



# The Cyber Defense Index

A benchmark of the digital security  
preparedness of enterprises  
across the threat landscapes of the  
world's top economies

**2022/23**

# Preface

The MIT Technology Review Insights Cyber Defense Index 2022/23 is research by MIT Technology Review Insights sponsored by Code42. The research was conducted through in-depth secondary research and analysis along with primary survey data, and interviews with global cybersecurity professionals, technology developers, analysts, and policymakers. It measures the extent to which the world's 20 largest and most digitally forward economies have adopted technology and digital practices to resist cyberattacks, and how well their governments and policy frameworks promote cybersecure digital transactions. The writer of the report was Ross O'Brien, the editors were Laurel Ruma, Michelle Brosnahan, and Jenn Webb. Nicola Crepaldi and Natasha Conteh were the producers.

## Acknowledgments

MIT Technology Review Insights would like to thank the following expert commentators for their time and insights:

**Magda Chelly**, senior cybersecurity expert, Founder of Women on Cyber, and Co-Founder of Responsible Cyber, Singapore

**Michael Henri Coden**, Co-Founder and Associate Director at Cybersecurity, MIT Sloan (CAMS), and Senior Advisor at BCG Platinion, United States

**Sadie Creese**, Director, Global Cyber Security Capacity Centre, and Professor of Cybersecurity, University of Oxford, United Kingdom

**Terry Cutler**, cybersecurity expert and Founder and CEO of Cyology Labs, Canada

**Alexander Klimburg**, Head of the Centre for Cybersecurity, World Economic Forum, Austria

**Manion Le Blanc**, Head of International Cyber Policy Sector, Security and Defence Policy Division, European External Action Service, Brussels

**Clay Lin**, Director, World Bank Information and Technology Solutions, and Chief Information Security Officer, United States

**Andrew W. Lo**, Professor of Finance, Director MIT Laboratory for Financial Engineering, United States

**Andrew Milroy**, Cybersecurity Advisor, Founder of Veqtor8, Singapore

**Taylor Reynolds**, Technology Policy Director, MIT Internet Policy Research Initiative, United States

**Denis Robitaille**, World Bank Group Vice President, Information and Technology Solutions, and WBG Chief Information Officer, United States

**Daniel Weitzner**, Founding Director, MIT Internet Policy Research Initiative, United States

**Yufei Wu**, Professor, Centre for Information and Communication Technology, University of Trinidad and Tobago, Republic of Trinidad and Tobago

# Contents

<b>Preface.....</b>	<b>2</b>	<b>03 The importance of securing critical infrastructure .....</b>	<b>13</b>
<b>Acknowledgments .....</b>	<b>2</b>	Threat landscape and risk tolerance.....	14
<b>Methodology: The Cyber Defense Index 2022/23 .....</b>	<b>4</b>	<b>04 Practice and policy: Cybersecurity resources ensure a safer digital economy .....</b>	<b>15</b>
<b>01 Executive summary .....</b>	<b>6</b>	Learning to live with insecurity .....	15
<b>02 Introduction.....</b>	<b>8</b>	Trust no one .....	17
The landscape of global cybersecurity.....	8	<b>05 Organizational capacity: The business end of cybersecurity.....</b>	<b>18</b>
Innovations benefit both sides .....	8	<b>06 Policy commitment: The root of the solution.....</b>	<b>21</b>
The rise of machines.....	9	<b>07 Conclusion.....</b>	<b>23</b>
The pandemic effect .....	9		
Motivation matters .....	9		
Cybersecurity's cognitive dissonance.....	9		
Cyber Defense Index overall scores .....	10		
Geopolitics has strong sway .....	10		
Not all giants are leaders .....	11		
Struggles at the trailhead, and a crowded summit.....	11		
Code42: Reimagining enterprise data protection for insider risk.....	12		

# Methodology:

## The Cyber Defense Index 2022/23

The MIT Technology Review Insights Cyber Defense Index (CDI) is the first annual comparative ranking of the world's 20 largest and most digitally forward economies on their preparation against, and response and recovery from, cybersecurity threat. It assesses 20 of the world's major economies (members of the Group of Twenty intergovernmental forum [G20], excluding Russia, and including Poland) based on how well their institutions have adopted technology and digital practices to be resilient against cyberattacks, and how well governments and policy frameworks promote cybersecure digital transactions.

This research focus informed our evaluation and selection of 31 distinct sets of country-level data to comprise the 16 indicators of the index. In addition to the Cyber Defense Index Survey (2022), the data came from a wide range of publicly available sources, including the following:

- United Nations E-Government Knowledgebase
- Data Center Map
- Worldometer
- Global Change Data Lab
- Global Cybersecurity Index (GCI) of the UN
- International Telecommunication Union (ITU)
- United Nations Conference on Trade and Development (UNCTAD)
- The World Bank Group
- Oxford Insights

Secondary source data, including global digital technology adoption statistics, policy, and regulatory data, was sourced from external international monitoring institutions. These benchmarks were drawn from quantitative measures of a country's cybersecurity resources and capabilities. The secondary sources were converted into scores.

The indicator data was subjected to trend analysis, informed by primary research interviews with global cybersecurity professionals, technology developers, analysts, and policymakers. This was complemented by a consultative peer-review process with cybersecurity technology analysts.

### Survey methodology



MIT Technology Review Insights conducted a global survey of 1,000 senior executives (with an equal number from each country ranked in the index) with cybersecurity responsibilities for their respective organizations. The data provides an assessment of operating conditions for maintaining cybersecure environments. About 43% of respondents were CIOs, CTOs, or chief security officers.

Survey data was gathered in a way similar to business confidence indexes, which incorporate the views of professionals on their own (or their country's) relative performance. Respondents rated the effectiveness of technology adoption, policy, and regulation formation, and their own cybersecurity activities, as well as their technology development priorities over the next two to three years. The survey response data was converted into scores, where each country's responses were ranked according to their variance from the mean of the global average.

## The four pillars of the CDI

The index's 16 individual indicators were developed based on the data, and were filtered through cross-comparative external data and the confidence levels of industry participants. Weightings were assigned to show the indicator's relative importance to an effective cybersecurity posture. Individual indicators are grouped into four pillars that quantify a category of overall cybersecurity.

The pillars organize findings under four categories to help clarify the state of cyber defense in each of the 20 countries. The four pillars of the CDI are as follows:

**Pillar 1: Critical Infrastructure.** This pillar examines how well each country is served by robust and secure digital and telecommunications networks and computing resources that underpin primary economic activity. The indicators measure:

- Information and communication technology infrastructure capacity.
- Colocation data centers per million population.
- Secure internet servers per million population in 2020.
- Perceived robustness, and the relative security of critical infrastructure assets in each country.
- Critical infrastructure comprehensiveness, for the relative strength of national cybersecurity capabilities such as public services, critical infrastructure, financial services, 5G mobile infrastructure, and IoT/edge security.

*This pillar represents 30% of the CDI score.*

**Pillar 2: Cybersecurity resources.** This pillar evaluates technological and legal enforcement for cybersecurity assets in each country. These mechanisms prevent improper access and enforce practices. The indicators include:

- A score for each country based on its cybersecurity commitments.
- A measure for each country based on its data privacy and protection legislation status.
- Evaluation of the relative strengths of several organizational cybersecurity capabilities: data and analytics, AI, blockchain and digital ledger technologies, antiphishing response resources, and anti-ransomware response resources.

*This pillar represents 35% of the CDI score.*

**Pillar 3: Organizational capacity.** This pillar measures the cybersecurity maturity and digital experience of businesses and other institutions in each country. The indicators include:

- The effectiveness of digital participation between governments and the private sector, and the engagement of citizens in policy and decision making.
- A score for government AI technology readiness, based on its preparedness to use AI in the delivery of public services.
- Measuring the extent to which organizations are familiar with AI, and the degree to which cybersecurity is a strategic asset.
- An assessment of how industry standard cybersecurity practices are integrated in overall operations.

*This pillar represents 20% of the CDI score.*

**Pillar 4: Policy commitment.** This pillar appraises government effectiveness and quality of cybersecurity regulation, and the robustness and completeness of regulation, to gauge regulatory efforts promoting resilient cybersecurity practices. The indicators measure:

- Regulatory quality, scoring each country based on its quality of primary laws and legislation.
- Government effectiveness based on its quality of public services, civil service, policy formulation, policy implementation, and credibility of commitment to cybersecurity.
- A measure of business perceptions of government regulatory robustness.
- An evaluation of cybersecurity framework comprehensiveness, drawn from responses to comparative evaluations of regulatory measures such as: data privacy laws and regulations, data sovereignty regulations, public-private national security cooperation, and government involvement in global CERT efforts.

*This pillar represents 15% of the CDI score.*

These pillars are constructed to comprehensively evaluate the world's largest and most digitally forward economies in their progress toward preparing against, responding to, and recovering from cybersecurity threats. It measures how well these institutions have adopted technology and digital practices to be resilient against cyberattacks, and how well governments and policy frameworks promote cybersecure digital transactions.

# 01 Executive summary



Today's cybersecurity landscape can impart a sense of precariousness—there appears to be no end to the deluge of malware or criminal hacking. Rich and poor countries seem equally vulnerable, for different reasons.

Mature digital economies have money and talent to mount cyber defense, but these riches make them attractive. Developing countries are vulnerable due to lack of resources.

Hope lies in the fact that most nations monitor and manage cyberattack events, invest in infrastructure resilience, and cultivate flexible and iterative policy. Moreover, the inevitability of cyberthreats is prompting a rethink among cybersecurity professionals, to shift investment away from protection of digital assets, toward business continuity and data and service recovery.

Brisk technology adoption favors bad actors, thanks to the broadening attack surface of a world blanketed by mobile and IoT devices. Cyberattackers are motivated, skilled, and enjoy safe harbors in powerful states. Ransomware is a global threat to data and financial security. The pandemic's assault on worker norms draws scrutiny to planning and security protocols.

The MIT Technology Review Insights "Cyber Defense Index (CDI) 2022/23" is the first annual comparative ranking of the world's 20 largest and most digitally forward

economies on their preparation against, and response and recovery from, cybersecurity threat. It measures how economies use technology and digital practices against cyberattacks, and how policy promotes secure digital transactions.

The top findings of the CDI are as follows:

- Australia's first-place CDI score reflects efforts to make robust digital infrastructure widely available.** The Australian government strives to use digital tools and regulations to safeguard personal data and digital transactions. It committed to overhauling cybersecurity laws, pledging to shelve a previous roadmap. The importance of this was underscored by a hack of Optus, its second-largest mobile carrier, in which 2.8 million records were stolen. Its business leaders have high confidence in the government's cybersecurity stance.
- The Netherlands, in second place, is a nerve center for pan-European cybersecurity.** The Hague is a digital security hub. It is home to the Global Forum for Cyber Expertise, and the cybersecurity operational headquarters for Europol and NATO. The Netherlands ranks high for cybersecurity resources, with comprehensive approaches to data privacy and well-coordinated domestic agencies. It benefits from the EU's consumer-friendly digital policy, reflected in the 2018 General Data Protection Regulation (GDPR) framework.

- **Geopolitics means high CDI rankings for South Korea (third place) and Poland (sixth place).** Both economies border some of the world's most notorious safe harbors for cyber malfeasance—Russia and North Korea—which implicitly and explicitly support bad actors. This forces increased vigilance.
- **China leads on several indicators (second place in organizational capacity), but overall ranks in the bottom 10.** China's advantages lie in its digital workers and the strategic importance its business leaders place on cybersecurity. Its overall score is bruised by its poorly regarded infrastructure resilience and difficult policy environment.
- **Germany scored in the bottom quarter of the CDI, lowest of any EU nation.** Germany has one of Europe's lowest e-participation scores, due to low adoption in its small-to-medium-sized enterprises (SMEs), its slow digital service delivery, and its dearth of talent.
- **India struggles, despite a digitally forward government and the world's largest IT-enabled service sectors.** This powerful tech force lacks critical infrastructure, has poor national digital economy adoption, and weak cybersecurity regulation. Despite cyberattacks and calls for cybersecurity laws and a dedicated ministry, India has opted out.
- **The EU benefits from its cybersecurity posture, expressed by the 2018 GDPR.** This preserves the rights of digital consumers and is a model for the top half of CDI-ranked countries. This posture affects Poland and France (sixth and eighth) and the UK and Switzerland (seventh and 10th), as well as non-EU European countries with large pan-European footprints in the financial service and insurance sectors.
- **Developing countries struggle for ground, due to lack of knowledge and resources.** Countries among the CDI top 10 score closely together—less than one point divides first-place Australia and ninth-place Japan. Those near the bottom score more diversely. The differentiator is access to investment. Cybersecurity advances lean on 5G technology, which requires upgrades to critical infrastructure. Where 5G is already in place, there is built-in access to innovation.



The inevitability of cyberthreats is prompting a rethink among cybersecurity professionals, to shift investment away from protection of digital assets, toward business continuity and data and service recovery.



# 02

## Introduction



### The landscape of global cybersecurity

The term “cybersecurity” (socioeconomic, geopolitical, or industrial) refers to a global war of attrition. Protagonists tally multitudes of dollars and hours spent on preventative tools and software. The opponents hatch multitudes of phishing attempts, drain dollars through hacks, and carry out ransomware attacks. The sector is rapidly expanding. Analyst firm Gartner estimates information security and risk-management investments will exceed \$172 billion in 2022, and grow 11% annually to \$267.3 billion by 2026—more than twice the growth of overall IT spending<sup>1</sup>.

Much of this spending is on sophisticated and increasingly mature cyber-defense tools. However, growing technology adoption could favor bad actors, thanks to the broadening attack surface of a world rapidly installing IoT devices and the amount of money at stake, says Michael Coden, associate director, MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. “The bad actors are ahead—and nimbler—particularly in use of AI. They have an asymmetric warfare advantage—they only must find one weakness out of millions, while we need to keep all the millions equally secure.”

### Innovations benefit both sides

The cost and time commitment required by cybersecurity contributes to the lack of breakthrough innovations, Coden says. However, radical shifts are emerging that may pay

dividends, such as database-oriented operating systems (DBOS). “The most revolutionary advance in computing in the last ten to 20 years,” Coden says. This relational database is “built on bare metal,” he says, and can roll back to a preattack state; a restoration can take five minutes, instead of days or weeks. “The next generation of operating systems will be cyber resilient inherently,” Coden says.

Innovative tools and methodologies are also at the root of gains by cybercriminals. Ransomware is a fast-growing threat to data and global financial security. These attacks—which block access to data until fees are paid—can be well-orchestrated customer experiences. Cybersecurity firm Bitdefender noted the U.S. Treasury identified \$5.2 billion in payments resulting from Solar Winds, Colonial Pipeline, and other high-profile ransomware attackers in 2021<sup>2</sup>. Cybersecurity Ventures estimates within a decade, these attacks will cost businesses up to \$265 billion worldwide<sup>3</sup>. This growing threat is a political agenda item: U.S. president Joe Biden, who has sounded warnings on ransomware (largely, state-backed actions from Russia or North Korea), signed a March 2022 executive order for responsible development of cryptocurrencies (payment method of choice for ransomware perpetrators) and authorized a Digital Assets Framework by the National Economic Council and National Security advisor, Jake Sullivan.<sup>4</sup>



## The rise of machines

Autonomous software and the growth of intelligent sensors, monitors, and controllers in an enterprise IT environment increases vulnerability. The maxim that human error causes most successful cyber incursions still holds, but machine-on-machine attacks, such as API incursions, constitute 57% of all data breaches in retail, according to Imperva Research.<sup>5</sup> Machines are a new and growing front for cyber defense, increasing the need for machine identity management.

## The pandemic effect

The impact of covid-19 on the digital economy provided succor for cybercriminals: it accelerated the shift to remote work, fueled e-commerce growth, and sowed uncertainty among business decision makers. The

pandemic's assault on operational norms makes it difficult for workers to maintain course, and draws scrutiny to their knowledge of strategic planning and security protocols. Lingering indecision exposes users to cybercriminals, and massively expands the threat landscape. Cybersecurity company ESET estimated the number of brute-force remote desktop protocol (RDP) attacks grew nearly 900% in 2021, at a cost of \$288 billion (of which Spain absorbed the largest share, \$51 billion, or 18% of the total). ESET blames the number of the world's office workers primarily logging in from home in 2021.<sup>6</sup>

## Motivation matters

The ability of business and government leaders to address threats is complicated by competing priorities, says Clay Lin, Director, World Bank Information and Technology Solutions, Security and Risk Management at World Bank Information and Technology Solutions. "The global threat landscape presents two adversaries: one motivated by profit, the other not. With for-profit actors, law enforcement can follow the money—even if ransomware is paid by Bitcoin, it must leave a trail behind," he explains. This is how the U.S. Department of Justice recovered some of the payments from the Colonial Pipeline incident.

More difficult, Lin continues, are criminals not motivated by profit—often, state-sponsored actors seeking political influence or publicity for diplomatic pressure. "This is not going to go away, because cyberattacks have become a very effective way to sow instability," he says. Lindy Cameron, chief executive of the UK's National Cyber Security Centre, warns Russia's ongoing attack on Ukraine is causing unprecedented expansion of cyberattacks globally.<sup>7</sup>

## Cybersecurity's cognitive dissonance

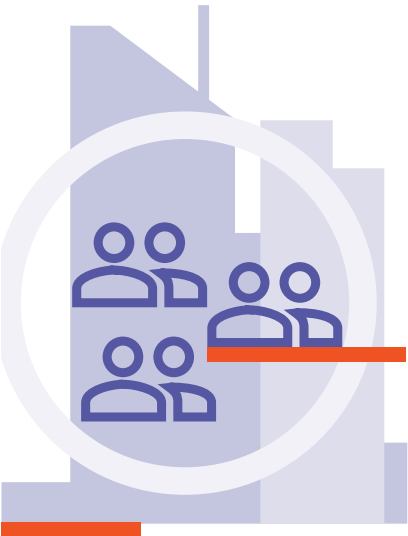
Collectively, trends shaping today's cybersecurity landscape mean no economy is immune to cyberattacks. Nor is there evidence mature digital economies can reduce their volume and velocity. The growing number of ransomware attempts, hacks, and incursions on critical infrastructure suggests the opposite is true.

Yet things are not so bleak: most nations, certainly those evaluated in the CDI, constantly monitor and manage cyberattack events, actively increase resilience in critical infrastructure, and cultivate flexible policy to iteratively adapt to multistakeholder perspectives. While cyberattackers are well-motivated, skilled, innovative, and enjoy safe harbors and sponsorship from powerful states, emerging

**Figure 1: All Cyber Defense Index country rankings, 2022-2023**

The leaders	The 5 countries making the greatest progress and commitment toward creating a cyber defense environment.	1	Australia	7.83
		2	Netherlands	7.61
		3	South Korea	7.41
		4	United States	7.13
		5	Canada	6.94
The challengers	The 10 countries making progress or commitment toward creating a cyber defense environment.	6	Poland	6.91
		7	United Kingdom	6.79
		8	France	6.78
		9	Japan	6.71
		10	Switzerland	6.45
		11	Italy	6.37
		12	China	6.27
		13	Germany	6.24
		14	Spain	6.13
		15	Saudi Arabia	5.55
Strivers	The 5 countries making slow and uneven progress or commitment toward creating a cyber defense environment.	16	Mexico	5.31
		17	India	4.87
		18	Brazil	4.75
		19	Turkey	4.26
		20	Indonesia	3.46

Source: MIT Technology Review Insights, 2022



The EU's landmark General Data Protection Regulation is a framework for governments in the top half of the GFI rankings, and also for non-EU countries with large pan-European footprints for financial and insurance sectors, which must follow GDPR principles.

and adaptive cyber-defense ecosystems offer powerful counterweights.

This creates cognitive dissonance: cyber-resilient countries (even the most capable ones) suffer the most attacks. Attacks routinely disrupt business and public infrastructure, and cost billions of dollars. Successful cyber-defense ecosystems must help enterprises and public institutions withstand attacks, recover, and restore operational continuity. This requires stakeholder participation, and their confidence in institutions and infrastructure. Countries are made more cybersecure by the strategic intent of businesses and the political will of governments.

### Cyber Defense Index overall scores

Australia takes a strong leading position in the CDI scores (see Figure 1), with a score of 7.83, and comes in first place in three out of four index pillars. The Australian government under prime minister Anthony Albanese made cybersecurity a primary policy plank since he took office in May 2022, including his first cabinet appointment, Clare O'Neil, minister for cyber security.

Australia's lead in the CDI is a function of several factors, such as its commitment to both maintain and adapt its policies around its multistakeholder digital transformation project, and the relative maturity of its critical infrastructure and digital economy assets. These factors (despite continuous chaos from bad actors) give business leaders and constituents tremendous confidence in Australia's cybersecurity ecosystem, and in their own ability to conduct secure digital transactions. Of the seven confidence indicators drawn from the CDI data, Australia ranks first place in three.

Australia is followed closely by the Netherlands with its score of 7.61. Dutch cybersecurity is bolstered by the Hague's stature as regional collaboration point for pan-European cybersecurity. The Netherlands hosts the Global Forum for Cyber Expertise, and the cybersecurity operational headquarters for Europol and NATO. The Dutch depth of resources (second place in its pillar) lends a comprehensive approach to data privacy. Its domestic agencies have a reputation for constituent collaboration. In September 2022, the government announced plans to merge three security bodies—the National Cyber Security Centre, Digital Trust Centre, and Cyber Security Incident Response Team for Digital Service Providers—into a single organization by 2024.

### Geopolitics has strong sway

The Netherlands, like all of Europe, benefits from an EU policy posture that seeks to preserve the rights of digital consumers, established in 2018 through the adoption of the landmark General Data Protection Regulation (GDPR). The GDPR is a framework for governments in the top half of the rankings, including Poland (sixth), the UK (seventh), France (eighth), and Switzerland (10th), and also for non-EU countries with large pan-European footprints in the financial and insurance sectors, which must follow GDPR principles to operate across the continent.

Geopolitics also accounts for the high CDI rankings of South Korea (third, with a score of 7.41) and Poland (sixth, at 6.91). Both economies share borders and complex relationships with safe harbors for cyber malfeasance, North Korea and Russia, respectively. Because of these circumstances, these governments and industry cybersecurity decision makers must use increased

vigilance. South Korean citizens and institutions lost over \$400 million in cryptocurrency in 2021 to North Korean hackers, according to cybersecurity analysts Chainalysis.

## Not all giants are leaders

Germany's economy, atypically, lacks digital savvy: Germany is the lowest-ranked EU member in the CDI, scoring in the bottom quarter. EuroCloud Deutschland reports fewer than one quarter of IT decision makers embrace modern cloud-native approaches to technology—many hampered by lack of workforce talent. The European Commission found German digital services expanded at the slowest pace among EU countries, with adoption of digital business services only slightly above the mean. German cybersecurity decision makers rate themselves poorly in five out of seven confidence indicators. Germany's Federal Office for Information Security is undergoing some turmoil following revelations that its cybersecurity chief had links to Russian security organizations. He was sacked by Germany's interior minister in October 2022.<sup>8</sup>

India, despite its digitally forward government and the world's largest (and arguably, highly cybersecurity-aware) IT-enabled service sectors, lags in its critical infrastructure. It has poor adoption in its broader national digital economy, and is particularly weak in cybersecurity regulatory structure. This pattern of cybersecurity deficits is a common tale for many other CDI poor performers, most of which are emerging economies.

## Struggles at the trailhead, and a crowded summit

Ranking scores at the top half of the CDI are close: roughly a single point differentiates Australia at number one and Japan at ninth in the index. As the list descends the 10-point scale, scores become more heterogeneous. Three points separate Switzerland's 10th-place rank from Indonesia's last-place score of 3.46. There are many large, sophisticated, and innovative digital technology markets among the less cybersecure in the CDI: these include China (12th) and Germany (13th), with neck-and-neck scores of 6.27 and 6.24 respectively, and India, at 17th place with a score of 4.87. Developing countries are at a disadvantage in creating cyber defense, says Professor Yufei Wu of the Centre for Information and Communication Technology at the University of Trinidad and Tobago. "Poorer countries suffer from a lack of investment, and lack of knowledge and resources. This creates challenges when significant upgrades are required to critical



**"Poorer countries suffer from a lack of investment, and lack of knowledge and resources. This creates challenges when significant upgrades are required to critical infrastructure."**

—Yufei Wu, Professor, Centre for Information and Communication Technology, University of Trinidad and Tobago

infrastructure," he says. Developing economies strain to access modern technology in response to rising consumer demand for mobile connectivity and enterprise demand for investment. "This requires moving from LTE networks to 5G, which usually requires a lot of advice, technical support, and experience from the network infrastructure community," Wu says.

For developing countries, the target will continue to rise higher. While 5G radically boosts an economy's critical infrastructure, Wu adds, "5G can make management of security environments much more complex, and as new parameters such as smart buildings, intelligent manufacturing, and autonomous driving come into focus, the need to maintain cybersecurity investments will only increase."

---

## Partner perspective

# Code42: Reimagining enterprise data protection for insider risk

**R**ansomware, hackers, and nation-state threat actors have long dominated the enterprise security conversation. These external threats often feel more urgent, more dangerous, carrying with them perceived greater potential consequences for businesses. And there's no question about the intent behind these threats—it's malicious.

Recently, however, insider threats have taken center stage, with major companies such as Tesla, Cartier, Apple, and Pfizer in the headlines for insider data breaches and trade secret theft. Though data loss via insiders is not a new problem, it has become more urgent and complex due to three main drivers: digital transformation, hybrid-remote work, and the Great Reshuffle. A noticeable uptick in the use of contractors and recent layoffs have contributed as well. With a recession and frozen budgets looming, now is the time to re-evaluate how to protect data from insider risk.

Insider risk occurs when sensitive corporate data—IP, customer records, trade secrets, source code, crown jewels—gets shared too broadly or moves to untrusted places like personal devices, email, or cloud destinations. This can be deliberate or unintended—as it was for a CFO we work with, who accidentally shared a document titled “Restructuring” with their entire organization. Whatever the motivations, these kinds of data movements equate to competitive, financial, privacy, and compliance risk for organizations.

How big is today's insider risk problem? Two-thirds of all data breaches involve an insider. It's even worse when employees switch jobs. One in three organizations loses IP when employees leave their company. And 71% of organizations don't know what and how much sensitive data those departing employees take to other companies.

## A new approach to data security

Insider risk management (IRM) has emerged as an important data security category, with Gartner, Forrester and IDC releasing new research into this growing area. At its core, IRM addresses the problems you may be trying to solve today with four separate technologies: data loss prevention (DLP), user and entity behavior analytics (UEBA), cloud access security brokers (CASB), and security education and awareness (SEA).

Code42 is the SaaS leader in IRM. With our end-to-end IRM solution—rooted in effective data protection for distributed and collaborative workforces who rely on cloud technologies to get their work done every day—security teams can solve these four critical problems. We're thinking differently about how to protect data, and our approach is a progressive shift, but we've been doing IRM successfully for several years. Just ask Lyft, Okta, Snowflake, or CrowdStrike how they're protecting data in their organizations without slowing down their teams.

Our customers come in all shapes and sizes, from a variety of industries, including high-tech, consulting, manufacturing, media and entertainment, biotech/pharma, insurance, and higher education. Code42 is here to support organizations made up of people who move fast and think big. The ones who work together to solve hard problems and relentlessly pursue better. We believe it's time to reimagine data security.

**Joe Payne**

*President and CEO, Code42*

# 03 The importance of securing critical infrastructure

In the context of cybersecurity, the first pillar of the index—critical infrastructure—can be thought of in terms of IT and communications networks, which transport and store the data that powers digitally driven economies. This envelops the transportation, electricity, public security, fuel, and food-production processes fundamental to the society's safety, health, and productivity. The rise of the digital economy means the two notions of critical infrastructure, IT and communications, are inexorably linked, and both factors are brought into focus in the CDI's first pillar (see Figure 2).

Most CDI top-scorers in this pillar are also overall leaders: Australia, the Netherlands, and South Korea occupy the top three slots in the critical infrastructure category, followed by Switzerland and the U.S. Switzerland has focused much of its cyber-resilience efforts around the digital infrastructure of its financial-services institutions;

understandable, given the importance of the banking hub's fintech sector. In September 2021, the Swiss Financial Market Supervisory Authority approved the launch of the Swiss Infrastructure and Exchange (SIX), an exchange for digital securities. In November 2021, SIX issued the world's first digital bond, and issued several more in 2022.

Many of the world's efforts to harden critical infrastructure focused on creating secure and tamperproof digital identities. This proved difficult even in the most advanced economies. Canada (ranked 10th in the pillar, and fifth overall) established the Pan-Canadian Trust Framework to promote its development in 2020, yet the Digital ID and Authentication Council of Canada (DIACC) has not been able to develop a national digital identification system, and most provincial governments are still only in the planning stages.

**Figure 2: Leaders and laggards of the critical infrastructure pillar**

#### Top and bottom scores

A high score means that robust and secure digital and telecommunications networks and computing resources are in place.

RANK	COUNTRY	SCORE
1	Australia	8.02
2	South Korea	7.74
3	Netherlands	7.72
4	Switzerland	7.52
5	United States	7.49

RANK	COUNTRY	SCORE
16	Mexico	4.84
17	Brazil	4.63
18	Turkey	4.31
19	Indonesia	3.03
20	India	2.78

## Threat landscape and risk tolerance

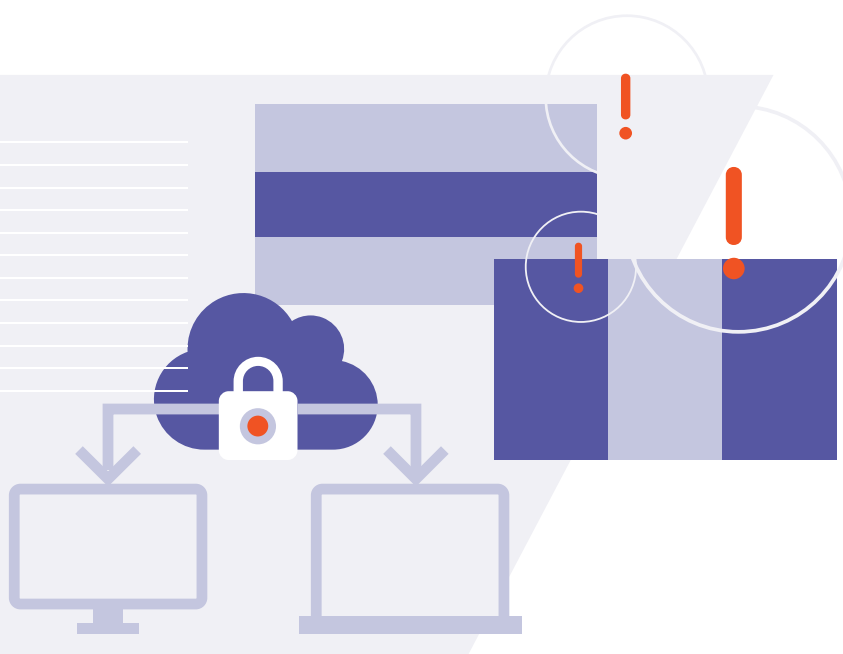
The growth of online channels, smartphones, and digital services globally has increased the threat landscape of a cybereconomy. These challenges add stress to national attempts to support critical infrastructure, particularly around mobile communications. In May 2022, the U.S. (ranked fifth in the pillar and fourth overall), through its federal Cybersecurity and Infrastructure Security Agency and the Department of Defense, created a 5G Security Evaluation Process Investigation to define and augment cybersecurity standards for federal agencies using 5G infrastructure. The U.S. government, like most technologically advanced nations, is hopeful that advancements in mobile data network infrastructure will speed adoption of IoT and Industry 4.0 (Fourth Industrial Revolution) automated applications. This is expected to increase efficiency and automation in factories and smart cities. To do this, governments need to increase involvement in hardening cybersecurity for mobile networks.

While fiber accounts for 86% of South Korea's fixed broadband subscribers, 5G is the focus of cybersecurity for its major telecom carriers through codevelopment efforts. The efforts focus on the future of connectivity—IoT, Industry 4.0 applications, and increasingly experimenting with new applications such as connected and autonomous vehicles. In October 2022, Korean mobile giant LG Uplus signed a memorandum of understanding with several technology partners to develop post-quantum cryptography tools to enhance security for next-generation cars and autonomous driving systems.<sup>9</sup>

Less cybersecure countries in the CDI also have ambitious plans. The Digital 2025 program of Spain (ranked 14th in the pillar and 14th overall) will invest an estimated €70 billion (US\$ 68.4 billion) on 50 programs, which include increasing digital infrastructure, particularly for its 5G networks, to enhance cybersecurity and digital skills.

Geopolitical instability is flowing into national agendas to secure critical infrastructure: amid growing concerns of cyberattacks resulting from Russia's conflict with Ukraine, Germany's interior minister announced plans to promote increased resilience among SMEs, providing critical infrastructure services and a centralized information exchange platform. International cybercriminal activity also underpinned a recent series of high-profile ransomware attacks on Italy's energy providers, including its largest fuel conglomerate, Eni, prompting a warning from the country's National Cyber Security Agency that cyberattacks on Italian critical infrastructure assets will increase in the near term.

There have been bright spots: Russian hacker group Killnet abruptly stopped its month-long campaign of cyberattacks on Japanese government ministries and public transportation companies in late September 2022, claiming financial difficulties forced their operational shutdown. However, critical infrastructure and businesses linked to foundational economic resources remain firmly and constantly in the sights of bad actors. Saudi oil giant Aramco's CEO recently deemed cybersecurity a risk on par with natural disasters. Since a malware attack in 2012 wiped out all its computers, Aramco has suffered numerous attacks, including a \$50 million ransomware attempt in 2021.



Geopolitical instability is flowing into national agendas to secure critical infrastructure.



# 04 Practice and policy: Cybersecurity resources ensure a safer digital economy

**D**eveloping and securing cybersecurity resources—the technological and legal assets which are the focus of the second CDI pillar—presents an ongoing challenge.

Countries that have both robust data-privacy practices and enforcement scored well (see Figure 3). France leads this pillar (and is eighth-ranked overall); the French data-protection authority Commission Nationale Informatique & Libertés (CNIL) is a vigilant prosecutor of data-privacy breaches, and it sits within a pan-EU data-rights regulation ecosystem that has proven even more vigilant. A €100,000 (US\$ 97,700 thousand) fine levied against French hotel group Accor by CNIL in early 2022 was increased sixfold by the European Data Protection Board in August 2022<sup>10</sup>.

While CDI laggards lack data protection infrastructure, many are attempting to build top-down, usually state-

sponsored, efforts to mitigate this. The National Strategy for Digital Transformation program in Saudi Arabia (ranked 19th in the second pillar and 15th overall) is a rolling five-year digital transformation framework. The program is in its third phase, working to develop a smart government-service platform by 2024 that leverages public data to enhance decision-making in the public sector. This vast data-analytics project is in development concurrently with the country's emerging national cybersecurity, privacy, and data-protection legislation.

## Learning to live with insecurity

The working principles of cybersecurity strategy are framed by several constancies. The first is the permanence of cyberthreats: there is no end to the deluge of malware, criminal hacking, and other modes of incursion globally. The inevitability of cyberthreats is prompting a rethink among cybersecurity professionals, to shift resources and

**Figure 3: Leaders and laggards of the cybersecurity resources pillar**

Top and bottom scores

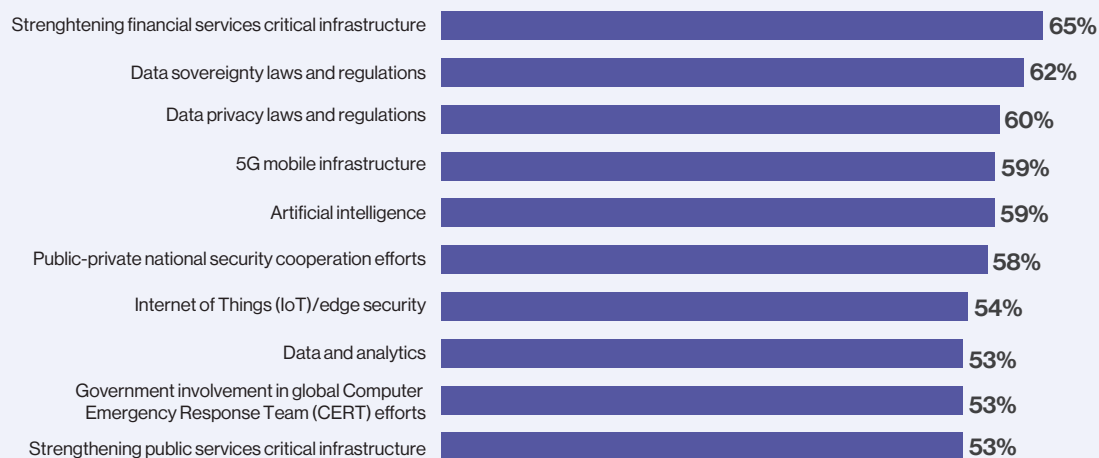
A high score means a better overall performance in the indicators covering views of the technological and legal assets.

RANK	COUNTRY	SCORE	RANK	COUNTRY	SCORE
1	France	8.29	16	Brazil	5.87
2	Netherlands	8.01	17	Turkey	5.59
3	United States	7.9	18	Mexico	5.42
4	South Korea	7.72	19	Saudi Arabia	5.04
5	Spain	7.06	20	Indonesia	4.72

MIT Technology Review Insights survey, 2022



**Figure 4: Respondents rank the following initiatives and technologies as the most important to bolster cybersecurity (% of respondents)**



MIT Technology Review Insights survey, 2022

investment away from traditional protection of digital assets, towards business continuity and data and service recovery where incursions occur. This thinking, however, is still nascent, according to MIT's Michael Coden, who notes that only about 20% of 2022 cybersecurity spend addresses recovery, while about 80% goes toward protection. "We have to shift cybersecurity strategy away from trying to protect ourselves against everything, toward trying to be resilient and recover from the cyberattacks that will happen. It's time to shift the focus a bit," Coden says.

Sadie Creese, director at the Global Cyber Security Capacity Centre and professor of cybersecurity at the University of Oxford, also believes there should be a shift in focus for emerging cybersecurity practices, particularly as innovative technologies continuously change the threat landscape. In her 2020 book, *Artificial Intelligence and the Law*<sup>11</sup>, she writes: "we view cybersecurity as a risk-based practice, where, in fact, achieving cybersecurity is really an acceptance of insecurity, but with controls available that allow us to continue operating in the face of risk." None of this, she continues, should "constitute an argument against discovery or use of AI. Rather they form an emerging case for checks-and-balances capacity, proper oversight, and consideration of protection mechanisms." She adds, "we will need to reflect upon whether we are investing enough in our

ability to defend against and be resilient in the face of AI used in a malign manner, given what we are investing in AI itself."

Another consistent feature of the cybersecurity landscape is that the cybercriminal industry has a boundless innovative spirit; this may be why many industry observers surmise bad actors have the upper hand in cyberattacks, particularly when it comes to AI and other advanced digital tools. Hackers have proven nimble and responsive. This informs a significant trend in cybersecurity: while human involvement is a necessary component in cybersecurity, there are growing efforts to mitigate human error and malfeasance, through the rapid development of so-called zero-trust architecture (see sidebar).

International cooperation, particularly around digitally linked economies in Europe, is increasingly a way of collectively boosting cybersecurity capacities. The foreign ministers of France and Germany issued a joint statement urging international cooperation on cybersecurity at the 77th annual United Nations General Assembly in September 2022. Switzerland became a member of NATO's Cooperative Cyber Defense Centre of Excellence in 2019, and in March 2022 expanded its domestic capabilities when the Swiss parliament voted to double the size of its national cyber-defense force by 2026.

Collaboration is also used internationally between neighbors with differing cybersecurity capabilities. Continuing efforts to mitigate international criminal activity in North America has seen the creation of a U.S.-Mexico Working Group on Cyber Issues, which

conducted its first round of bilateral talks to increase cyber-defense cooperation around shared and national critical information infrastructure, and to share intelligence around cybercrime investigation.



## Trust no one

“The focus of hackers today has been steadily shifting toward social engineering,” says Denis Robitaille, Vice President, Information and Technology Solutions and Chief Information Officer at the World Bank Group. Despite the growing technological competencies of cybercriminals, he says, it remains more efficient for them to provoke and exploit human error “rather than spending a lot of time trying to break the system.” “The human factor introduces non-error implications for cybersecurity,” says Joe Payne, president and CEO of U.S. cybersecurity firm Code42, such as the unintended effects of pro-privacy organizations. “There’s a greater appreciation for privacy, particularly in Europe, which is fantastic in some ways, but not when organizations fail to monitor their own operations for data loss because they’re worried that they will offend the privacy of their employees. Data privacy is critical, but it should not replace the monitoring of employees, who could move critical data to untrusted locations.”

The cybersecurity implications of human fallibility were underscored for Robitaille’s team several years ago when, reviewing findings of a 20-element assessment of the World Bank’s cybersecurity

strategy, “we found the human elements were much weaker than our systems.” This, Robitaille explains, prompted the World Bank’s decision to move to a zero-trust architecture to combat hackers.

**Zero-trust architecture** is a cybersecurity strategy that attempts to remove the ability of a single individual to inappropriately access network resources, and provides strong authentication that uniquely validates each digital interaction. “It means you don’t trust anybody or any device that connects to the network: everything’s logged, everything’s being double authenticated,” says Terry Cutler, a Canadian cybersecurity expert and founder and CEO of the cybersecurity firm Cyology Labs. The concept of zero trust has been around for over two decades, but is only now gaining traction, in part Cutler believes, because it is extremely resource intensive: “You need experts on hand, you have to deploy sensors across your network to monitor the endpoint, the network, and the cloud simultaneously through one dashboard.”

While implementing zero trust requires a significant undertaking for organizations, it does provide security environments with a rigor that employees often lack, in Cutler’s view. “Many don’t necessarily care what they’re clicking on because they think the IT guys have it covered,” Cutler says. The World Bank’s Robitaille sees zero trust as the most effective tactical approach to rebalance cybersecurity resources away from pure defense, and toward resilience and recovery. “When we segment our applications and our network, we ensure that there are no lateral moves for hackers. It protects our data better, and recovers our data and our system better. While we would prefer to focus on developing AI machine learning tools that could identify the very sophisticated approaches of hackers, right now they are just much more advanced than we can be,” Robitaille says.

# 05 Organizational capacity: The business end of cybersecurity

In the third pillar, the CDI weighs and ranks the organizational capacity of each country. It measures the factors which make up cybersecurity maturity and the experience of each country's businesses and other institutions. As this pillar is concerned with the capabilities of each digital economy participant, the views of decision makers are of particular importance. More than half of the weight of this pillar's score is placed on the findings of two of our seven confidence indicators: strategic intent, in which respondents in each country self-evaluated the degree to which cybersecurity is a strategic asset, and industry standards and practices, in which respondents rank themselves on the degree to which world-class cybersecurity practices are integrated in overall operations.

Measured this way, most leaders in this pillar are leaders overall in the CDI rankings (see Figure 5); cybersecurity

leaders in advanced digital economies feel they have senior leadership support for cybersecurity initiatives, and believe they run tight ships to comply with industry best practices and legal frameworks. Australia ranks highly. Although the relatively small country may not be the world's most sophisticated digital economy, Australian business and technology leaders feel they possess exemplary cybersecurity capability and vision. This is also the case for Chinese organizations (second place in the pillar). While China's cybersecurity landscape may appear rigid to the rest of the world, Chinese enterprises clearly feel their domestic practices are excellent.

A large majority, across all countries, regard their cybersecurity practices to be well-implemented and best in class (see Figure 6). Respondents in leading CDI countries are among the most confident, particularly those from Australia, South Korea, and Canada. Decision makers from

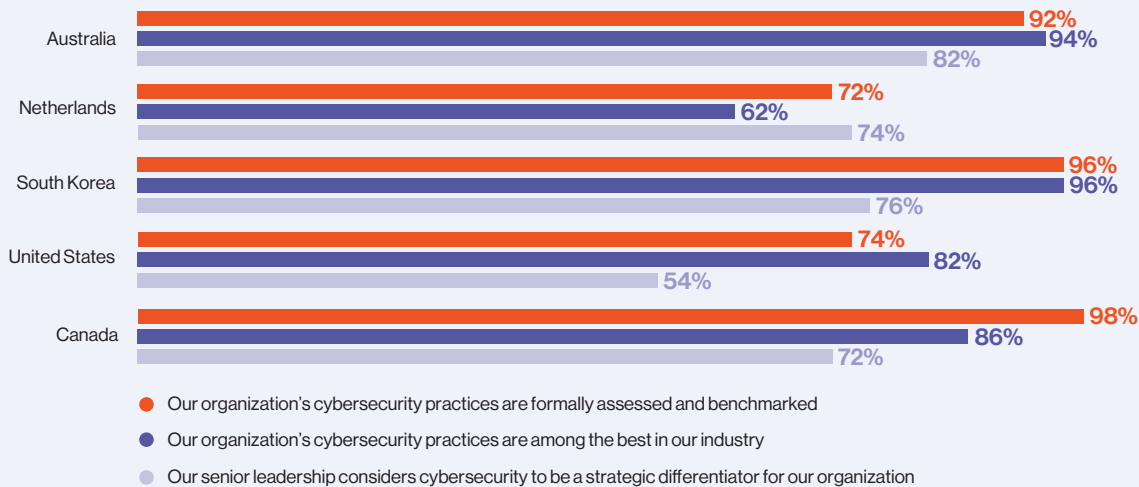
**Figure 5: Leaders and laggards of the organizational capacity pillar**

Top and bottom scores

A high score means a better overall performance in the indicators covering relative cybersecurity maturity and digital experience.

RANK	COUNTRY	SCORE
1	Australia	8.45
2	China	7.54
3	Canada	7.29
4	Netherlands	7.02
5	Japan	6.92

RANK	COUNTRY	SCORE
16	Saudi Arabia	4.52
17	Italy	4.46
18	Brazil	4.24
19	Turkey	2.09
20	Indonesia	1.79

**Figure 6: Respondents from the top 5 Cyber Defense Index countries rank strategic intent**

Source: MIT Technology Review Insights survey, 2022

“The bad actors are ahead—and nimbler—particularly in use of AI. They have an asymmetric warfare advantage—they only must find one weakness out of millions, while we need to keep all the millions equally secure.”

— Michael Coden, Associate Director, MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

several lower-scoring countries—notably Mexico, China, and Saudi Arabia—also hold their own efforts in high regard. This is likely a reflection of the vigilance these cybersecurity executives feel they must maintain while operating in such pernicious threat landscapes.

Despite this reported enterprise rigor, however, much more work must be done to maintain resilient and flexible operational technology cybersecurity. “We have seen in the last couple of years that chief information and security officers and others with governance responsibility in many organizations—including critical infrastructure providers in the private and public sector—lack a principled empirical basis for making investment decisions to prioritize cybersecurity strategies,” says Daniel Weitzner, founding director of MIT’s Internet Policy Research Initiative, describing his team’s creation of the cyber risk benchmarking and risk pricing project, Secure Cyber Risk, Aggregation and Measurement (SCRAM).

SCRAM’s major focus is on better cybersecurity endurance underwriting for organizations and the companies that provide them with risk management and insurance. “Insurance is a key cybersecurity market mechanism, one that is supposed to provide discipline—but it does not appear to be working. A lot of insurers today fail to do proper underwriting and failed to anticipate attacks, and are now pulling back in very dramatic ways: loss ratios and premiums are going way up as a result, and recovery thresholds are going down.” When organizations use SCRAM, Weitzner says “they will be able to get aggregate pictures of loss patterns, and ultimately put a price on risk, and to guide enterprise risk behavior on an empirical basis.”

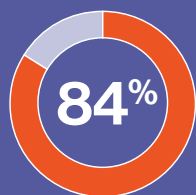
Leveraging comprehensive risk assessment tools is increasingly important for development of cybersecurity capacity. Research shows that in 2022, over one-fifth of surveyed organizations are increasing cybersecurity

investments more than 15% over 2021 (see Figure 7), and 43% will raise spending more than 10%. Some feel mounting cyberattack pressures may require even more attention. “In the last two years in particular, Asia’s manufacturing industries have been facing massive ransomware attacks causing disruption of their production lines,” says Magda Chelly, co-founder of the

Singapore-based cybersecurity startup Responsible Cyber. Those attacks raise awareness around operational technology cybersecurity, which refers to the entire infrastructure, business processes, and personnel deployed to protect an organization’s operational IT, and points to the conclusion that further attention and investment is required.

Figure 7: Top 5 countries by cybersecurity investment

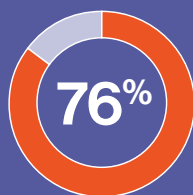
CDI leaders are investing to maintain their positions...



Australia

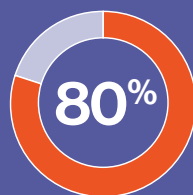


South Korea

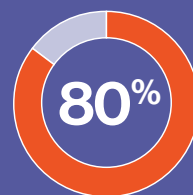


United States

...but strivers appear intent on catching up



Saudi Arabia



Mexico

● Survey respondents who increased cybersecurity spending 10% or more

Source: MIT Technology Review Insights survey, 2022



“When we segment our applications and our network, we ensure that there are no lateral moves for hackers. It protects our data better, and recovers our data and our system better.”

—Denis Robitaille, Chief Information Officer,  
World Bank Group

# 06 Policy commitment: The root of the solution

The fourth pillar appraises policy commitment, or government efforts to promote resilient cybersecurity practices. The indicators measure the quality of cybersecurity regulation, and the robustness and completeness of regulation.

Cybersecurity policy creation and enforcement may be a domestic policy item, but the borderlessness of the internet and ubiquity of digital channels means governments must fold in international diplomacy and cross-border cooperation (see figure 8). These efforts are often forged in crisis: Russia's ongoing hostilities against Ukraine have fueled a rise in cyber malfeasance globally, which has prompted governments to firm up cooperative defense agreements. The Cyberspace Defense Force of Poland (ranked seventh in the pillar and seventh overall) is noted for its support of Ukraine, and is working toward a memorandum of understanding to strengthen regional cybersecurity collaboration.

There are points of divergence between the perceptions of cybersecurity regulatory robustness and policy activities. The government of the UK (12th in the pillar, and seventh overall) has actively cultivated private-private partnerships and a "whole of society" approach to implementing its January 2022 Government Cyber Security Strategy. The government created a Cyber Security Advisory Board to incorporate perspectives from industry and academia. However, the UK ranks second lowest in perceived regulatory robustness, suggesting its approach may not be perceived as effective.

Countries highly confident in their regulatory robustness may be confusing overbearing and draconian enforcement with strength. China (13th in the pillar, and 12th overall) has the second-highest confidence indicator score for business perceptions of regulatory robustness, due to ferocity with which its Cyberspace Administration enforces its 2017 cybersecurity law. These regulations are a punitive

**Figure 8: Leaders and laggards in the policy commitment pillar**

Top and bottom scores

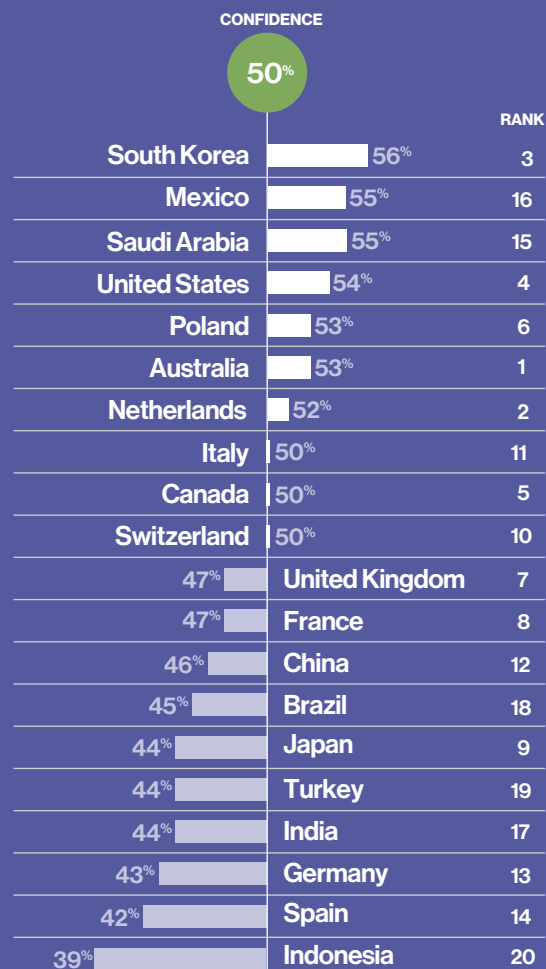
A high score means that comprehensive and effective regulatory cybersecurity practices are in place.

RANK	COUNTRY	SCORE	RANK	COUNTRY	SCORE
1	Australia	7.72	16	France	4.54
2	South Korea	7.34	17	India	3.78
3	Netherlands	7.22	18	Indonesia	3.01
4	Canada	7.04	19	Brazil	3.04
5	Switzerland	6.08	20	Turkey	2.88

MIT Technology Review Insights, 2022

**Figure 9: Perception vs. reality**

This chart shows how confident respondents are in their country's cybersecurity measures vs. the country's index ranking.



Source: MIT Technology Review Insights survey, 2022

tool to keep China's domestic digital giants in check. China is reportedly considering increasing fines for cybersecurity violations, targeting critical infrastructure operators for failing to conduct security reviews on supplier products and services.

Turkey (last place in the pillar, 19th overall), like China, has a history of repressive regulation, but scored last place in business confidence in regulatory robustness. Turkey's government introduced a vaguely defined 7.5% digital services tax on online advertisers and content providers in March 2020, which has become a frequent target of industry criticism.

Laggards in this category are adopting global regulatory best practices to jumpstart their efforts. The EU's GDPR framework has become the gold standard, and governments including Brazil (19th in the pillar, 18th overall) have sought to emulate it. In August 2022, Brazil's Autoridade Nacional de Proteção de Dados (ANPD), the cybersecurity body enforcing the country's GDPR-like 2018 general data-protection law, held its first public consultation to shape its regulatory agenda.

Aging, inconsistent, or incomplete cybersecurity legislation dragged down the overall CDI scores of many countries. A lack of foundational regulation in many countries is linked to rising levels of cyberattacks. In the first six months of 2022, India (ranked 17th both in the pillar and overall) saw its Computer Emergency Response Team respond to over 674,000 cybersecurity incidents, a tremendous increase over 2021. This prompted calls for a national cybersecurity law and a dedicated ministry – both of which India lacks. Similarly in Indonesia (18th in the pillar, and 20th overall), the country's Electronic Information and Transactions Act was last amended in 2016, and is not considered a comprehensive cybersecurity or data privacy law. This is a growing concern in a country that suffered 11.8 million attacks in 2022's first quarter.



**“The global threat is not going to go away, because cyberattacks have become a very effective way to sow instability.”**

– Clay Lin, Director, World Bank Information and Technology Solutions, and Chief Information Security Officer



# 07 Conclusion



**A**cross the CDI-rated landscape, the volume of attacks is not abating, and the ingenuity and effectiveness of hackers and cybercriminals continues. This is despite the increasing amount of time and money businesses and governments invest in cyber defense. The strategic shift away from strengthening existing defenses and toward a more comprehensive and proactive threat assessment is evolving, but for security professionals in most markets, there is still a long way to go. "There are very big skill gaps in operational technology cybersecurity, and therefore anything that is done is largely reactive, not strategically proactive," says Chelly. "This of course creates bigger issues, because a cybersecurity strategy roadmap won't address the entirety of the threat landscape of any particular company and their global operations and supply chain partners."

Many leading CDI countries are building organizational and policy capabilities, and countries which commit to holistic development of both (such as Australia and South Korea) create a virtuous cycle. Cybersecurity practitioners in those markets express confidence they are performing optimally.

Yet cognitive dissonance persists. Despite growing awareness and knowledge, there is a gap between maintaining rigorous operational discipline and being truly secure. The future of cyberdefense depends on the

collective capabilities of its organizations and institutions to continuously assess new data.

Andrew W. Lo, professor of finance and director of the MIT Laboratory for Financial Engineering, says the answer is in the data. Complete data—about the systems involved in cyberattacks, frequency of attacks, information about the attackers, actions by the companies including any errors made, losses and expected losses, and other sophisticated data—is needed to create a new, secure, and rigorous operational discipline.

"We can't even get basic data because companies are extraordinarily sensitive about sharing it due to legal liability issues," Lo says. Big banks in particular, Lo says, have "billions of dollars of losses at stake, given the amount of monies that they transact."

Cyber security leaders at these companies want to collaborate, Lo says. "They'd like to share certain aspects of the data, but they don't want to have any legal exposure." Nascent efforts have experimented with ways to create a protocol to share this data in a secure, anonymized way that cannot be reverse engineered, he said. Work is progressing to get more relevant stakeholders and governing bodies to participate.

"It's a breakthrough—this is the first attempt to actually measure cyber risk exposure," Lo says.

# About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of *MIT Technology Review*, the world's longest-running technology magazine, backed by the world's foremost technology institution—producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Insights Panel has unparalleled access to senior-level executives, innovators, and thought leaders worldwide for surveys and in-depth interviews.

## Footnotes

1. <https://www.gartner.com/en/documents/4016190> and <https://www.gartner.com/en/newsroom/press-releases/2022-04-06-gartner-forecasts-worldwide-it-spending-to-reach-4-point-four-trillion-in-2022>
2. <https://businessinsights.bitdefender.com/bitdefender-issues-top-5-cybersecurity-predictions-for-2022>
3. <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>
4. <https://www.bankinfosecurity.com/biden-administration-vows-crackdown-on-illicit-crypto-a-20090> and <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/statement-by-nec-director-brian-deese-and-national-security-advisor-jake-sullivan-on-digital-assets-framework/>
5. [https://www.imperva.com/resources/reports/TheState\\_ofSecurityWithin\\_eCommerce2021\\_report.pdf](https://www.imperva.com/resources/reports/TheState_ofSecurityWithin_eCommerce2021_report.pdf)
6. [eset\\_threat\\_report\\_t32021.pdf \(welivesecurity.com\)](#)
7. <https://therecord.media/russia-waging-most-sustained-and-intensive-cyber-campaign-on-record-ncsc-ceo-says/>
8. <https://www.reuters.com/world/europe/german-government-relieves-cyber-security-chief-duty-spiegel-2022-10-18/>
9. <https://ciosea.economictimes.indiatimes.com/news/security/ig-signs-mou-to-bring-enhanced-cybersecurity-to-connected-vehicles/94653830>
10. <https://www.complianceweek.com/regulatory-enforcement/accor-fined-600k-under-gdpr-after-edpb-intervention/32019.article>
11. <https://www.taylorfrancis.com/chapters/edit/10.4324/9780429344015-9/threat-ai-sadie-creese>

---

## Illustrations

Report designed by Shultz Design Collaborative. All Illustrations assembled by Shultz Design Collaborative. Icons provide by Shutterstock: Target by Djent; Server by Goldman99, Map by Andrei Minsk, Cityscape by jongcreative,

*While every effort has been taken to verify the accuracy of this information, MIT Technology Review Insights cannot accept any responsibility or liability for reliance by any person in this report or any of the information, opinions, or conclusions set out in this report.*


© Copyright MIT Technology Review Insights, 2022. All rights reserved.



## MIT Technology Review Insights

 [www.technologyreview.com](http://www.technologyreview.com)

 @techreview @mit\_insights

 [insights@technologyreview.com](mailto:insights@technologyreview.com)