
World Trade Organization

Economic Research and Statistics Division

INTERNATIONAL TRADE AND CYBER-READINESS: A REVIEW OF MICRO, SMALL AND MEDIUM-SIZED ENTERPRISE (MSME) PERCEPTION AND PRACTICE^{1,2}

Kathryn Lundquist[†] Rahul Jha^β Reetuparna Vishwanath³ and Chi Pok Cheang^α

Manuscript date: September 08, 2026

Abstract

With the continuing trend of digitalization and its impacts on international trade participation of firms, this paper considers how cyber-readiness impacts trade participation rates, especially of micro-, small- and medium-sized enterprises (MSMEs). First, the paper seeks to define what cyber-readiness is, exploring the multiple components that support MSME digitalization and digital transformation including digital security. The paper then presents the results of a 2023 survey of businesses and policymakers that previously engaged with the International Telecommunication Union on how cyber-readiness is viewed by these groups. Lastly, the paper builds a cyber-readiness score to explore how this concept could be tested against trade participation. Although no correlation was found between the constructed index and international trade by either MSMEs or large firms, a positive correlation emerged between the cyber-readiness score and MSME productivity.

JEL codes: F14, L25, M21, O33

Keywords: Cyber-readiness, cybersecurity, digitalization, digital transformation, small and medium-sized enterprises, MSMEs, firm productivity, trade participation, international trade, firm-level survey

Disclaimer: The opinions expressed in this paper are those of the authors. They do not represent the positions or opinions of the WTO or its Members and are without prejudice to Members' rights and obligations under the WTO. Any errors are attributable to the authors.

Contents

¹ The authors wish to thank Brian Cute, Arti Daswani, Anoush Der Boghossian, Socrates Majune, Simon Neumueller, Aji Putro, Giulia Rampa, and Gill Thomas for their review and contributions. This is a working paper, and hence it represents research in progress.

² At the ITU and the WTO, MSME engagement and consideration of MSMEs in international trade negotiations emerged in 2015. The ITU initiated the ITU Digital World SME Programme in which MSMEs from around the world came together to leverage the ITU's membership base to support the MSME ecosystem. Although the Digital World SME Programme has since ended, the World Summit on Information Society (WSIS) continues to engage ICT professional for development including through a dedicated track on MSMEs.

[†] World Trade Organization. Kathryn.lundquist@wto.org, corresponding author.

^β International Telecommunication Union, rahul.jha@itu.int.

³ HEC Lausanne, Reetuparna.vishwanath@unil.ch

^α UBS Graduate Talent Program, cpc@u.nus.edu

1.	INTRODUCTION.....	3
1.1	What is Cyber-readiness?	4
1.2	How is cyber-readiness a trade inclusiveness issue?	7
2.	SURVEY – HOW DO FIRMS AND POLICYMAKERS PERCEIVE CYBER-READINESS	8
2.1	What do respondents understand is meant by Cyber-readiness?	11
2.2	Survey conclusions	15
3.	MODELING MSME CYBER-READINESS AND TRADE PARTICIPATON	16
3.1	Data Sources and the Composite Cyber-readiness Score.....	16
3.2	Index	20
3.3	Cyber-readiness Score and Trade.....	21
3.4	Cyber-readiness Score and Productivity	21
3.5	Interpretation and Implications.....	22
3.6	Limitations.....	23
3.7	Index Correlation Findings and Suggestions for Future Research.....	23
4	OBSERVATIONS ON MSME CYBER-READINES AND INTERNAITONAL TRADE.....	24
5	CONCLUSION.....	24
6	BIBLIOGRAPHY	26
7	ANNEXES.....	1
7.1	Annex 1: ISO 27001 issued by economy, 2006-2024	1
7.2	Annex 2: ISO 27001 Certificates by Sector, 2006-2024	1
7.3	Annex 3: Components of the Eurostat digital intensity score	3
7.4	Annex 4: WEF GCI Legal framework's adaptability to digital business models	4
7.5	Annex 5: Boxplots of the four components of the Cyber-readiness Score for the years 2017, 2018 and 2019.....	5
7.6.	Annex 6: Index variables correlation matrix	6

1. INTRODUCTION

Since its inception, the internet, information and communications technology (ICT), and digitalization have revolutionized trade for micro, small and medium-sized enterprises (MSMEs) by reducing traditional trade barriers like access to information or finance and providing cost-effective ways to access international markets (Cassetta et al., 2020; Hagsten & Kotnik, 2017; Hamill & Gregory, 1997). MSMEs have emerged as an important part of international trade, accounting for more than a third of exports in developed economies and a noteworthy share of trade in developing economies (Ganne et al., 2022a, 2022b; World Trade Organization (WTO), 2016). Business websites and retail SMS (where text messages are used to promote products and services, especially through messaging applications like WhatsApp (Rosyidah et al., 2023)), have increased network opportunities across borders and digital marketplaces like Alibaba and eBay have become launchpads for digitally connected MSMEs aiming to enter international markets (Jin & Hurd, 2018; Kanyosa & Chacha Magasi, 2025; Lendle et al., 2016). Notably, eBay reported that as early as 2016, 97% of its small-business users were exporters (eBay, 2016), a trend that has continued in recent reviews where 64% of eBay sellers sold to customers in three or more economies (eBay, 2024) demonstrating the powerful role of digital platforms for MSME internationalization

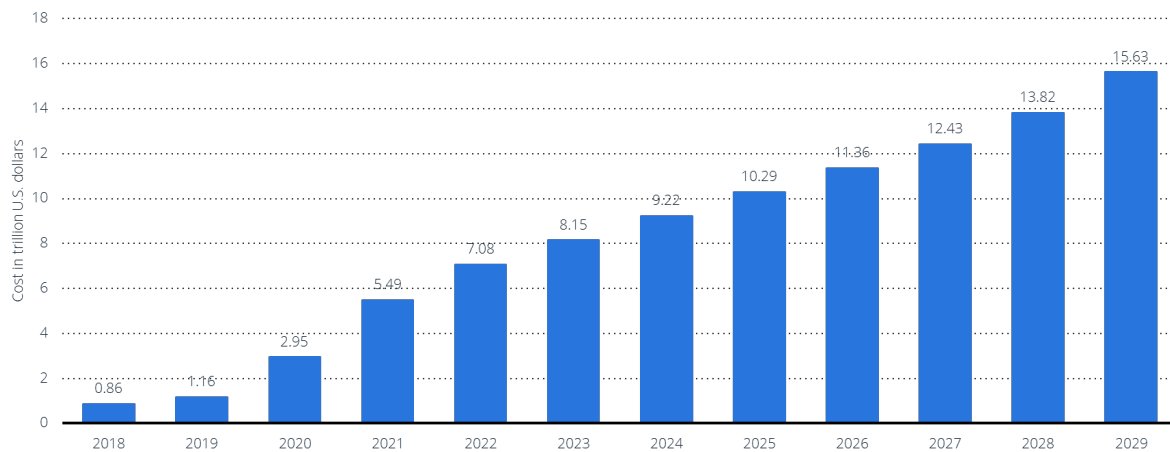
Yet, with these increased opportunities, discrepancies in digital access are even more apparent and new challenges have emerged, especially cybersecurity risks such as phishing, ransomware, or poor internal cybersecurity hygiene that threaten inclusive participation in global trade. This raises an essential question: How can MSMEs be supported to become cyber-ready in all its dimensions, ensuring they can harness the benefits of digital trade safely and inclusively?

Global value chains (GVCs) themselves are reliant on digital technology for communication tools, trade facilitation, and data sharing (Asian Development Bank (ADB), 2021). To actively participate in GVCs, MSME suppliers need the capacity to communicate, use billing software, provide shipment details etc. With the advent of digital supply chains, it is also becoming increasingly necessary for MSME suppliers to adopt digital transformation to increase their competitiveness and avoid exclusion (Menon & Shah, 2020). Real-time tracking and greater transparency of supply chains are increasingly required of suppliers for good supply chain management and environmental, social and governance reporting (C.-L. Chen, 2019; Sibony, 2024).

However, the rise in digital adoption has simultaneously amplified cyber risks. Breaches caused an estimated USD 9.22 trillion of damage in 2024 and were forecast to continue growing (Figure 1). Differences in regional levels of digitalization and the jump in the growth of using digital tools during the Covid-19 pandemic also created significant risk exposure for MSMEs when malicious actors took advantage of the increased reliance on digital technologies and the preexisting vulnerabilities of many of these firms that were amplified during this time period (OECD, 2021). Industry 4.0 is making cyber-risk critical for every sector and whereas some industries, like finance, are more prepared, others, like manufacturing, are less so (Phipson, 2022). Manufacturing now leads as the most targeted sector for cyber-attacks, with implications for MSMEs which are more incorporated in manufacturing than in other sectors, such as the better protected financial sector (Alvarez, 2024;

Organisation for Economic Co-Operation and Development (OECD), n.d.). To some extent businesses are recognizing the increasing risk and "...in 2024, the average annual increase in IT security budgets was expected to reach 5.7%. In fact, for companies worldwide, enhancing the cyber resilience of their cybersecurity teams was the top spending priority in 2023" (Statista, 2024).

Figure 1: Estimated cost of cybercrime worldwide 2018-2029 (in trillion U.S. dollars)



Source: (Statista, 2024)

Note: The global indicator 'Estimated Cost of Cybercrime' in the cybersecurity market was forecast to continuously increase between 2024 and 2029 by 6.4 trillion U.S. dollars (up 69.41%).

While literature exists on MSME digitalization and international trade participation (Añón Higón & Bonvin, 2024; Gopalan et al., 2022; Rosyidah et al., 2023) and the broader implications of Industry 4.0 for MSMEs (Grufman et al., 2020; OECD, 2021), the intersection of these trends with digital security has not been well-explored. Although some foundational work has been done on cyber security (Junior et al., 2023; Perozzo et al., 2022) a holistic understanding of how cyber-readiness feeds into MSME internationalization is limited. This represents a striking gap, particularly given new and emerging digital technologies.

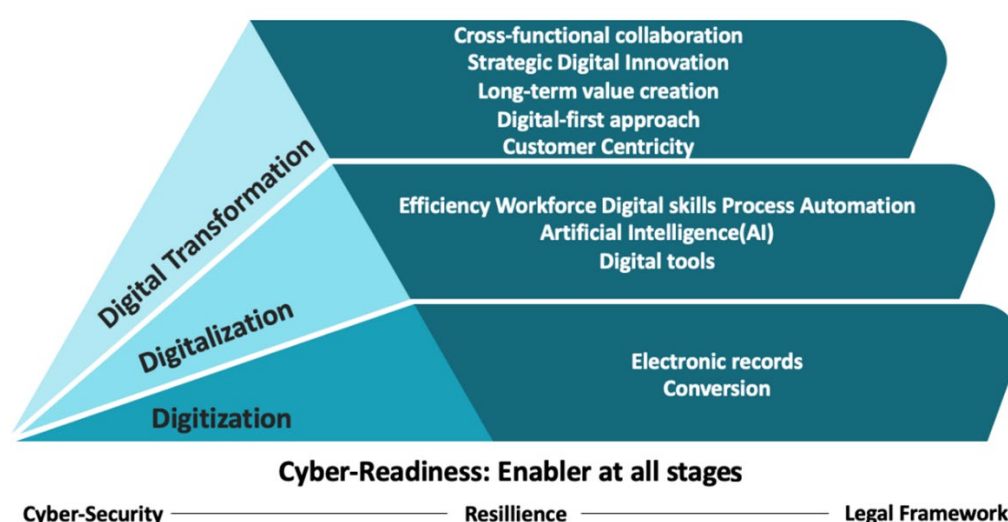
Building on this background, this paper contributes to the literature by explicitly defining “cyber-readiness” within the context of MSMEs engaged in international trade and emphasizing its critical role in ensuring trade inclusivity. Using a voluntary 2023 survey of MSMEs and policymakers engaged with the International Telecommunication Union (ITU), it examines perceptions of cyber readiness and emerging issues such as the role of artificial intelligence (AI) in digital transformation. The study further develops a novel cyber-readiness index, combining publicly available time series data on digital intensity, cybersecurity preparedness, cyber-attack incidence, and related indicators, to explore correlations with MSME internationalization. This index serves as a first step for future research to review the impact of cyber-readiness on SME international trade participation.

1.1 What is Cyber-readiness?

Cyber-readiness is the foundation underpinning digitization, digitalization, and digital transformation (McKinsey, 2022). The following diagram has been developed to help explain cyber-readiness from both an industry and government perspective (Figure 2). At the base, digitization, or the process of

converting analogue information into a digital format (a process often involving the transformation of physical records like text or paper documents into digital files) is the first step (Georgieva, 2022). Next, digitalization "...encompasses the transition to digital economies, governments, and societies, focusing on inclusive access to the internet and stimulating demand for digital applications, skills, and platforms" (World Bank, n.d.). Finally, digital transformation comes with the integration of digital processes for collaboration across organizations and looking forward to long-term value creation. Cyber readiness goes beyond cyber security and includes the ability to work with available digital tools to increase productivity and collaborate across digital platforms with a view towards innovation.

Figure 2: Cyber-readiness



Authors' illustration

Cyber-readiness requires action by both businesses and governments (Asian Development Bank (ADB), 2021; Organisation for Economic Co-operation and Development (OECD), 2021). Achieving cyber-readiness requires six key factors (see also table 1):

- 1) digital literacy;
- 2) affordable and reliable access to the internet and digital tools;
- 3) access to digital finance and payment systems;
- 4) access to software and systems;
- 5) training for digital skills development; and
- 6) cybersecurity systems

As a first step, MSMEs must have basic digital literacy to be cyber-ready, meaning knowledge of the existence of digital technologies and the ability to use them to create and communicate (Cyber Readiness Institute, 2024; UNESCO Institute for Statistics, 2018a). Building on basic literacy, digitalization strategies for ongoing technological changes are a long-term investment for business longevity. Knowledge of digital technologies must be accompanied by access to equipment and reliable infrastructure, including computers, phones, electricity, internet, and data services (Asian Development Bank (ADB), 2021). Although internet connectivity is becoming more widespread and

hence e-commerce and the associated benefits are more easily accessible, in a 2023 study by the Global System for Mobile communications Association (GSMA) of six developing economies in Africa, respondents cited unreliable internet connectivity and access to electricity as the top two barriers for selling online, underscoring ongoing differences in access to digital infrastructure (GSMA, 2023). Additionally, access to digital finance and payment systems are crucial for modern business operations, especially in international transactions. MSMEs need relevant software, like communication apps and supply chain management tools, which are vital for maintaining smooth operations and working with clients. Training on digital tools and analytics further supports informed decision-making and efficient use of resources (Asian Development Bank (ADB), 2023; C.-L. Chen, 2019). A risk-based approach to cybersecurity, meaning flexibility in how cyber risks are addressed rather than defined requirements for security, is also important for MSMEs (Botting, 2021). This ensures the necessary flexibility for smaller businesses with differing resource levels to respond to emerging threats, a particularly important consideration given that MSMEs are frequently targeted as potential entry points into larger companies within a supply chain. (Cyber Readiness Institute, 2024).

Table 1. Cyber-readiness

Digital literacy	Digital literacy involves the confident and critical use of a full range of digital technologies for information, communication and basic problem-solving in all aspects of life. It is underpinned by basic skills in ICT: the use of computers to retrieve, assess, store, produce, present and exchange information, and to communicate and participate in collaborative networks via the Internet (UNESCO Institute for Statistics, 2018a).
Affordable and reliable access to the internet and digital tools	Affordable and reliable access to the internet and digital tools is the ability to connect to and use the internet consistently and without interruption, which requires physical connectivity (i.e., there is internet coverage) and resources to use the internet. Affordable access means that individuals can engage in digital activities without financial barriers and is distinct from internet availability. (International Telecommunication Union (ITU) & UNESCO Institute for Statistics, 2020; Thakur, 2018)
Access to digital finance and payment systems	Digital finance is the use of new technologies to conduct financial transactions, access credit, and manage finances through digital platforms such as mobile banking and online payment systems. Digital payments are payments made using a computer or mobile device to purchase goods and services either through an app, through a website, or at a store by interacting with a terminal. (J. Chen et al., 2023; European Commission, n.d.)
Access to software and systems	Access to software is the ability of individuals and organizations to use various software applications and systems (including operating systems, productivity tools, and enterprise software) necessary for digital operations and productivity. (International Telecommunication Union (ITU) et al., 2017)

Digital skills development	Digital skills are defined as the range of abilities to use digital devices, communication applications, and networks to access and manage information. They enable people to create and share digital content, communicate and collaborate. (UNESCO Institute for Statistics, 2018b)
Cybersecurity Systems	Cybersecurity systems refer to the technologies and processes designed to protect digitally connected assets like computers, networks, and data from unauthorized access, attacks, or damage, ensuring the confidentiality, integrity, and availability of information. (National Institute of Standards and Technology (NIST), 2018)

Cyber-readiness should also be considered from the perspective of gender inclusivity. Studies have shown ongoing gender gaps in access to technology, digital skills and technology industry participation (Martínez-Cantos, 2017; Marzano & Lubkina, 2019; Rashid, 2016). This research indicates the challenges women face in entering and thriving within the technology sector, often due to societal barriers, systemic biases, and limited access to resources. Women also face greater cyber harassment and online threats than men, impacting their digital presence (UN Women, 2025). However, findings presented by Moeini Gharagozloo et al. (2023) suggest that the overall digital readiness of an economy can play an active role in enhancing women's entrepreneurship. This points to the importance of fostering an equitable digital landscape that promotes inclusive participation.

1.2 How is cyber-readiness a trade inclusiveness issue?

Cyber readiness is growing in its importance for MSME trade participation. As already noted, modern trade is increasingly conducted or facilitated online (UNCTAD, 2024). E-commerce sales were estimated to have risen to \$27 trillion in 2022, with between 12-14% of sales being digitally ordered exports (UNCTAD, 2024). MSMEs need digital readiness to access market information, find customers, create a website, access e-commerce or online marketplaces and many other business functions. Mobile message services and social media are also important for MSMEs to find buyers, especially in developing economies (Solomon et al., 2023). The Covid-19 pandemic further revealed the benefits of digitalization for MSMEs in terms of crisis response and continuity of operations (Guo et al., 2020) and MSMEs throughout the world turned to new digital tools (IFC & UKAid, 2021; Takeda et al., 2022). Artificial intelligence is also creating new opportunities for MSMEs by providing a powerful tool for supply chain management and data analysis; facilitating understanding of cross-border regulatory requirements and automatic form filling; access to finance since AI can be used as a tool for business risk assessment; and real-time translation and legal form development for working with international clients (Nesbitt, 2023). These digital tools are no longer a bonus for those MSMEs that have the capacity to use them, they are now a requirement to improve efficiency and effectively execute international transactions.

Digital processes are also becoming requirements for MSMEs to join global value chains since multinational companies in every industry rely on digital communication to contact their suppliers, digital systems for operations, and digital measures to keep information secure (Boyes, 2015; C.-L. Chen, 2019). Multinational companies both rely on MSME suppliers and face system challenges

because of these suppliers since MSME cyber vulnerability is often the gateway into larger multinational systems. An estimated two thirds of cyber-attacks are on MSMEs and the incident rate continues to grow (Cyber Readiness Institute, 2024; Hiscox Ltd, 2023). This challenge is recognized in the business community, with 83% of surveyed supply chains rating MSME supplier cybersecurity as ineffective (Cyber Readiness Institute, 2024). Despite these trends in terms of cyber-attacks, small businesses still have a low level of awareness with few believing that they might be targeted. Having fewer financial and human resources, MSMEs also often prioritize other investments over strong cyber security, finding the cost too high. MSMEs face additional challenges when it comes to digitalization and supply chain participation, especially in terms of differences in digital systems and a lack of standardization. For example, even complying with the different digitized invoicing applications between clients, a must for a supplier to receive payment, can be a significant effort for smaller businesses (*Is Digitalisation a Game Changer for SME Sustainable Finance?*, 2024).

Divergent cyber laws are also a growing trade issue for MSMEs. They create market barriers through disparate requirements, inconsistent regulations, and regulatory complexity. These differences are particularly challenging for MSMEs (Botting, 2021). For example, there are more than 80 national strategies for critical infrastructure and cyber security around the world with different agendas and requirements (United Nations Institute for Disarmament Research (UNIDIR), n.d.). Further, certain regulations favor domestic companies by requiring specific registration, certifications, or data localization. These requirements may be achievable by larger firms with sufficient resources but can prohibit smaller businesses from entering the market.

2. SURVEY – HOW DO FIRMS AND POLICYMAKERS PERCEIVE CYBER-READINESS

To begin the review of how cyber-readiness and trade is perceived in practice, a non-representative survey was developed for this paper and issued online in two separate versions to 237 MSMEs and government representatives that have engaged with the ITU. Respondents completed the survey between 11 May 2023 and 2 June 2023. The survey questions covered topics such as demographic information, the level of business connectivity, the extent of international business participation, digital presence, data ownership, cybersecurity awareness, artificial intelligence awareness, and government support.

A total of 89 business representatives from 40 economies from every region of the world responded (Table 2). Summary statistics show that respondents primarily consisted of individuals working in MSMEs (63%), with 34% identifying as employees, 17% as managers, 15% as owners, and 34% holding dual roles as both owners and managers (Table 3). Further, over half of the companies (56%) reported earning less than 10 million USD, indicating a prevalence of smaller-scale operations among the respondents.

Table 2: Number of Respondents for the survey

	Do you own, manage, or work for a private sector company?	Regulatory or Government Body Official	Total
Number of Respondents	89	114	203

Note: Analysis of data from the authors' survey

Table 3: Descriptive Statistics of businesses for respondents working in the private sector

Respondents working in the private sector			
Position	%	Number of employees in the company	%
Employee	34	250 or more	38
Manager	17	50-249	9
Owner	15	10-49	23
Owner and Manager	34	0-9	31
Annual revenue	%	Operating Years	%
Less than 10 million USD	56	Less than 1 year	5
10 - 50 million USD	15	Between 1-5 years	21
50 million - 1.5 billion USD	11	Between 5-10 years	23
More than 1.5 billion USD	18	More than 10 years	51
Gender	%	Age	%
Male	79	18-29	10
Female	20	30-39	27
Prefer not to say	1	40-49	29
		50-59	19
		60+	15

Note: Analysis of data from the authors' survey

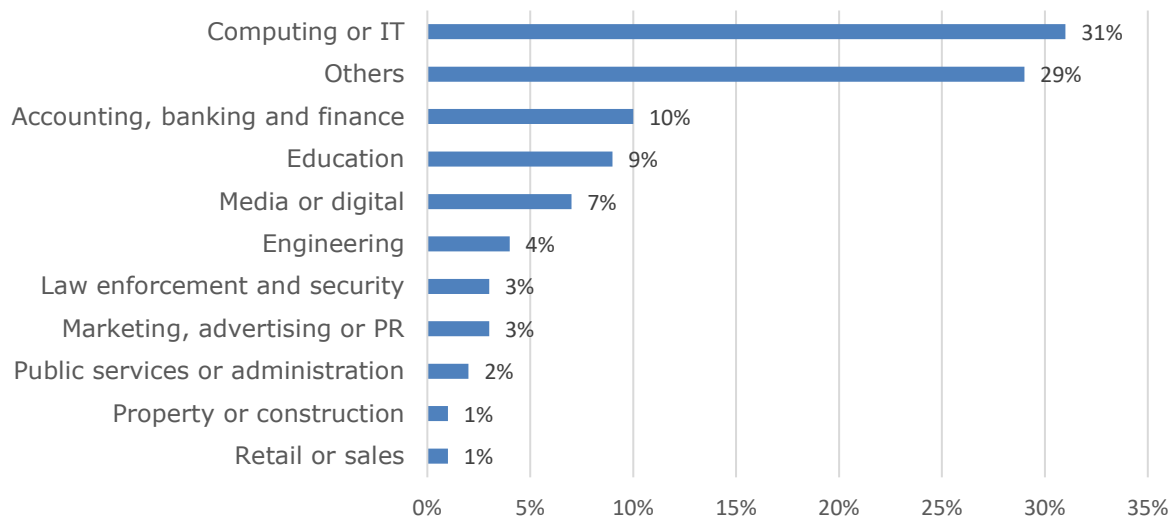
Business respondents primarily identified as male (79%), a very high share that may have to do with the reported industries, which skewed towards the technology sector where women are historically underrepresented.⁴ Age-wise the largest groups were those between 30-39 (27%) and 40-49 (29%) years old, suggesting a mature workforce with experience in their field. Over half (51%) of respondents were from businesses that had been operating for more than 10 years, further adding to the impression of experience among the participants, not only at an individual level but also industry level. Overall, the data reflect a group of knowledgeable professionals from established private sector companies.

In terms of sector, most respondents came from the computing or IT sector (31%) (see Figure 3). 'Other' categories followed second, making up 29% of responses and including various industries

⁴ To illustrate, a 2023 Women in Tech survey found that women accounted for only 26% of people working in IT (Women in Tech, 2023) and a U.S. survey found that women make up just 35% of employees in science, technology, engineering and mathematics (STEM).

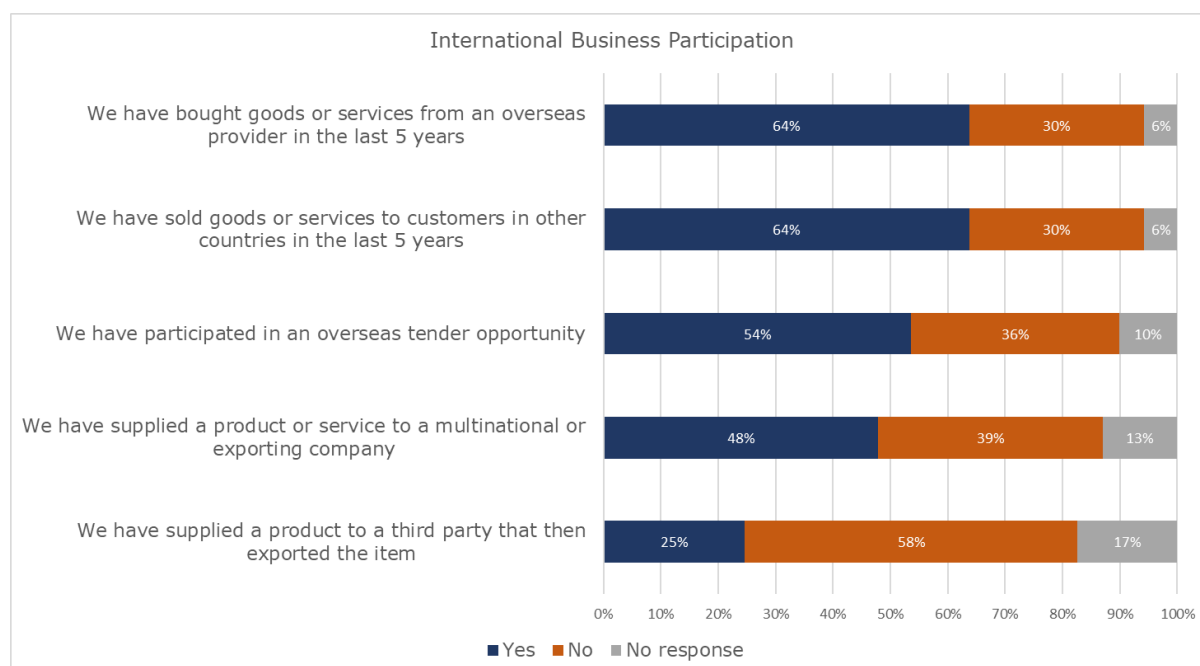
such as telecommunications, e-commerce, and renewable energy. Accounting, banking and finance, and education are also notable sectors, each comprising around 10% of the survey respondents. The data reflect the strong presence of technology-oriented businesses given their engagement with the ITU.

Figure 3: The sectoral breakdown of business survey responses



Note: Analysis of data from the authors' survey

Surveyed firms were active in international markets (see Figure 4). Two thirds of business respondents noted that they had bought goods or services from an overseas provider within the last 5 years (64%), and a similar share noted selling goods or services to foreign customers during the same period (64%). This survey sample also had a high rate of participation in overseas tender opportunities, with more than half (54%) responding yes. This large share reporting international transactions is exceptional given most respondents were small firms, which ordinarily trade at lower rates based on WTO estimates of around 10-50% of a region's MSMEs conducting international trade depending on firm size and level of economic development (Ganne et al., 2022a, 2022b; WTO, 2016). However, the unusual sample of highly digital businesses may have contributed to this high level of international trade given that firms that trade internationally in digital services tend to be smaller (Kerner & Kitsing, 2023).

Figure 4: International business participation of survey respondents

Note: Analysis of data from the authors' survey

2.1 What do respondents understand is meant by Cyber-readiness?

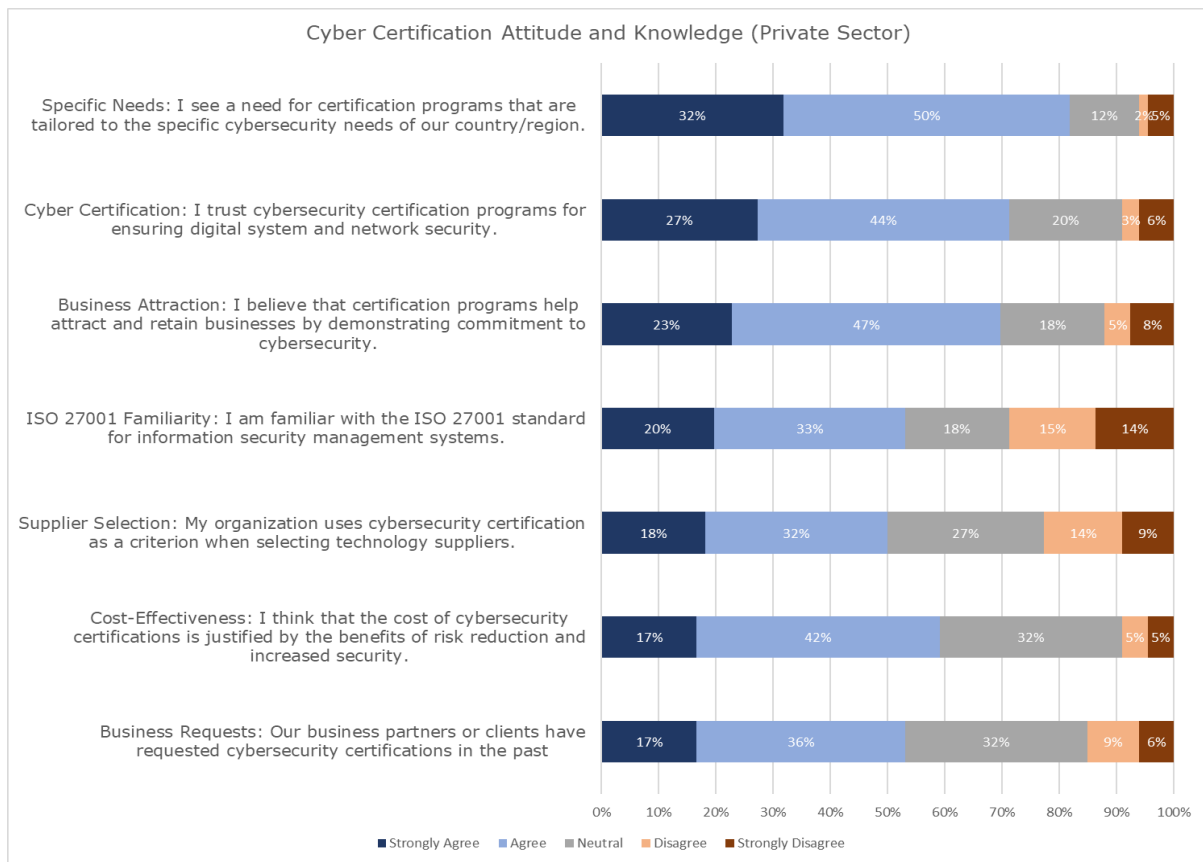
Business respondents were asked what the term "Cyber-Readiness" meant to them. To the respondents, this was highly linked with the concept of cybersecurity rather than the broader definition including digitalization and digital transformation put forward in the first section of this paper. This can be seen in the responses received that focused on words like threat, monitoring and protection (Figure 5).

Figure 5: Word cloud on cyber-readiness

Note: Analysis of data from the authors' survey

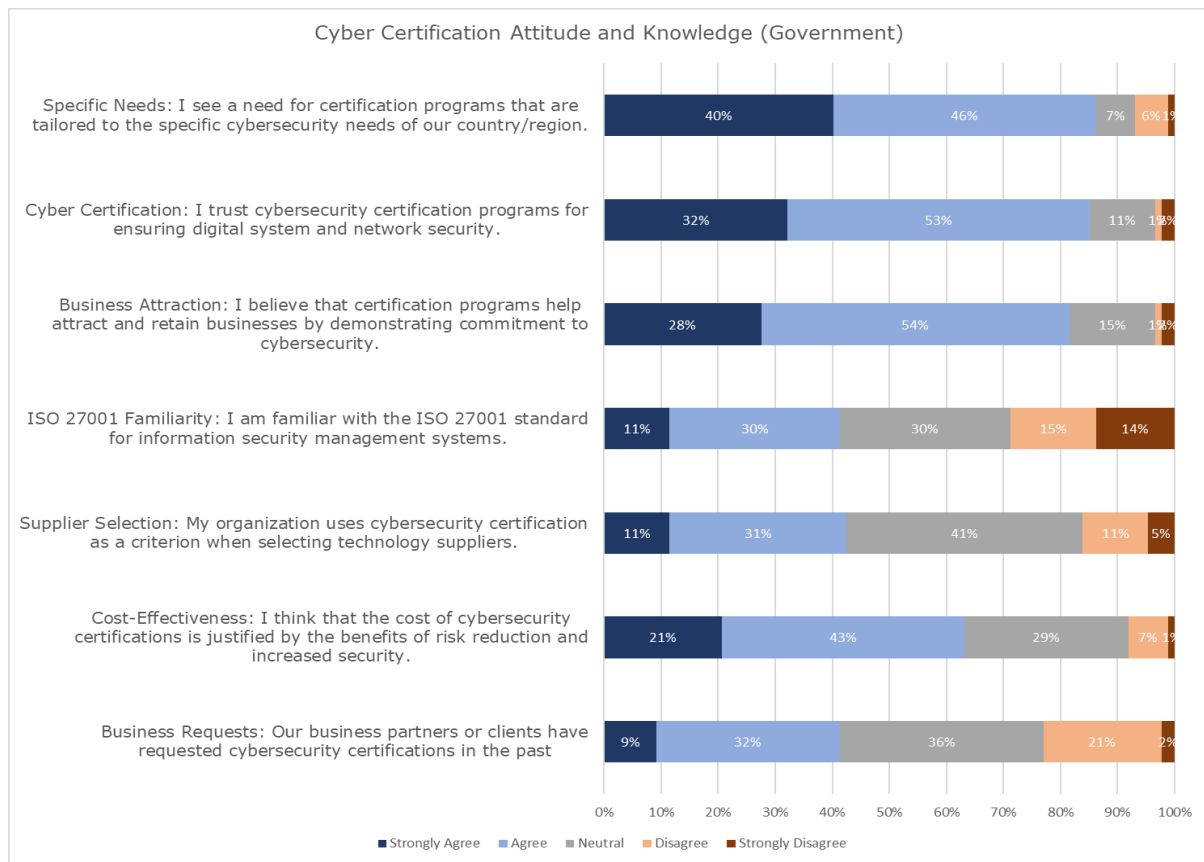
In this vein, the majority (82%) of business respondents identified a need for cybersecurity certification programs tailored for their economy or region to support their businesses. This indicates variability in the cyber-risks that are faced and the importance of customizable and region-specific certification frameworks to address diverse cybersecurity challenges (Figure 6). For those cybersecurity certification programs that exist, 71% affirmed they trusted these certification programs for ensuring digital system and network security. These programs would include national certification schemes, such as Cybersecure Canada (Higgins & Alexandre P russe, 2021), which may be aligned with other economic partner schemes, or international programs like the ITU cybersecurity CIRT framework (International Telecommunication Union (ITU), 2021b) or ISO 27001 Information Security Management standard⁵ (Fomin & Barlette, 2008). In terms of how the certifications assist with industry relationships, 70% indicated that certification programs help attract and retain business, 50% noted that they use certifications to select their own suppliers and 51% said that business partners or clients have requested certificates of their firm in the past. This suggests that MSMEs recognize the value proposition of cybersecurity certifications for enhancing their reputation and competitiveness in the market. Given this strong use of cybersecurity certificates, it is unsurprising that 59% of respondents noted they thought the costs of attaining these certifications was justified. This is despite costs for ISO 27001 certification, for example, that can range from USD 6,000 on the low end to USD 40,000 or more (Vanta, n.d.).

⁵ Despite the response that businesses trusted cybersecurity certification programs, responses to the question addressing familiarity with the ISO 27001 standard were relatively low at only 53% of respondents. Growth of ISO issued ISO 27001 certificates from 2006 to 2024 increased 20-fold across sectors ranging from textiles and apparel to transport and storage. Data of reported ISO 27001 certificates issued by economy and industry are available in Annex 1 and 2.

Figure 6: Cyber certification attitude and knowledge of business survey respondents

Note: Analysis of data from the authors' survey

Although less detailed information was collected from policymakers, 114 responses from government respondents in 50 economies from every region of the world were received. The key findings include that more than half (58%) of government representatives reported that they have a cyber incident policy in place and 53% indicated that regular cybersecurity reports are generated (See Figure 7). This points towards a growing acknowledgement that transparency in this area is important and regular updates from government officials are valued. Like MSMEs, most government representatives also indicate having a cyber security certification (63%) and a similar share (61%) have a response plan in the case of a data breach of their systems. This shows the level of seriousness governments are placing on cyber-attacks and ways to ensure continuity of operations.

Figure 7: Cyber certification attitude and knowledge of government survey respondents

Note: Analysis of data from the authors' survey

Separately, government representatives were asked about government support measures. Two fifths of government respondents noted that financial or non-financial support have been provided to MSMEs in the past in connection with digitalization and cyber-readiness components. This shows that many governments are recognizing the need to support MSMEs in their efforts to be cyber-ready.

Box 1: MSME Artificial Intelligence (AI) awareness

As part of looking ahead and digital transformation for cyber-readiness, the survey included questions on AI aimed to gauge MSMEs' attitudes towards adoption, perceived benefits, concerns, and readiness to use new generative AI technologies in their businesses.

Key Findings:

Intent to use AI for product enhancement: most respondents, 68%, indicated their intent to use AI in their production.

Skills gap in AI implementation: while there is a desire to leverage AI, a significant portion of respondents (44%) expressed a lack of skills in utilizing AI technologies effectively.

Perceived cost reduction with AI adoption: many respondents (63%) recognized the potential of AI in reducing costs and operational expenditures. This suggests a positive perception of AI's ability to enhance efficiency and streamline business operations.

Ethical concerns surrounding AI Use: over 45% of respondents indicated varying levels of concern about the ethical implications of AI usage in their businesses, highlighting the importance of ethical frameworks and guidelines in AI development and deployment.

Expectation of AI in enhancing cybersecurity: while almost half of respondents (49%) believed that AI would bolster cybersecurity measures, half had no opinion or were concerned that it would increase cyber risks. Further education on AI's role in cybersecurity and its limitations may be necessary to align expectations.

The survey findings underscore the diverse perceptions and readiness levels among MSMEs regarding AI adoption. Addressing the skills gap, scepticism, and ethical concerns are critical steps towards fostering a conducive environment for AI integration in MSMEs, ultimately driving innovation, competitiveness, and sustainable growth in the digital era.

2.2 Survey conclusions

This survey provided insights on perception and application of cyber-readiness, principally on the aspect of cybersecurity. Respondents themselves indicated that cybersecurity is how many interpret the term "cyber-readiness," something that may benefit from expansion given the many different and developing aspects of this term. Although the responses did not indicate that there was a direct connection between cyber-readiness and international trade, the business respondents themselves were very international with a positive attitude towards cybersecurity certification programs as they increase trust and may be required by business partners. However, challenges such as cost concerns and the need for greater awareness and familiarity with international standards remain areas for improvement. Response plans to breaches of cybersecurity would also help to establish credibility when supplying to multinational companies. Addressing these challenges can empower MSMEs to enhance their cybersecurity resilience and competitiveness in an increasingly digital and interconnected business landscape. Policymakers already indicate providing support for MSMEs, but this survey indicates there is still a need to provide comprehensive cyber training programs to enhance international business sales (ITU, 2021b). Lastly, this survey indicates that going forward, it may be good to establish ethical guidelines and frameworks tailored to MSMEs to address concerns and promote responsible AI deployment.

3. MODELING MSME CYBER-READINESS AND TRADE PARTICIPATION

Surveys have been the traditional means of measuring digitalization and the use of cyber tools by business characteristics. However, as seen in the survey issued for this paper, it is not easy to include the broad range of factors that are included in the concept of "cyber-readiness" in a survey or to tie this directly with international trade. For this last section of the paper, a new cyber-readiness score was developed to try to test the link between cyber-readiness and MSME international trade participation. This new index tried to incorporate the broad definition of cyber-readiness proposed in this paper and was composed of components representing use of digital technology, cybersecurity, national frameworks and the level of cyber-attacks.

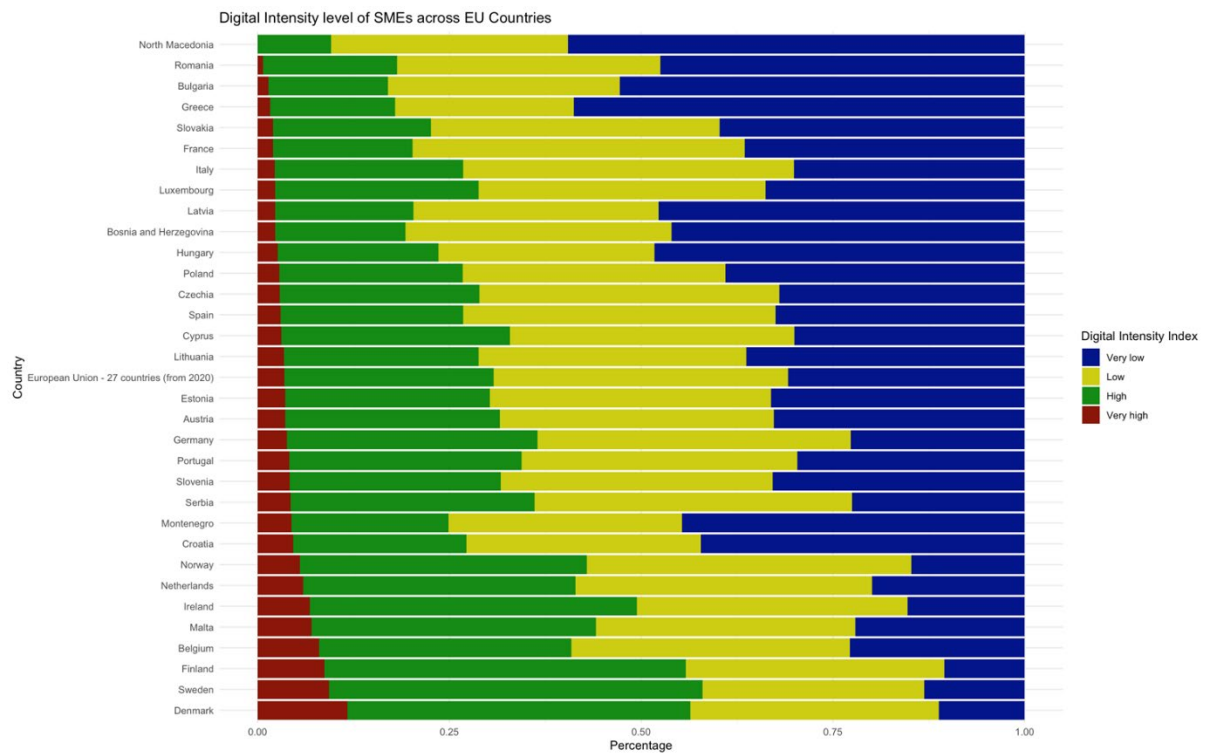
3.1 Data Sources and the Composite Cyber-readiness Score

The data for the Cyber-readiness Score is composed of four parts: digitalization and trade, cybersecurity, national frameworks to support digital trade, and cyber incidents selected from the following sources: 1) Eurostat's Digital Intensity Index, 2) the ITU's Global Cyber-security Index, 3) the World Economic Forum (WEF)'s Global Competitiveness Index, and 4) the University of Maryland CISSM cyber-attacks database. Other data sources were explored, but not selected for reasons such as data availability, missing data or incomparable time periods. Databases that were investigated included the OECD sector level digitalization rankings, the World Bank's digital adoption index (DAI), the ITU digital development dashboard, the ITC SME competitiveness grid, and surveys like the World Bank Enterprise Surveys.

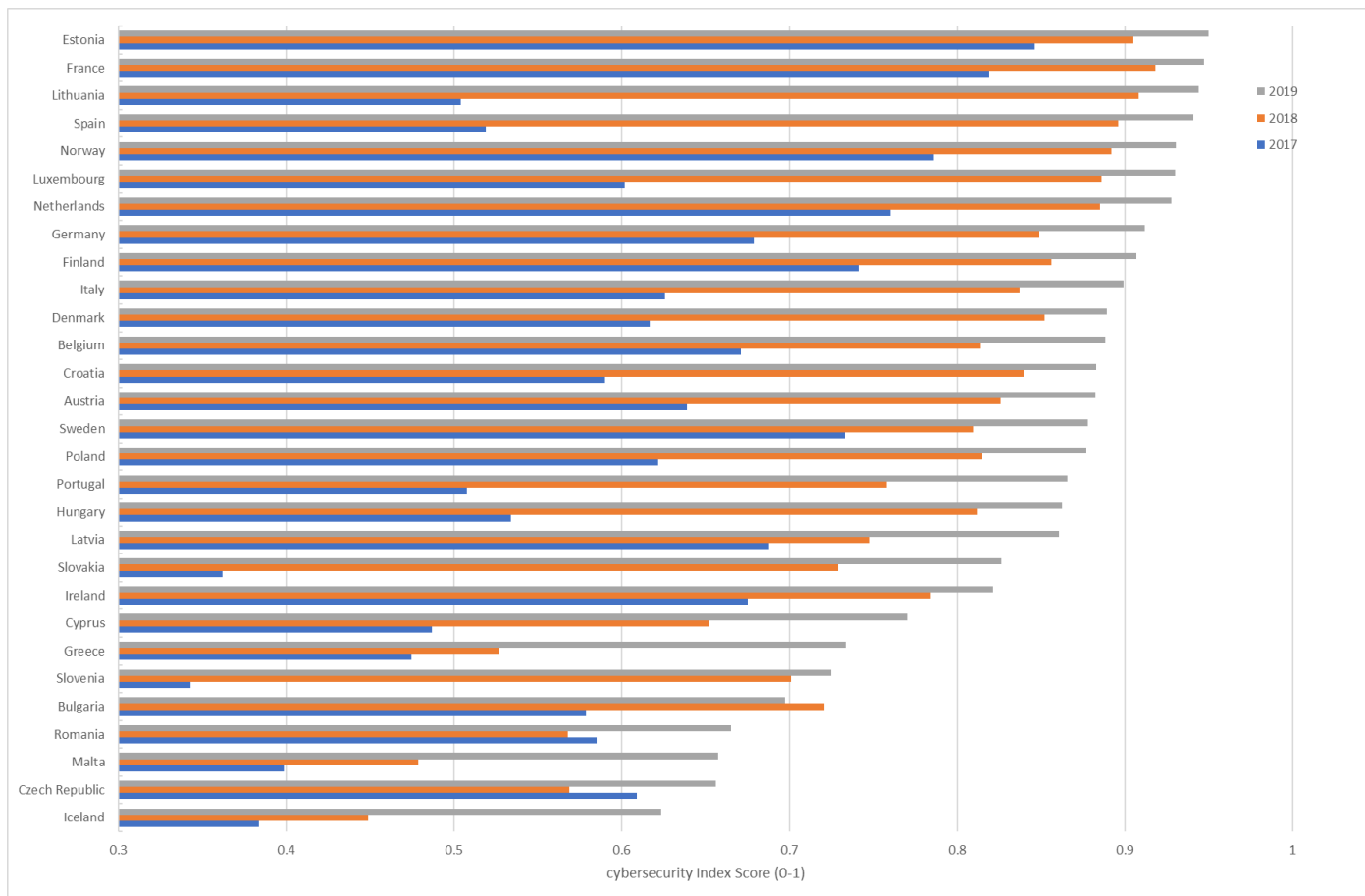
The search for data with a digital-readiness component and firm-size characteristics led to the selection of Eurostat's detailed Eurostat Digital Intensity Index as a way of gauging the level of firm digitalization. Although this limited the analysis to the European Union, it provided a first step in the process to link cyber-readiness with international trade for enterprises of different sizes. The Eurostat Digital Intensity Index, derived from Eurostat's survey on ICT usage and ecommerce in enterprises, comprises a composite measure of twelve conditions⁶ indicative of the digital engagement of enterprises and broken down by enterprise size class (Eurostat, n.d.). These conditions encompass a variety of factors from internet usage for business purposes to the employment of ICT specialists and the adoption of cybersecurity measures. The size of the firm is categorized as either an SME (10-249 employees) or large firm (250 or more employees). The index assigns one point for each condition met, yielding a score with a range from 0 to 12 (0 being low digital intensity and 12 being high). Figure 8 represents a visualization of the digital intensity level of SMEs in select European economies.

⁶ The components of the digital intensity score are detailed in Annex 3.

Figure 8: Digital Intensity level of SMEs across EU Economies, 2019



Next, a Cybersecurity Index Score was sourced from the ITU's Global Cybersecurity Index for a comparison of cybersecurity levels in the European economies reviewed (ITU, 2021a). This was included to approximate the security of the digital environment that the businesses were operating in at a national level. The Global Cybersecurity Index is based on five pillars and looks at an economy's legal measures, technical measures, organizational measures, capacity development and cooperation. Data were available for the years 2014, 2017, 2018, and 2020, and therefore required modification to align with the Eurostat data for 2017-2019. In addressing the data gap for 2019, the average of the 2018 scores and a rescaled 2020 score was used since the 2020 score originally used a scale of 1-100 that needed adjusting to a 0-1 scale. Figure 9 represents a visualization of the scores over the three years, sorted by the imputed 2019 score from highest to lowest (Figure 9).

Figure 9: ITU Cybersecurity Index Score 2017-2019*

Source: ITU 2021

Note: Data for 2019 are calculated.

For the third component of the composite cyber-readiness score, Legal Framework Adaptability data describing the selected economies were taken from the Global Competitiveness Index produced by the World Economic Forum (World Economic Forum et al., 2020). Ensuring that the legal framework is adapting to business needs is important for business operations. The Legal Framework Adaptability Value is generated from survey responses to the question "...how fast is the legal framework of your country adapting to digital business models (e.g., e-commerce, sharing economy, fintech, etc.)". Response values ranged from 1 to 7 with higher numbers indicating faster adaptability, thereby indicating the agility and responsiveness of national legal structures to the evolving digital landscape within the economy based on survey responses (see Annex 4 for a table of the data).

Data on cyber-attacks were extracted from the University of Maryland CISSM Cyber Attacks Database to complete the composite cyber-readiness score to approximate the vulnerability of firms in the selected European economies (University of Maryland, n.d.). The CISSM Cyber Events Database provides information on publicly acknowledged cyber events for public and private organizations. Data are collected using Python web-scraping technology and are reviewed (University of Maryland, n.d.). Limitations of this database are that these attacks are not private-sector specific, meaning they also include attacks on government entities, and web-scraping

technology can only identify publicly shared attacks published online meaning an unknown number of cyber attacks were missing. The focus of the compiled data was on non-finance, non-insurance, and non-public administration sectors to concentrate on business-related attacks per economy. To facilitate cross-economy comparisons given their varied sizes and levels of population, the data were normalized by calculating the frequency of business attacks per internet user. Scores ranged from .44 to -8.8, with positive scores indicating fewer acknowledged cyber-attacks and more negative scores noting a relatively larger number of publicly cited cyber-attacks per internet user for a given economy.

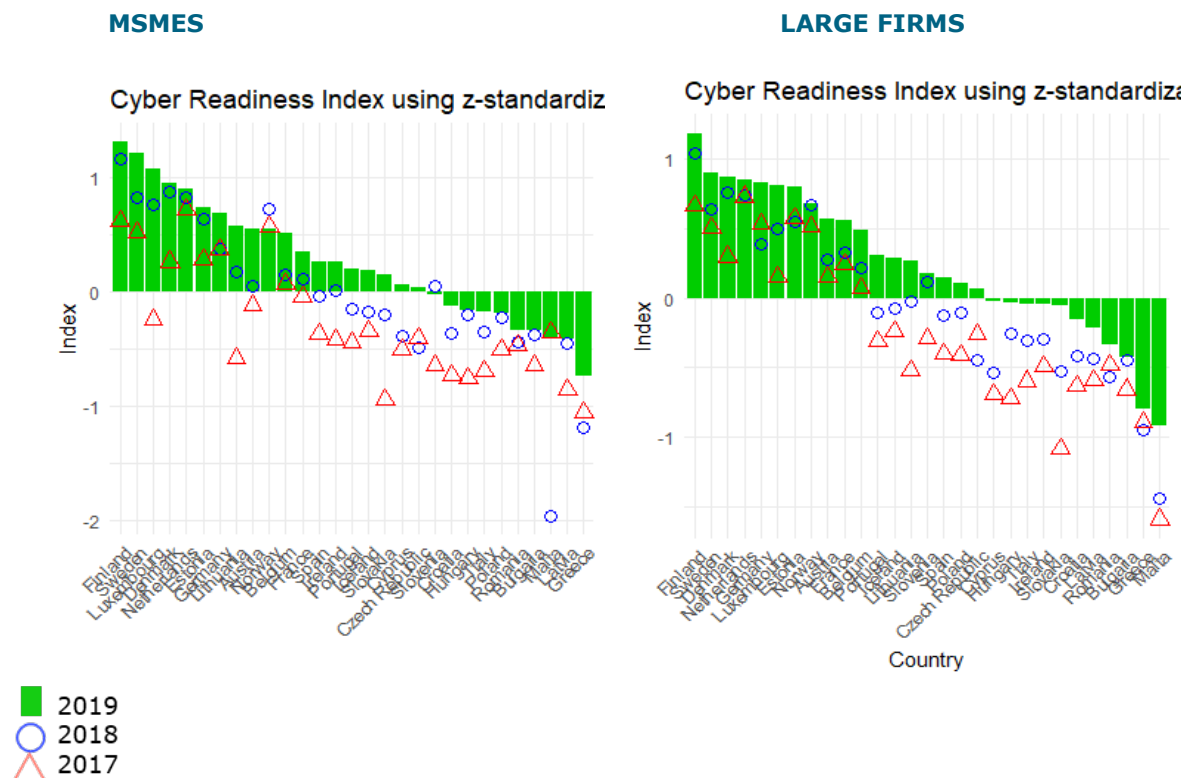
Based on these four data sources, the composite cyber-readiness score was created to reflect the overall cyber-readiness of MSMEs in each EU economy. The creation of this score involved the following steps:

- 1. Normalization:** Each selected variable was normalized to ensure comparability using method z-score standardization.
- 2. Weight Assignment:** Each normalized variable was assigned equal weightage in the formation of the composite cyber-readiness measure.⁷
- 3. Composite Score Calculation:** The composite score was calculated by taking the mean of all standardized variables for each year and economy. The cyber-attacks per internet user standardized score was incorporated negatively in the composite score such that a higher attack count per internet user would lower the cyber-readiness composite score. See Annex 5 for a boxplot visualization of the four variables.

The final composite score represents the cyber-readiness level of MSMEs in each European economy, with higher scores indicating more cyber-readiness among businesses and national policies. Based on the years with the most available data, a panel composite cyber-readiness score dataset was developed for the years 2017, 2018 and 2019 across 29 European economies (the EU27 plus Norway and Iceland). Plotting the Cyber-readiness Score using z-standardization provides Figure 9, indicating a possible trend of increasing cyber-readiness as defined by the score within each economy over the three available years for both MSMEs and large firms (the green column, 2019, is generally higher than the other markers).

⁷ The correlation between variables in the annex was low except between the level of digital intensity and legal framework adaptability (.59), indicating immediate reason for weighting the components (see Annex 4).

Figure 9: Plot of the composite cyber-readiness scores of selected European economies in the years 2017, 2018 and 2019 using z-score standardization:



Note: Authors' calculations

3.2 Index

Given data limitations, only correlation could be used to see preliminary links between the composite cyber-readiness scores and levels of trade for MSMEs and large firms. As a comparison, the correlation between the cyber-readiness scores and productivity was also analyzed.

Two separate variables were selected to compare: first global trade for the selected European economies (from Eurostat) and second labour productivity (from OECD statistics). A total global trade variable was developed as the aggregate of exports and imports in thousands of euros for SMEs, considered as those firms with 1-249 employees. And second, labour productivity data by size class of enterprises, although this time with SMEs defined as firms with 10-249 employees due to the OECD data structure. The labour productivity data were also converted to euros using average annual exchange rates for uniformity.

To select the type of correlation, the distributions of the variables were inspected. The composite cyber-readiness score exhibited normal distribution according to a Shapiro test, however neither trade nor productivity were normally distributed meaning a Spearman's correlation was selected. The variables were standardized before the correlations were executed.

3.3 Cyber-readiness Score and Trade

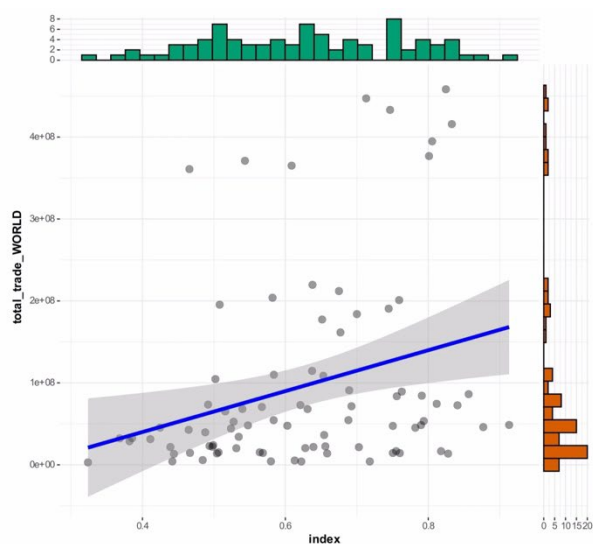
Preliminary findings show essentially no correlation between the cyber-readiness score and international trade for both MSMEs (0.29) and large firms (0.31) (Table 4). Further testing showed that each correlation between the separate components of the cyber-readiness score and international trade were weak.

Table 4: Cyber-Readiness Score and Trade Correlation

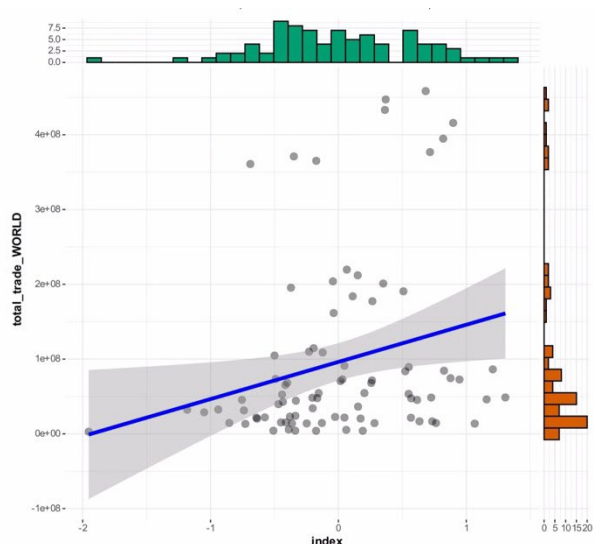
Spearman's rho	MSME (<250 employees)	Large Firms (250+ employees)
Cyber-readiness Score and International Trade	0.29	0.31

Figure 10: Cyber-Readiness Score and Trade Correlation

MSME (<250 employees)



Large Firms (250+ employees)



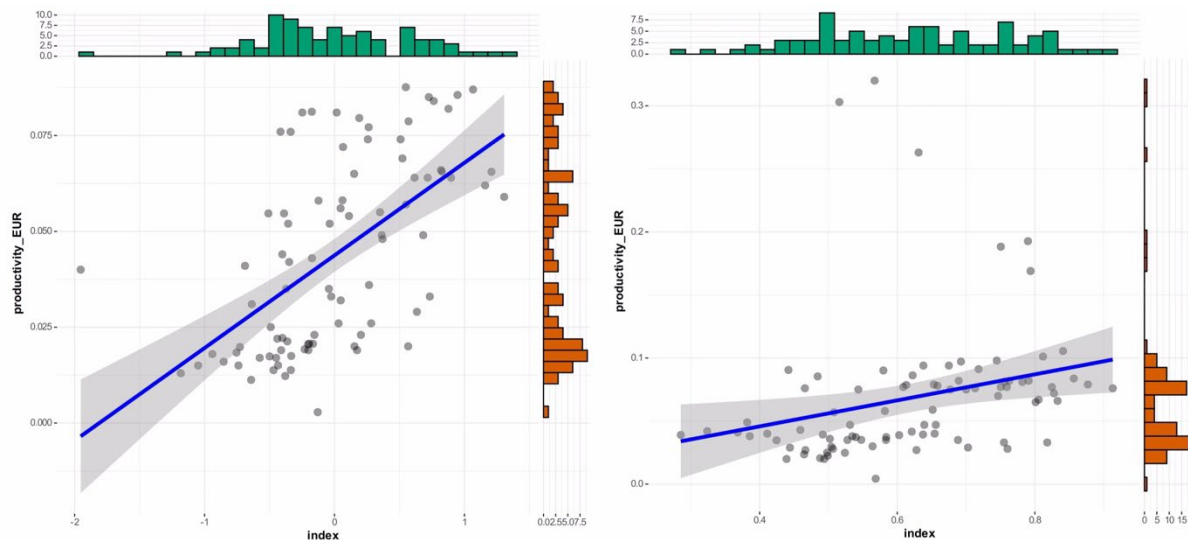
Note: Authors' calculations

3.4 Cyber-readiness Score and Productivity

The correlation between cyber-readiness and productivity was then tested and showed noticeably higher correlations than for international trade, especially for MSMEs (0.64). Within each of the different parts of the score, productivity was the most correlated with an economy's digital legal framework and digital intensity.

Table 5: Cyber-readiness Score and Productivity Correlation

Spearman's rho	MSME (<250 employees)	Large Firm (250+ employees)
Cyber-readiness Score and Productivity	0.64	0.48

Figure 11: Cyber-readiness Score and Productivity Correlation**MSME (<250 employees)****Large Firms (250+ employees)**

Note: Authors' calculations

3.5 Interpretation and Implications

The analysis shows only a weak positive correlation between cyber-readiness and trade. This is in line with other literature that has indicated a positive impact of digital tools on European trade (Dziubanovska et al., 2023) and other work showing a link between digitalization and MSME trade participation (Lanz et al., 2018). Reasons for only a weak positive correlation may be that other factors, such as access to finance, access to logistics, or access to information may be more related to trade participation, and digitalization is an indirect factor facilitating access to each of these pieces leading to the weaker link that appears in these data. Another possibility may be that components of the cyber-readiness score are too domestic-focused, such as the digital legal framework or cyber-attack variables. The digital legal framework variable is from a survey of firms about domestic policy development with no reflection on its implications for international transactions and the cyber-attacks information cover one-off events that may or may not impact international trade.

In contrast, the stronger correlation with productivity, especially for MSMEs relative to large firms, indicates potential for further developing the index. This result may also suggest that (as posited for one of the reasons the cyber-readiness index does not correlate with international trade) the cyber-readiness score is more focused on domestic aspects of the economy. The results also suggest that there is a link between cyber-readiness and competitiveness for smaller businesses specifically, which could be of interest for future study.

3.6 Limitations

Looking forward, there are three main limitations identified in the index that was developed.

1. **Data Gaps:** The analysis was constrained by data availability, particularly for the cybersecurity index score for 2019 that required imputed data. This approach, while practical, introduced assumptions that affect the precision of the findings. Further, the data only covered 29 European economies, leaving the analysis far from global. Data for additional economies in more regions would improve the analysis.
2. **Scope of the Cyber-readiness Score:** The composite cyber-readiness score, though broad, does not capture all dimensions of cyber-readiness relevant to MSME trade and may be too focused on domestic components. Future iterations of this research could benefit from incorporating additional measures of cyber-readiness, such as digital infrastructure or adoption of international digital legal frameworks such as UNCITRAL's Model Law on Electronic Transferable Records (MLETR) (UNCITRAL, 2017).
3. **No Causal Inference:** Given the observational nature of the study, the findings in no means imply causation.

3.7 Index Correlation Findings and Suggestions for Future Research

These first steps to create a cyber-readiness score to find a correlation with international trade found mixed success. Future work to broaden this study will require additional research and investigation to find data with fuller series, greater coverage and longer time series. More focus on international components of digitalization and trade relationships will likely be necessary. The positive correlation between MSME cyber-readiness and productivity is at least a reassurance that this could be a starting point for further investigation.

Building on the foundation laid by this study, future research could address the various limitations and explore new avenues through:

1. **Modifications to the Cyber-readiness Score:** Future studies could incorporate additional variables that capture other dimensions of international digital engagement and cyber threat mitigation to provide a more relevant index of cyber-readiness as it applies to international trade. Data availability, especially with a greater regional diversity, should also continue to be explored
2. **Causal Analysis:** Employing methodologies that allow for causal inference, such as instrumental variable techniques or natural experiments, could further elucidate the causal impact of cyber-readiness on MSME productivity and trade.
3. **Longitudinal Analysis:** As more data become available, a longitudinal study covering a broader time span could provide deeper insights into the evolving impact of cyber-readiness on trade and productivity.
4. **Sector-Specific Analysis:** Examining the impact of cyber-readiness within specific sectors could reveal industry-specific dynamics and inform targeted policy and business strategies.

4. OBSERVATIONS ON MSME CYBER-READINESS AND INTERNATIONAL TRADE

Overall, from the research, survey and attempt to develop an index for this paper, the authors have made a number of observations related to MSME cyber-readiness and international trade. First, government investments in essential infrastructure, such as reliable electricity and affordable internet, are associated with enhanced digital readiness among MSMEs. Establishing these fundamentals appears to correlate with improvements in cyber-readiness and trade facilitation when complemented by national strategies or frameworks that align with international standards (Potomac Institute for Policy Studies, 2015). However, as of 2023, only nine economies have been identified as having “mature national frameworks” (International Telecommunication Union (ITU) & World Bank, 2023).

At the individual level, effective cyber protection often relies on awareness and the proper implementation of basic cyber hygiene practices (e.g., strong passwords, regular software updates, and consistent data backups). The evidence indicates that improving information sharing and training, especially initiatives designed to address the persisting gender imbalance in the digital sector, could enhance MSME cyber-readiness. In this context, financial incentives such as grants, subsidies, or tax breaks for digitalization and cybersecurity investments have been suggested to play a supportive role (Cyber Readiness Institute, 2024).

Businesses themselves increasingly recognize their vulnerabilities to cyber incidents. For example, more than half of MSMEs in the eight high-income economies surveyed by Hiscox in 2024 acquired insurance policies against a cyber incident (Cyber Readiness Institute, 2024; Hiscox Ltd, 2023). Further, as seen in the survey presented in this paper, there is interest by businesses to demonstrate their cyber-readiness through certification that signals awareness and demonstrates capacity, for example the United Kingdom’s Cyber Essentials or Cybersecure Canada initiatives. Greater access to an affordable cyber-readiness signalling tool could benefit MSMEs.

Observations also suggest that the absence of robust reporting obligations for cyber incidents may inhibit businesses from learning from past attacks and significantly hinders research. For instance, during the January 2023 Hive ransomware incident, only about 20% of affected organizations reported paying a ransom (Daniel, 2023). The available evidence highlights how enhanced data collection and information sharing, including insights from emerging trends such as AI, which can both increase risks and help identify system vulnerabilities, could contribute to more proactive risk management.

5. CONCLUSION

This study embarked on an exploration of what cyber-readiness means and how to review its impact on inclusive international trade participation by MSMEs. Based on the research, cyber-readiness was defined to be the foundation underpinning digitization, digitalization and digital transformation. For MSMEs, this includes digital literacy, affordable and reliable access to digital tools and infrastructure,

access to digital finance and payment systems, access to software and systems, training for digital skills development, and cybersecurity systems.

Following from this concept of cyber-readiness, a survey was administered online to contacts engaged with the ITU to gauge how businesses and government representatives considered this term. The results offered insights into the perception of cyber-readiness, however respondents generally equated "cyber-readiness" with a narrower cybersecurity definition, suggesting a need for a broader understanding. While the survey did not establish a direct link between cyber-readiness and international trade, it revealed that many of the business respondents were highly internationalized and viewed cybersecurity certification programs favorably for building trust and business partnerships. However, challenges were raised such as concerns about costs of certification and the need for greater awareness and familiarity with international standards. Developing response plans for cybersecurity breaches can also enhance credibility with multinational clients and came out as an issue to address. Overcoming these challenges can help MSMEs strengthen their resilience and competitiveness in a digital, interconnected business environment. Policymakers have shown support for MSMEs, but the survey highlights a need for comprehensive cyber training programs. Finally, the survey suggests that establishing ethical guidelines and frameworks tailored to MSMEs could address concerns and promote responsible AI use and adoption.

Lastly, a new cyber-readiness score was developed to try to explore if any relation with MSME trade participation, and productivity, could be seen across 29 European economies over the years 2017 to 2019. Although no strong link with trade was found, cyber-readiness and MSME productivity showed a positive correlation. This suggests that the benefits of cyber-readiness may manifest in aspects of business performance not directly captured by trade volume metrics. It also suggests the importance of digital security measures in bolstering operational efficiency and output, suggesting that investments in cyber-readiness may be tied with productivity gains, but this requires formal modelling and further research.

These findings are a first step. This research appears to indicate that policymakers and business leaders should continue to prioritize enhancing cyber-readiness, especially within the MSME sector, and new areas for future work are identified. This focus on cyber-readiness is particularly pertinent in the digital age, where cyber threats pose increasing risks to business operations and economic security.

6. BIBLIOGRAPHY

- Alvarez, M. (2024, May). Manufacturing Is #1 in Cyber Attacks for Third Straight Year. What Can Be Done? *Industry Week*.
- Añón Higón, D., & Bonvin, D. (2024). Digitalization and trade participation of SMEs. *Small Business Economics*, 62(3), 857–877. <https://doi.org/10.1007/s11187-023-00799-7>
- Asian Development Bank (ADB). (2021). *Global Value Chain Development Report 2021*: Asian Development Bank (ADB). <https://doi.org/10.22617/TCS210400-2>
- Asian Development Bank (ADB). (2023). *Harnessing the Fourth Industrial Revolution through Skills Development in High-Growth Industries in Central and West Asia—Pakistan*. Asian Development Bank. <https://doi.org/10.22617/TCS230155-3>
- Botting, A. (2021, September). *Coalition to Reduce Cyber Risk (CR2)*. Regular Meeting of the MSME Informal Working Group, World Trade Organization. https://www.wto.org/english/tratop_e/msmes_e/cr2_sept21.pdf
- Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*.
- Cassetta, E., Monarca, U., Dileo, I., Di Berardino, C., & Pini, M. (2020). The relationship between digital technologies and internationalisation. Evidence from Italian SMEs. *Industry and Innovation*, 27(4), 311–339. <https://doi.org/10.1080/13662716.2019.1696182>
- Chen, C.-L. (2019). Value Creation by SMEs Participating in Global Value Chains under Industry 4.0 Trend: Case Study of Textile Industry in Taiwan. *Journal of Global Information Technology Management*, 22(2), 120–145. <https://doi.org/10.1080/1097198X.2019.1603512>
- Chen, J., Deepa Mahajan, Marie-Claude Nadeau, & Roshan Varadarajan. (2023). *Consumer digital payments: Already mainstream, increasingly embedded, still evolving* [Survey]. McKinsey. <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving>
- Cyber Readiness Institute. (2024). *Low Awareness, Lagging Implementation, Little Incentive: The State of Cyber Readiness Among Small and Medium-sized Businesses 2024*. <https://cyberreadinessinstitute.org/resource/low-awareness-lagging-implementation-little-incentive-the-state-of-cyber-readiness-among-small-and-medium-sized-businesses-2024/>
- Dziubanovska, N., Maslii, V., Krysovaty, A., Desyatnyuk, O., & Drelich-Skulska, B. (2023). The Effects of Digital Economy on International Trade: An Empirical Analysis of EU Countries Panel Data. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, 216–219. <https://doi.org/10.1109/ACIT58437.2023.10275723>
- eBay. (2016, January). *Small Online Business Growth Report: Towards an inclusive global economy*.
- eBay. (2024). *eBay Small Business Report*. 2023 Small Business Report.
- European Commission. (n.d.). *Overview of digital finance*. Retrieved https://finance.ec.europa.eu/digital-finance/overview-digital-finance_en#:~:text=Digital%20finance%20is%20the%20term,providing%20banking%20and%20financial%20services.
- Eurostat. (n.d.). *Digital Intensity Index (DII) composition overview 2015-2024*. Retrieved August 21, 2024, from https://ec.europa.eu/eurostat/cache/metadata/Annexes/isoc_e_dii_esmsip2_an_1.pdf
- Fomin, V. V., & Barlette, Y. (2008). *ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption*. <https://www.researchgate.net/publication/228898807>
- Ganne, E., Imessaoudene, Z., & Lundquist, K. (2022a). *Recent Evolution of Developed-economy MSME Participation in International Trade: MSME Research Note 1*. World Trade Organization (WTO).
- Ganne, E., Imessaoudene, Z., & Lundquist, K. (2022b). *Small and Medium Manufacturing Enterprise Trade Participation in Developing Economies: MSME Research Note 2*. World Trade Organization (WTO).
- Georgieva, E. (2022). Digitization, digitalization, and digital transformation: What's the difference? *Resolute*.
- Gopalan, S., Reddy, K., & Sasidharan, S. (2022). Does digitalization spur global value chain participation? Firm-level evidence from emerging markets. *Information Economics and Policy*, 59, 100972. <https://doi.org/10.1016/j.infoecopol.2022.100972>

- Grufman, N., Lyons, S., & Sneiders, E. (2020). Exploring Readiness of SMEs for Industry 4.0. *Complex Systems Informatics and Modeling Quarterly*, (25), 54–86. <https://doi.org/10.7250/csimq.2020-25.04>
- GSMA. (2023). *E-commerce in Africa: Unleashing the opportunity for MSMEs*. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2023/10/E-CommerceInAfrica_R_WebSingles.pdf
- Guo, H., Yang, Z., Huang, R., & Guo, A. (2020). The digitalization and public crisis responses of small and medium enterprises: Implications from a COVID-19 survey. *Frontiers of Business Research in China*, 14(1), 19. <https://doi.org/10.1186/s11782-020-00087-1>
- Hagsten, E., & Kotnik, P. (2017). ICT as facilitator of internationalisation in small- and medium-sized firms. *Small Business Economics*, 48(2), 431–446. <https://doi.org/10.1007/s11187-016-9781-2>
- Hamill, J., & Gregory, K. (1997). Internet marketing in the internationalisation of UK SMEs. *Journal of Marketing Management*, 13(1–3), 9–28. <https://doi.org/10.1080/0267257X.1997.9964456>
- Higgins, E. & Alexandre Pérusse. (2021, February). *Canadian SME Cybersecurity Initiatives & Programs*. Regular Open-ended Meeting of the MSME Informal Working Group, World Trade Organization.
- Hiscox Ltd. (2023). *Hiscox Cyber Readiness Report 2023*. <https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf>
- International Finance Corporation (IFC) & UKAid. (2021). *Covid-19 and Women-led MSMEs in Sub-Saharan Africa: Examining the impact, Responses, and Solutions*. IFC. <https://www.ifc.org/content/dam/ifc/doc/mgrt/202103-covid-19-and-women-led-msmes-sub-saharan-africa.pdf>
- International Telecommunication Union (ITU). (2021a). *Global Cybersecurity Index 2020*. International Telecommunication Union. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- International Telecommunication Union (ITU). (2021b). *ITU cybersecurity programme: CIRT framework*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYBERSEC-2021-01-PDF-E.pdf
- International Telecommunication Union (ITU), Broadband Commission for Sustainable Development. Working Group on Education, & UNESCO Institute for Statistics. (2017). *Working Group on Education: Digital skills for life and work*. <https://unesdoc.unesco.org/ark:/48223/pf0000259013>
- International Telecommunication Union (ITU) & UNESCO Institute for Statistics. (2020). *The State of Broadband: Tackling digital inequalities A decade for action*. International Telecommunications Union (ITU). https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.21-2020-PDF-E.pdf
- International Telecommunication Union (ITU) & World Bank. (2023, July 16). *National digital transformation strategy – mapping the digital journey*. Digital Regulation Platform. <https://digitalregulation.org/national-digital-transformation-strategy-mapping-the-digital-journey/#post-3004697-footnote-6>
- Is Digitalisation a Game Changer for SME Sustainable Finance? Hearing before the Centre for Entrepreneurship, SME and Entrepreneurship Division, OECD* (2024).
- Jin, H., & Hurd, F. (2018). Exploring the Impact of Digital Platforms on SME Internationalization: New Zealand SMEs Use of the Alibaba Platform for Chinese Market Entry. *Journal of Asia-Pacific Business*, 19(2), 72–95. <https://doi.org/10.1080/10599231.2018.1453743>
- Junior, C. R., Becker, I., & Johnson, S. (2023). *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity* (arXiv:2309.17186). arXiv. <https://doi.org/10.48550/arXiv.2309.17186>
- Kanyosa, G. R. & Chacha Magasi. (2025). Leveraging Social Media for Sales Performance: Evidence from SMEs Selling Electrical Devices in Dodoma City. *International Journal of Management Research and Emerging Sciences*, 15(2), 147–166.
- Kerner, R., & Kitsing, M. (2023). Small is Beautiful and Important: Economies and Firms Trading in Digital Services. *Journal of Business Economics and Management*, 24(1), 93–111. <https://doi.org/10.3846/jbem.2023.18585>
- Lanz, R., Lundquist, K., Mansio, G., Maurer, A., & Teh, R. (2018). *E-commerce and Developing Country-SME Participation in Global Value Chains* (WTO Working Papers No. 2018/13; WTO Working Papers, Vol. 2018/13). <https://doi.org/10.30875/ec5f0f21-en>

- Lendle, A., Olarreaga, M., Schropp, S., & Vézina, P.-L. (2016). There Goes Gravity: eBay and the Death of Distance. *The Economic Journal*, 126(591), 406–441.
<https://doi.org/10.1111/eoj.12286>
- Martínez-Cantos, J. L. (2017). Digital skills gaps: A pending subject for gender digital inclusion in the European Union. *European Journal of Communication*, 32(5), 419–438.
<https://doi.org/10.1177/0267323117718464>
- Marzano, G., & Lubkina, V. (2019). The Digital Gender Divide: An Overview. *Society. Integration. Education. Proceedings of the International Scientific Conference*, 5, 413.
<https://doi.org/10.17770/sie2019vol5.3849>
- McKinsey. (2022). *What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?*
[https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#/?](https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#/)
- Menon, S., & Shah, S. (2020). Growth of Digital Supply Chains for SME Transformation. 2020 *IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, 1–6. <https://doi.org/10.1109/ICTMOD49425.2020.9380603>
- Moeini Gharagozloo, M. M., Forghani Bajestani, M., Moeini Gharagozloo, A., Amini Sedeh, A., & Askarzadeh, F. (2023). The role of digitalization in decreasing gender gap in opportunity driven entrepreneurship. *Information Technology for Development*, 29(4), 645–664.
<https://doi.org/10.1080/02681102.2023.2237470>
- National Institute of Standards and Technology (NIST). (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity*.
<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>
- Nesbitt, J. (2023, September 20). 5 ways AI is transforming international trade Original article: <https://www.tradeready.ca/2023/featured-stories/5-ways-ai-is-transforming-international-trade/>. Tradeready. <https://www.tradeready.ca/2023/featured-stories/5-ways-ai-is-transforming-international-trade/>
- OECD. (2021). *The Digital Transformation of SMEs*. OECD. <https://doi.org/10.1787/bdb9256a-en>
- Organisation for Economic Co-Operation and Development (OECD). (n.d.). *Structural and Demographic Business Statistics* [Dataset]. OECD.
- Organisation for Economic Co-operation and Development (OECD). (2021). *OECD SME and Entrepreneurship Outlook 2021*. OECD. <https://doi.org/10.1787/97a5bbfe-en>
- Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. *Complex Systems Informatics and Modeling Quarterly*, (33), 53–66. <https://doi.org/10.7250/csimq.2022-33.04>
- Phipson, S. (2022, July). How vulnerable supply chains deliver a world of trouble. *IMD*.
<https://www.imd.org/ibyimd/magazine/how-vulnerable-supply-chains-deliver-a-world-of-trouble/>
- Potomac Institute for Policy Studies. (2015). *Cyber Readiness Index 2.0, A Plan for Cyber Readiness: A baseline and an Index*.
<https://www.potomacinstitute.org/images/CRI/crindex2.0.pdf>
- Rashid, A. T. (2016). Digital Inclusion and Social Inequality: Gender Differences in ICT Access and Use in Five Developing Countries. *Gender, Technology and Development*, 20(3), 306–332. <https://doi.org/10.1177/0971852416660651>
- Rosyidah, U., Sudarmiatin, S., & Sumarsono, H. (2023). Digitalization and internationalization of SMEs: A Systematic Literature Review. *Journal of Enterprise and Development*, 5(3), 479–499. <https://doi.org/10.20414/jed.v5i3.7196>
- Sibony, O. (2024, March). How to ensure ESG integrity across your supply chain. *SME Guidance for Business Growth*. <https://www.smeweb.com/how-to-ensure-esg-integrity-across-your-supply-chain/>
- Solomon, O. H., Allen, T., & Wangombe, W. (2023). Analysing the factors that influence social media adoption among SMEs in developing countries. *Journal of International Entrepreneurship*. <https://doi.org/10.1007/s10843-023-00330-9>
- Statista. (2024). *Annual cost of cybercrime worldwide 2018-2029* [Survey].
- Takeda, A., Truong, H. T., & Sonobe, T. (2022). The impacts of the COVID-19 pandemic on micro, small, and medium enterprises in Asia and their digitalization responses. *Journal of Asian Economics*, 82. <https://doi.org/10.1016/j.asieco.2022.101533>
- Thakur, D. (2018, April 13). What IS affordable internet access anyway? *Web Foundation*.
<https://webfoundation.org/2018/04/what-is-affordable-internet-access-anyway/>
- UN Women. (2025, November 13). *FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls*. UN Women – Headquarters.
<https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>

- UNCTAD. (2024). *Business e-commerce sales and the role of online platforms*. United Nations.
- UNESCO Institute for Statistics. (2018a). Digital literacy. In *A global framework of reference on digital literacy skills for indicator 4.4.2*.
<https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en>
- UNESCO Institute for Statistics. (2018b, March 15). *Digital skills critical for jobs and social inclusion*. <https://www.unesco.org/en/articles/digital-skills-critical-jobs-and-social-inclusion>
- United Nations Institute for Disarmament Research (UNIDIR). (n.d.). *Cyber Policy Portal* [Dataset]. <https://cyberpolicyportal.org/>
- University of Maryland. (n.d.). *University of Maryland CISSM Cyber Attacks Database* [Dataset]. Retrieved August 21, 2024, from <https://cissm.liquifiedapps.com/>
- Vanta. (n.d.). *How much does ISO 27001 certification cost?* Retrieved August 23, 2024, from <https://www.vanta.com/collection/iso-27001/iso-27001-certification-cost>
- Women in Tech. (2023). *Women in Tech Survey 2023*. Women in Tech.
<https://www.womenintech.co.uk/wp-content/uploads/2022/12/Women-in-Tech-Survey-2023.pdf>
- World Bank. (n.d.). *Digital Development Overview: Development news, research, data*.
<https://www.worldbank.org/en/topic/digitaldevelopment/overview>
- World Economic Forum, Schwab, K., & Zahidi, S. (2020). *The Global Competitiveness Report Special Edition 2020* (2020 ed). World Economic Forum.
- World Trade Organization (WTO). (2016). *World Trade Report 2016: Levelling the trading field for SMEs*. WTO.

1 ANNEXES

1.1 Annex 1: ISO 27001 issued by economy, 2006-2024

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Afghanistan				2	1	5				5						343		11	2
Åland Islands																			1
Albania						3	2	7	8	22	44	15	19	33	33	41	52	93	129
Algeria						1	1	2			4	5	1	1	1	1	1	2	3
Andorra									1	1	1	2	1	1	1		1	1	3
Angola				1	1							2	4	2					3
Argentina	1	1	6	4	8	24	33	40	23	52	88	57	48	38	57	118	100	144	81
Armenia			1				3	7	3	22	22	37	12	19	17	20	10	14	41
Aruba																			1
Australia	59	55	63	55	82	94	113	138	157	176	531	404	264	325	562	775	717	1,012	2,217
Austria	16	23	32	37	54	59	28	75	87	91	146	146	157	81	188	75	253	75	413
Azerbaijan									2	2	2	5	2	3	3	5	9	12	22
Bahamas												2	1			1			1
Bahrain	3	5	8	12	8	6	15	20	26	27	24	24	26	44	53	45	43	51	44
Bangladesh				2	1	1	9	9	15	9	11	4	8	12	43	40	39	62	120
Barbados				1	1						1	2							1
Belarus				1	1	1	1	1	1	3	2	9	15	15	33	56	46	68	26
Belgium	4	9	15	19	26	29	31	47	43	53	98	127	94	114	141	190	228	185	347
Belize										1	1	1	1	1	1	1	1	1	1
Benin												1						1	2
Bermuda												1	1	1	1	1		2	3
Bhutan													1	3	6	2	5	3	9

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Bolivia (Plurinational State of)				1	1	3	1	1	1	1	6	7	5	6	4	12	6	3	9
Bosnia and Herzegovina				4	4	2	7	9	9	13	17	27	24	31	51	64	58	60	86
Botswana							1		1	1	3	4	2	1	1	11	1	1	
Brazil	10	25	40	48	41	50	53	82	85	94	117	170	110	133	148	165	279	309	373
Brunei Darussalam												1				1			2
Bulgaria		8	23	60	116	132	208	278	330	273	261	250	339	367	372	454	515	554	752
Burundi				1	1							1							
Cabo Verde										1	1	1	2	4	1	1	1	2	2
Cambodia				1	1						1	4	1	2	3	6	5	8	8
Cameroon												1		1	1			1	3
Canada	1	5	13	21	26	50	62	66	66	94	133	276	118	148	200	295	261	240	354
Cayman Islands												5	3		1	2	1	6	13
Chad												1							
Chile	2	3	7	10	13	18	23	24	24	32	49	64	54	77	89	74	85	123	134
China	75	146	236	459	509	664	790	965	1,210	1,469	2,618	5,069	7,199	8,356	12,403	18,446	26,301	4,108	33,359
Colombia	3	8	11	14	23	27	58	82	78	103	163	148	146	189	238	269	338	395	282
Comoros										1								2	
Congo (the Democratic Republic of the)																2	3	3	2
Congo, Republic of				1	1		1			1	1	5	1		2	1		1	1
Costa Rica			2	5	6	7	7	10	22	4	21	21	6	2	5	13	8	15	14
Côte d'Ivoire										1	1	2		2	1	3	2	8	7
Croatia	2	5	10	22	24	32	58	69	96	55	110	123	138	190	302	333	300	325	379
Cuba			1	1	2														
Curaçao																			2
Cyprus				3	4	5	9	16	9	13	11	32	32	39	42	59	61	78	116
Czech Republic	27	77	88	264	529	301	264	399	276	381	507	463	543	462	394	671	713	711	703
Denmark	3	4	4	9	6	5	7	8	13	29	68	57	48	69	81	120	145	130	157

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Djibouti												2					1	1	1
Dominica												1							1
Dominican Republic				1	1	2	3	4	3	4	8	5	5	6	6	6	5	7	12
Ecuador				1	1	1	3	5	7	6	11	8	6	9	13	11	28	42	64
Egypt	1	2	3	7	8	6	11	17	11	7	20	25	17	14	18	21	28	37	78
El Salvador					1	1	1	1	1	1	4	4		3	4	5	4	5	5
Estonia		1	1	1	1	1	2	2	3	2	4	9	9	10	17	28	32	51	49
Eswatini							1				1	2	1			6		1	1
Ethiopia				1	1											1	2	3	5
Faroe Islands (the)																			1
Fiji							1				2	1				1	1	1	2
Finland	1	14	13	18	23	27	28	32	33	44	54	72	59	66	102	180	139	183	162
France	5	9	14	15	31	46	66	94	155	227	209	342	223	351	392	606	927	1,019	791
French Polynesia																			1
Gabon							1					3					1		1
Gambia														3	1	1	1	1	
Georgia								1			2	2	2	2	3	3	6	6	21
Germany	95	135	239	253	357	424	488	581	634	994	1,338	1,339	1,057	1,175	1,281	1,673	1,582	1,563	2,444
Ghana				3	1	3		3		6	13	14	19	30	42	62	59	82	97
Gibraltar (UK)				1						5	3	3	2		1	5	4	4	3
Greece	3	5	20	28	44	45	49	77	62	136	150	727	240	336	454	474	477	576	1,410
Greenland																			1
Grenada																			412
Guadeloupe																			2
Guatemala					1	1	1	2	3	2	5	6	4	7	13	16	19	18	17
Guernsey																			3
Guinea												1							1

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Guyana				1	1														
Haiti													1	1	1		1	1	1
Honduras						1	1		1		5	3	1	4	6	5	5	10	3
Hong Kong, China	29	36	59	72	78	99	110	124	125	141	173	182	72	158	186	216	243	184	214
Hungary	54	81	135	146	151	178	199	280	295	323	421	472	484	554	#N/A	661	680	718	622
Iceland	10	11	13	16	20	21	20	26	31	29	57	60	39	48	52	4	53	2	44
India	369	508	813	1,240	1,281	1,427	1,611	1,931	2,168	2,490	2,902	3,272	2,161	2,309	2,226	2,775	2,969	3,877	6,758
Indonesia	2	3	7	13	22	29	35	48	62	65	115	222	163	274	542	702	822	783	1,339
Iran, Islamic Republic of		1	1	6	7	13	4	9	23	23	23	16	20	23	14	4			12
Iraq				10		1			1								1	15	39
Ireland	6	7	10	21	24	30	48	54	131	140	175	209	214	221	89	361	414	123	265
Isle of Man																			6
Israel		24	61	78	86	110	130	185	201	246	416	345	439	695	837	1,056	1,467	1,712	1,694
Italy	175	148	233	297	374	425	495	901	969	1,013	1,220	958	1,041	1,365	1,827	1,924	2,424	3,176	3,284
Jamaica				1	1						10	11	1	1	1	1	1	2	2
Japan	3,790	4,896	4,425	5,508	6,237	6,914	7,199	7,140	7,171	8,240	8,945	9,161	5,093	5,245	5,645	6,587	6,987	5,599	6,644
Jersey																			16
Jordan		1	1	1	2	1	3	2	2	1	7	44	14	23	24	30	30	46	49
Kazakhstan			3	4	3	3	5	8	7	7	12	30	15	9	16	18	23	12	35
Kenya				1	1				4	12	6	11	7	14	14	26	27	32	62
Korea, Democratic People's Republic of			95		1		1		2	1	1	2				2	34		27
Korea, Republic of	50	77	94	174	166	191	230	252	288	305	364	369	353	442	438	460	451	607	918
Kosovo																			63
Kuwait	4	6	7	10	18	15	17	15	18	20	13	21	30	29	44	58	40	71	125
Kyrgyzstan		1	1	2	1							1							5
Lao People's Democratic Republic										1	2	4	3	2	2	2	4	1	2
Latvia			1	2	6	9	9	18	24	24	30	42	36	45	48	58	73	77	57

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Lebanon	1			1	1	3	3	3	1	2	4	7	8	14	13	14	16	11	23
Lesotho				1	1														
Liberia																			1
Libya																1	2	3	2
Liechtenstein												1			1	1	2	5	7
Lithuania		2	3	7	11	14	19	23	25	35	43	85	92	56	88	107	59	80	99
Luxembourg	1	2	2	2	5	8	7	5	7	10	20	25	24	27	17	43	53	47	58
Macao	2	5	2	7	9	12	13	15	16	19	13	14	13	18	21	18	11	2	8
Madagascar																		1	3
Malawi				1	1						1	3							
Malaysia	18	23	34	38	60	72	100	181	232	240	260	317	276	314	290	290	366	336	677
Maldives																	1		1
Mali													1	1	1	2	1		1
Malta		1	1	1	2	2	5	7	7	7	53	18	18	26	32	33	66	54	82
Marshall Islands												1							1
Mauritius			1	2	3	4	8	11	9	8	12	17	16	17	19	22	25	26	22
Mexico	9	13	31	49	56	70	75	80	94	104	221	315	218	252	258	279	385	589	475
Micronesia (Federal States of)												1							
Moldova, Republic of	1	1	1	2	2	1	1	3	7	7	10	2	10	4	11	13	4	6	15
Monaco												2	2	3	1	5	6	6	7
Mongolia								1	1	1	2	2	2	3	5	4	7	45	75
Montenegro								1	5	1		2	11	11	9	3	10	26	40
Morocco			2	2	1	5	7	9	5	18	28	30	12	16	34	42	40	35	36
Mozambique				1	1				1	1	1	2				2	2	1	5
Myanmar				1	1						1	1	1		2	2	5	7	12
Namibia												4							6
Nepal				1	1					1		1	1	4	5	14	19	17	40

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Netherlands	41	41	56	76	97	125	190	316	335	455	670	913	788	938	1,326	1,508	1,741	1,349	1,568
Netherlands Antilles (NL)												1		1			1		
New Zealand	1	1	4	5	5	5	5	12	1	7	27	28	17	39	66	79	89	67	154
Nicaragua												6							3
Niger				1	2														
Nigeria						5	9	12	16	39	49	54	43	55	62	93	105	144	162
North Macedonia																			74
North Macedonia	1	1	4	6	7	7	5	9	9	13	13	27							74
Norway	15	22	16	17	25	31	16	26	70	49	81	87	74	98	120	127	169	171	230
Oman	3	4	3	8	9	11	10	11	8	7	20	12	19	18	23	31	30	27	64
Pakistan	1	4	12	28	18	19	16	17	28	31	29	35	34	32	35	83	127	177	183
Palau												1							
Palestine				1	1		1	1		1	1	1		1			2		3
Panama					1	1	2	1			2	8	1	2	3	4	6	14	24
Papua New Guinea												1			1	2	2	5	7
Paraguay												2	1	2	2	3	2	5	9
Peru	1	1	2	6	9	5	7	9	12	22	32	43	49	79	85	61	107	161	193
Philippines	10	24	27	47	38	59	66	73	47	38	168	174	94	102	110	139	122	127	155
Poland	11	45	75	187	229	233	279	307	310	448	657	705	700	652	710	876	789	846	1,410
Portugal	1	4	4	5	17	20	34	58	55	56	96	112	85	121	90	101	106	208	170
Puerto Rico			2	2	2	2	2	2			2	1		1	2	1	1		5
Qatar			1	3	6	9	7	23	28	35	40	39	38	45	58	66	90	90	135
Réunion																			1
Romania	4	16	44	303	350	575	866	840	893	1,078	513	440	585	654	729	951	1,043	1,510	792
Russian Federation	5	9	17	53	72	31	27	48	43	55	62	78	70	81	90	95	30	25	53
Rwanda				1	1						2	4	1	4	4	5	6	9	7
Saint Kitts and Nevis																1			

[illegible]

Country	Year																		
	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Togo												2	1	2	2	2	1	1	
Trinidad and Tobago							1	1	1	1	2	2	1			1	1	1	5
Tunisia				2		1	2	8	5	8	12	15	18	21	27	32	16	21	35
Türkiye	10	27	33	86	117	100	132	181	224	268	500	531	707	729	881	706	774	983	3,202
Turkmenistan																1	1	2	2
Turks and Caicos Islands (the)																			1
Uganda				1	1						2	3		1	4		12	15	19
Ukraine	1	1	3	5	1	6	7	12	9	12	22	47	49	55	59	75	87	87	97
United Arab Emirates	14	15	27	53	57	73	96	123	131	179	199	345	208	230	235	272	256	298	563
United Kingdom	486	519	738	946	1,157	1,464	1,701	1,923	2,253	2,790	3,367	4,503	2,444	2,818	3,327	5,256	6,084	3,630	4,455
United States of America	69	94	168	252	247	315	415	566	654	1,247	1,115	1,517	911	757	1,058	1,742	1,980	1,898	4,260
Uruguay	1		1	4	4	7	7	8	11	21	28	31	13	19	13	48	59	75	61
Uzbekistan												1				1	1	3	14
Vanuatu												1	1			1	1	1	3
Venezuela								1	1	8	4								
Viet Nam	1	2	7	5	21	36	44	39	94	70	64	198	113	327	348	375	293	293	430
Virgin Islands (British)																			1
Yemen			1																4
Zambia				1	2	1					2	4		3	4	4	4	3	7
Zimbabwe				1	1						1	3					2	3	3
Total	5,797	7,732	9,246	12,935	15,178	16,800	18,920	21,604	23,005	27,536	33,290	39,501	31,872	36,304	44,443	58,637	71,491	47,229	96,781

Note: Certificates are issued by accredited certification bodies. Reporting is not standard in all of these bodies and therefore these figures are illustrative and do not include all certificates issued.

Source: IAF ISO Survey [ISO Survey | Powered by IAF CertSearch](#)

1.2 Annex 2: ISO 27001 Certificates by Sector, 2006-2024

Year																							
ISO/IEC 27001 BY INDUSTRIAL SECTOR	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
Agriculture, fishing	1	45	1	13	8	14	13	13	10	9	5	11	18	16	13	20	13	13	1				
Mining and quarrying		1	3	6	2	12	31	34	25	8	9	7	11	80	13	10	15	10	84				
Food products, beverages and tobacco	3	14	1	10	6	8	10	24	10	12	61	17	24	181	24	47	85	283	172				
Textiles and textile products		1	1	3	3	2	12	10	4	10	132	11	20	499	37	84	99	1,143	622				
Leather and leather products				1	2	5	1	2		1	1	2	2	22		3	6	5	4				
Wood and wood products				1	3	5	4	4	1	12	12	12	1		1	6	20	21	1				
Pulp, paper and paper products	2	6	6	7	4	7	13	17	15	9	10	12	9	38	12	19	30	46	5				
Publishing companies	1	5	6	10	11	20	18	22	20	11	10	17	22	22	18	21	20	26	4				
Printing companies	34	84	30	62	78	101	121	148	126	143	130	187	130	168	164	172	177	164	8				
Manufacture of coke & refined petroleum products	3	6	9	8	3	5	4	14	10	4	3	7	42	20	10	13	16	13	10				
Nuclear fuel						1	1	2			-	1	1	2	1	2	2	2	1				
Chemicals, chemical products & fibres	7	3	3	9	9	9	11	24	12	10	18	20	38	30	24	31	58	64	6				
Pharmaceuticals		1	3	4	6	3		3	6	6	9	9	6	8	3	16	24	16	12				
Rubber and plastic products	7	5		10	15	16	16	36	14	16	32	36	38	45	41	45	114	138	43				
Non-metallic mineral products	1	3		16	16	8		5	13	3	7	1	5	8	7	2	18	17	28				
Concrete, cement, lime, plaster, etc.	1	1	1	6	6	14	27	25	26	13	17	7		4	5	5	11	19	55				
Basic metal & fabricated metal products	10	5	2	16	25	28	36	50	42	37	51	50	55	121	108	71	219	214	85				
Machinery and equipment	18	10	9	29	31	36	43	52	66	51	68	73	104	99	102	113	132	171	60				
Electrical and optical equipment	38	58	50	135	221	280	342	289	287	296	311	316	227	368	388	477	602	579	513				
Shipbuilding			2	5	3	3	4	8	4	1	2		1	16	3	5	22	17	26				
Aerospace		7	12	22	24	17	22	18	19	21	27	29	12	19	13	21	9	18	6				
Other transport equipment	1	3	2	4	4	7	4	25	10	19	27	13	15	15	42	19	52	64	33				
Manufacturing not elsewhere classified	4	14	2	5	5	23	8	5	7	6	13	22	18	38	18	25	43	33	8				
Recycling	2	10	4	11	32	44	61	72	57	36	57	49	57	59	52	60	45	56	19				
Electricity supply	8	10	11	20	9	12	15	45	38	34	61	87	64	140	129	120	181	150	99				
Gas supply		2	2	4	3	2	6	6	10	10	12	25	28	44	22	19	19	22	20				
Water supply	1	1	2	11	13	13	10	23	24	23	19	20	8	53	40	63	62	46	88				
Construction	55	17	12	127	266	350	409	396	454	186	216	193	309	410	417	527	589	773	96				
Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household goods	12	38	26	93	164	214	215	224	206	198	202	283	304	366	404	562	475	560	265				
Hotels and restaurants	2	4		6	10	32	4	5	2	6	7	10	9	25	14	17	31	21	20				
Transport, storage and communication	60	70	63	170	184	241	288	322	327	301	401	930	369	989	620	6,909	7,511	1,043	1,058				
Financial intermediation, real estate, rental	47	54	68	148	185	113	138	169	187	197	250	344	276	560	564	645	638	701	348				
Information technology	890	1,236	1,152	2,086	3,217	3,588	4,558	5,059	4,933	5,573	6,578	7,478	6,822	8,562	10,167	10,644	11,916	11,191	4,671				
Engineering Services	25	33	48	173	122	126	189	211	217	201	245	382	291	369	399	630	532	647	288				
Other Services	189	204	228	380	579	564	755	849	867	959	1,432	1,369	893	1,435	1,359	1,693	1,667	1,604	1,097				
Public administration	23	33	79	181	79	106	155	192	191	212	235	185	281	272	321	338	382	271	255				

Education	8	9	25	47	75	65	102	101	83	104	109	54	137	176	187	262	232	207	187
Health and social work	14	10	61	102	102	145	201	201	215	231	220	216	278	408	389	393	382	300	598
Other social services	8	13	16	46	54	75	98	106	102	125	163	105	155	195	188	219	262	616	220

Note: Certificates are issued by accredited certification bodies. Reporting is not standard in all of these bodies and therefore these figures are illustrative and do not include all certificates issued.

Source: IAF ISO Survey [ISO Survey | Powered by IAF CertSearch](#)

1.3 Annex 3: Components of the Eurostat digital intensity score

2017	2018	2019
Enterprises where more than 50% Of the persons employed used computers with access to the internet for business purposes.	Enterprises where more than 50% Of the persons employed used computers with access to the internet for business purposes.	Enterprises where more than 50% Of the persons employed used computers with access to the internet for business purposes.
Employ ICT specialists	Employ ICT specialists	Use at least 3 ICT security measures
The maximum contracted download speed of the fastest internet connection is at least 30 Mb/s	The maximum contracted download speed of the fastest internet connection is at least 30 Mb/s	The maximum contracted download speed of the fastest internet connection is at least 30 Mb/s
Provide more than 20% of the employed persons with a portable device that allows internet connection via mobile telephone networks for business purposes	Provide more than 20% of the employed persons with a portable device that allows internet connection via mobile telephone networks for business purposes	Provide more than 20% of the employed persons with a portable device that allows internet connection via mobile telephone networks for business purposes
Have a website	Have a website	Enterprises make persons employed aware of their obligations in ICT security related issues
Website has at least one of description of goods or services, price lists; possibility for visitors to customise or design online goods or services; tracking or status of orders placed; personalised content in the website for regular/ recurrent visitors	Website has at least one of description of goods or services, price lists; possibility for visitors to customise or design online goods or services; tracking or status of orders placed; personalised content in the website for regular/ recurrent visitors	Received electronic orders (web or EDI) from customers from other EU countries
use any social media	Website has links or references to the enterprise's social media profiles	use any social media
Have Enterprise Resource Planning (ERP) software package to share information between different functional areas	Buy medium-high call center (CC) services	Have Enterprise Resource Planning (ERP) software package to share information between different functional areas
Have Customer Relationship Management (CRM)	e-Invoices sent, suitable for automated processing	Have Customer Relationship Management (CRM)
Share supply chain management information electronically with other enterprises, either suppliers or customers	Pay to advertise on the Internet	use social media for at least two purposes
Used any computer networks for sales (at least 1%)	Used any computer networks for sales (at least 1%)	Used any computer networks for sales (at least 1%)
Enterprises where web sales are more than 1 % of the total turnover and B2C web sales more than 10% of the web sales	Enterprises where web sales are more than 1 % of the total turnover and B2C web sales more than 10% of the web sales	Enterprises where web sales are more than 1 % of the total turnover and B2C web sales more than 10% of the web sales

*Highlighted cells indicate a change compared to the previous year.

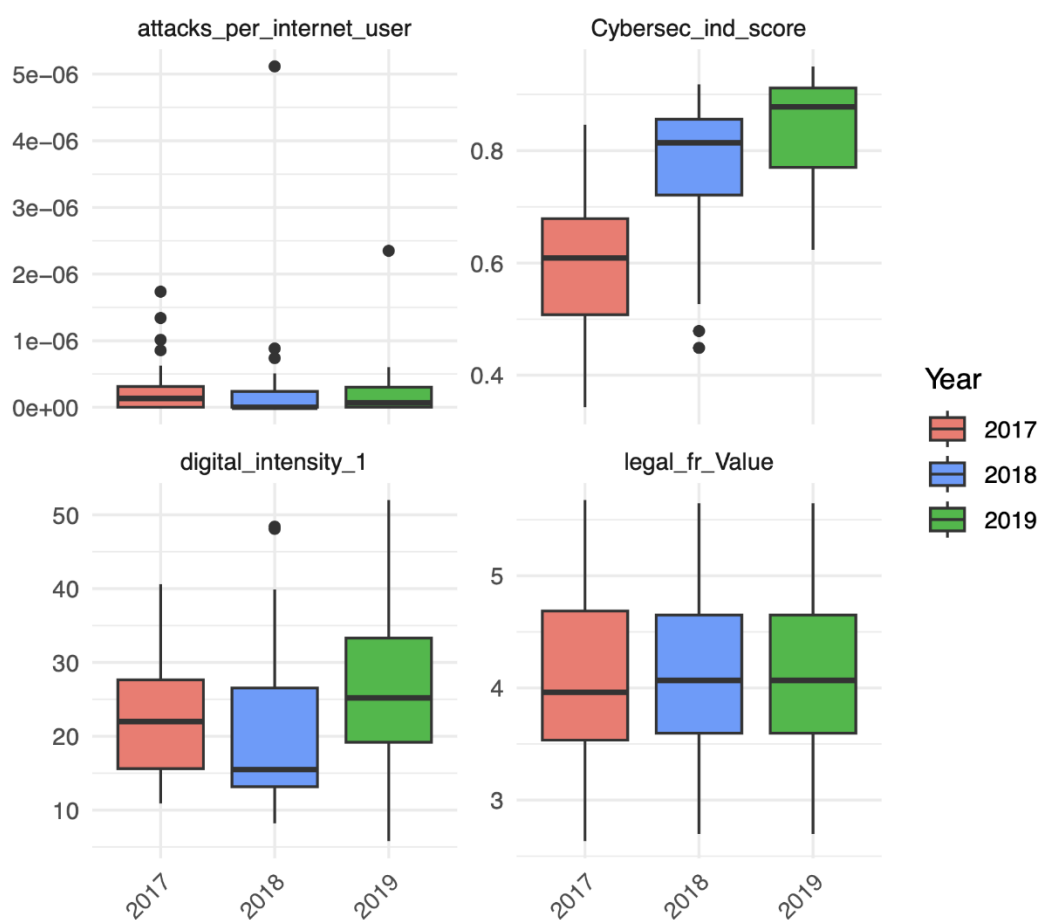
Source: (Eurostat, n.d.)

1.4 Annex 4: WEF GCI Legal framework's adaptability to digital business models

Economy	2017	2018	2019
Austria	4.241758	4.241758	4.241758
Belgium	3.695652	3.695652	3.695652
Bulgaria	3.35	3.35	3.35
Croatia	2.721519	2.721519	2.721519
Cyprus	3.485714	3.485714	3.485714
Czech Republic	3.592592	3.592592	3.592592
Denmark	4.392405	4.392405	4.392405
Estonia	5.28	5.28	5.28
Finland	5.133333	5.133333	5.133333
France	3.932432	3.932432	3.932432
Germany	5.0875	5.0875	5.0875
Greece	2.633803	2.633803	2.633803
Hungary	3.194805	3.194805	3.194805
Iceland	4.676923	4.676923	4.676923
Ireland	4.081633	4.081633	4.081633
Italy	3.128981	3.128981	3.128981
Latvia	2.956522	2.956522	2.956522
Lithuania	4.255319	4.255319	4.255319
Luxembourg	5.675	5.675	5.675
Malta	4.22449	4.22449	4.22449
Netherlands	5.135135	5.135135	5.135135
Norway	4.714286	4.714286	4.714286
Poland	3.550505	3.550505	3.550505
Portugal	3.597015	3.597015	3.597015
Romania	3.989583	3.989583	3.989583
Slovak Republic	3.330097	3.330097	3.330097
Slovenia	3.872093	3.872093	3.872093
Spain	3.695652	3.695652	3.695652
Sweden	5.230769	5.230769	5.230769

Source: WEF

1.5 Annex 5: Boxplots of the four components of the Cyber-readiness Score for the years 2017, 2018 and 2019.



Source: Authors' calculations

1.1 Annex 6: Index variables correlation matrix

	Cybersec_ind_s core	digital_intensit y_1	legal_fr_Val ue	attacks_per_internet_ user
Cybersec_ind_score	1.00	0.26	0.32	-0.20
digital_intensity_1	0.26	1.00	0.59	0.20
legal_fr_Value	0.32	0.59	1.00	0.18
attacks_per_internet_user	-0.20	0.20	0.18	1.00

Source: Authors' calculations