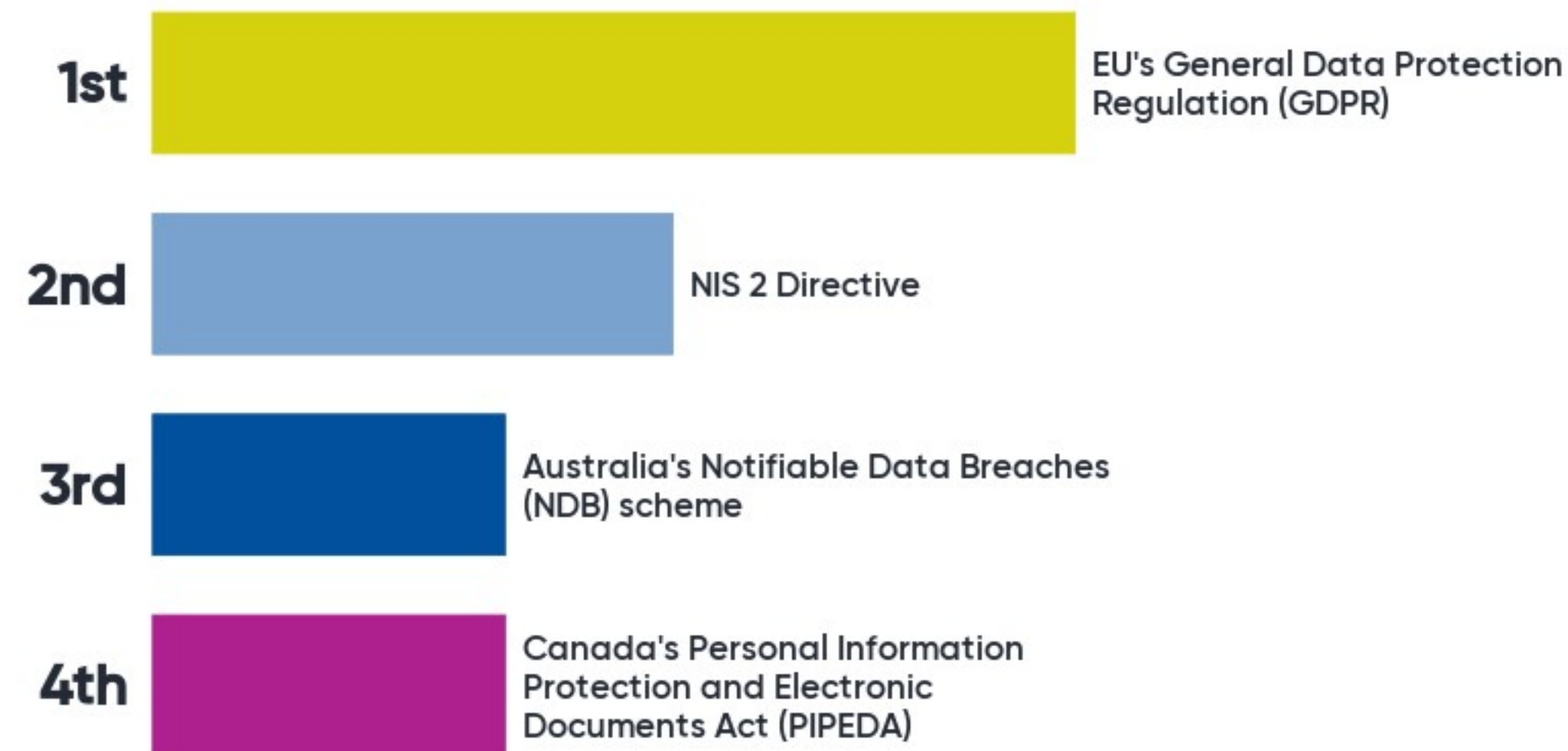
Regulations guarantee that organizations will not experience any cyber attacks.

0

Regulations focus solely on financial reporting and accounting accuracy.



Rank these regulations by the strictness of their personal data breach notification requirements.



NIS2 Directive



Geographical Scope: EU member states

Entities Covered: Essential and important entities operating in sectors with a high degree of interconnectedness and dependency on ICT

Notification Requirements:

- Entities must notify the relevant national authority “without undue delay” and no later than 24 hours after having become aware of the incident.
- Notification should include information necessary to assess the incident's impact and nature.
- The directive emphasizes the importance of confidentiality in the notification process.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Geographical Scope: Canada



Entities Covered: Private-sector organizations

Notification Requirements:

- Organizations must report any breach of security safeguards involving personal information under their control to the Privacy Commissioner of Canada if it is reasonable in the circumstances to believe that the breach creates a “real risk of significant harm” to an individual.
- Affected individuals must also be notified if the breach poses a real risk of significant harm.
- The notification must contain sufficient information to allow the individual to understand the significance of the breach and take steps to mitigate or prevent any resulting harm.

General Data Protection Regulation (GDPR)



Geographical Scope: EU member states (and applicable to entities outside the EU offering goods/services to or monitoring behavior of EU residents)

Entities Covered: All entities that process personal data

Notification Requirements:

- Entities must notify the supervisory authority “without undue delay” and, where feasible, not later than 72 hours after becoming aware of the data breach.
- If the breach is likely to result in a high risk to the rights and freedoms of individuals, entities must also notify affected individuals “without undue delay.”
- Notifications must include the nature of the breach, categories and approximate number of affected individuals, likely consequences, and measures taken or proposed to address the breach.

Australia's Notifiable Data Breaches (NDB) Scheme



Geographical Scope: Australia

Entities Covered: Australian Government agencies, businesses, and not-for-profit organizations with an annual turnover of AU\$3 million or more, credit reporting bodies, health service providers, and TFN recipients

Notification Requirements:

- Entities must notify affected individuals and the Australian Information Commissioner when a data breach is likely to result in serious harm to any individuals whose personal information is involved.
- Notifications must include recommendations about the steps individuals should take in response to the breach.
- The entity has 30 days to assess whether a notifiable data breach has occurred after becoming aware of a potential data breach.



Which cyber incident violated Gramm-Leach-Bliley Act?



Despite its failure to implement basic security measures, Equifax's privacy policy at the time stated that it limited access to consumers' personal information and implemented "reasonable physical, technical and procedural safeguards" to protect consumer data.

The FTC alleges that Equifax violated the FTC Act's prohibition against unfair and deceptive practices and the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of customer information.

Equifax Settlement with FTC (source: FTC Website)

Equifax Data Breach

Background:

- **Company:** Equifax, one of the three largest credit agencies in the U.S.
- **Date:** Discovered in July 2017.
- **Impact:** Personal data of 147 million people was exposed, including Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers.

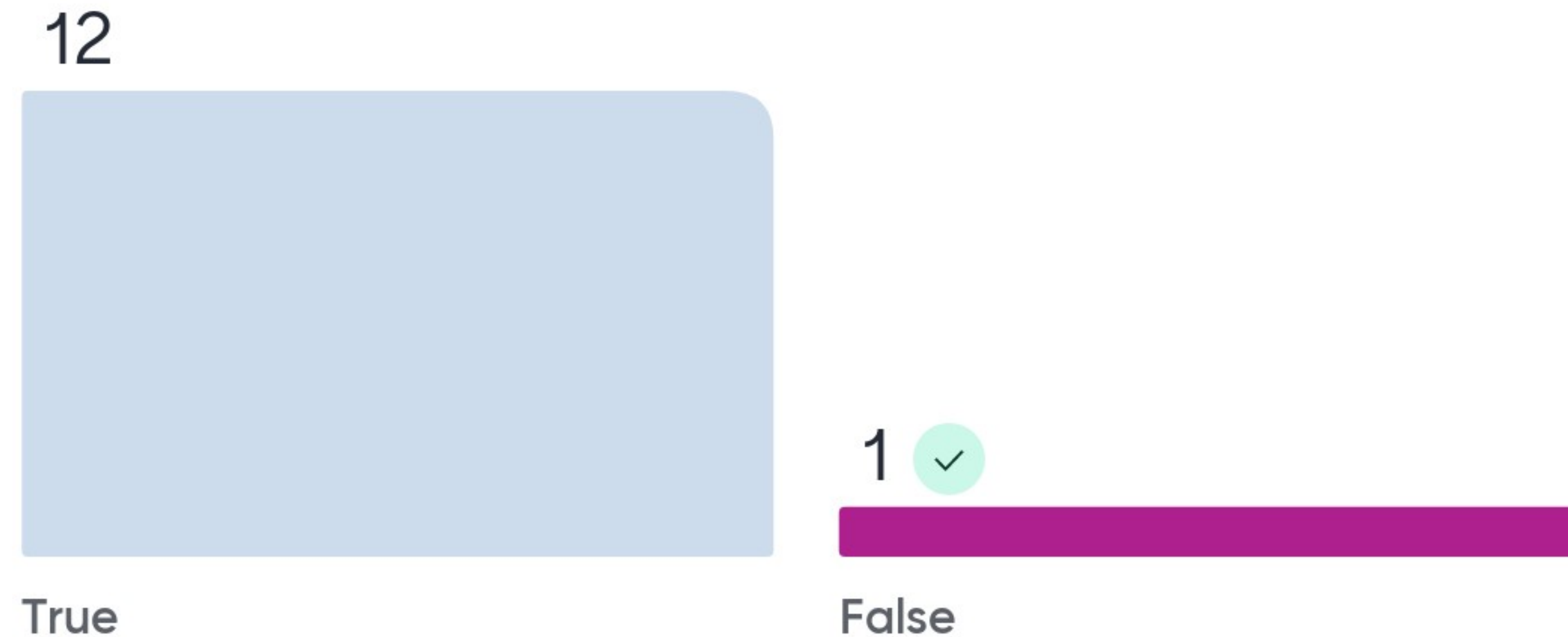
What Happened:

- The breach was due to a vulnerability in a website application.
- Equifax failed to patch a known vulnerability in the Apache Struts web application framework.

Aftermath:

- Equifax faced significant backlash from the public, regulators, and shareholders.
- The breach led to several high-profile resignations within the company.
- Equifax agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories, which included up to pay \$575 Million as part of settlement with FTC, CFPB, and States.

The Equifax breach led to the introduction of new federal cybersecurity regulations in the U.S.



Equifax Breach Prompts Scrutiny, but New Rules May Not Follow

Share full article



Thomas Quadman, a United States Chamber of Commerce official, testifying at the hearing last week in Washington.

By Stacy Cowley, Tara Siegel Bernard and Danny Hakim
Sept. 15, 2017


At a [congressional hearing](#) last week, financial industry representatives pushed for legislation that would chip away at consumer protection rules governing the three major credit reporting bureaus. Loosening those regulations “would provide economic stability” by capping the industry’s exposure to class-action claims, a trade group official [testified](#).

Hours later, one of the three bureaus, Equifax, [disclosed a major data breach](#), which has potentially compromised the sensitive personal data of more than 143 million Americans.

Capitol Hill is now demanding answers about the cyberattack. The Consumer Financial Protection Bureau, the Federal Trade Commission, and at least six state attorneys general have opened investigations.

- Increased scrutiny and discussion around data security and privacy
- Did not immediately result in new federal laws, it significantly influenced the regulatory landscape and encouraged legislative proposals to strengthen data security across the United States.

BILL Hide Overview X

Sponsor: [Sen. Warren, Elizabeth \[D-MA\]](#) (Introduced 01/10/2018)
Committees: Senate - Banking, Housing, and Urban Affairs
Latest Action: Senate - 07/12/2018 Committee on Banking, Housing, and Urban Affairs. Hearings held. ([All Actions](#))
Tracker:  **Introduced**

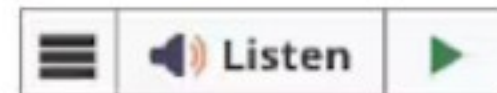
More on This Bill
[CBO Cost Estimates \[0\]](#)

Subject — Policy Area:
 Finance and Financial Sector
[View subjects >>](#)

Summary (1) Text (1) Actions (2) Titles (2) Amendments (0) Cosponsors (3) Committees (1) Related Bills (0)

Summary: S.2289 — 115th Congress (2017-2018)

[All Information](#) (Except Text)



There is one summary for S.2289. [Bill summaries](#) are authored by [CRS](#).

Shown Here:

Introduced in Senate (01/10/2018)

Data Breach Prevention and Compensation Act of 2018

This bill creates the Office of Cybersecurity within the Federal Trade Commission (FTC) that, in part, must:

- supervise, evaluate, and regulate specified agencies' management of data security;
- examine agencies annually for compliance with regulations;
- investigate an agency in the event of a breach covered by the bill or suspected noncompliance with regulations, and report on any findings of such investigation; and
- coordinate with the National Institute of Standards and Technology and the National Cybersecurity and Communications Integration Center of the Department of Homeland Security.

The office is authorized to: (1) investigate an agency's compliance with regulations regarding any data breach, and (2) enjoin an agency from violating specified regulations.

Specified consumer reporting agencies, in part, must:

- provide the office with information relating to security measures,
- demonstrate reasonable data protection measures, and
- notify the FTC of a covered breach.

The bill establishes civil penalties for violations and directs the FTC to enforce compliance.

Legislative proposals were introduced



Influencing some state-level legislation

New York State Issues New Cybersecurity Regulations Following Equifax Breach

by: Brian G. Cesaratto of Epstein Becker & Green, P.C. - *Technology Employment Law*

© Posted On Tuesday, September 26, 2017



RELATED PRACTICES & JURISDICTIONS

Communications Media
Internet

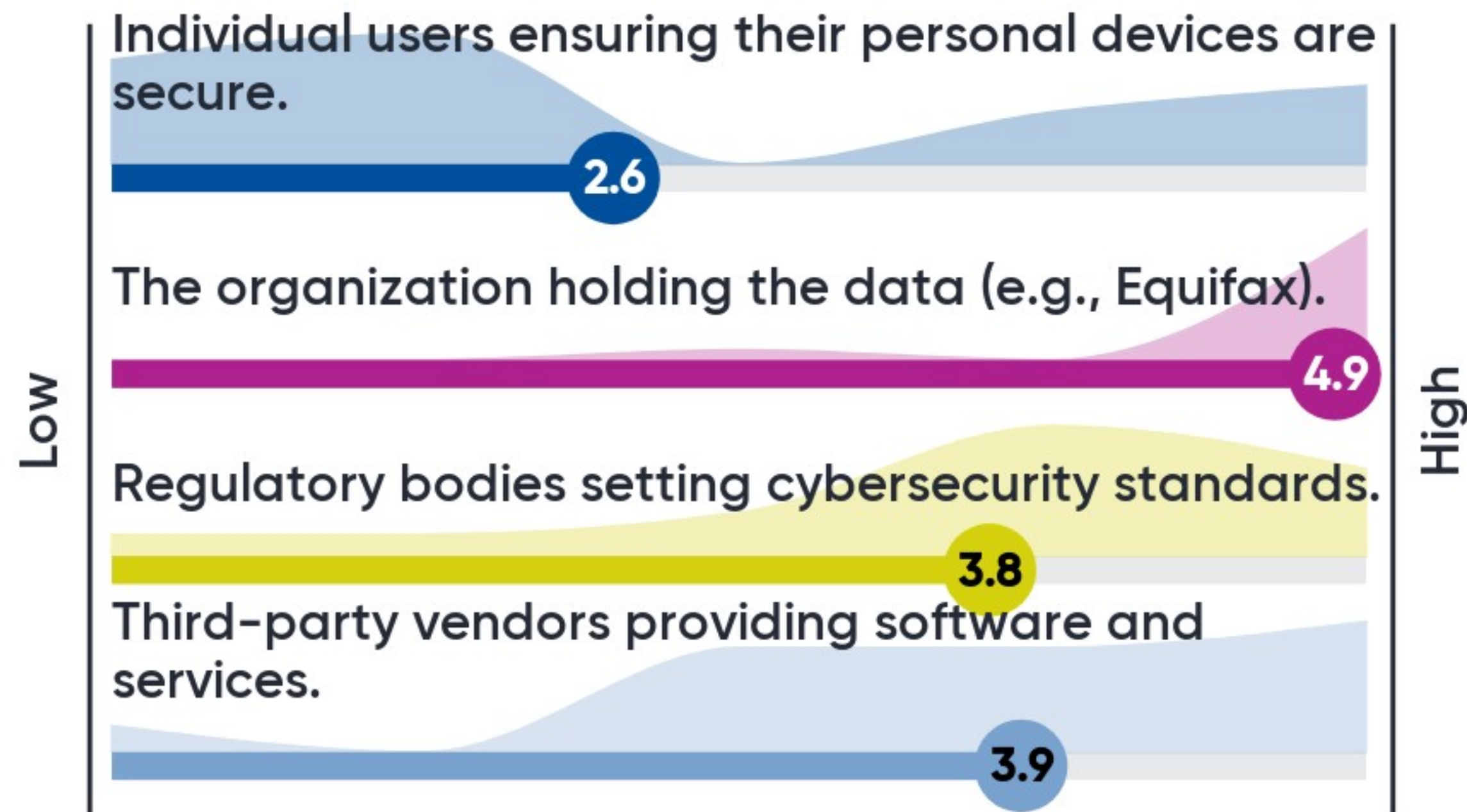
New York

Print, Email, Download, Info icons

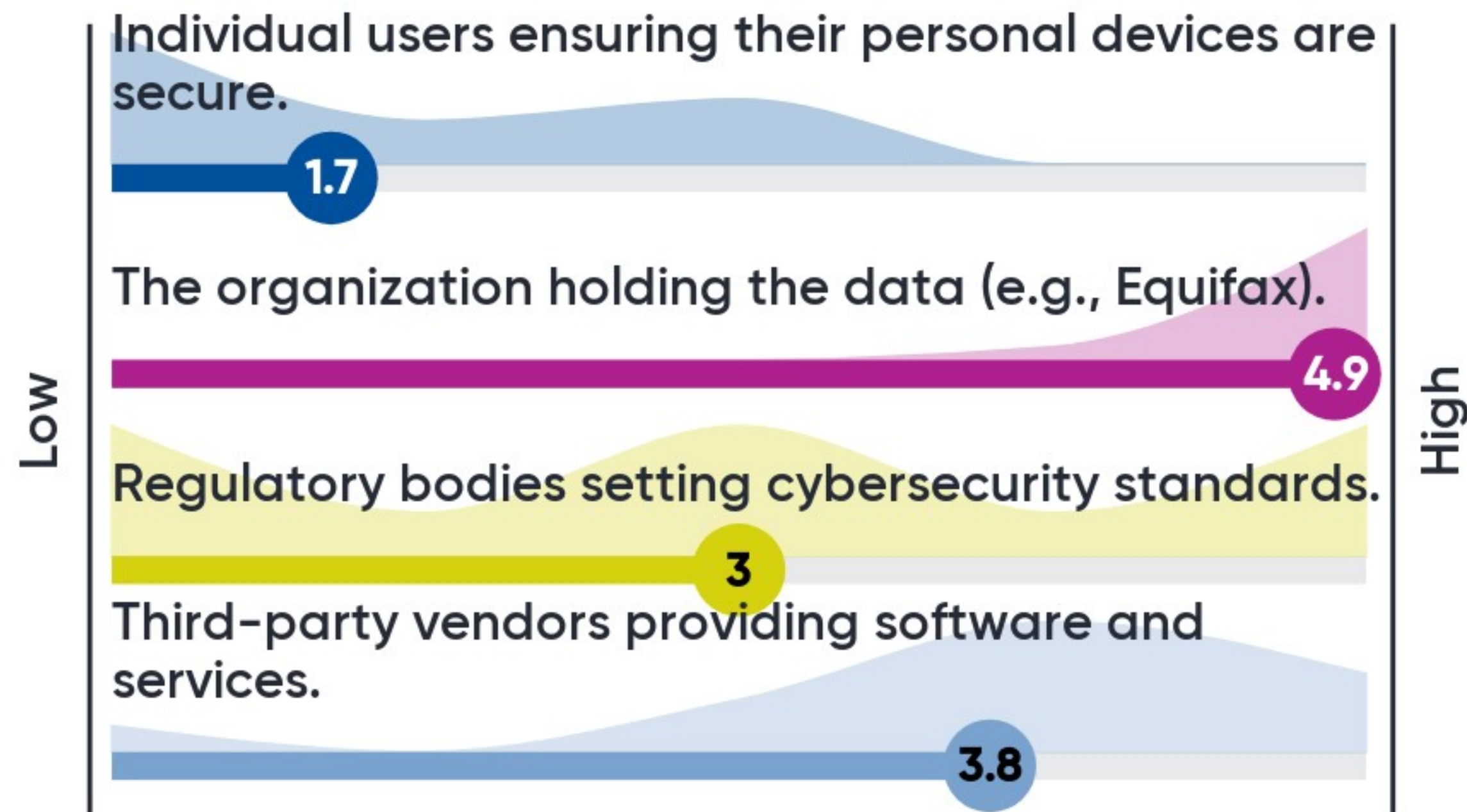
New York State has issued proposed regulations extending existing regulations requiring banks and other financial institutions to have in place a comprehensive cybersecurity program to credit reporting agencies. Governor Mario Cuomo announced that "The Equifax breach was a wakeup call and with this action New York is raising the bar for consumer protections that we hope will be replicated across the nation."



Based on the Equifax breach, rate the following entities based on their responsibility to ensure data security



Based on the Equifax breach, rate the following entities based on their accountability to ensure data security



Rank the following regulatory measures based on their potential effectiveness in preventing breaches like the Equifax incident:

- 1st** | Mandatory regular third-party security audits
- 2nd** | Stricter penalties for late breach disclosures
- 3rd** | Mandatory patching of known vulnerabilities within a specified timeframe
- 4th** | Regularly updated cybersecurity training for all employees



Part 2: Threats Posed by Cybersecurity Regulations

- Examination of how regulations can pose risks to businesses
- Discussion on determinants and implications of regulatory risks
- Analysis of the challenges organizations face in investing in cybersecurity due to regulatory risks
- Discussion on the mitigative and protective controls



Increasing cybersecurity investments in private sector firms

Lawrence A. Gordon, Martin P. Loeb , William Lucyshyn, Lei Zhou

Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 3–17,
<https://doi.org/10.1093/cybsec/tyv011>

Published: 27 November 2015 **Article history** ▼

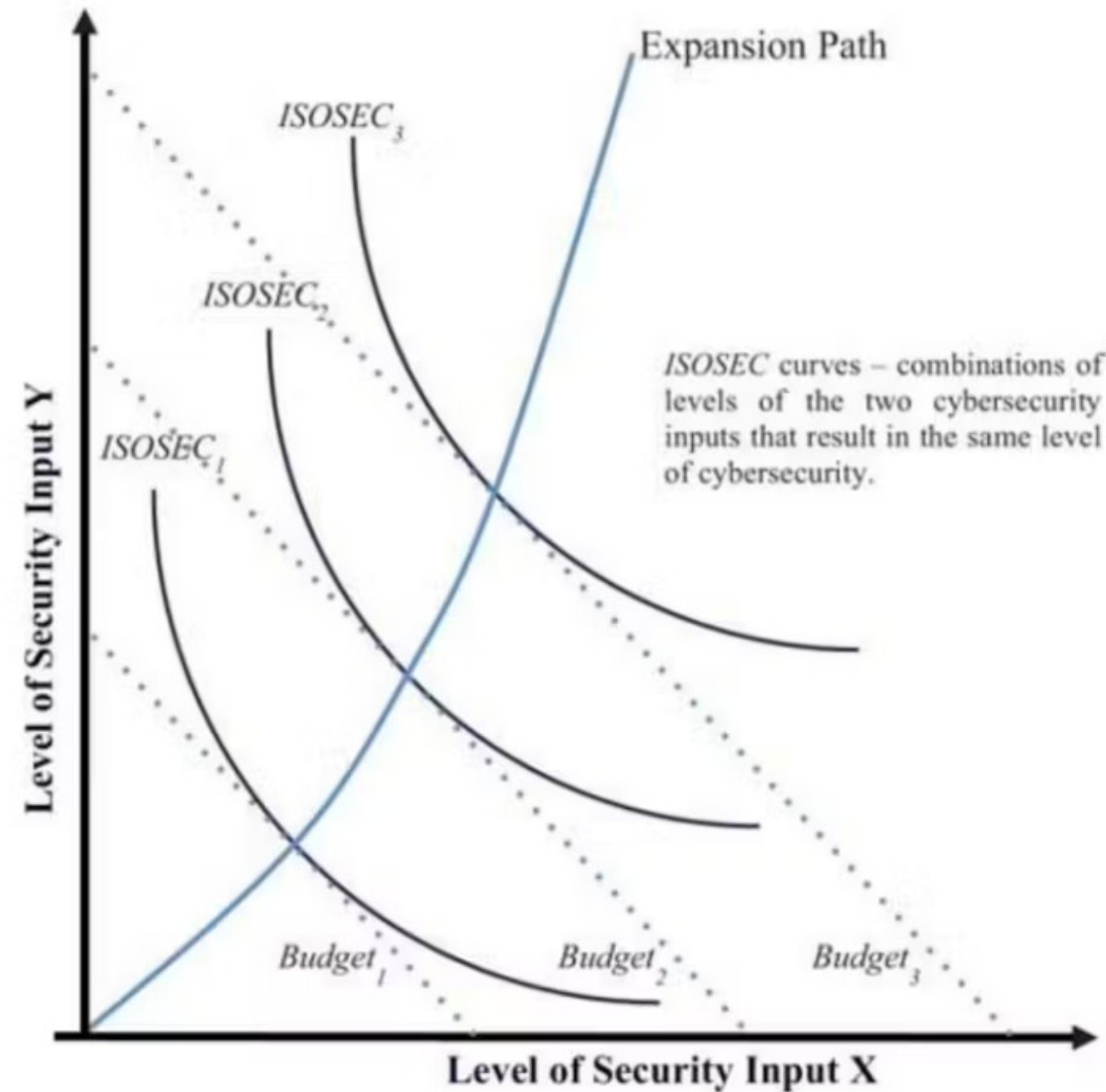
 PDF  Split View  Cite  Permissions  Share ▼

Abstract

The primary objective of this article is to develop an economics-based analytical framework for assessing the impact of government incentives/regulations designed to offset the tendency to underinvest in cybersecurity related activities by private sector firms. The analysis provided in the article shows that the potential for government incentives/regulations to increase cybersecurity investments by private sector firms is dependent on the following two fundamental issues: (i) whether or not firms are utilizing the optimal mix of inputs to cybersecurity, and (ii) whether or not firms are able, and willing, to increase their investments in cybersecurity activities. The implications of these findings are also discussed in this article, as well as a formal analysis of these implications. In addition, this article provides a discussion of existing actions by the US federal government that should be more effectively utilized before, or at least in conjunction with, considering new government incentives/regulations for increasing cybersecurity investments by private sector firms.

Issue Section: [research articles](#)

Cybersecurity expansion path



$$\{(x,y)|x \geq 0, y \geq 0, \text{ and } x+y=B\}$$

$$S_x = \frac{\partial S(x,y,v)}{\partial x} < 0, \tag{1}$$

$$S_y = \frac{\partial S(x,y,v)}{\partial y} < 0, \tag{2}$$

$$S_{xx} = \frac{\partial^2 S(x,y,v)}{\partial x^2} > 0, \tag{3}$$

$$S_{yy} = \frac{\partial^2 S(x,y,v)}{\partial y^2} > 0. \tag{4}$$

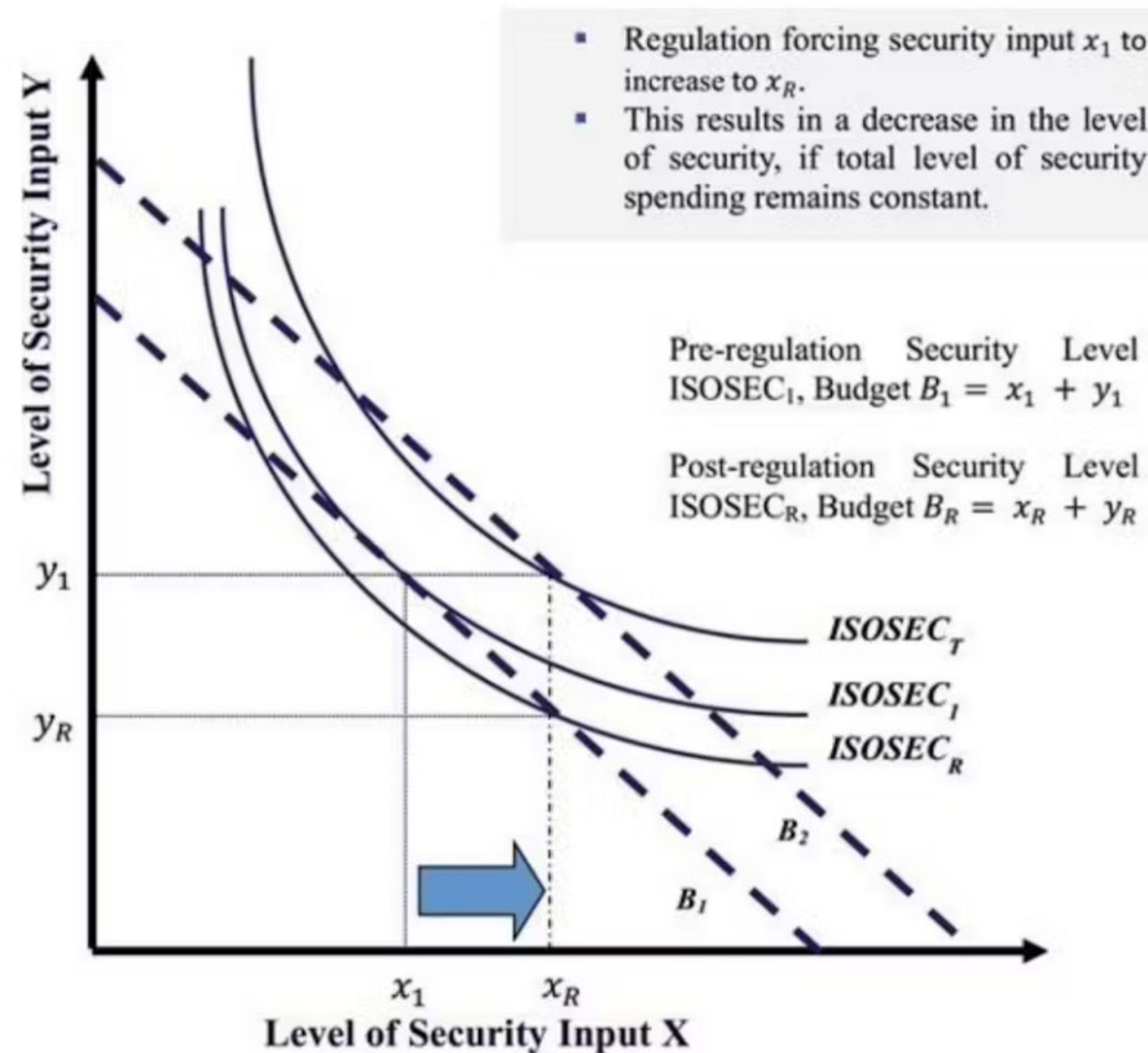
$$\max_{x,y} [v - S(x,y,v)] L - x - y$$

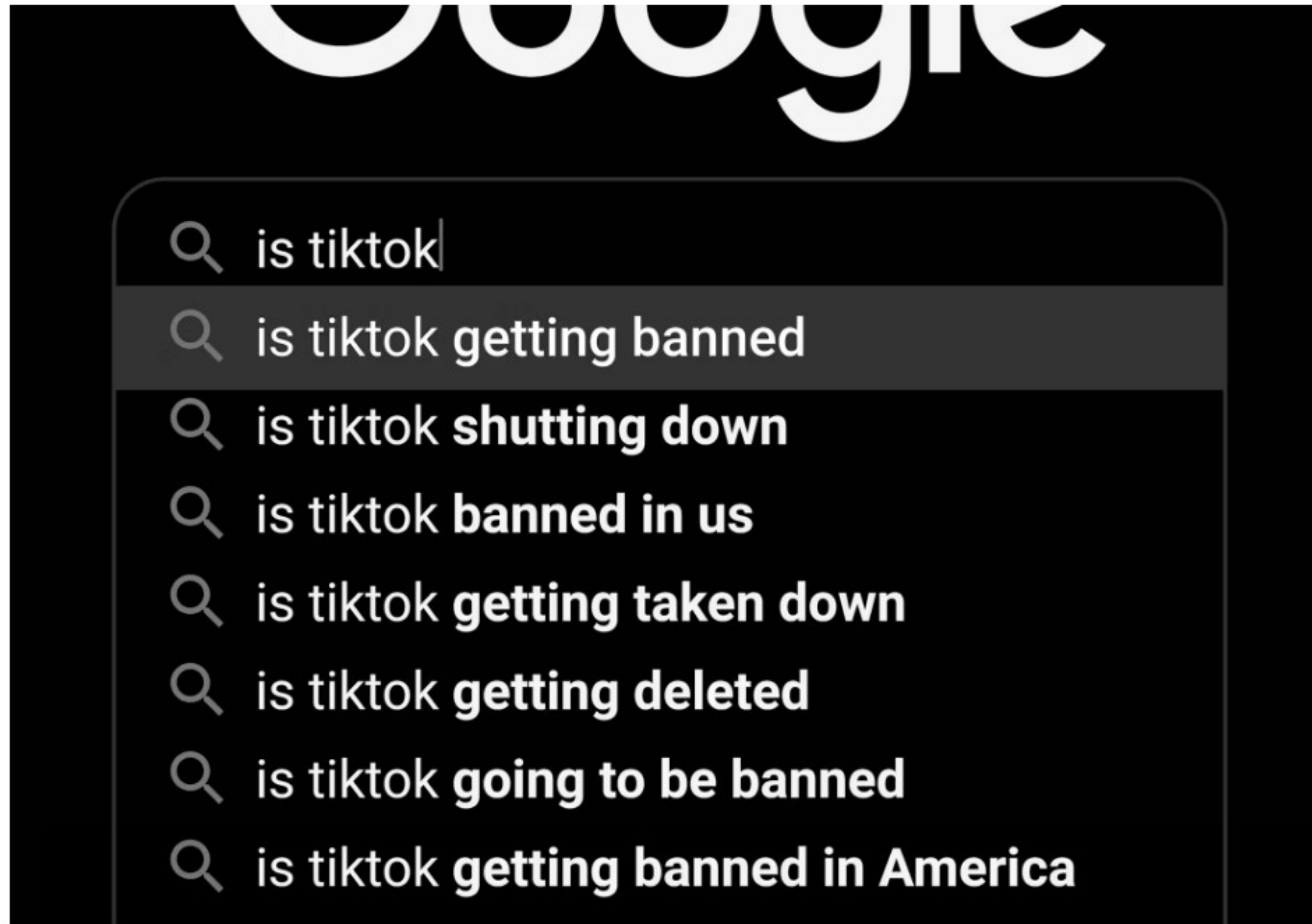
$$s.t. \quad x + y = B_1$$

$$x \geq x_R$$



Inappropriate regulatory strategies can cause firms to reduce their overall levels of cybersecurity.





Let's Help MarketingWithUs Inc.



Company Background:

MarketingWithUs Inc., an international marketing firm, relies heavily on TikTok for digital marketing campaigns. Serving clients across North America, Europe, and Asia, TikTok generates over 60% of annual revenue of MarketingWithUs. The company has invested heavily in cybersecurity infrastructure to protect client data and ensure compliance with various data protection regulations.

Situation:

In early 2024, the U.S. government passes the Protecting Americans from Foreign Adversary Controlled Applications Act, mandating ByteDance to sell TikTok or face a nationwide ban. The EU follows with its own set of stringent regulations, requiring foreign-owned apps to undergo rigorous data privacy audits. Asian countries, however, have not imposed restrictions on TikTok and this platform is still one of the most popular platforms in these countries.

History of the Ban:

The concern over TikTok's security began in 2020 when President Donald Trump issued an executive order to ban TikTok, citing national security threats. The administration claimed that TikTok, owned by Chinese company ByteDance, could share American users' data with the Chinese government. Legal challenges emerged, with TikTok and its users filing lawsuits against the ban, arguing it violated free speech rights and due process. Courts blocked the ban, ruling that the administration exceeded its authority. In 2023, the Biden administration continued to express concerns, leading to new legislation in 2024 aimed at addressing these security issues.

1. What are the influencing factors in this situation?

21 responses



2. What are the implications of this situation on MarketingWithUs?

18 responses



3. What preventive controls can MarketingWithUs implement to avoid undesired consequences?

18 responses



4. What mitigative controls can MarketingWithUs implement to minimize the impacts of this situation?

17 responses



Regulatory Risks

The risk that a change in laws and regulations (new or existing ones) will materially impact a security, business, sector, or market.



Regulatory Risks

≠



Cybersecurity Risks

≠



Compliance Risks





Regulatory Risks



Cybersecurity Risks

Threat Source

A complex, uncertain, and evolving regulatory landscape, compliance gaps, legal uncertainties, and failure to maintain industry standards.

Malicious actors, insider threats, and vulnerable devices or networks.

Focus

Complying with legal and regulatory requirements related to data privacy, consumer protection, and safety.

Protecting information systems, devices, networks, and user information from malicious actors seeking to exploit vulnerabilities.

Consequences

Fines, legal liabilities, increased costs of compliance, potential loss of business opportunities, significant changes in business models or operations, damage to reputation, etc.

Data breaches, loss of sensitive information, damage to critical infrastructure, loss of customer trust, financial losses, reputational damage, intellectual property theft, etc.

Mitigation

Establishment and monitoring of compliance programs, policies, and procedures that align with applicable laws, regulations, and industry standards.

Implementation of technical and organizational measures, as well as employee training and awareness programs.



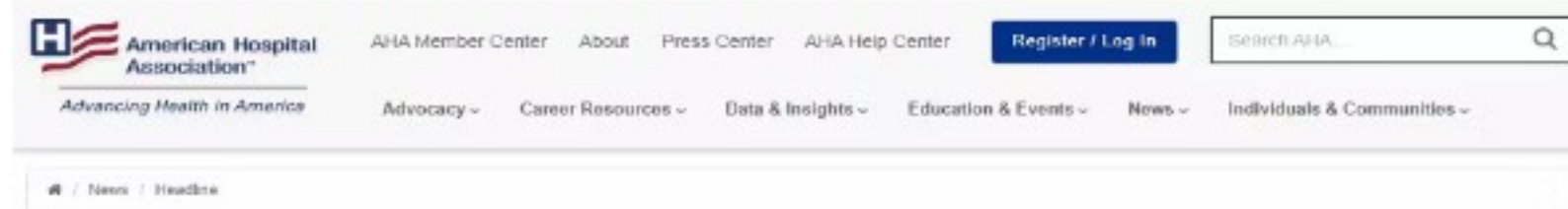
FDA reports potential cybersecurity risk with insulin pump system

© Sep 20, 2022 - 03:24 PM



The communications protocol for the Medtronic MiniMed 600 Series Insulin Pump System could allow an unauthorized person to access the pump to deliver too much or too little insulin, the Food and Drug Administration [alerted](#) users today. The agency said it is not aware of any reports related to this cybersecurity vulnerability. Medtronic recommends users take certain actions and [precautions](#) to protect their device from unauthorized access.

What is the type of this risk?



FDA reports potential cybersecurity risk with insulin pump system

© Sep 20, 2022 - 03:24 PM



The communications protocol for the Medtronic MiniMed 600 Series Insulin Pump System could allow an unauthorized person to access the pump to deliver too much or too little insulin, the Food and Drug Administration [alerted](#) users today. The agency said it is not aware of any reports related to this cybersecurity vulnerability. Medtronic recommends users take certain actions and [precautions](#) to protect their device from unauthorized access.

0

Regulatory Risk

8 ✓

Cybersecurity Risk

5

Compliance Risk

2



13



TECH · A.I.

ChatGPT accused of violating EU data privacy rules by Italian regulators

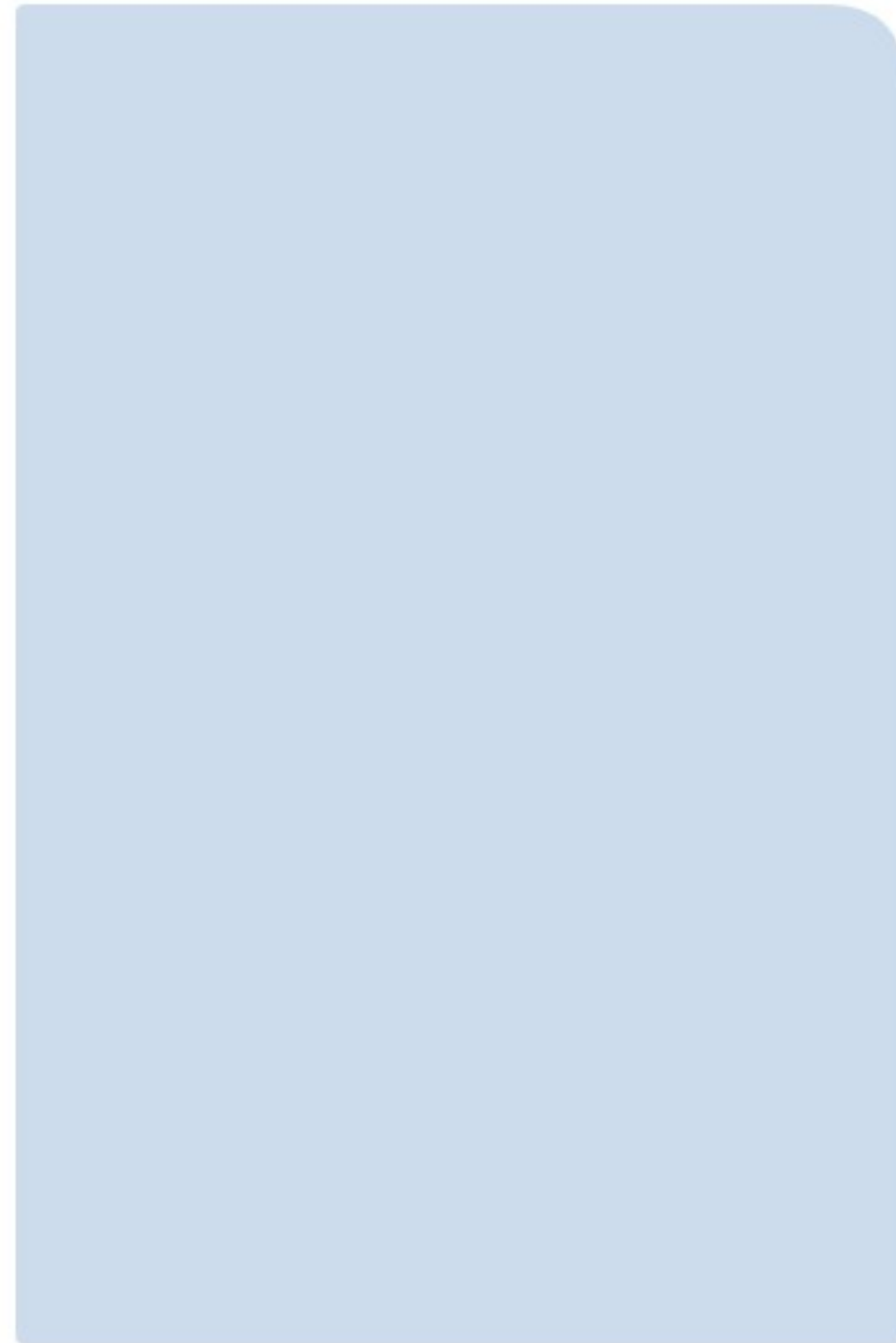
BY [KELVIN CHAN](#) AND [THE ASSOCIATED PRESS](#)
January 30, 2024 at 7:51 PM GMT+1



OpenAI CEO Sam Altman.
STEFAN WERMUTH/BLOOMBERG VIA GETTY IMAGES

What is the type of this risk?

9



Regulatory Risk

0



Cybersecurity Risk

6 ✓



Compliance Risk





Porsche to Halt Macan SUV Sales in Europe Over Regulatory Concerns

Category: [Cybersecurity Regulation](#), [Featured Post](#)
🕒 December 18, 2023



What is the type of this risk?

13 ✓



Regulatory Risk

2

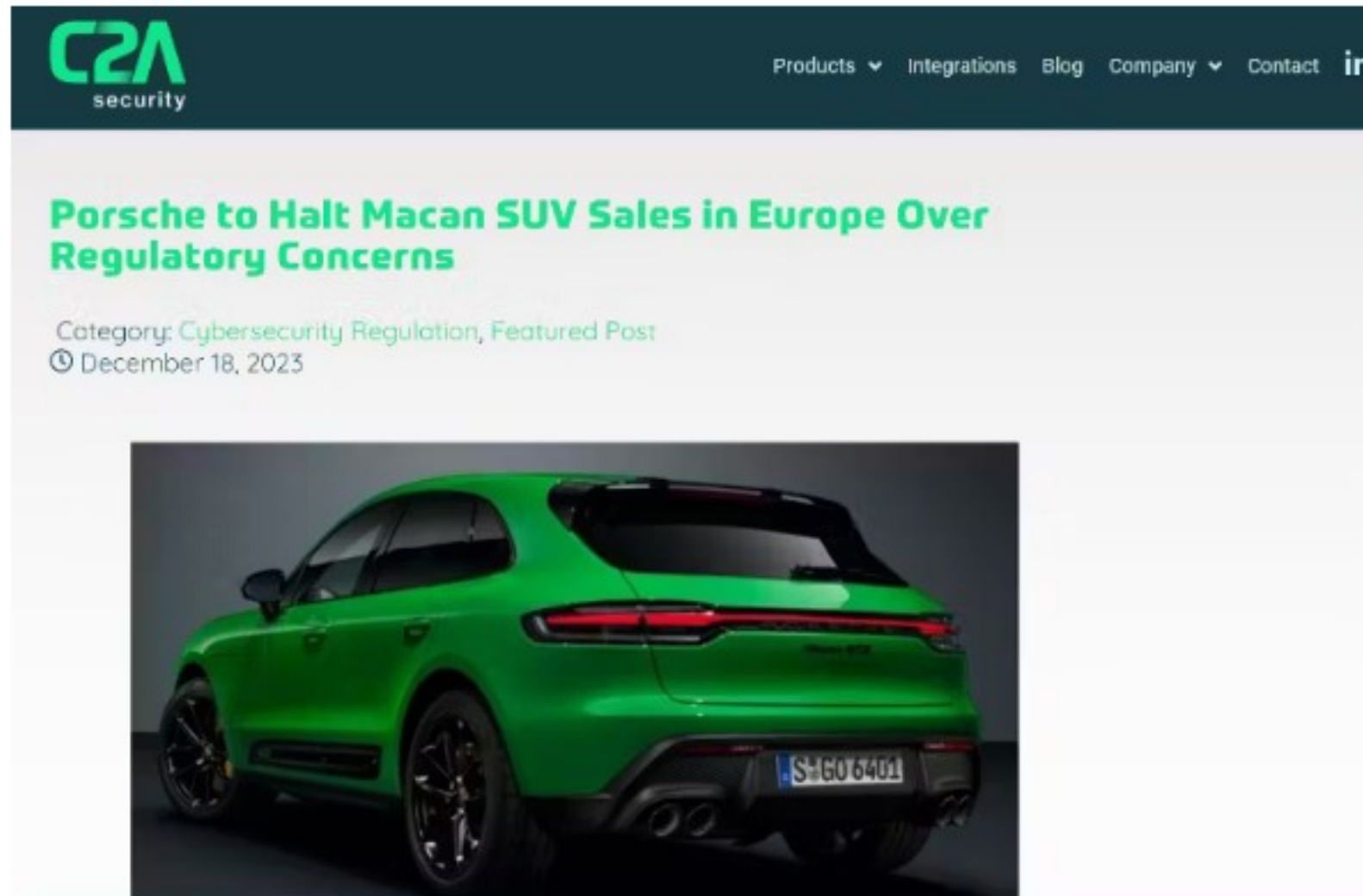


Cybersecurity Risk

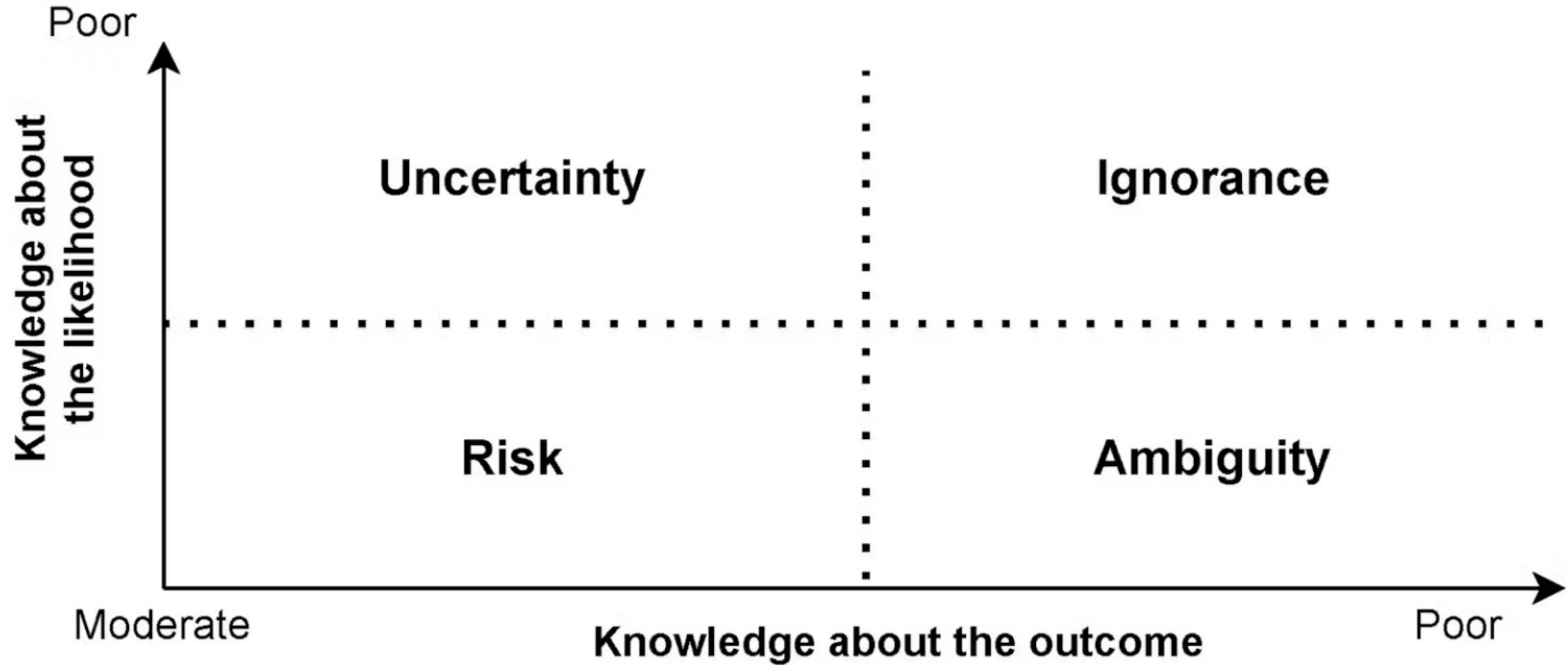
2



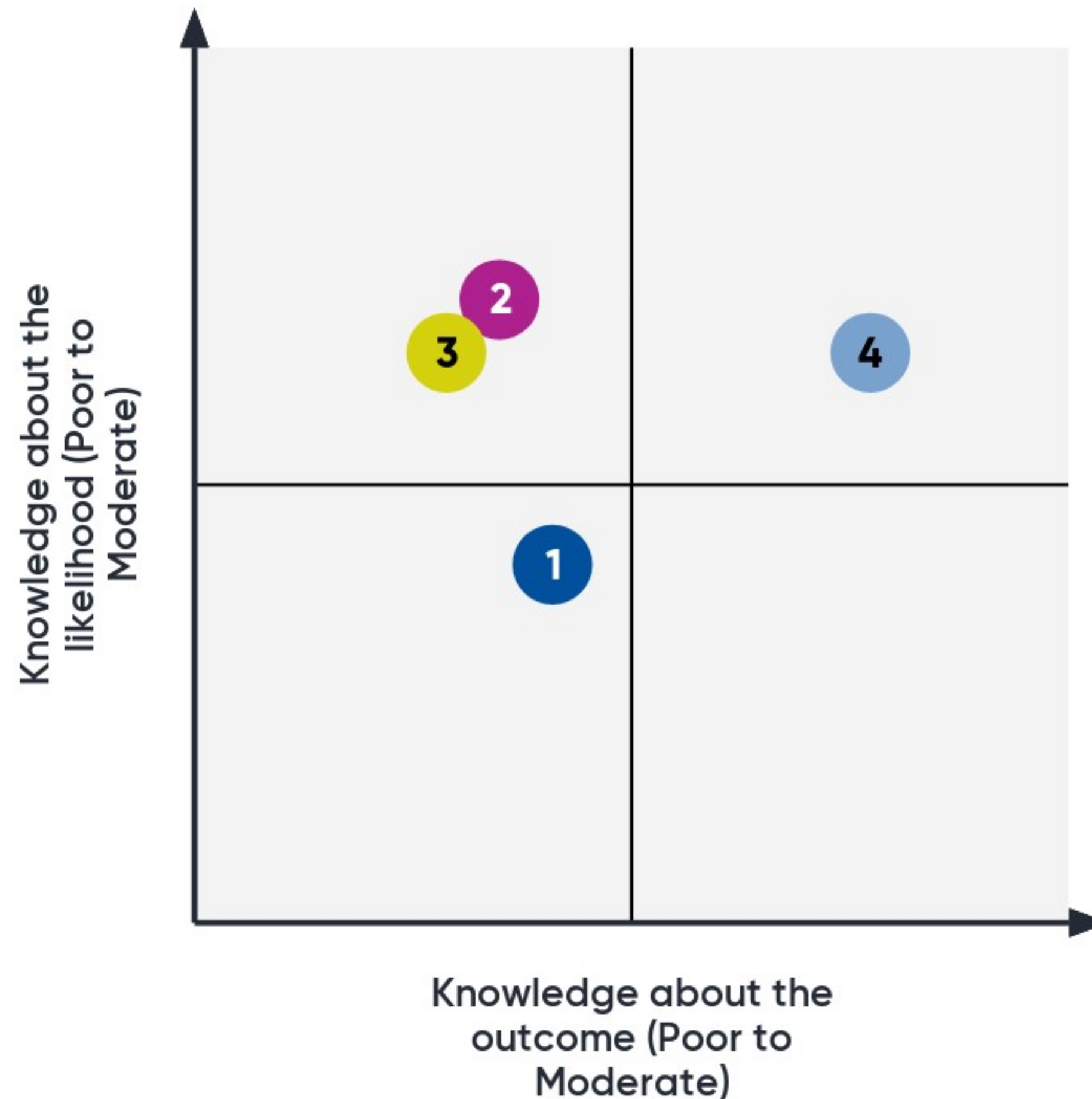
Compliance Risk



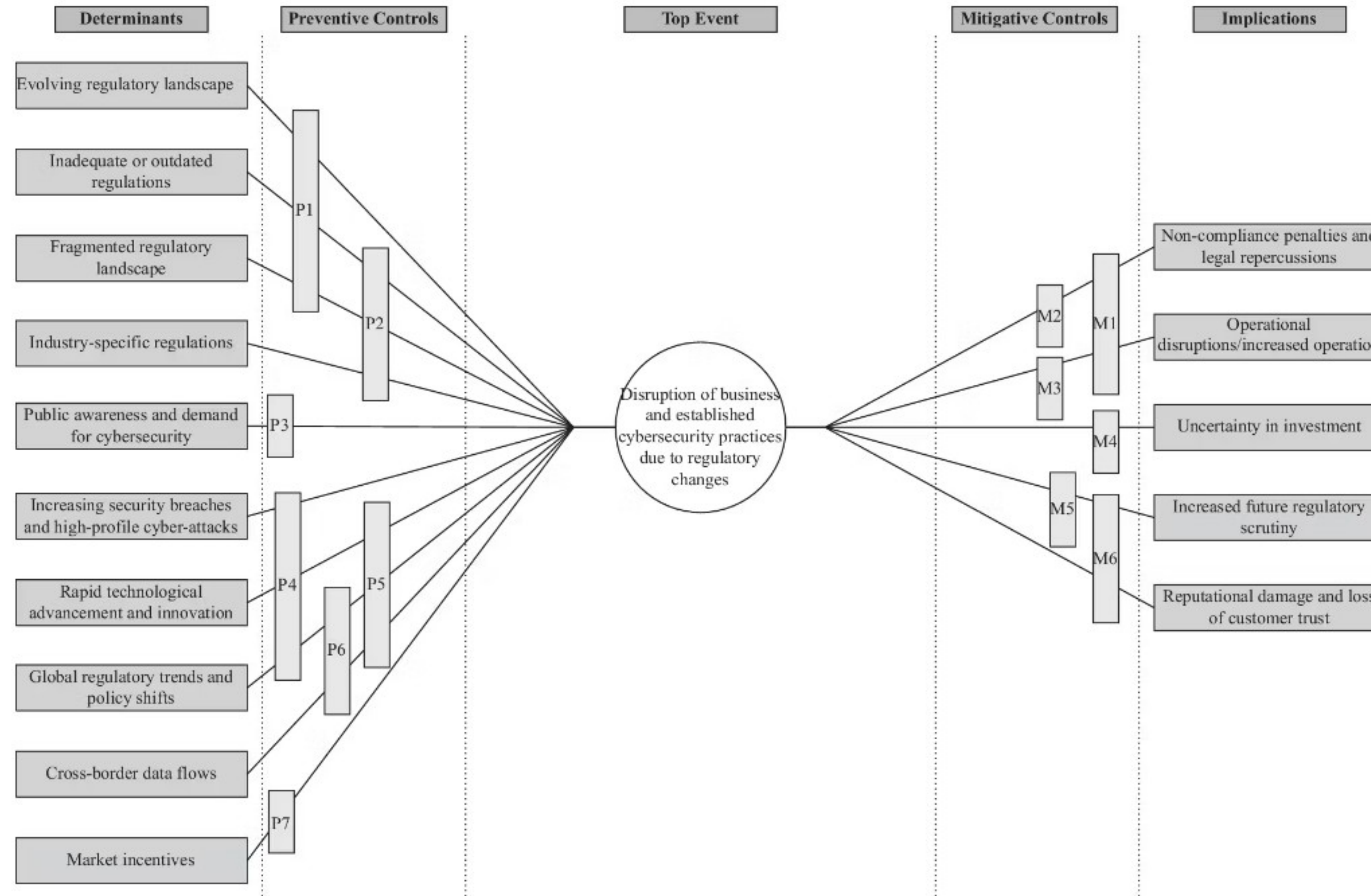
Risk != Uncertainty



Risk, Uncertainty, Ambiguity, and Ignorance



- 1 An organization is considering the adoption of a new, cutting-edge cybersecurity technology to protect against potential future threats.
- 2 A regulation states that organizations must ensure "adequate protection" of user data but does not specify what "adequate protection" entails.
- 3 There is growing concern about potential cybersecurity threats from quantum computing, but no specific regulations have been developed yet.
- 4 A new regulation requires all organizations to implement MFA by the end of the year. Historical data shows a clear reduction in breaches with MFA.



The bowtie diagram of the determinants and implications of regulatory risks associated with cybersecurity.



Determinants of Regulatory Risks



Evolving regulatory landscape



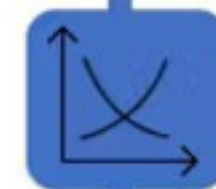
Fragmented regulatory environment



Increasing data breaches and high-profile cyber-attacks



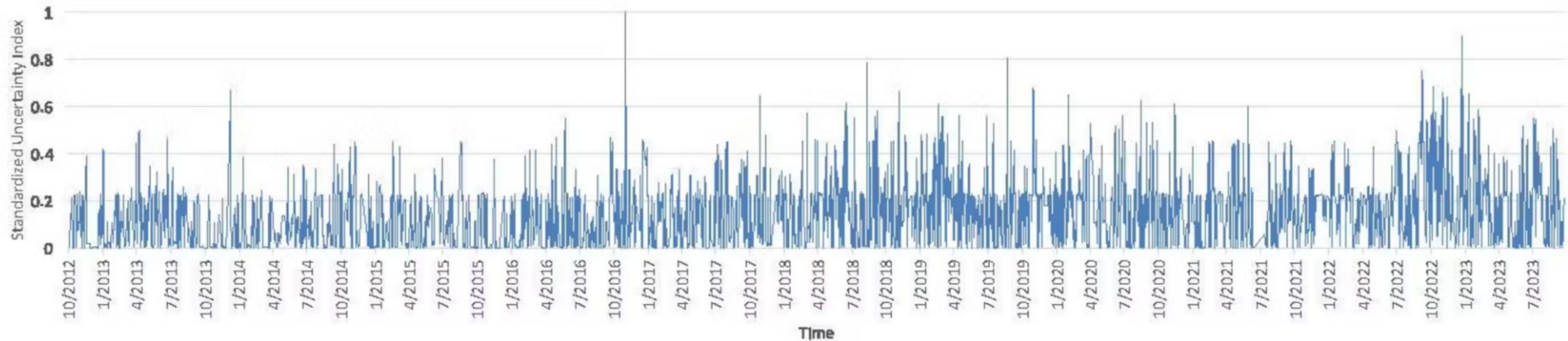
Rapid technological advancements and innovation



Market incentives

Regulatory Uncertainty

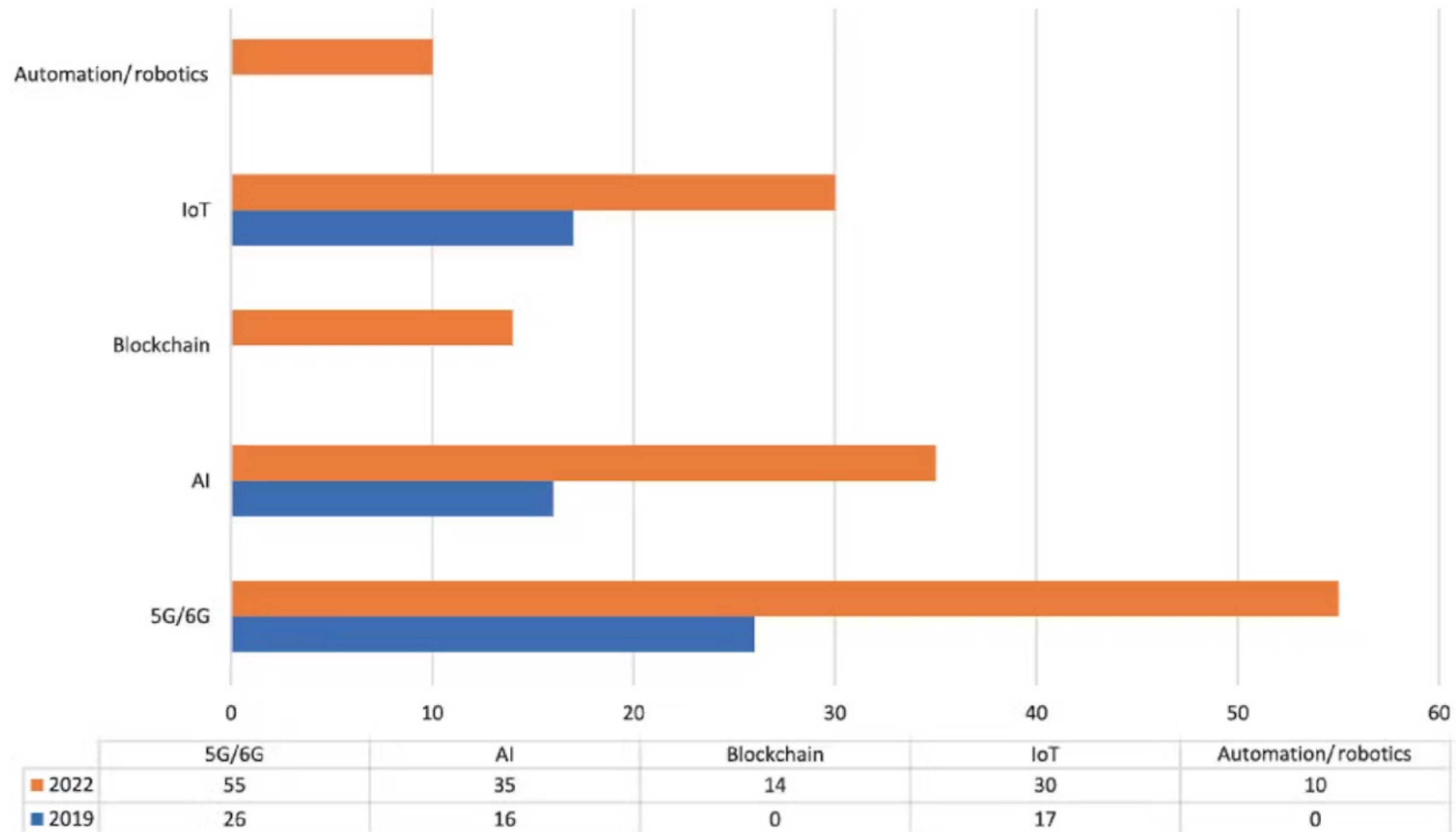
Regulatory uncertainty is defined as a condition of perceived inability of a business to predict the future state of the regulatory environment



“*The EC and 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. GDPR comes into force in May 2018, but there is plenty of work ahead for businesses and governments before that deadline.*”

25 NOV 2016 [\(Link\)](#)

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



Implications of Regulatory Risks



Noncompliance penalties



Operational disruptions/increased operation cost



Uncertainty in investment decisions



Increased future regulatory scrutiny



Reputational damage and loss of customer trust





Cybersecurity Investment under Regulatory Risks

Results from an Economic Model

[Home](#) > [International Cybersecurity Law Review](#) > Article

More than malware: unmasking the hidden risk of cybersecurity regulations

Original Paper | [Open access](#) | Published: 02 February 2024

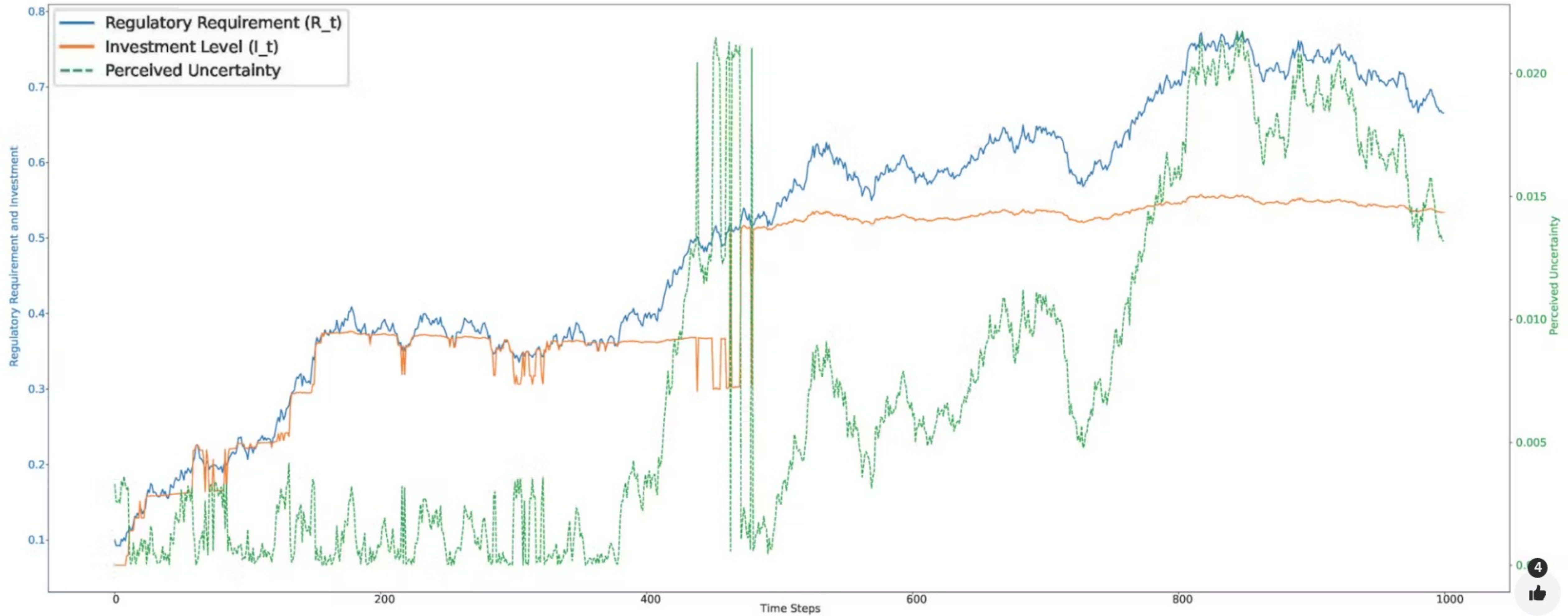
Volume 5, pages 169–212, (2024) [Cite this article](#)



Perceived Uncertainty

- Represents the firm's perception of regulatory uncertainty at time t
 - The rate at which actual regulatory requirements adjust towards the target level (Adaptation Rate)
 - The extent to which regulatory changes can deviate unexpectedly from the anticipated path (Deviation)
 - The penalties for misalignment between the firm's cybersecurity investment and the regulatory requirements (Penalties)

The changes in the firm's perception of regulatory uncertainty over time.



What would the Data Protection and Digital Information (No. 2) Bill do?

The [Data Protection and Digital Information \(No. 2\) Bill](#) [Bill 265 2022-23] was introduced in the House of Commons on 8 March 2023.

Much of the Bill is the same as the [Data Protection and Digital Information Bill](#) [Bill 143 2022-23] which was introduced in the Commons on 18 July 2022. The Bill was scheduled to have its second reading on 5 September 2022. A [Library Briefing on the Bill](#) (PDF) (31 August 2022) was published for the debate. However, in a [Business Statement](#) on 5 September 2022, the Government said that, following the election of Elizabeth Truss as Conservative Party leader, second reading would not take place. This was to allow Ministers to consider the Bill further. The Bill was withdrawn on 8 March 2023.

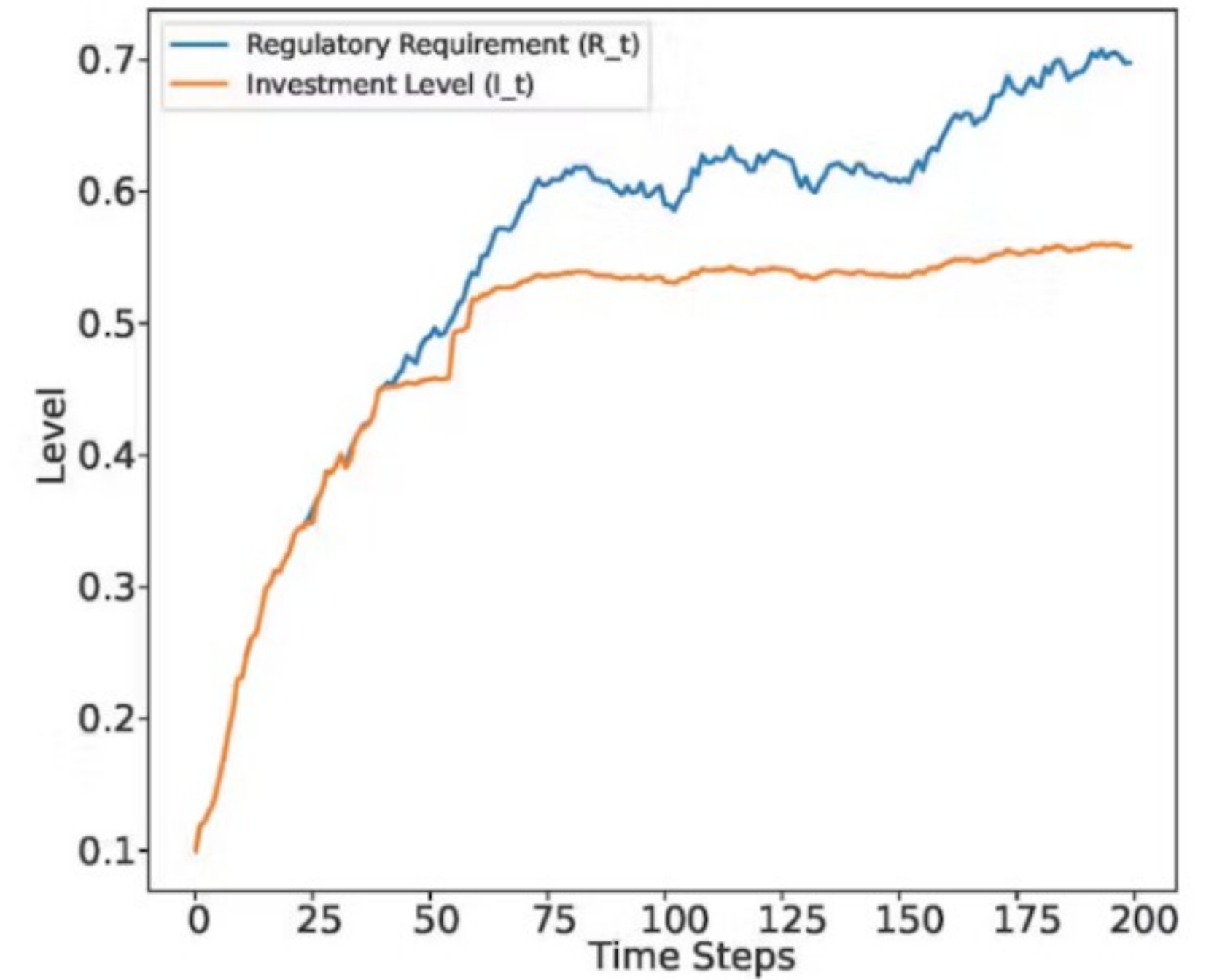
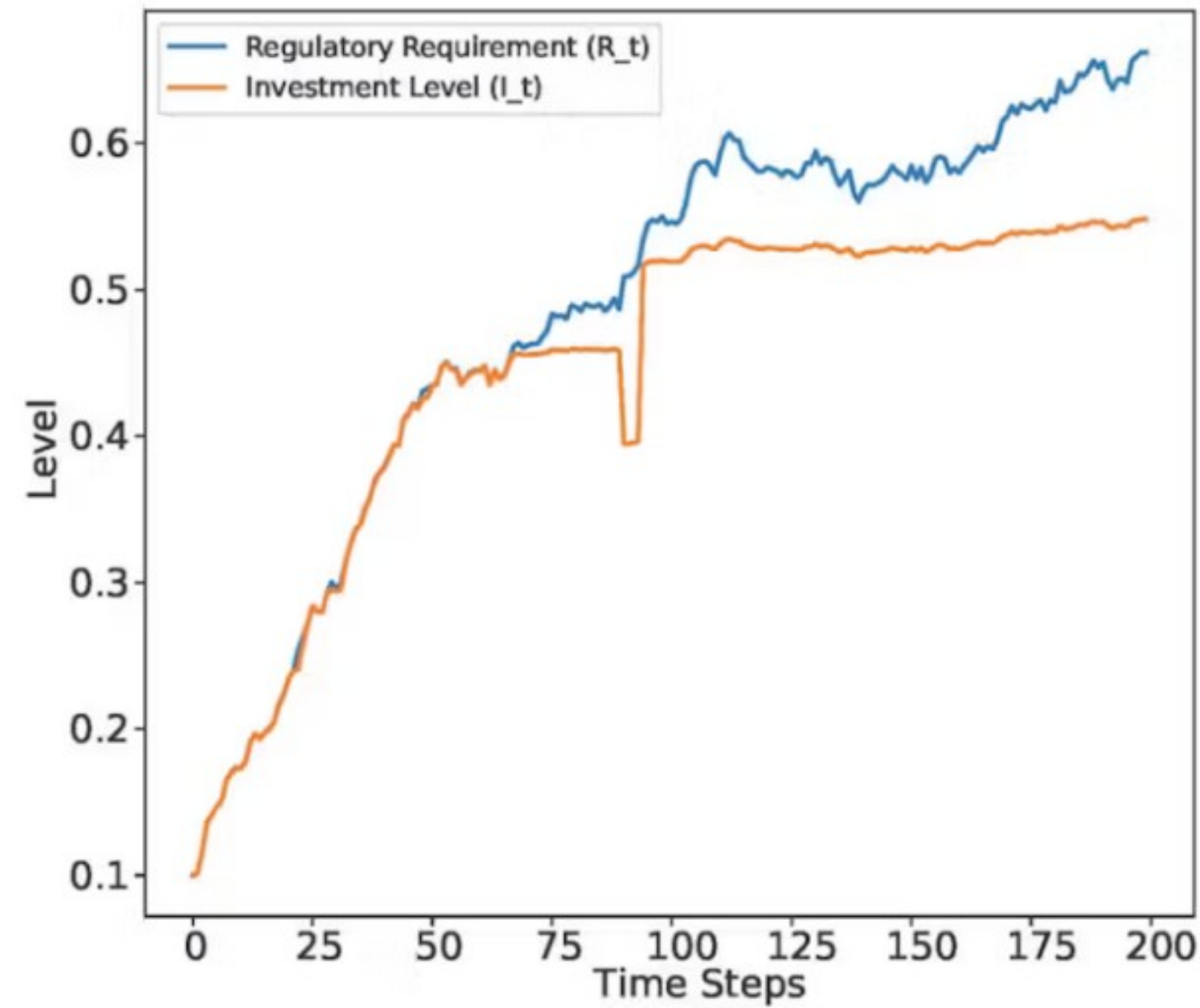
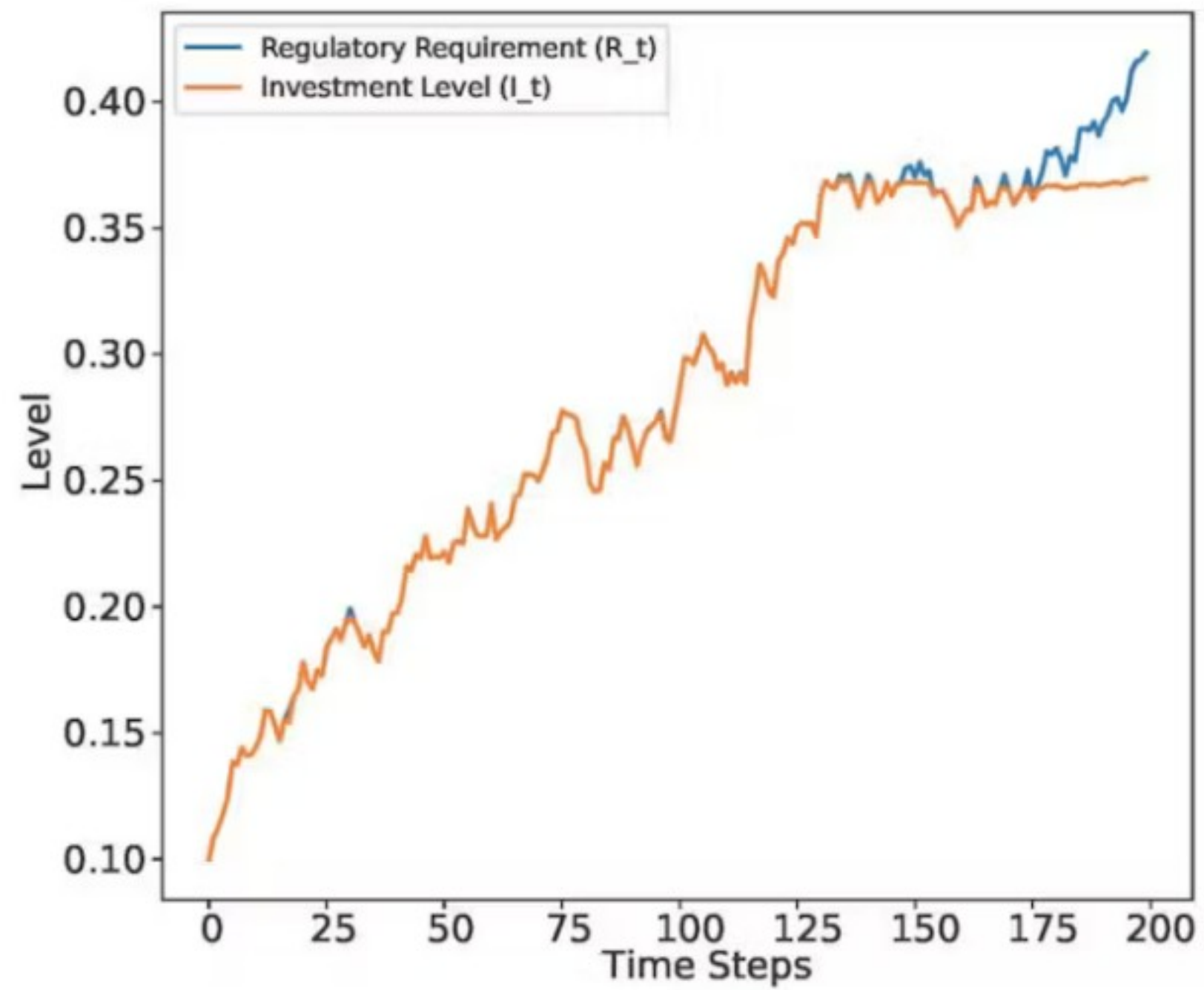
In a Written Ministerial Statement of 8 March 2023, Michelle Donelan, Secretary of State for Science, Innovation and Technology, [said the new Bill followed a detailed codesign process with industry, business, privacy and consumer groups](#). The Bill would seize the post-Brexit opportunity to “create a new UK data rights regime tailor-made for our needs”. It would reduce burdens on businesses and researchers and would boost the economy by £4.7 billion over the next decade. The Secretary of State [explained that changes had been made to the original Bill that would](#):

- reduce compliance costs in the sector and reduce the amount of paperwork that organisations need to complete to demonstrate compliance.
- reduce burdens by enabling businesses to continue to use their existing cross-border transfer mechanisms if they are already compliant.
- give organisations greater confidence about the circumstances in which they can progress personal data without consent.
- increase public and business confidence in AI technologies.

[HTTPS://COMMONSLIBRARY.PARLIAMENT.UK/RESEARCH-BRIEFINGS/CBP-9803/](https://commonslibrary.parliament.uk/research-briefings/cbp-9803/)

Regulatory adjustments, exemptions, and temporary relaxations can lead to decreased financial burdens for organizations in various sectors.

Adaptation Rate

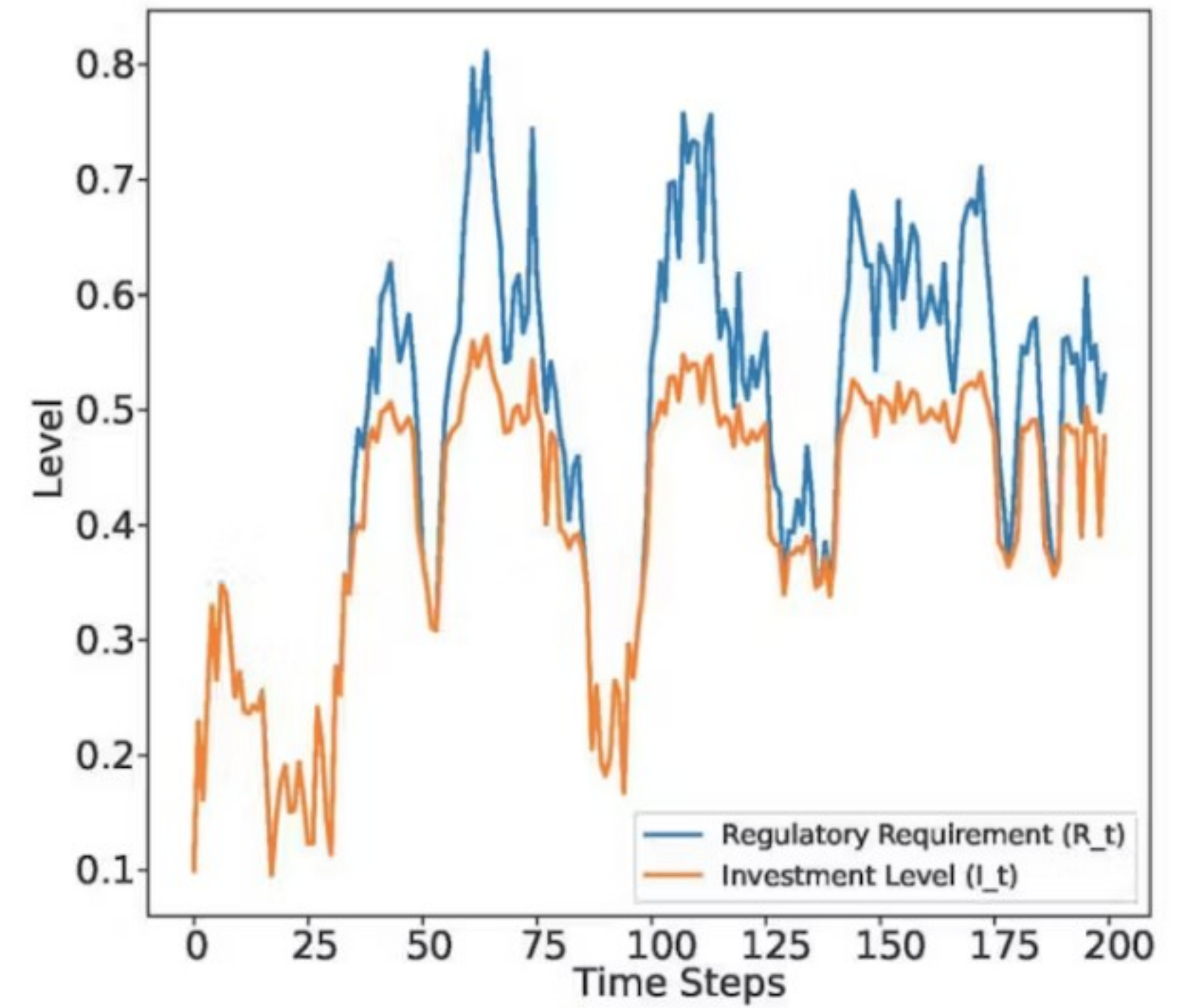
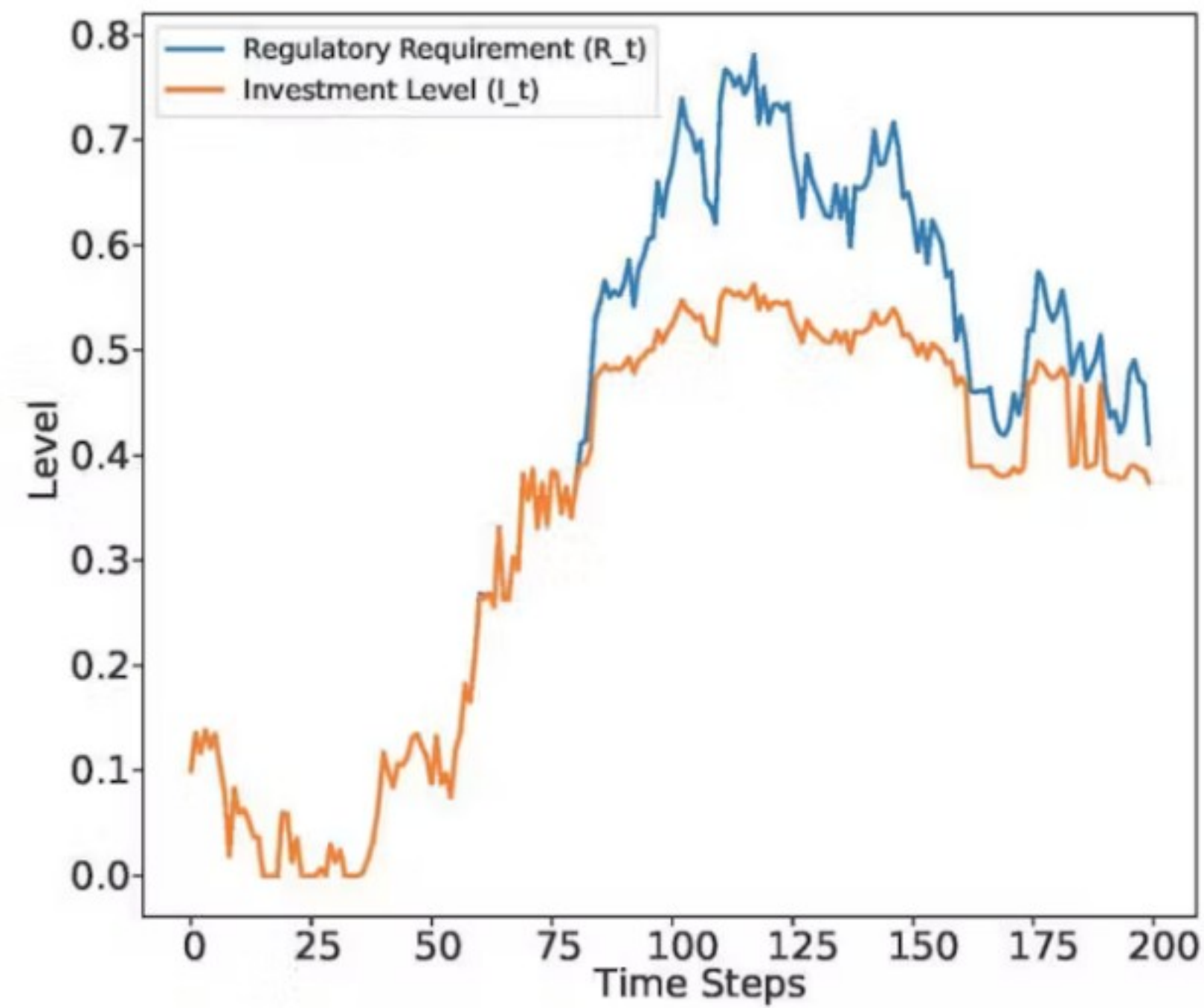
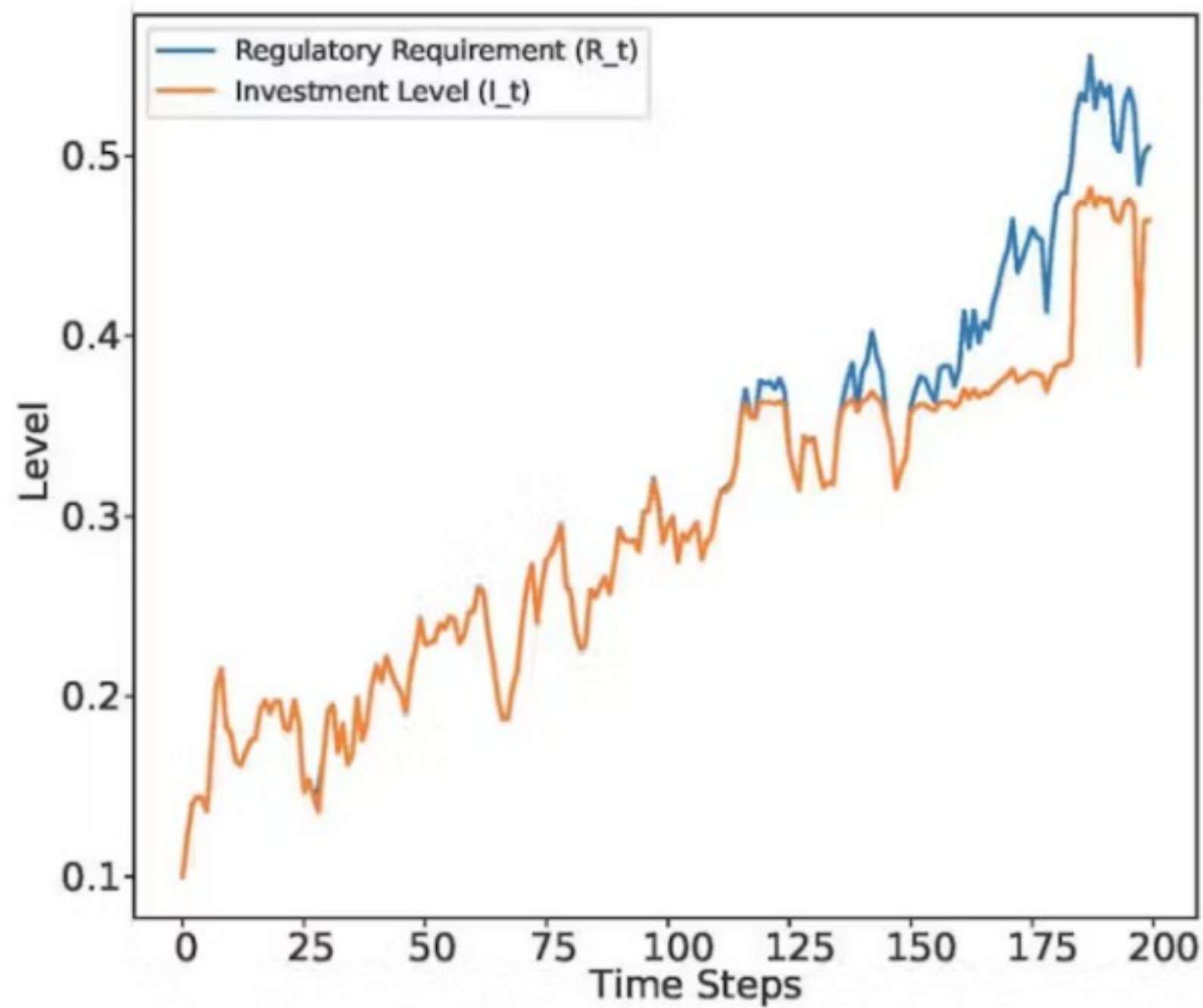


Low

High



Unexpected Deviations

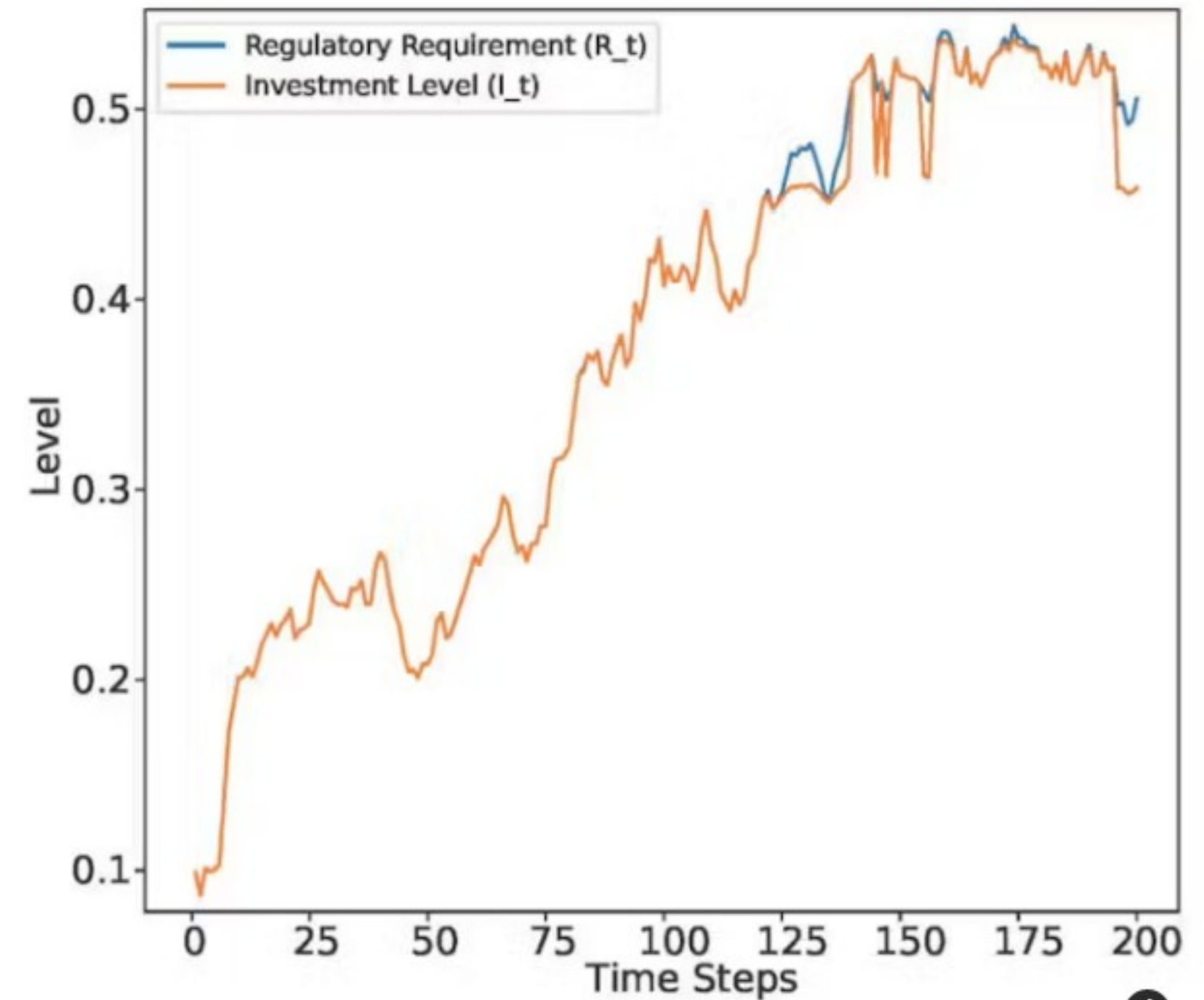
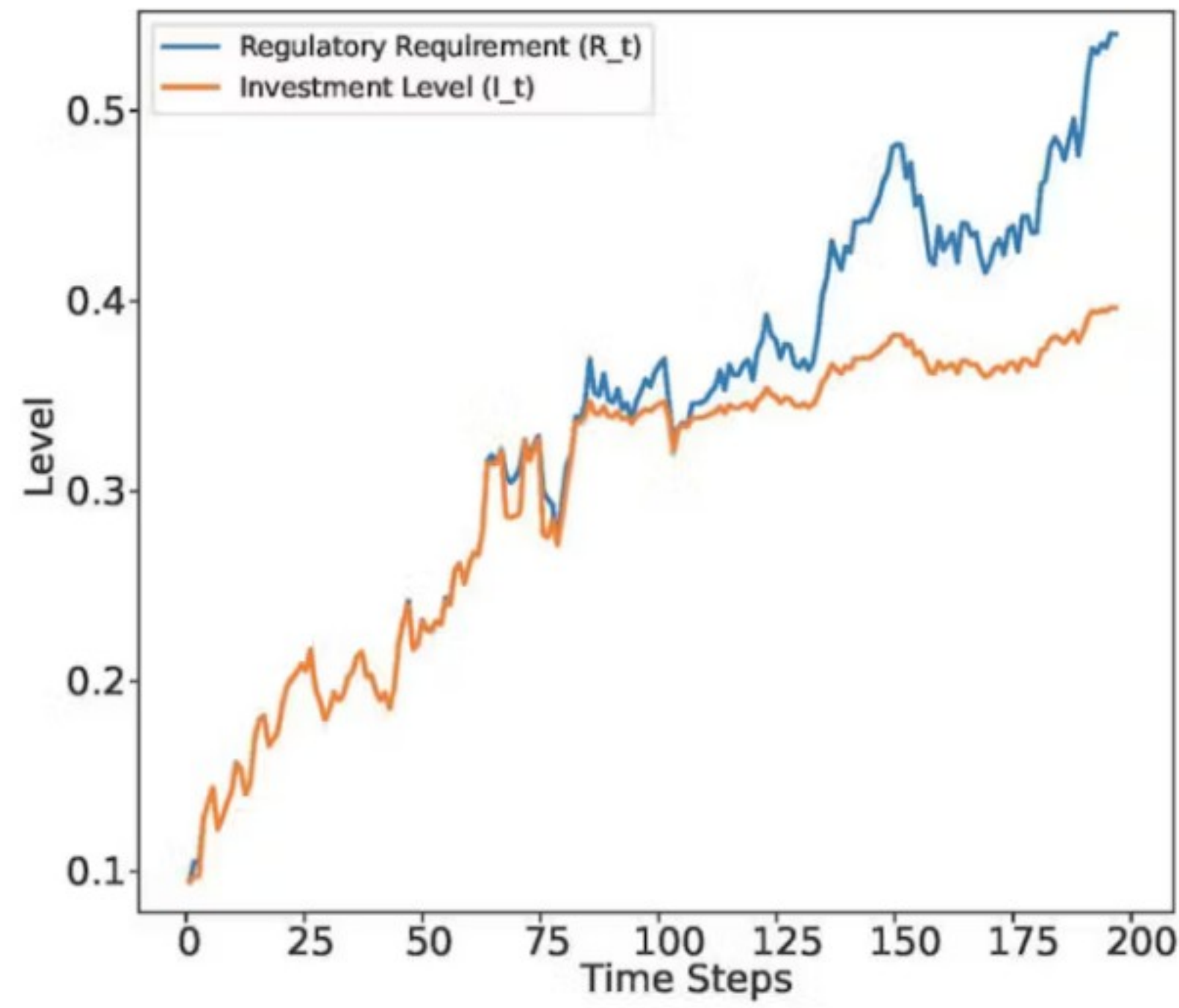
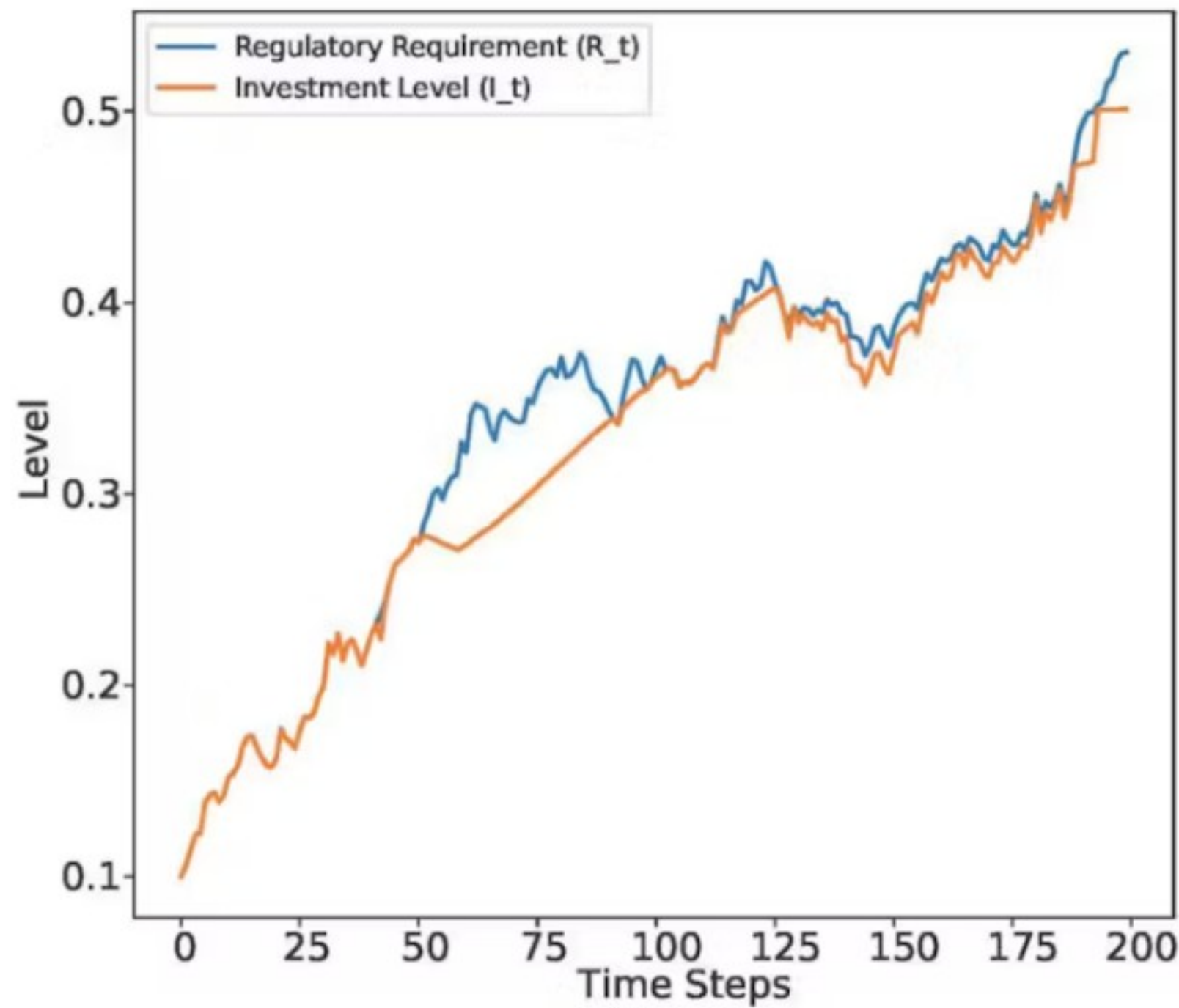


Low

High



Misalignment Penalties



Low

High



Wait-and-See Approach

Characteristics of the "Wait-and-See" Approach

- Deferred Decision-Making
- Minimizing Immediate Expenditures
- Reactive Posture

Reasons for Adopting "Wait-and-See"

- Regulatory Uncertainty
- Cost Concerns
- Resource Allocation
- Risk Aversion

What are potential consequences of the "Wait-and-See" approach?

21 responses





Best Practices for Managing Regulatory Risks Associated with Cybersecurity

Preventive controls



**REGULATORY HORIZON
SCANNING**



**FEEDBACK LOOPS WITH
REGULATORS AND
COLLABORATIVE POLICY
DEVELOPMENT**



**ADAPTIVE GOVERNANCE AND
DYNAMIC INVESTMENT
STRATEGIES**



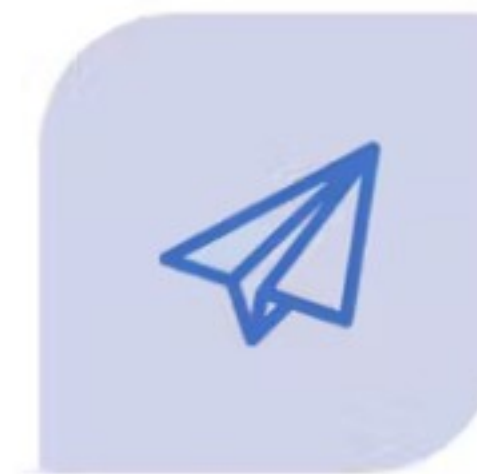
SCENARIO PLANNING



**CROSS-JURISDICTIONAL
REGULATORY MAPPING AND
ENGAGEMENT WITH LOCAL
REGULATORY BODIES**



**MARKET INCENTIVE
REALIGNMENT**



**PUBLIC RELATIONS AND
COMMUNICATION
STRATEGIES**

Mitigative control



**ACCOUNTABILITY
STRUCTURES**



**LEGAL EXPERTISE AND
COUNSEL**



**CONTINGENCY FUNDING
AND PLANNING**



**FINANCIAL STRATEGY
ADAPTATION**



**REGULATORY GAP
ANALYSIS**



**TRANSPARENCY AND
DISCLOSURE PROTOCOLS**

Final Remarks

- The necessity for robust cybersecurity regulations is undeniable.
- It is important to recognize the challenges and potential downsides they present.
- The balance between necessity and threats requires adaptable and risk-based approaches, not one-size-fits-all solutions
- It requires continuous dialogue and collaboration between regulatory bodies and industry stakeholders.
- Regulations need to promote enhanced cybersecurity practices not a tick-box culture.



03.07.2024

Thank you!

Mazaher Kianpour (mazaher.kianpour@ntnu.no)

SUMMER SCHOOL

CYBER IN
NORMANDY