



APAC Cybersecurity Fund



The Asia Foundation

# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs In The APAC Region

---



**From Vulnerability To Resilience Cybersecurity Challenges For MSMEs In The APAC Region.**

KUALA LUMPUR, MALAYSIA. July 2024.

© The Asia Foundation 2024.

All rights reserved. No part of this report may be reproduced without written permission by The Asia Foundation.



## Executive Summary

The COVID-19 pandemic sparked an acceleration of digitalization in micro, small, and medium enterprises (MSMEs) that has increased the exposure of these enterprises to cyber threats. Ransomware\*, phishing\*, and other forms of cyberattacks exploit the vulnerabilities of MSMEs, which are often less equipped than larger corporations to defend against digital assaults. Organizations in the nonprofit sector are also moving quickly toward greater digitalization, but often lack the necessary resources or commitment to implement sufficient cybersecurity mechanisms, despite frequently handling sensitive data from donors and stakeholders. In the Asia-Pacific (APAC) region, this is compounded by variabilities in the digital infrastructure, with some countries boasting advanced capabilities while others lag significantly behind.

This report provides a comprehensive analysis of the cybersecurity landscape for MSMEs across 12 countries in the APAC region, with a particular focus on how the COVID-19 pandemic, alongside other factors, has shaped the cybersecurity threats now faced by these businesses. It also offers a summary of the cyber threat landscape confronting nonprofit organizations (NPOs) and non-governmental organizations (NGOs) in the region. Utilizing a blend of primary and secondary research methodologies, it captures the experiences and views of a range of stakeholders and experts, including those affected by cybersecurity challenges.



One of the stark findings of this research is the extent to which cybersecurity incidents are underreported by MSMEs and by NPOs, many of which opt to hide the occurrence of these breaches, fearing reputational damage and a subsequent loss of business or donor trust. At the same time, there is a notable lack of cybersecurity awareness and training within and among these enterprises and organizations. Absent the requisite digital literacy and an operational understanding of cybersecurity measures, these entities are at an increased risk from cyber threats, but may not have the wherewithal to realize it. Hence, many allocate too little of their budget towards cybersecurity, having underestimated their own vulnerabilities.

In some of the countries under study, the prevalence of informal economic activity adds complexity to the cybersecurity landscape and complicates the design of potential cybersecurity interventions. For example, high levels of informal employment present challenges to data gathering and risk assessment for cybersecurity initiatives. Moreover, this can make it difficult to develop comprehensive strategies that encompass all the economic activities in which MSMEs are engaged.

Because MSMEs form an essential part of the economy of the APAC region, their vulnerability to cyber threats poses a risk not only to individual businesses but also to regional economic stability. The findings of this research thus highlight an urgent need for tailored educational programming and resources aimed at improving the cybersecurity practices of MSMEs in the APAC region. This should include awareness raising related to the nature and objectives of cyber threats and capacity building to better equip MSMEs to effectively manage and mitigate potential cyberattacks.

There is little question that the digital age has delivered new opportunities for economic growth and expansion for MSMEs, across the APAC region and elsewhere, but it has also ushered in new challenges that require careful management through a proactive approach. To thrive in this digital age, while enjoying security and stability, MSMEs as well as NPOs and more specifically NGOs must be able to assess their cybersecurity risks and implement appropriate measures preemptively. The APAC Cybersecurity Fund (ACF) seeks to strengthen the cybersecurity ecosystem of the region by equipping these businesses and organizations with the skills necessary to navigate the internet safely and confidently.



# Table Of Contents

## Country Analysis





## Acknowledgment

We would like to express our deepest gratitude to the numerous organizations and individuals whose support and contributions were instrumental to the creation of this report. Their expertise, resources, and unwavering commitment greatly enriched this research, and offered valuable insights into cybersecurity landscapes across the APAC region.



The Asia Foundation is a nonprofit international development organization committed to improving lives and expanding opportunities across Asia and the Pacific. Informed by 70 years of experience and deep local knowledge, our work is focused on governance, climate action, gender equality, education and leadership, inclusive growth, and international cooperation. We work in more than 20 countries through our 17 permanent country offices and programs across Asia and the Pacific, supported by a headquarters in San Francisco and an office in Washington, DC. Our funding comes from a diverse array of bilateral and multilateral development agencies, foundations, corporations, and individuals.



GLG Partners is an award-winning program for nonprofits around the world, helping them answer technical, operational and/or strategic challenges – all at no cost. GLG is the world’s insight network and the pioneer of the expert economy. We connect decision makers to the right experts so they can act with the confidence that comes from true clarity. Our network of experts is the world’s most varied and qualified source of first-hand expertise, and we recruit thousands of new experts every day. Thank you to GLG for providing us with pro bono access to their services through GLG Partners.



MercyCorps Indonesia Mercy Corps is a global team of humanitarians working together on the front lines of today’s biggest crises to create a future of possibility, where everyone can prosper. Its mission: to alleviate suffering, poverty, and oppression by helping people build secure, productive, and just communities. Thank you to MercyCorps Indonesia for their insights and contributions to the research.





SJK Geostrategic Advisory: is founded and led by its Executive Director Dr Shashi Jayakumar. With his extensive background in the security sector in the government of Singapore's Administrative Service as well as in security and policy think tanks, SJK Geostrategic Advisory's product combines real-world experience with deep insight and academic rigour. Practical and actionable analysis is brought to bear on pressing geopolitical and security issues. Thank you to SJK Geostrategic Advisory for their contributions in the Singapore and Malaysia chapters.



James Cook University Singapore, School of Science and Technology: the Singapore campus of James Cook University is fully owned by James Cook University Australia, which is ranked in the top 2% of universities in the world. James Cook University Australia established its Singapore campus in 2003 as part of its expressed intent of internationalizing its activities and offers a suite of university level programs at the Singapore campus. Thank you to Roberto Dillon, the Academic Head of Science and Technology and Associate Professor of Information Technology and Dr. Steve Kerrison, senior lecturer in cybersecurity for their contributions.



Google.org, Google's philanthropy, brings the best of Google to help solve some of humanity's biggest challenges combining funding, product donations and technical expertise to support underserved communities and provide opportunity for everyone. We engage nonprofits, social enterprises and civic entities who make a significant impact on the communities they serve, and whose work has the potential to produce scalable, meaningful change.



The Global Cyber Alliance (GCA) is an international nonprofit dedicated to building communities to deploy tools, services, and programs that provide cybersecurity at global scale. We achieve this in three ways: working with communities; engaging infrastructure owners and operators; and driving ecosystem engagement for collective action on cybersecurity. GCA is a 501(c)(3) in the U.S. and a nonprofit in the U.K. and Belgium.

# Introduction

## Background & Objectives

The digital era has introduced unparalleled opportunities for growth and innovation across the Asia-Pacific (APAC) region, enhancing the economic climate for micro, small, and medium enterprises (MSMEs), and making it easier for nonprofit organizations (NPOs) which includes nongovernmental organizations (NGOs) to extend their reach. For instance in 2020, Indonesia, Malaysia, the Philippines, Singapore, Vietnam, and Thailand collectively accounted for 40 million new internet users, a notable majority of which have engaged in online commercial activities<sup>1</sup>. This surge in digital participation has been instrumental in driving the regional economy forward, empowering even the smallest businesses and social entities to reach broader markets, and to streamline their operations through online platforms.

However, an increase in online activity has also made the APAC region a prime target for cybercriminals, and in 2022, nearly one-third (31%) of global cyberattacks occurred in the region.<sup>2</sup> This evolving cyber threat landscape calls for a rigorous and detailed assessment, with the goal of protecting vulnerable sectors such as the MSME and non-profit sectors, while supporting continued digital advancement for stakeholders in those sectors. In fact, the World Economic Forum has labeled the region: “the new ‘ground zero’ for cybercrime incidents.”<sup>3</sup>

The purpose of this report is to provide a comprehensive overview of the cyber threats currently impacting MSMEs and NPOs in the APAC region. It also explores the specific vulnerabilities of these entities, and identifies emerging trends that could shape future security strategies. The analysis is grounded in extensive research conducted across 12 countries (Japan, Korea, Singapore, Malaysia, Indonesia, Thailand, Vietnam, The Philippines, Sri Lanka, India, Bangladesh, and Pakistan), offering insights into regional differences and similarities.

This report aligns with the broader objectives of the APAC Cybersecurity Fund (ACF), an initiative led by The Asia Foundation in partnership with the CyberPeace Institute and Global Cyber Alliance, with the support of Google.org, Google’s philanthropic arm. In order to bolster the cybersecurity capabilities of 300,000 underserved communities, the ACF equips them with the tools and skills to safely navigate an increasingly complex digital environment. By enhancing understanding and awareness of cyber hygiene\*, the initiative aims to mitigate the impacts of cyber threats and foster a secure digital ecosystem across the APAC region.

Importantly, this report not only addresses the technical and strategic aspects of cybersecurity but also its socio-economic implications in the APAC region. Such an approach enriches the findings and recommendations, and provides stakeholders with truly actionable insights that can lead to enhanced cyber resilience. It is this kind of practical cybersecurity outcome that is crucial to securing the digital future of the region's vibrant economic landscape.

## Methodology

This comprehensive study explored the cybersecurity landscape in 12 APAC countries, employing a mixed-methods approach that integrated both primary and secondary research to ensure a robust analysis. This helped researchers understand the impacts and relevance of specific factors, such as the COVID-19 pandemic, on regional cybersecurity. It also shed light on which cybersecurity challenges are shared across the region, and where local contexts may add further barriers to digital access and security.

### Secondary Research

An extensive review of secondary sources was undertaken, including of government databases, academic journals, industry white papers, local and international news articles, and reports from NGOs. This was critical to understanding the cyber threats faced by MSMEs and the nonprofit sector, and helped establish which cybersecurity challenges are most prevalent in the APAC region, providing context for the primary research findings. Recent digitalization efforts and pandemic-related shifts, which include an increase in remote-working, made this review especially valuable, and researchers concentrated particularly on materials from 2020 and later, due to the drastic changes many businesses and organizations underwent as a result of the COVID-19 pandemic.





## Primary Research

Data was also collected in structured interviews with regional cybersecurity experts, representatives of local organizations, and business owners directly impacted by cyber threats. Firsthand accounts of the cybersecurity challenges encountered by MSMEs added significant depth to researchers' understanding of how these businesses are managing cybersecurity risks. In some countries, interviews with local employees of NPOs further enhanced the analysis and offered important perspectives on the effectiveness of ongoing digital security initiatives.

## Challenges Encountered

In all the countries under study, researchers had difficulty accessing detailed data and case studies specific to MSMEs and relevant to cybersecurity. These smaller businesses are often underrepresented in official documentation and media coverage, which generally focus on the cybersecurity of larger corporations and government. In several countries, high levels of informal employment posed an additional challenge to gathering accurate data, as government sources often fail to reflect the true nature of the MSME sector. An underreporting of cyber incidents by MSMEs, as well as by NPOs, whether due to fear of reputational damage or a lack of awareness, also impacted the comprehensiveness of the data.

## Opportunities For Future Research

The dynamic nature of cyber threats and the ongoing process of digitalization in many countries makes the continuous monitoring and updating of cybersecurity strategies an imperative. Opportunities abound to conduct research that is more granular in regions where data is currently scarce, particularly outside of urban centers, and with businesses operating predominantly in the informal economy. A more in-depth look at how the non-profit sector can be supported in mainstreaming a culture of cybersecurity awareness, even among small organizations with limited resources, is also warranted.



# APAC Cyber Threat Landscape For MSMEs

## APAC Cyber Threat Landscape For MSMEs

In the APAC region, a complex and dynamic cyber threat landscape impacts MSMEs and NPOs in significant ways. This is intensified in some countries by levels of technological advancement and cybersecurity readiness, which vary across the region. Indeed, the disparity in cybersecurity readiness between the region's advanced economies and emerging economies is substantial. Japan, South Korea, and Singapore feature robust cybersecurity frameworks that provide good resistance against cyber threats, while the underfunding of cybersecurity measures and a lack of skilled cybersecurity professionals in Bangladesh, Pakistan, and Sri Lanka make them significantly more vulnerable to cyberattacks. Nevertheless, for their collective wellbeing, every country in the APAC region must work towards developing a cohesive cybersecurity strategy that incorporates international collaboration and adheres to technical standards.

In advanced economies like Korea and Japan, the strength of their cybersecurity frameworks is matched by heightened risks, particularly in technology-driven sectors, resulting from their high levels of digital engagement and the targeting of technological assets by sophisticated threat actors. But where cybersecurity is less robust, such as India and Indonesia, both of which have large MSME and informal sectors, cyber threats are widespread across various industries and are compounded by the rapid adoption of cloud technologies without adequate security measures and by the challenges of managing a hybrid workforce.<sup>4</sup> In these less regulated environments, a lack of mature cybersecurity infrastructure and limited oversight further exacerbates any vulnerability.

Across the APAC region, the MSME and non-profit sectors face a wide range of cybersecurity challenges, among which phishing\* and ransomware\* attacks are the most common, as attackers seek to exploit the inadequate defenses of smaller enterprises and organizations. A 2023 study found that nearly eight in ten (78%) MSMEs in the region had experienced at least one cybersecurity incident in the previous year, for example, and many reported multiple breaches.<sup>5</sup> These attacks are driven by financial and political motivations alike. For regional NPOs, contentious geopolitical climates can particularly affect the cyber threats they face.

The cybersecurity landscape in the APAC region is complicated by a universal underfunding of cybersecurity measures and a significant shortage of skilled professionals. In fact, demand far exceeds supply—especially in rapidly digitizing countries like Malaysia and Vietnam—and the number of cybersecurity professionals in the region must increase threefold to meet it.<sup>6/7</sup> This context makes the region's MSME and non-profit sectors even more attractive targets for cybercriminals, and only heightens the need to enhance security measures in both.



The cyber threat landscape in which MSMEs and NPOs find themselves is one of increasing complexity and sophistication. The tactics of cybercriminals are continuously evolving, as they learn to manipulate new technologies and adapt to new cybersecurity measures at ever greater speed. On top of this, the rise of the ransomware-as-a-service (RaaS)\* model allows even less technically-skilled attackers to launch ransomware campaigns, and the use of artificial intelligence (AI) and machine learning has given attackers the ability to automate attacks and craft phishing campaigns that can bypass traditional security defenses. In countries like Indonesia and Thailand, social engineering attacks\* are thus becoming more refined, and leveraging more detailed personal information. There are also growing concerns about the targeting of supply chains, especially in countries such as Japan and Korea, where a single vulnerability can have cascading effects across multiple entities and international markets.

These trends underscore the urgent need for the wide adoption of proactive and dynamic cybersecurity strategies by enterprises and organizations in the APAC region, to ensure they can adapt to this rapidly evolving threat environment. Regulatory frameworks vary considerably across the region, however; they are robust and advanced in countries like Singapore, Japan, and South Korea, and are still in development in countries like Bangladesh and Pakistan. This clearly impacts the cybersecurity preparedness and responsiveness of MSMEs and NPOs in these countries, and this disparity within the region highlights the need for enhanced regional cooperation, facilitating a unified but tailored approach that meets the unique cybersecurity needs of each country. As cyber threats constantly evolve anew, enterprises and organizations must be prepared to invest in training, advanced technologies, and human resources to safeguard their digital assets and ensure the continuity of their business or services.





Sultan  
King  
#28  
1KG



# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Bangladesh |







# BANGLADESH

79 million MSMEs<sup>8</sup>

Digital Services Most Used for E-Commerce<sup>9/10/11</sup>

facebook

WhatsApp

নগদ

বিকাশ

Bikroy.com  
বাংলাদেশের সবচেয়ে বড় মার্কেটপ্লেস

Daraz

shohoz

## Top Cyber Threats Faced By MSMEs<sup>12</sup>

FRAUD



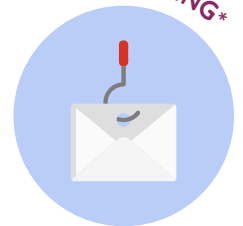
MOBILE FINANCIAL SERVICES SCAMS



DATA BREACHES\*



PHISHING\*

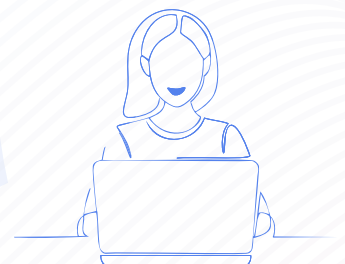


## Key Facts



In 2022, more than **92%** of MSME operators lacked an awareness of cybersecurity & **40%** had been the direct or indirect victim of a cyberattack.<sup>13</sup>

**55%** of all ransomware attacks target small businesses with less than 100 employees. The absence of cybersecurity knowledge and awareness remains a persistent challenge for online MSMEs.<sup>14</sup>



## DEFINITION OF MSME<sup>15</sup>

### MICRO INDUSTRY



Employees  
16 to 30



Amount of Investment  
1 million to 7.5 million BDT

### SMALL INDUSTRY

#### Manufacturing



Employees  
31 to 120



Amount of Investment  
7.5 million to 150 million BDT

#### Services



Employees  
16 to 50



Amount of Investment  
1 million to 20 million BDT

### MEDIUM INDUSTRY

#### Manufacturing



Employees  
121 to 300



Annual Income  
150 million to 500 million BDT

#### Services



Employees  
51 to 120



Annual Income  
20 million to 300 million BDT

## Executive Summary

The digital ecosystem of Bangladesh has grown progressively over the last decade, especially since the COVID-19 pandemic.<sup>16</sup> Although the country has only a 39% internet penetration rate, almost the entire population is connected to at least a 3G cellular network.<sup>17/18</sup> But ambitious digital development plans for Bangladesh are often overshadowed by what is lacking in the country, including cohesive regulatory and legal frameworks, highly-skilled expertise, and digital literacy in both public and private institutions.<sup>19/20</sup>

Limited digital literacy, as well as a large urban-rural digital divide and poor quality internet services, put all Bangladeshis and especially MSMEs at risk.<sup>21</sup> MSMEs employ 87% of the population, comprise nearly all (99%) non-farming enterprises in the country, and contribute 25% of GDP.<sup>22/23</sup> And, despite low internet penetration in the country, a high percentage of MSMEs rely on digital tools\* and platforms to operate their businesses.<sup>24</sup> This exposes them to cybersecurity risks from spam\*, phishing\*, malware\*, ransomware\*, scams, and insider threats\*.<sup>25/26</sup> These smaller enterprises are particularly vulnerable because they lack cybersecurity awareness or training, have little access to expertise, and tend to operate on limited funds without a budget for digital security.<sup>27</sup> The extremely large size of the informal sector in Bangladesh, constituting up to 92% of the economy in some rural areas, also means there is little recourse for many MSMEs if they are impacted by cyber threats.<sup>28</sup>

Special challenges to cybersecurity exist in Bangladesh, including the need to upskill a large workforce that already exists in the tech sector, to help them be more competitive and productive for existing public and private enterprises.<sup>29</sup> Curricula for schools, from primary to university, must also be updated, and teachers and professors upskilled in order to harness the opportunities presented by a majority youth population that seeks a positive cyber future.<sup>30/31</sup> An extreme urban-rural divide continues to mark Bangladesh as well, and can be seen in its digitalization, and many city-centric cybersecurity solutions will need to be adapted for rural communities. This is especially true given the high number of MSMEs based outside of cities.<sup>32</sup> On top of this, Bangladesh has not enacted a data privacy law.<sup>33</sup> A draft Data Protection Act was taken up in 2023 and was moving through the government as of April 2024, but there is no indication when it will be adopted, as privacy advocates have pushed for further modifications.<sup>34/35</sup>

It is difficult to find data on cyberattacks that have impacted MSMEs in Bangladesh, due to the informality of the economy and a lack of reporting. It is also too early to measure the longer-term outcomes of recently implemented, ongoing efforts to raise cybersecurity awareness in the country, especially among MSMEs. Even so, USAID and other international development organizations have published

preliminary reports indicating positive trends towards a more cyber secure population.<sup>36</sup> Initiatives to build and promote digital literacy and cybersecurity awareness are vital complements to the work of the government to improve internet connectivity and infrastructure, which will provide more economic opportunities for Bangladeshi MSMEs.





## The General Cybersecurity Context In Bangladesh

Over the past decade, the digital ecosystem of Bangladesh has experienced continuous growth, largely owing to the government's Digital Bangladesh Initiative and a progressive private sector. The COVID-19 pandemic accelerated this, as the adoption of technology and the shift to remote work became a necessity, to keep the economy afloat.<sup>37</sup> Yet, there is still only a 39% internet penetration rate in Bangladesh, even if over 98% of the population can access at least a 3G cellular network.<sup>38/39</sup> A large digital divide between urban and rural areas continues to exist as well, marked by the poor quality of internet services, and limited awareness of cybersecurity and online safety continue to put Bangladeshis at risk.<sup>40</sup>

According to the government, spam\* emails are the number one cyber threat in Bangladesh, followed by phishing\*, smishing\*, ransomware\*, malware\*, and insider threats\*.<sup>41</sup> However, better cybersecurity is often hindered by regulatory gaps at the national level, which can lead to a lack of coordination. There are two laws that primarily govern cyberspace in Bangladesh—the wide-ranging Information and Communication (ICT) Act of 2006, and The Cyber Security Act of 2023, which specifically addresses cybercrime—and research has shown they are inadequate, with legislative weaknesses that cybercriminals can exploit.<sup>42</sup> The Cyber Security Act of 2023 is being looked at by the interim government. There might be some changes in the coming months and so far, nothing concrete has been done. Furthermore, a draft Personal Data Protection Act (2023) is yet to make its way successfully through the government.<sup>43/44</sup> While there is a large tech talent pool in Bangladesh, these workers are typically disadvantaged by having been exposed to outdated curricula in schools and universities, leaving them low-skilled.<sup>45</sup> There is therefore a need for teachers throughout the educational system to be upskilled, especially because over three-fifths (62%) of the population is under the age of 34.<sup>46</sup> There is also a need for upskilling programs meant for current cybersecurity and IT professionals in Bangladesh, who may need to refresh or update their skills but are unable to access training due to the cost.

## The Context For MSMEs In Bangladesh

MSMEs in Bangladesh contribute 25% to the country's GDP and make up around 87% of the non-agricultural economy, totaling an estimated 7.9 million enterprises.<sup>47/48</sup> In fact, 99% of all non-farming enterprises in the country are either a micro or small enterprise. And notably, over six in ten (60% to 65%) MSMEs are located outside the metropolitan areas of Dhaka and Chittagong.<sup>49/50</sup> When the COVID-19 pandemic emerged, MSMEs turned to digital tools\* and online platforms to survive, accelerating the digital transformation of the sector out of necessity. However, with little knowledge about cybersecurity or the risks that can accompany digitalization, many were and are vulnerable to major business losses.<sup>51</sup>

## Prevalence Of The Informal Sector

The informal sector accounts for 85% of employment in Bangladesh. Informal employment is even higher in rural areas, where women make up 98% of the informal workforce.<sup>52</sup> Many MSMEs operate in the informal sector, without business bank accounts, using the e-commerce tools on social media platforms like TikTok and Facebook to complete transactions. Indeed, over three-quarters (77%) of the entrepreneurs running a business online in Bangladesh are operating in the informal sector without a business bank account, and approximately half of these are women.<sup>53</sup>

The gendered nature of the informal e-commerce market in Bangladesh has fueled criticism of a new regulation that obligates Facebook sellers to register their business, as it largely affects female micro entrepreneurs who are leveraging social media to make a safer living than if they resorted to selling items for cash outside the home.<sup>54</sup> Female MSME owners typically use mobile financial service (MFS) platforms because they cannot open a bank account for their business unless they register with the government, a process they find daunting for various reasons.<sup>55</sup> This makes them susceptible to cyber threats so long as they lack important cybersecurity knowledge.<sup>56</sup> While being formalized through registration offers a number of advantages to MSMEs when it comes to cybersecurity, bringing these smaller enterprises into the formal economy will require mitigating the barriers, many of which are financial, that prevent businesses from registering.

## High Risk Platforms And Most Used E-Commerce/Social Media Platforms

Bangladesh is among the top ten countries globally for number of Facebook users, with nearly 45 million active accounts.<sup>57</sup> Hence, what has become known as “F-commerce” (i.e., e-commerce on Facebook), continues to increase as e-commerce expands more generally. According to the World Bank, in 2020 alone, e-commerce revenues in Bangladesh increased by 70% to 80%.<sup>58</sup> Other popular e-commerce platforms include Clickbd, Chaldal, Bikroy, Daraz, and Shohoz.<sup>59</sup>

## Key Trends In Cybersecurity Among MSMEs In Bangladesh

In a 2022 study, more than 92% of MSME operators in Bangladesh lacked an awareness of cybersecurity despite the fact that 40% had been the direct or indirect victim of a cyberattack.<sup>60</sup> Additionally, 82% described cybersecurity as irrelevant to them or their business, even though half the MSMEs operating in Bangladesh that year were using digital tools\* and internet platforms for their business operations.<sup>61</sup> The speed with which digitalization is occurring in Bangladesh was exemplified by a 70% growth in e-commerce businesses from 2021 to 2022.<sup>62</sup>

The USAID-backed South Asian Regional Digital Initiative (SARDI) in Bangladesh has found that fraud, mobile financial service scams, data breaches, and phishing\* are the most common cyber threats faced by MSMEs in the country.<sup>63</sup> Over half (55%) of all ransomware\* attacks on enterprises in the country

also target small businesses with less than 100 employees.<sup>64</sup> Because most MSME owners hail from rural and remote areas and lack formal education, let alone knowledge of cybersecurity, they are more vulnerable to cyberattacks and are therefore targeted by cybercriminals.<sup>65</sup> Thus, many initiatives have been launched to help bring Bangladeshi MSMEs into a more cyber secure posture, but sustained efforts will be necessary, particularly as a growing number of young people and women show an interest in starting businesses and entering the MSME sector. Many young Bangladeshis view entrepreneurship as a promising way to build a career, and many women see it as a way to earn a living while experiencing fewer gender barriers than they face in other work environments.

### Case Study 1

Recently, the online clothing business of a young Bangladeshi woman who employs six people was scammed by cybercriminals. Taking advantage of the pay on delivery system, the scammers input fake payment information or false personal information to receive orders of clothing. A lack of protections by payment apps and limited digital knowledge on the part of MSME operators and employees has made scams such as this more frequent, costing businesses quite a lot of money. Recently, the owner of this online clothing business therefore implemented a rule that customers pay 50% up front in order to receive an order, with the remainder paid on delivery, but even this has been circumnavigated by cybercriminals using fake receipts to fool employees into believing they paid half up front. She believes her business could benefit from training for employees on common cyber scams, especially those involving banking apps and payment platforms.<sup>66</sup>

### Case Study 2

A small business owner who sells imported products through an online platform linked to his personal social media account received a convincing email from a company indicating that he was chosen to receive an investment. He felt the email was trustworthy and provided his mobile banking account and PIN number, as it requested. Afterward, he found that 256 USD had been fraudulently deducted from his bKash account, which was subsequently blocked, and he lost all his earnings for that month.<sup>67</sup>



# Current Cybersecurity Measures for MSMEs

## Government Initiatives

- The Bangladesh Computer Incident Response Team (BGD e-Gov CIRT), established in 2016, is responsible for maintaining cybersecurity in the country for both public and private enterprises, by handling and investigating cyber incidents and spreading awareness.<sup>68</sup>
- The Digital Bangladesh Initiative is meant to bridge the digital divide, including by expanding access to digitized services, as a part of the government's Vision 2041 Agenda.<sup>69</sup>
- The Aspire to Innovate (a2i) Program, implemented in partnership with the United Nations Development Programme (UNDP) and USAID, is aimed at simplifying public service processes and making them more accessible to the general public, including MSMEs, particularly in rural and underserved areas.<sup>70</sup> It is currently under review by the interim government.<sup>71</sup>

## Industry Initiatives

- The South Asian Regional Digital Initiative (SARDI), a project of DAI and USAID, is focused on digital development and cybersecurity for MSMEs.<sup>72</sup>
- Inspira Advisory & Consulting conducts workshops in Bangladesh designed to empower MSMEs vis-à-vis cybersecurity.<sup>73</sup>

# Challenges and Barriers to Cybersecurity for MSMEs

MSMEs in Bangladesh face a variety of challenges and barriers to cybersecurity. They suffer from the same constraints as most MSMEs worldwide, such as a lack of awareness, training, funds, and expertise, but also confront some that are more unique to Bangladesh. For example, the country's large informal sector equates to low levels of business registration, and unregistered MSMEs may have little recourse against cyberattacks as they are unable to utilize the government's cybercrime reporting mechanisms. The fact that many MSMEs operate in rural areas presents another challenge to cybersecurity in this sector, as the bulk of IT infrastructure solutions, particularly those designed for e-commerce and tech startups, are available in urban areas.<sup>74</sup>

A significant challenge also lies at the government level, and certainly trickles down to impact private enterprises and MSMEs. The government has ambitious plans for a comprehensive digitalization process that includes both the deployment of infrastructure and business development initiatives to support growth in the digital economy. But limited digital literacy and a lack of highly skilled professionals who can operationalize the government's very technical plans has made realizing them difficult.<sup>75</sup>



## Conclusion

This overview of the cybersecurity landscape of Bangladesh, especially as it relates to MSMEs, highlights the specific challenges they face as a result of the country's digital goals combined with a widespread lack of digital literacy. Recent reports on this issue by USAID and other development organizations provided a considerable amount of relevant data and research, compared to other countries in the APAC region. Nevertheless, as MSMEs in Bangladesh are still in the beginning stages of implementing any cybersecurity measures newly adopted due to recent digital initiatives, the impact may not be seen until further studies are undertaken in the future. In fact, this provides opportunities for researchers to conduct primary research on this topic, especially in rural areas, where the prevalence of the informal economy means there is little government data on cyber threats to MSMEs.

## Methodology

This qualitative research was designed to understand the nature and impact of cyber threats on MSMEs in Bangladesh from 2020 to the present. The methodology combined a review of secondary sources, including news articles, social media posts, industry reports, and academic articles, with primary data collection through interviews, to provide a comprehensive analysis. The secondary research helped identify key trends and discussions on the cyber threats faced by MSMEs, establishing a foundational understanding of the cybersecurity landscape. Interviews for the primary research were conducted with key stakeholders, including a local organization working with MSMEs, a cybersecurity expert, and a business owner affected by a cyber threat, to gain insights into real-world challenges and cybersecurity practices within this sector. Challenges to the research included a notable scarcity of governmental data, as well as an underreporting of cyber incidents by MSMEs, often due to a lack of awareness and fear of reputational damage. Despite this, the research outlined here provides valuable perspectives on the vulnerabilities and needs of MSMEs in Bangladesh as they confront cyber threats, and on the importance of enhanced protective measures for these businesses.







# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

India | 

# INDIA



63.4 million MSMEs<sup>76</sup>

## Digital Services Most Used for E-Commerce<sup>77</sup>

Meta



amazon.in

Flipkart



Myntra

indiamart<sup>®</sup>

## Top Cyber Threats Faced By MSMEs<sup>78/79</sup>

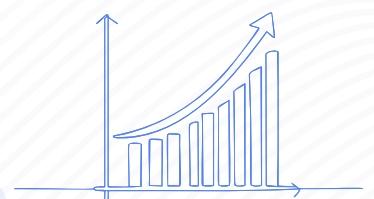


## Key Facts



In 2021, **74%** of small and medium businesses said they suffered a cyberincident.<sup>80</sup>

In 2021-23, attacks on SMEs increased by **508%**.<sup>81</sup>





## DEFINITION OF MSME<sup>82</sup>

### MICRO ENTERPRISE

#### Manufacturing & Services

- Investments between 1 Cr Rs and 5 Cr Rs

### SMALL ENTERPRISE

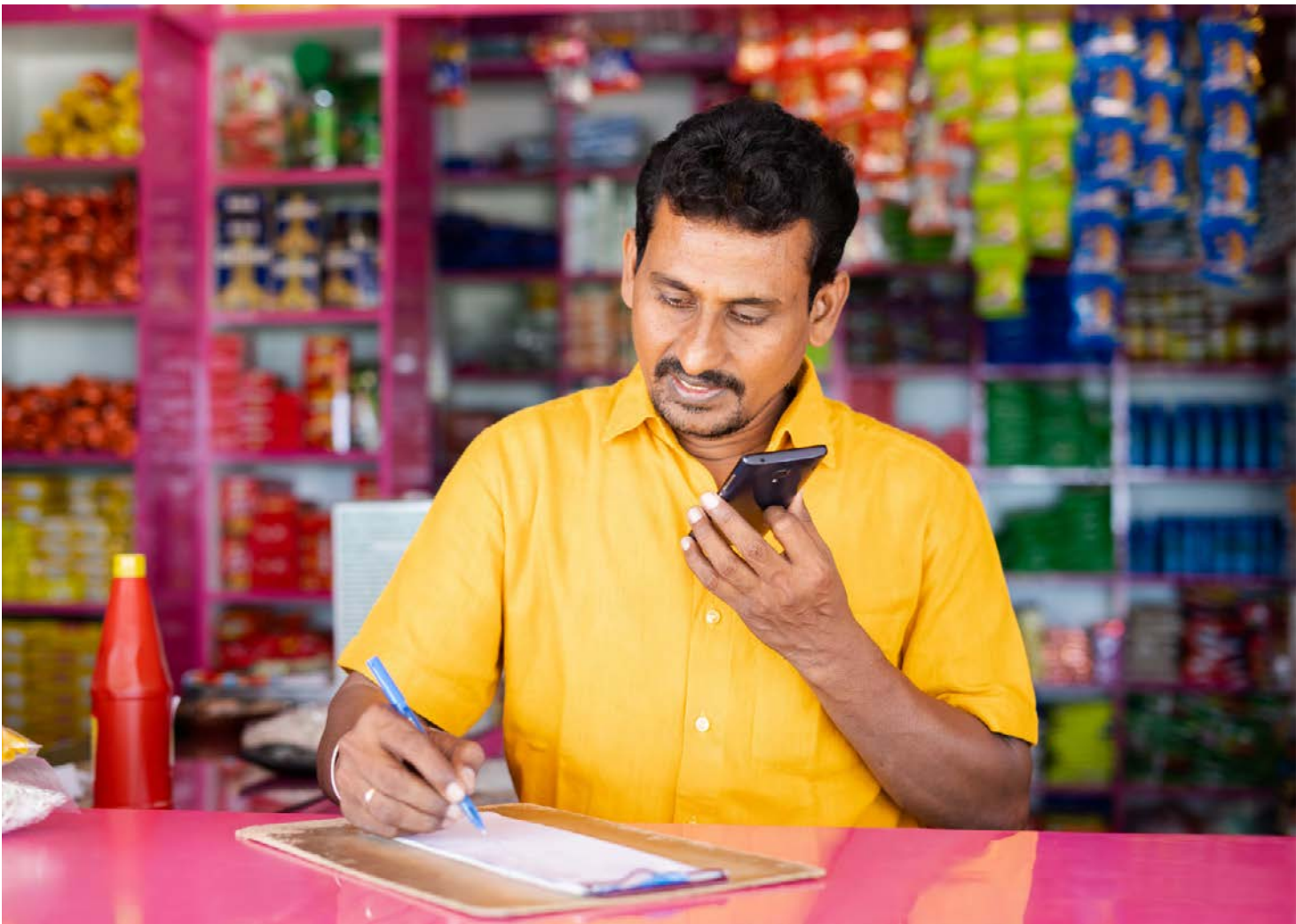
#### Manufacturing & Services

- Investments between 10 Cr Rs and 50 Cr Rs

### MEDIUM ENTERPRISE

#### Manufacturing & Services

- Investments between 50 Cr Rs and 250 Cr Rs



## Executive Summary

In 2023, India was rated 49th (of 64) in the World Digital Competitiveness Ranking, a drop from the previous year that was largely related to questions of future readiness. As India's digital economy grows, with a projected increase from 11% of GDP in 2023 to 20% by 2026, the country's cybersecurity landscape is marked by a parallel escalation in cyber threats.<sup>83</sup> This made India the most targeted country in the world by cyberattacks in 2023, accounting for 14% of all attacks globally.<sup>84</sup> For businesses and organizations in India, 83% of which have reported cybersecurity breaches, these attacks often result in substantial financial harm.<sup>85</sup> The sector that most frequently faces attacks is IT and business process outsourcing (BPO), which was targeted by 14% of cyberattacks in India between March 2021 and September 2023, followed by the manufacturing (12% of attacks), healthcare (10%), and education (10%) sectors.<sup>86</sup>

MSMEs are a cornerstone of the Indian economy, contributing significantly to employment, innovation, and overall economic growth. As of 2023, these enterprises provide around 120 million formal and informal jobs.<sup>87</sup> But MSMEs in India face significant vulnerabilities, as illustrated by a report showing a 508% increase in targeted cyberattacks on startups and SMEs from 2021 to 2023.<sup>88</sup> This cybersecurity landscape is dominated by malware\* and phishing\* threats.<sup>89</sup> Yet, many MSMEs lack adequate cybersecurity infrastructure to combat these threats, often because they prioritize operational growth over cybersecurity investments.<sup>90</sup> Additionally, many small businesses rely on outdated technology and lack the expertise of skilled cybersecurity professionals.<sup>91</sup>

Government initiatives such as the Skill India Digital Platform, launched in February 2023, along with various industry initiatives, are helping MSMEs in India enhance their skills and build capacities for digital development.<sup>92/93</sup> Given the high incidence of cyberattacks across several sectors, the government has also strengthened regulatory measures, introducing both the Digital Personal Data Protection Act (DPDP Act) and the National Cyber Security Policy in 2023.<sup>94/95</sup> These important legislative advances are aimed at safeguarding personal data and securing the national cyber infrastructure.<sup>96/97</sup> Nevertheless, the readiness of businesses in India to defend against cyber threats remains low, highlighting a critical vulnerability\* of the economy, especially the MSME sector.<sup>98</sup>

## The General Cybersecurity Context In India

According to Rajeev Chandrashekhkar, India's Union Minister of State for Electronics and Information Technology, Skill Development, and Entrepreneurship, the country's digital economy is projected to grow significantly in the coming years, essentially doubling in size to 20% of GDP by the end of 2026.<sup>99</sup> However, this growth has brought a rise in cyberattacks, making India the country most targeted globally in 2023, accounting for 14% of all attacks in the world, despite an internet penetration rate of just 49%.<sup>100/101</sup> India also confronts a higher proportion of foreign state-influenced cyberattacks compared to the global average.<sup>102</sup> Over eight in ten (83%) Indian organizations and enterprises thus reported cybersecurity incidents in 2023, including web attacks and supply chain infiltrations, nearly half (48%) of which resulted in financial damages exceeding one million USD.<sup>103</sup>

In 2024, India is thus far the 5th most targeted country worldwide by ransomware\* attacks, and the 4th most targeted country in Asia by email threats.<sup>104</sup> These cyber threats pose a danger to a diverse range of sectors, from IT and BPO, to manufacturing, to healthcare and education. The IT and BPO sector is targeted most frequently, facing 14% of cyberattacks in the country, followed by manufacturing (12%), healthcare, education, retail, government agencies, and banking and financial services (all roughly 10%), the automobile industry (8%), and airlines (6%).<sup>105</sup>

The widespread vulnerabilities that exist across industries underscore the need for skilled cybersecurity professionals in India, where the demand for cybersecurity expertise exceeds the global average by 9% but nearly half of businesses struggle to hire qualified personnel.<sup>106</sup> With hiring processes that can take up to six months, India is facing a shortage of some 3 million cybersecurity experts, presenting significant challenges to cybersecurity.<sup>107</sup> Hence, Indian businesses are ill-prepared to tackle the significant threat landscape they face. Indeed, as of 2022, the CISCO Cybersecurity Readiness Index found that only a quarter (24%) of Indian enterprises had the necessary resources and capacities to effectively address cybersecurity issues.<sup>108</sup> However, in 2023, the Indian government took significant steps to strengthen digital security for enterprises, enacting the DPDP Act to protect data privacy and adopting the National Cyber Security Policy to protect cyberspace\* infrastructure and establish a 24/7 cybersecurity body.<sup>109/110</sup>



## The Context For MSMEs In India

In India, MSMEs are regulated by the Micro, Small, and Medium Enterprises Development (MSMED) Act of 2006, which provides a legal framework for the sector, addresses issues such as delayed payments and credit access, and removes a 24% equity cap on industrial investments in smaller enterprises.<sup>111</sup> The MSME sector stands as a crucial pillar of the Indian economy, significantly contributing to job creation, boosting exports, and promoting inclusive growth. MSMEs account for most of the enterprises in India, numbering more than 63 million, over 99% of which are micro businesses.<sup>112</sup>

These enterprises employ more than 110 million people, including some 26 million women, and are distributed relatively evenly between rural and urban areas.<sup>113</sup> MSMEs play a vital role in job creation in India, providing employment across a range of industries and contributing approximately one-third of GDP.<sup>114</sup> They particularly contribute (at 45%) to the country's industrial production, and account for 40% of its exports.<sup>115</sup>

### Prevalence Of The Informal Sector

India's informal sector is among the largest in the world, accounting for over 85% of employment.<sup>116</sup> Women are overwhelmingly working in this sector, with 80% of the female workforce employed in informal jobs, about half of which are in agriculture.<sup>117</sup> The Indian informal economy encompasses everything from the low-skilled work of porters and street vendors, to the more-skilled work of informal manufacturing, to highly-skilled trades.<sup>118</sup>

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

According to a study conducted by Appknox in 2022, 75% of the top 100 Android apps used in India contained security risks.<sup>119</sup> Nearly eight in ten were affected by network misconfiguration and also lacked sufficient code obfuscation\*.<sup>120</sup> Given that the Android market share in India was 95% as of March 2024, security risks like these heighten the vulnerability of many users to cyberattacks and potential breaches of sensitive data.<sup>121</sup>

This exemplifies why concerns for digital safety have arisen alongside the rapid growth of the Indian e-commerce sector. The India Brand Equity Foundation (IBEF) forecasts that the Indian e-commerce market will reach approximately 350 billion USD by 2030, with over 200 million online shoppers by 2025.<sup>122</sup> Growth in this market has primarily been driven by an increase in online grocery and apparel purchases.<sup>123</sup> But producers of household goods, handicrafts, and agricultural products, most of whom operate MSMEs or work in the informal sector, are also starting to leverage e-commerce platforms.<sup>124</sup>

Some of the e-commerce sites most commonly used in India are Amazon India, Flipkart, Myntra, Meesho, and IndiaMART.<sup>125/126</sup> Social media has also become increasingly essential to MSMEs in India, playing a crucial role in building brand loyalty and enhancing visibility, but also in allowing business owners to effectively reach target audiences.<sup>127</sup> The platforms used most widely in India are Instagram (75% of users), Facebook (71%), X (formerly Twitter) (43%), LinkedIn (36%), and Moj (30%).<sup>128</sup>

### Key Trends In Cybersecurity Among MSMEs In India

The cybersecurity landscape for MSMEs in India is evolving rapidly amidst their growing adoption of digital technologies. Approximately half of these enterprises (53% of small and medium businesses, and 47% of micro businesses) have implemented digital sales platforms, a sizable increase from the pre-COVID figure of 29%.<sup>129</sup> But MSMEs have also seen a dramatic escalation in cyberattacks.<sup>130</sup> During a two-and-a-half year period spanning early 2021 to late 2023, targeted cyberattacks on startups and small enterprises in India increased by over five-fold.<sup>131</sup>

MSMEs are particularly susceptible to cyber threats, including basic email attacks, as they tend to have very limited cybersecurity infrastructure.<sup>132</sup> Some of the common threats they face include malware\* and phishing\*. In fact, a 2021 Cisco study found that 92% of small and medium businesses in India had been affected by malware\* attacks, and 76% by phishing\*, in the year prior.<sup>133</sup> MSMEs also confront cyber threats such as ransomware\*, APT attacks\*, insider-based attacks\*, DDoS\*, man-in-the-middle (MitM)\* attacks, password targeting attacks\*, SQL injection attacks\*, and zero-day attacks\*.<sup>134</sup>

#### Case Study

In December 2021, a small book publishing company in West Bengal fell victim to a ransomware-as-a-service (RaaS)\* attack. Subsequently, the chief executive revealed that even after eight months of paying a ransom, the company was still unable to fully access its files.<sup>135</sup> Hacker groups perpetrating these crimes function like conventional businesses, complete with departments such as human resources, finance, administration, coding, and research. Moreover, these groups adhere to specific policies for processing code and employ best practices to keep the identities of their members concealed.<sup>136</sup>

# Current Cybersecurity Measures For MSMEs

## Government Initiatives

- The Information Technology (IT) Act, 2000, is the primary legislation dealing with cybersecurity, data protection and cybercrime. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (2013 rules), established the Computer Emergency Response Team (CERT-In) as the administrative agency responsible for collecting, analysing and disseminating information on cybersecurity incidents, and taking emergency response measures.
- These rules also put in place obligations on intermediaries and service providers to report cybersecurity incidents to the CERT-In. The Ministry of Home Affairs looks at internal security, including cybersecurity. For this purpose, it has set up the cyber and information security division, comprising a cybercrime wing, cybersecurity wing and monitoring unit. To combat cybercrime, it also established the Indian Cyber Crime Co-ordination Centre in 2018.
- The Ministry of Home Affairs created a Cyber and Information Security Division in 2017, which includes a cybercrime wing, a cybersecurity wing, and a monitoring unit, and launched the Indian Cybercrime Coordination Centre in 2018 to combat cybercrime.<sup>137/138</sup>
- The Reserve Bank of India uses the KYC or “know your customer” procedure, a mandatory verification process applied by financial institutions to minimize illegal activities since 2005.<sup>139</sup>
- The Ministry of Electronics and Information Technology (MeitY) launched Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) in 2017, as part of its Digital India initiative, to create a secure Indian cyberspace by detecting botnet infections and notifying users, enabling the cleaning and securing of their systems to prevent further infections.<sup>140</sup>

## Industry Initiatives

- Aditya Birla Capital introduced Udyog Plus in May 2022, a MSME-focused portal that offers a range of business solutions, including online loans up to 120,000 USD.<sup>141</sup>
- The Technology Development Board (TDB) and the Small Industries Development Bank of India (SIDBI) signed a Memorandum of Understanding in 2023 to facilitate easier credit access for MSMEs, with a focus on enterprises engaged in technology development and application.<sup>142</sup>

## Challenges And Barriers In Cybersecurity for MSMEs

MSMEs in India tend to focus more of their resources on business growth than cybersecurity, prioritizing operational scaling over investments in digital security, and often outsourcing digital tasks (such as online tax return filing) to third-party vendors who may lack robust cybersecurity measures.<sup>143</sup> This has heightened the vulnerability of these enterprises to cyber threats, especially with the rise of remote work and online transactions since the COVID-19 pandemic. A Cisco study conducted approximately six months into the pandemic found that almost three-quarters (73%) of organizations and enterprises in India had experienced an increase in cyber threats due to digitalization.<sup>144</sup>

Additionally, the use of personal devices to access workplace networks can represent a risk to these networks.<sup>145</sup> MSMEs are particularly vulnerable to cyber threats of this sort due to a reliance on outdated technology and a shortage of skilled cybersecurity staff. As hybrid work cultures are normalized, these businesses will only be further exposed to cybercriminals who see the MSME sector as an increasingly attractive target.<sup>146</sup>





## Conclusion

India's growing digital economy represents robust economic potential but has made the country a leading global target of cybercrime. Despite advancements in the legal framework aimed at fortifying digital infrastructures, the readiness of enterprises in India to tackle cyber threats remains alarmingly low. Critical vulnerabilities particularly exist within the MSME sector, which is foundational to the Indian economy, contributing significantly to both employment and GDP.

To address this, the MSME sector will need to be equipped with the knowledge to recognize and counteract cyber threats, perhaps through a national cybersecurity curriculum that is tailored to the needs of smaller enterprises. Support for MSMEs must include clear guidelines and resources to help these businesses enhance their cybersecurity, as well as investments in advanced digital infrastructure to support robust cybersecurity defenses in this sector. Financial incentives and aid, such as through grants, subsidies, and tax breaks, should be used to encourage MSMEs to adopt and maintain effective cybersecurity practices, alongside the promotion of public-private partnerships that foster collaboration between government, industry, and academic institutions to drive innovation in cybersecurity and ensure MSMEs have access to the latest technologies and expertise. The Government of India already has legislations and frameworks in place. However, greater awareness is required to help MSMEs understand and combat these cyberattacks effectively.

## Methodology

This research primarily employed secondary methods, gathering data from academic journals, local and international news, and government databases. Supplementing this were interviews with representatives from local organizations. Though detailed case studies of cyberattacks that specifically targeted MSMEs were limited, likely due to a combination of underreporting and an overfocus by media on larger cases, one cyber incident involving a small business was uncovered and provided valuable insight despite lacking detailed impact data. Challenges were encountered in identifying specific apps, websites, or platforms that were the targets of cyberattacks in India; though it can be assumed that the most popular e-commerce apps listed in this report are likely prime targets for cybercriminals.





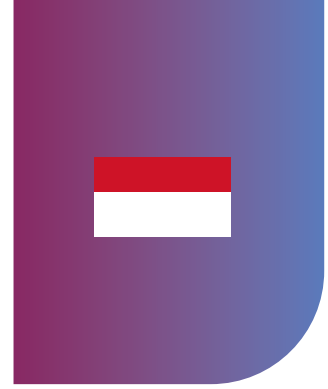
# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Indonesia | 

# INDONESIA



66 million MSMEs<sup>147</sup>

## Digital Services Most Used for E-Commerce<sup>148/149/150</sup>

facebook

TikTok

tokopedia

gojek

Shopee

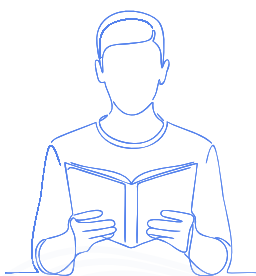
Instagram

WhatsApp

## Top Cyber Threats Faced By MSMEs<sup>151/152</sup>



## Key Facts



Malware attacks in Indonesia increased by over **124%** between 2022 and 2023.<sup>153</sup>

In 2021, **33%** of small and medium businesses experienced cyber incidents.<sup>154</sup>





## DEFINITION OF MSME<sup>155</sup>

### MICRO ENTERPRISE



Employees  
1-4 employees



Annual turnover  
Less than 300 million IDR

### SMALL ENTERPRISE



Employees  
5-19 employees



Annual Turnover  
Between 300 million and 2.5 billion IDR

### MEDIUM ENTERPRISE



Employees  
20-99 employees



Annual Turnover  
Between 2.5 to 50 billion IDR



## Executive Summary

Indonesia is the largest economy in Southeast Asia and the sixth largest in the APAC region, as well as the fourth most populous country in the world. By integrating digital technology into the broader economy of the country, the government's "Industry 4.0" initiative aims to bring Indonesia into the world's top 10 largest economies by 2030.<sup>156</sup> Indonesia is also on the path to achieving its goal of country-wide digital penetration, with three-quarters (74%) of the population online, and that number rising quickly.<sup>157</sup> Combined with its strategic location, this makes it a very attractive target for cybercriminals.

To grow the Indonesian economy, Industry 4.0 focuses heavily on encouraging and enabling MSMEs to adopt digital technologies as a means of expanding their businesses.<sup>158</sup> The uptake for this may be higher in Indonesia than in regional countries with aging populations, as over 40% of Indonesia's population is under the age of 24, and 85% is under the age of 55.<sup>159</sup> Furthermore, a study of MSMEs in Indonesia showed that a majority of business owners in this sector are under 45, which is likely to ease digitalization efforts, due to the higher capacity and willingness of younger generations to adopt new technologies.<sup>160</sup> This is notable given that almost all (99%) businesses in Indonesia are MSMEs, accounting for 97% of the economy and 62% of GDP.<sup>161</sup>

For MSMEs that survived the COVID-19 pandemic, it served as a catalyst for their digitalization and encouraged the Indonesian government to prioritize projects like "MSMEs Go Online"—which has supported active selling on online market platforms by enabling them with digital development initiatives since 2021.<sup>162</sup> However, MSMEs, especially in rural areas, continue to lack sufficient awareness and resources to combat cyber threats, and face barriers to cybersecurity including its complexity, an absence of trained personnel, cost considerations, and questions of compliance with legal regulations.<sup>163</sup> Still, in October 2022, Indonesia enacted a Personal Data Protection Bill (PDP) based on the EU's General Data Protection Regulation, and gave the "persons, public bodies, and international organizations" to which it applies two years to comply; this includes any business that collects personal data such as financial information.<sup>164</sup> Given the economic strength of Indonesia, the size of its population, and its cultural relevance in the region, full implementation of the PDP law is likely to have broader impacts on data protection in both the APAC region and globally.

## The General Cybersecurity Context In Indonesia

For strategic, economic, and political reasons, Indonesia is an attractive target for cybercriminals seeking to gain financially, destabilize infrastructure, and/or influence geopolitics. But the government's goal of becoming one of the world's largest economies by 2030, supported by its ambitious digitalization programs for industrial sectors, has opened the country up to cyber vulnerabilities on a scale unheard of before the pandemic.<sup>165/166</sup> In 2022, Indonesia recorded close to one billion traffic anomalies associated with potential cyberattacks, and at least 15 million online data breaches\*.<sup>167</sup>

A study conducted by Cloudflare in 2023 showed that 70% of Indonesian businesses had experienced a cyber incident in the previous 12 months, primarily web attacks (68%), phishing\* (62%), and the compromise of business email (42%), the leading objectives of which were data exfiltration (60%) and financial gain (55%).<sup>168</sup> Yet, only about half (53%) of respondents said they were prepared to prevent cyber incidents such as these. Just 5% of MSMEs in Indonesia reported using no solutions for cybersecurity at all, however, which is lower than the APAC region average of approximately 14%.<sup>169</sup>

The wide-ranging Personal Data Protection (PDP) Law passed by Indonesia in October 2022 may change this to some degree, as it applies to both the public and private domain, including MSMEs.<sup>170/171</sup> Its implementation provides a legal basis for the enforcement of laws pertaining to data breaches\* and violations, as well as a legal mechanism for reporting cyber threats involving personal data. To date, there has not been any comprehensive reporting on its effectiveness, perhaps because the law stipulated a two-year transition period during which organizations could enter compliance, which will end in October 2024.<sup>172</sup>

## The Context For MSMEs In Indonesia

The MSME sector is over 64 million strong in Indonesia, accounting for nearly all enterprises, employing almost all (97%) of the country's labor force, and constituting 61% of GDP.<sup>173</sup> Before the COVID-19 pandemic, the Asian Development Bank found that almost two-thirds (64%) of Indonesian MSMEs were operating in retail, with 17% in manufacturing and 8% in transportation and telecommunications.<sup>174</sup> However, the pandemic undoubtedly impacted these numbers; a June 2021 survey conducted by DAI showed that a considerable majority (77%) of MSMEs had moved online, and by 2023, an even greater proportion (87%) had done so.<sup>175/176</sup>



This steady increase in use of the internet by MSMEs may also be explained by large investments made by the government to encourage the digitalization of these enterprises in recent years, especially those located outside urban areas.<sup>177</sup> The government's Industry 4.0 initiative is focused largely on MSMEs in food and beverages, textiles and clothing, automotive, electronics, chemicals, and pharmacy, seeking to accelerate their digitalization and their utilization of online market platforms. And as the graph shown in Indonesia–Figure 1\* illustrates, the rate of 4G internet connection accessibility in Indonesian villages clearly correlates with the rate at which MSMEs utilize online platforms to sell products and services.<sup>178</sup>

The MSMEs Go Online program, mentioned earlier, is aimed at helping MSMEs adapt to this digital transformation. Still, according to research undertaken in 2022, a majority of the MSMEs that benefited from this program already had some cyber capacity.<sup>179</sup> The same research noted that almost three-quarters (72%) of respondents from MSMEs (i.e., owners) were under the age of 45, and well over half (61%) were female.<sup>180</sup> This may indicate that older people running MSMEs in Indonesia are not digitally savvy enough to utilize the government's digitalization support programs and need more assistance both to digitize and to protect themselves from cyber threats.

### **Prevalence Of The Informal Sector**

Approximately 60% of Indonesia's economy operates in the informal sector. This is especially true in rural areas, in the construction and agricultural industries.<sup>181</sup> Thus, recent efforts by the government to digitalize rural areas may serve to formalize more of the economy. This should help mitigate some cyber risks. For example, one expert in cybersecurity in Indonesia explained that most of the country uses digital payments for services, with mostly older people still using cash, and only at smaller street markets.<sup>182</sup> This heavy utilization of digital payment systems, mixed with a large informal economy, opens up many Indonesians to cyber threats and scams.



## High Risk Platforms And Most Used E-Commerce/Social Media Platforms

According to research conducted by DAI in 2021, Meta apps (Facebook, Instagram, and WhatsApp) were most commonly cited by MSMEs as apps that helped them conduct their business, with 87% using Facebook/Instagram and 83% using WhatsApp to communicate with customers and suppliers, advertise, conduct sales, and engage in other business activities.<sup>183</sup> These findings were echoed by another 2021 study by Deloitte that found that 88% of small businesses in Indonesia deemed Facebook and Instagram important to their success.

TikTok is quickly becoming more popular in Indonesia as well. The app offers several programs and workshops for MSMEs, designed to assist business owners in using the application for sales purposes.<sup>184</sup> On top of this, e-commerce apps such as Tokopedia, Shopee, and Bukalapak are used widely by MSMEs in Indonesia to sell goods.<sup>185</sup>

## Key Trends In Cybersecurity Among MSMEs In Indonesia

In the wake of the COVID-19 pandemic, in 2020 and 2021, cyberattacks on MSMEs in Indonesia surged and small e-commerce stores became the prime target for cybercriminals. Nearly one-fifth (18%) of all recorded cyberattacks in Indonesia in 2020 were against e-commerce operations.<sup>186</sup> Attackers took advantage of MSMEs in particular because they knew that the quick shift to digital services and platforms had not been matched by sufficient investments in cybersecurity by these smaller enterprises.<sup>187</sup>

From 2020 to 2023, the top cyber threats faced by MSMEs in Indonesia were phishing\*, malware\* (especially Trojan Password Stealing Ware\*), and ransomware-as-a-service (RaaS)\* attacks.<sup>188/189/190/191</sup> In 2023 alone, malware\* attacks rose by 124% compared to the previous year.<sup>192</sup> This increase in cyberattacks against MSMEs in Indonesia is a response both to their digitalization in recent years as well as their potential for high economic growth in the coming years. For instance, many MSMEs are unable to access credit via banks, and resort to using online lending services, some of which are fraudulent.<sup>193</sup> Or, cybercriminals send WhatsApp links hoping that recipients will click and download a file, providing access to their data and even their bank accounts. In a recent national study, three-quarters (75%) of respondents said they had received an illegal online loan fraud message.<sup>194</sup>

### Case Study 1

E-commerce sellers in Indonesia, which make up many micro and small businesses, are often affected by “fictitious buyer” cybercriminals, looking to use cyber threats to steal money. Claiming they are having payment or delivery problems, these “buyers” will typically show a fake money transfer receipt to convince the business that they have already paid for items, and persuade the business to “refund” them. These cybercriminals create and use fake accounts for the sole purpose of defrauding small businesses.<sup>195/196</sup>

## Case Study 2

A young female MSME owner in Jakarta, who produces curtains, received a substantial order by phone, presumably from a potential buyer who had seen her advertisement on Facebook. Given the significant monetary amount involved, she requested a down payment. However, the buyer insisted on an unconventional payment method and guided her through a process over the phone that led the business owner to transfer funds into a fraudulent account instead of receiving them. When she attempted to call the fake buyer, her number had been blocked.<sup>197</sup>

### Government Initiatives:

- The Ministry of Communication and Informatics oversees internet governance and the development of digital infrastructure, and is the primary regulatory body for Information and Communications Technology (ICT) in the country. The Ministry partners with industry and academia to support digital infrastructure initiatives for MSMEs, including MSMEs Go Online, and to publish research on digital policy and strategies.<sup>198/199/200</sup>
- The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara) coordinates national efforts to protect against cyber threats, across all sectors, and provides guidelines and support to MSMEs.<sup>201</sup>
- The Indonesia National Police Cyber Patrol Unit (Patroli Siber) monitors, prevents, and investigates cybercrimes while actively engaging in public education, particularly to help citizens understand the Information and Electronic Transactions (ITE) law.<sup>202</sup>

### Industry Initiatives:

- Relawan TIK, the largest ICT activist organization in Indonesia, seeks to close the digital divide between rural and urban centers by providing outreach, education, and competence for people in remote areas of the country, in collaboration with the Ministry of Communication and Informatics.<sup>203</sup>
- MicroMentor Indonesia is an online business mentoring platform available through Mercy Corps Indonesia and supported by Mastercard that brings together micro enterprise entrepreneurs and business mentors and offers cybersecurity training and toolkits.<sup>204</sup>
- The Indonesia Computer Emergency Response Team (ID-CERT) distributes alerts and advisories about new vulnerabilities and threats and facilitates the sharing of cybersecurity knowledge and best practices among organizations, government entities, and the public.<sup>205</sup>



# Challenges And Barriers In Cybersecurity For MSMEs

The vulnerability\* of MSMEs in Indonesia to cyberattacks is primarily due to limited financial resources and cost considerations, insufficient awareness, the complexity of cybersecurity and a lack of trained personnel, and an absence of compliance with regulations.<sup>206</sup> During the COVID-19 pandemic, these smaller enterprises were largely forced to either digitalize or close. Many did not survive this drastic transformation, as they were ill-prepared to adopt digital platforms in such a short amount of time and to make the almost complete digital shift needed to stay in business. Indonesia's older population has been especially resistant to digitalization and digital literacy efforts, let alone to cybersecurity, even if they own a business.

Indonesia's geography—an archipelago featuring multiple urban centers that give way to vast rural areas—has historically been considered a barrier to economic and digital development. Hence, a study published in 2023 recommended that the Indonesian government focus on closing the urban-rural digital divide, particularly in mountainous areas to aid rural economic actors (typically MSMEs). It is also worth noting that, according to a cybersecurity expert interviewed for this research, many initiatives aimed towards cybersecurity awareness for MSMEs in Indonesia's rural areas take place via video conferencing, because industry and government actors are located in urban areas.<sup>207</sup> Yet, a study carried out by DAI in 2021 discovered that 76% of online MSMEs reported learning to use digital tools\* from friends and family, suggesting that a community-based training model may be more beneficial to overcoming barriers to cybersecurity in rural parts of Indonesia.<sup>208</sup>



## Conclusion

This overview of the cybersecurity landscape for MSMEs in Indonesia highlights the unique challenges they face as a part of the largest economy in the APAC region, including the country's considerable size and the challenges of a significant urban-rural digital divide. Indonesia has a relatively young population that is comfortable engaging in e-commerce, especially through social media apps, creating more opportunities for micro and small businesses to thrive with little more than a mobile internet connection. However, this presents more opportunities for cyber threat actors\*, against which Indonesia's MSMEs are poorly equipped to protect themselves, as they lack cybersecurity awareness, expertise, and funding.

Studies have shown that community-based education models may be the best way to help MSMEs in Indonesia understand and implement important cybersecurity tools, especially in rural areas. But much of the relevant research on this question, prompted by the surge in cyberattacks that followed the movement of businesses online during the COVID-19 pandemic, is ongoing. The researchers, institutions, and organizations responsible for these studies may be important sources of information about where research gaps still exist. There is also a known lack of primary research on cyber threats specific to micro enterprises and micro entrepreneurs in Indonesia, presenting an opportunity to speak in depth with owners of MSMEs to understand the types of cyberattacks that pose the greatest threat to their business.

## Methodology

This report relied primarily on secondary research and focused on materials from post-2020, to capture the impacts of the COVID-19 pandemic on the cybersecurity challenges of MSMEs, though some earlier data was also referenced. Sources included government databases, academic articles, industry white papers, and both local and international news. Supplementary interviews with regional cybersecurity experts and the local staff of an NPO enriched the analysis. Challenges arose in investigating the specific cyber threats facing micro and small businesses, because despite many recent studies and initiatives in Indonesia seeking to explore and address this issue, most are still ongoing. This is because the country's digitalization efforts began in earnest in the post-pandemic period, making it still premature in many cases to evaluate their effectiveness and outcomes. Further, due to the fact that many of Indonesia's MSMEs, especially micro businesses, operate outside the formal economy, it is difficult to find secondary research sources of accurate data and information on these enterprises. This presents opportunities for primary research, however, especially outside Indonesia's urban centers, as many government initiatives are nearing several years of implementation and will soon have produced enough relevant data to assess their value to MSMEs.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Japan | 



# JAPAN

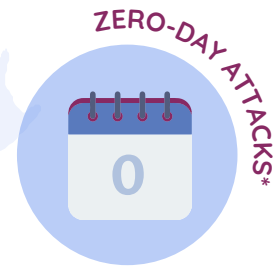


3.6 million MSMEs<sup>209</sup>

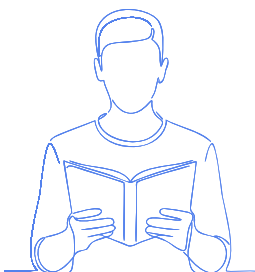
## Digital Services Most Used for E-Commerce<sup>210</sup>



## Top Cyber Threats Faced By MSMEs<sup>211</sup>



## Key Facts






In 2018, only **4%** of small and medium businesses in Japan followed government cybersecurity guidelines.<sup>212</sup>

The data breach rate for Japanese organizations is **26%**, much lower than the global average of **60%**. However, the financial cost of those breaches in Japan was **60%** higher than the global average.<sup>213</sup>






## DEFINITION OF MSME\*214




### MANUFACTURING

-  Employees | Small  
20 or less
-  Employees | Medium  
300 or less
-  Capital  
300 million yen or less


### WHOLESALE

-  Employees | Small  
5 or less
-  Employees | Medium  
100 or less
-  Capital  
100 million yen or less

### RETAIL

-  Employees | Small  
5 or less
-  Employees | Medium  
50 or less
-  Capital  
50 million yen or less

### SERVICES

-  Employees | Small  
5 or less
-  Employees | Medium  
100 or less
-  Capital  
50 million yen or less

\*The Japanese government does not define a micro enterprise by any one size or sector, but it acknowledges that they play a vital role in the community and may offer programs or policies impacting these businesses.



## Executive Summary

In Japan, MSMEs confront a cybersecurity environment shaped equally by the country's advanced digital infrastructure and by its failure to implement new digital technology or raise awareness and capacity. While the country experiences fewer reported data breaches than the global average, its role as a worldwide manufacturing hub means that any vulnerabilities in MSMEs which support the manufacturing sector can affect supply chains at the national and international levels.<sup>215/216</sup> Ransomware\* is therefore deployed rampantly in Japan, as cybercriminals understand the high stakes of interruptions to global supply chains.<sup>217</sup>

The internet usage rate in Japan is notably high, with 83% of the population having access to the internet as of the start of 2023.<sup>218</sup> When they do so, they enjoy relatively strong legal protections of their data, as a result of Japan's fairly robust regulatory framework; which also includes resources and training opportunities for MSMEs and the general population.<sup>219</sup> Even so, there is too little awareness of and funding for cybersecurity measures directed at MSMEs, the implementation of which is complicated by factors ranging from outdated software\* and equipment, to a lack of talent to fill cybersecurity roles, to the slow pace at which regulatory and legal frameworks are adopted.<sup>220/221/222/223</sup> Hence, improving cybersecurity for MSMEs in Japan, which is essential to maintaining the country's economic vitality and its pivotal role in global supply chains, will require commitment and investment by businesses, employees, and regulatory bodies alike.



## The General Cybersecurity Context In Japan

Japan is actively working to complete a digital transformation, dubbed “Society 5.0” by the government and described as an effort to connect cyberspace to the physical world.<sup>224</sup> But when the country’s digitalization was accelerated by the COVID-19 pandemic, gaps in data protection were revealed.<sup>225</sup> And though a 2023 study found that Japanese organizations reported data breaches\* at a rate of just 26%, well below the global average of 60%, the cumulative cost of those breaches amounted to a loss of 460 million yen (roughly 3.2 million USD), which was 60% higher than the global average.<sup>226</sup> This is likely linked to Japan’s prominent role in global supply chains, especially in the automotive and semiconductor industries, as their disruption is extremely costly not only to Japan but to the global economy.<sup>227</sup> That same 2023 study also determined that the push to remote work which took place during and after the COVID-19 pandemic exacerbated the country’s cybersecurity challenges, as only 39% of employers moved to accelerate their digital transformation in order to support remote workers.<sup>228</sup>

In 2023, the leading cyberattack vector in Japan was phishing\* emails. It was ransomware\* attacks that most often resulted in a data breach\* (65%), however, followed by phishing (46%) and zero-day attacks\* (27%).<sup>229</sup> Though the success of these attacks relies in part on user behavior, there are no laws mandating that Japanese companies require or provide cybersecurity training for employees, or perform risk assessments. That said, the country’s legal framework for cybersecurity is relatively robust. It includes the Basic Act on Cybersecurity (BAC), which sets out relevant principles and measures for all industries and businesses; the “Companies Act”, which obliges directors of companies to establish cybersecurity systems; and the Act on the Protection of Personal Information (APPI), Japan’s data privacy law.<sup>230</sup> There are also multiple regulatory bodies with authority over a wide range of cybersecurity issues.

Nonetheless, Japan has faced challenges in efforts to achieve greater digital security. For instance, in 2018, when the Osaka Chamber of Commerce conducted a survey of small and medium enterprises, only 4% had implemented cybersecurity measures in accordance with guidelines issued by the Japanese government.<sup>231</sup> This finding reflects the degree to which the country’s cybersecurity is dependent on further cultural, structural, and operational changes in organizations and in regulatory bodies, especially in regard to MSMEs. Without these changes, the country’s aging population, shortage of human resources, and outdated digital infrastructure (which is especially used by MSMEs) will result in significant economic losses and operational inefficiencies in the coming years, as Japan reaches the safe “digital cliff” that its Ministry of Economy, Trade and Industry (METI) has warned is imminent.<sup>232</sup>

## The Context For MSMEs In Japan

There are 3.58 million MSMEs in Japan, constituting nearly all enterprises (over 99%) in the country and employing seven in ten (69%) employees in the business economy.<sup>233/234</sup> Approximately 22% of the Japanese workforce is employed in micro enterprises specifically.<sup>235</sup> Yet, MSMEs in Japan tend to have poor cybersecurity practices, little to no dedicated IT or cybersecurity personnel, and therefore lack cybersecurity training for employees and use outdated software\* and systems, making them easy targets for attackers.

### Prevalence Of The Informal Sector

The informal sector in Japan comprises just under 10% of its economy. This is far lower than the regional average of 60%, a disparity that results from Japan's developed economy and comprehensive regulatory systems.<sup>236/237</sup> Retail and services, the most common components of the informal sector in Japan, would likely be categorized as micro enterprises if this was a legal designation of the government.<sup>238</sup>

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

The most commonly used platform in Japan is the app Line, popular with businesses because it centralizes their ability to advertise, sell goods and services, accept mobile payments, and communicate with customers.<sup>239</sup> In 2023, there were 93 million Line users in the country, compared to 25 million Facebook users.<sup>240</sup> To carry out e-commerce, Japanese MSMEs also utilize Rakuten, Amazon Japan, and Yahoo! Which are known for their ease of use and low barrier to entry.<sup>241</sup> In the next few years, online sales are projected to increase seven to ten times faster than retail sales in Japan, especially now that the Japanese government has recognized the value of supporting MSMEs in developing e-commerce platforms and has implemented initiatives to help them do so.<sup>242</sup> But these platforms are not without risk, and in 2023, Japan saw cyber and phone scams increase by over 8% to the highest number in a decade.<sup>243</sup>

### Key Trends In Cybersecurity Among MSMEs In Japan

While there is little consensus on the cyber threats that pose the greatest risk to Japanese MSMEs, attacks on these businesses typically follow the pattern of attacks carried out on Japanese industrial giants, and in Japan more generally, meaning that they tend to involve ransomware\*. This is a major concern in Japan due to the ability of such attacks to interrupt the supply chain. Notably, the Japanese National Police Agency has determined that more than half (53%) of ransomware\* attacks are targeted at MSMEs.<sup>244</sup> Attackers use this method to then gain entry into the systems of larger enterprises that may sub-contract with the smaller business, exploiting the supplier-customer relationship and any access to credentials used by the larger entity.

In 2023, one-third (33%) of the ransomware\* attacks reported in Japan were directed against the manufacturing industry, and one-fifth (21%) targeted the service industry.<sup>245</sup> In a majority of cases, the infection routes for ransomware\* were traced to VPN\* devices and the use of remote desktop services. In other words, vulnerabilities in the devices used for remote work are being exploited by cybercriminals.<sup>246</sup> This shines a light on gaps in cybersecurity preparedness among MSMEs, and the degree to which their investments in cybersecurity vary.

Discussions with regional experts revealed that MSMEs in Japan are approximately 15 years behind where they should be in terms of cybersecurity preparedness. Many businesses still use outdated software\* and operating systems, or mistakenly believe that on-site physical security assets are safer than cloud solutions. There is also a cultural tendency to view threats as emanating only from external sources; but internal threats are prevalent, whether malicious or accidental.<sup>247</sup>

### Case Study

In late February 2022, the medium-sized enterprise Kojima Industries was hacked as the result of a ransomware\* attack. Although Kojima supplies only cup holders, USB sockets, and door pockets for car interiors, the incident brought Toyota's production to a halt. The breach cost Kojima around 375 million USD, as well as the months it took to recover. Moreover, the attack affected not only Toyota, but many other smaller business subsidiaries that were, like Kojima, producing parts for its cars. This tactic, of attacking the "low hanging fruit" in hopes of gaining access to or disrupting a larger enterprise, is used widely in Japan by cybercriminals, due to the country's position as a global hub for the manufacturing and supply of high-tech products.<sup>248</sup>



## Current Cybersecurity Measures For MSMEs

Japan enjoys a fairly robust regulatory framework for cybersecurity, which is crucial to supporting the digital security of MSMEs. This framework is governed primarily by the BAC and APPI, which set strict guidelines for personal data handling by businesses and government entities. On top of this, the Personal Information Protection Commission (PPC) serves as the central authority for data protection, ensuring compliance and addressing violations.

Because Japan's informal economy accounts for so little of its overall economy, it is safe to assume that most MSMEs in the country are bound to comply with the government's data protection standard, but it is difficult to know how many are actually complying or if they understand how to comply. The survey mentioned earlier, conducted in 2018 by the Osaka Chamber of Commerce, captured only a small sample of MSMEs, but indicated that very few businesses had achieved compliance at that time. While the government has invested in measures to support MSMEs in receiving training, implementing technical improvements, and developing partnerships with cybersecurity firms at reduced costs, businesses must be aware of and have the capacity to take advantage of these programs. Given the pattern in Japan of third-party breaches of MSMEs in attacks aimed at larger corporations, the law may also need to consider the responsibility of those larger enterprises in the context of data protection by smaller subsidiaries.

### Government Initiatives

- The Ministry of Economy, Trade and Industry (METI) formulates policies to support MSMEs in enhancing their cybersecurity.<sup>249</sup>
- The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) coordinates national cybersecurity strategies.<sup>250</sup>
- The Personal Information Protection Commission (PPC) ensures compliance for data protection, including in MSMEs.<sup>251</sup>
- The Information-technology Promotion Agency (IPA) provides services to the public, including MSMEs, such as cybersecurity training.<sup>252</sup>
- The cybercrime division of the National Police Agency operates an account through which MSMEs can report cybercrimes.<sup>253</sup>

### Industry Initiatives

- The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is the primary cybersecurity incident response\* organization for private entities and is promoted by NISC.<sup>254</sup>
- The Cybersecurity Strategic Headquarters seeks to enhance public-private partnerships that are focused on strengthening cyber defenses and improving incident response\* capabilities.



## Challenges And Barriers To Cybersecurity For MSMEs

The challenges and barriers facing Japanese MSMEs are varied and complex. Still, some patterns have emerged. Budget constraints and the absence of internal expertise are common, and these are compounded by the flight of Japanese cybersecurity professionals to higher-paying markets and a lack of local interest in entering the field due to the heavy workload and low pay. Additionally, many businesses in Japan struggle to achieve digital security due to the aging population—which may constitute both their staff and their consumer base. These factors combine with various cultural specificities, in ways that inhibit accountability and change in MSMEs.

For example, there is a cultural resistance to disclosing cybersecurity attacks in Japan, in part because it is considered offensive to be suspicious of others, especially one's own employees, and there is a strong stigma against assigning blame.<sup>255/256/257</sup> Seniority culture is also entrenched in the Japanese business model. Yet, senior management teams composed of older employees may not understand the importance of cybersecurity or the risks associated with information technology, and they can be rather averse to change, as they seek to retain the current age-based hierarchy and the outdated practices that come with it.<sup>258</sup> Meanwhile, IT and cybersecurity staff are often younger and lack “status” or rank, leaving them with less power and influence, even when it comes to cybersecurity concerns.<sup>259</sup>

This may explain the hesitance among young people in Japan to enter information technology fields. Indeed, these cultural factors have very real consequences. A 2023 cybersecurity study found, for instance, that more than half (53%) of Japanese companies had waited up to 24 hours to investigate a cyber threat; a rate that likely reflects how the culture of saving face leads to a reluctance to report these threats, especially if a business risks reputational damage.<sup>260</sup> In that same study, 8% of respondents claimed that lives had been lost as the result of a data breach\* in the 12 months prior.<sup>261</sup>



## Conclusion

This overview of the cybersecurity landscape in which MSMEs operate in Japan highlights the unique challenges these businesses face in the context of the country's advanced digital infrastructure and critical role in global supply chains. In Japan, cyber threats to MSMEs have the capacity to impact the global economy and world markets. MSMEs must therefore be monitored closely and supported continuously to achieve the highest levels of security possible. Despite a robust regulatory framework in the country and various measures available to support MSMEs, businesses in Japan still exhibit low levels of awareness and a resistance to change, face budget constraints, and use outdated systems. In the near future, this could lead to negative consequences that ripple across the economy.

The comparatively developed economy of Japan has meant that few studies by international and domestic organizations on micro and small businesses have been undertaken in the country. And existing domestic reports do not differentiate micro businesses from small businesses, as the Japanese government does not officially define micro enterprises by size or sector. Without more detailed primary research, it is difficult to quantify the threats confronted by micro businesses in Japan and the barriers they encounter to achieving better digital security. While experts explained that these businesses tend to operate using cash or personal bank accounts, as well as mobile phones, this sector of the economy certainly presents opportunities for further research, to identify how government or industry partners can best support Japanese micro enterprises.

## Methodology

This report relied primarily on secondary research sources, especially materials published after 2020, to capture the impacts of the COVID-19 pandemic on MSMEs in Japan. These sources included government databases, academic articles, industry white papers, and local and international news reports. Supplementary interviews with regional cybersecurity experts enriched the analysis. Challenges arose in gathering data on micro businesses, which are not officially defined in Japan, and on smaller enterprises generally, as they are often overlooked in the context of cybersecurity, where the focus tends to be on larger businesses and government.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Korea | 





# KOREA

7.7 million MSMEs<sup>262</sup>

## Digital Services Most Used for E-Commerce<sup>263</sup>



NAVER

toss

Meta



Gmarket

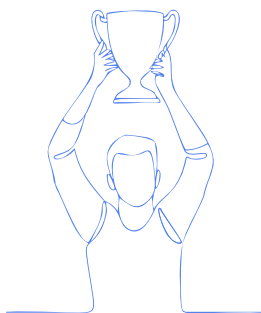
AUCTION.

coupang

## Top Cyber Threats Faced By MSMEs<sup>264</sup>



## Key Facts




In 2020, Korea ranks **#1** in the Asia-Pacific region, tied with Singapore, in terms of good cybersecurity practices.<sup>265</sup>

In 2022, **88%** of cyber attack victims in Korea were MSMEs.<sup>266</sup>




## DEFINITION OF MSME\*267/268


### MICRO ENTERPRISE\*\*

-  Employees  
9 or less (mining, manufacturing, construction and transportation sectors)  
4 or less (other sectors)

### SMALL ENTERPRISE

-  Annual turnover  
Between 1 and 12 billion KRW

### MEDIUM ENTERPRISE

-  Annual turnover  
Between 40 and 150 billion KRW

\*The definition of MSMEs varies depending on the context in Korea

\*\* 383 million employees (17.4% of the total workforce) work for micro-enterprises with less than 5 employees.



## Executive Summary

In a 2023 study conducted by the International Institute for Management Development (IMD), the Republic of Korea ranked second in the APAC region in terms of digital competitiveness. This assessed knowledge, technology, and future readiness in systems and regulatory frameworks.<sup>269</sup> Internet access in the country is widespread, with 92% of the population digitally connected, allowing for people to work, shop, and connect online in a way that truly integrates society with cyberspace.<sup>270</sup>

The COVID-19 pandemic accelerated a shift to online services in Korea, and to ease the transition, the Ministry of Science and ICT introduced the Korean Digital New Deal in June 2020.<sup>271</sup> This expanded government investments in information security by increasing funding to research and development.<sup>272</sup> And the need for enhanced cybersecurity measures could not be more critical, as cyberattacks have increased at a rate of 120% over the last 6 years, and have particularly been aimed at private companies.<sup>273</sup>

In 2023, 92% of the companies targeted by cyberattacks in Korea were MSMEs.<sup>274</sup> Even though awareness regarding the importance of cybersecurity is very high in the country, only about one-quarter (27%) of Korean businesses report having developed an internal policy to protect their enterprise, meaning that nearly three-quarters (73%) have no such policy.<sup>275</sup> This is largely due to a lack of cybersecurity professionals and insufficient budget allocations for cybersecurity by MSMEs.<sup>276</sup>

There are several regulatory bodies and cybersecurity frameworks in place in Korea, but the need remains for a unified cybersecurity law, as well as more targeted support for MSMEs. Investment by the government in the country's economic growth, especially in the MSME sector, will need to take the form of increased funding for cybersecurity readiness. There is strong public-private cooperation when it comes to cybersecurity for large corporations and government security organizations, and to ensure cybersecurity readiness on a national level among the public, but this has not been effectively translated into the MSME sector.<sup>277</sup> Korea has been a relative beacon of IT and cybersecurity success in the region, but it must continuously work to stay ahead of rapidly developing threats, and must take proactive steps to protect its economy by supporting better protections for MSMEs.

## The General Cybersecurity Context In Korea

Korea's advanced digital infrastructure is the cornerstone of its economic strategy. The country has one of the fastest internet speeds in the world, there is a high level of adoption (92%) of its information and communication technology (ICT) ecosystem, and the government and private sector have deployed advanced cybersecurity measures.<sup>278/279/280</sup> Korea also maintains a strong global presence in international markets, and offers cross-border digital services and e-commerce.<sup>281</sup>

In June 2020, when the Korean Digital New Deal was launched, the goal of the South Korean Ministry of Science and ICT was to ease society's digital transition and begin to overcome the digital challenges presented by the COVID-19 pandemic.<sup>282</sup> Investments in the information security industry, particularly in research and development and in planning capacity, are intended to increase the IT and cybersecurity workforce.<sup>283</sup> While this is expected to support economic growth more broadly and extend the country's global reach, it could also bring more cyberattacks, and on an even larger scale, as points of vulnerability\* in Korea continue to multiply. In fact, a rise in cyberattacks since the rollout of the Digital New Deal underscores the need for constant revisions of the country's cybersecurity strategy to account for an ever-changing cyber threat landscape.

Data privacy is protected by a robust legal and regulatory framework in Korea, and primarily by the Personal Information Protection Act (PIPA).<sup>284</sup> Every organization and enterprise operating in Korea is required to abide by the Act and other relevant laws, or face legal repercussions. Korea has also made considerable investments in cybersecurity, and directs a substantial amount of the cybersecurity budget towards cyber capabilities that impact national security. In 2020, Korea ranked 4th on the Global Cybersecurity Index, behind Estonia, Saudi Arabia and the United Kingdom (tied for 2nd place), and the United States.<sup>285</sup> Compared to other developed countries, though, the proportion of the Korean budget that is allocated towards developing cybersecurity experts and protections for businesses falls short.<sup>286</sup>



## The Context For MSMEs In Korea

In Korea, MSMEs account for almost all (just short of 100%) domestic businesses and 81% of all jobs.<sup>287/288</sup> Of these businesses, 46% are micro enterprises, many of which engage in retail and e-commerce activities.<sup>289</sup> There is typically a very low barrier to entry for micro or small businesses in Korea, which may explain this high number of micro e-commerce enterprises.<sup>290</sup> Still, large corporations constitute 69% of the country's production and 66% of national value added.<sup>291</sup>

### Prevalence Of The Informal Sector

The informal sector is estimated to constitute around 23% of the Korean economy. This makes it larger than those in other advanced economies in the APAC region, such as Japan and Hong Kong.<sup>292</sup> In Korea, this rate likely accounts for micro businesses like street vendors, various home-based businesses, and small retail operations.

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

Korea-based Kakaotalk is the most-used social media app in the country, followed by Instagram and Facebook.<sup>293</sup> In 2021, Kakao Corporation, the parent company of Kakaotalk, launched an e-commerce platform, which has led to a proliferation of impersonation fraud, impacting both customers and MSMEs.<sup>294</sup> The Korea Fair Trade Commission has also considered imposing sanctions on Meta, the parent company of Instagram and Facebook, for failing to protect users of its online marketplaces.<sup>295</sup> Both Instagram and Facebook are frequently leveraged by MSMEs to sell products and services, and to promote their business, and because it is common for small business owners to use personal social media accounts for dual purposes, vulnerabilities in these platforms put MSMEs at risk through multiple entry points.<sup>296</sup>

### Key Trends In Cybersecurity Among MSMEs In Korea

Cyberattacks against Korean MSMEs have been on the rise, increasing by 14 times between 2019 and 2023, at a cost of 695.6 billion KRW (approximately 500 million USD).<sup>297/298</sup> In 2022 and 2023, the most common of these involved malware\* and web-based malware\*, supply chain attacks\*, phishing\*, and ransomware\* attacks.<sup>299/300</sup> According to a 2021 survey, 88% of cyberattacks in Korea were directed against MSMEs.<sup>301</sup> Yet, research undertaken by the Korean government in 2023 found that while 89% of total businesses and 88% of micro businesses (with less than 5 employees) were aware of the importance of information security, only 27% of total businesses had adopted internal policies on information security.<sup>302</sup> This is starkly lower than the 94% of large corporations in Korea that have put cybersecurity policies in place.<sup>303</sup>

The government's research also determined that an overwhelming majority (95%) of MSMEs had experienced some type of cyberattack, at least once<sup>304</sup>. Nevertheless, a mere 12% of total businesses have a dedicated information security team and just 27% of total businesses have a separate budget allocation for information security. Among large Korean corporations, 82% have dedicated cybersecurity staff and 98% budget separately for cybersecurity.<sup>305</sup>

### Case Study

Many of the micro businesses in Korea are street vendors, selling popular street foods. During the COVID-19 pandemic, street vendors selling bungeoppang (Korean fish-shaped pastries filled with red bean) realized that customers were uncomfortable handling cash due to the fear of becoming infected with the virus, and transitioned to fintech\* and banking apps to receive payments. Many vendors posted a sign with information that made it easy for customers to send their payment and show proof of receipt, without realizing that this posed cybersecurity risks. In some cases, vendors were scammed by people who showed a payment had been processed without actually paying; but more sophisticated cybercriminals gathered bank account information from these vendors and used their identities to commit online crimes, so they could not be traced back to the real perpetrators. This inevitably affected the bank accounts of street vendors, which were investigated or closed, negatively impacting their businesses or forcing them to stop operating.<sup>306</sup>

## Current Cybersecurity Measures For MSMEs

### Government Initiatives

- The Korea Internet & Security Agency (KISA) provides services including cyberattack response and a diagnosis platform, as well as guidebooks that help users prevent and address different types of attacks, while fostering partnerships with MSMEs and cybersecurity solutions providers.<sup>307/308/309</sup>
- The National Cyber Security Center (NCSC) is responsible for national cybersecurity policy and coordination, with the goal of strengthening cybersecurity infrastructure to benefit all businesses in Korea.<sup>310</sup>
- The Personal Information Protection Commission (PIPC), the central administrative agency for personal data protection, enforces privacy laws and regulations and provides guidelines and resources to MSMEs to understand and comply with data protection requirements.<sup>311</sup>
- The Ministry of Science and ICT (MSIT) develops policies and initiatives to foster a secure information technology ecosystem.<sup>312</sup>
- The Ministry of SMEs and Startups supports MSMEs in various ways, including in adopting new technology and implementing security measures.<sup>313</sup>

## Industry Initiatives

- The Korea Federation of SMEs (KBIZ) advocates for the interests of MSMEs, including on issues related to digital security.<sup>314</sup>
- The Korea Information Security Industry Association (KISIA) works to advance the information security industry and enhance levels of information security across national industries.<sup>315</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

In Korea, many MSMEs are prevented from instituting cybersecurity measures by the cost. In fact, a study conducted by KISA found that 32% of MSMEs cited this cost burden as the number one reason for their insufficient cybersecurity preparedness; followed by the lack of relevant experts (12%), difficulty finding necessary cybersecurity programs (12%), and a lack of knowledge about cybersecurity (9%).<sup>316</sup> Research by Hansung University in 2021 identified these same challenges for MSMEs, as well as a lack of compliance with data protection regulations, insufficient incident response\* and recovery plans, reliance on third-party vendors for critical business operations, and remote work vulnerabilities.<sup>317</sup>

One expert in Korea also pointed to legacy IT infrastructure as a main barrier to cybersecurity, and noted a general reluctance to upgrade these systems.<sup>318</sup> Some of this is likely cultural. As in other countries in the APAC region, Korea has an aging population and seniority-based company hierarchies, and younger employees in IT and security roles may be dismissed because they lack status.



## Conclusion

Korea's remarkable digital competitiveness and extensive internet penetration serve as pillars of its robust MSME economy, and have accelerated the digital transformation of smaller Korean companies in the post-COVID-19 era. While the country's forward-looking policies are steering it toward a future of increasing technological sophistication, the growing shadow of cyber threats looms. Amid heightened vulnerabilities, the critical MSME sector—which is at the very heart of Korea's economy—is a particular target of cybercriminals.

Given the challenges Korea has faced in deploying effective internal policies, and a continued reliance on outdated IT infrastructure, there is an urgent need for enhanced support to MSMEs from both the government and industry. This includes initiatives to address cost-driven constraints, cultivate a culture that values IT and cybersecurity awareness across generations, and make significant investments in nurturing future cybersecurity talent. Protecting MSMEs should not be viewed only as a means of securing the business environment in Korea, but as a way to strengthen the economy and safeguard the nation's digital future.

A lack of research by international and domestic organizations on micro and small businesses in Korea means there is little primary data on the challenges facing these businesses specifically. This makes it difficult to quantify the cyber threats to micro enterprises in Korea and the barriers preventing them from attaining greater digital security. Additionally, as in Japan, any reports that do exist do not differentiate micro businesses from small businesses, and experts said that because micro businesses in Korea tend to use mobile payment apps tied to personal bank accounts and personal laptops, there is a lack of data on their operations. Hence, there are opportunities to dive deeper into this sector of the Korean economy in future research, to identify how MSMEs can best be supported by government or industry partners.

## Methodology

This report relied largely on secondary research sources, including government databases, academic articles, industry white papers, and local and international news, and focused on materials from the post-2020 period to capture the impacts of the COVID-19 pandemic on the cybersecurity of MSMEs in Korea. Supplementary interviews with regional cybersecurity experts and the local staff of a regional NPO enriched the analysis. Challenges arose in gathering data and case studies on or about micro and small businesses in Korea, as these are often overlooked in official documentation and reports, which tend to concentrate on the cybersecurity efforts of larger businesses and the government.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Malaysia | 



# MALAYSIA

1.1 million MSMEs<sup>319</sup>

## Digital Services Most Used for E-Commerce<sup>320/321/322</sup>

facebook

Instagram

Telegram

Shopee

Lazada

WhatsApp

## Top Cyber Threats Faced By MSMEs<sup>323/324</sup>

FRAUD



MALWARE\* AND WEB-BASED MALWARE\*



PHISHING\*



### Key Facts




Cybersecurity breaches could lead to potential losses of over **10 billion USD**, representing more than **4%** of the country's GDP.<sup>325</sup>

In 2021, **84%** of MSMEs experienced cyber threats, and **76%** of them are subject to repeated attacks.<sup>326</sup>



## DEFINITION OF MSME<sup>327</sup>

### MICRO ENTERPRISE


-  Employees  
4 or less
-  Annual Turnover  
Less than 300,000 MYR

### SMALL ENTERPRISE

#### Manufacturing


-  Employees  
5-74 employees
-  Annual Turnover  
300,000 to 15 million MYR

#### Services & Other sectors



-  Employees  
5-29 employees
-  Annual Turnover  
300,000 to 3 million MYR

### MEDIUM ENTERPRISE

#### Manufacturing

-  Employees  
75-200 employees
-  Annual Turnover  
15 million to 50 million MYR

#### Services & Other sectors

-  Employees  
30-75 employees
-  Annual Turnover  
3 million to 20 million MYR



## Executive Summary

Malaysia's advanced digital infrastructure facilitates internet access for nearly its entire (97%) population, positioning it as a significant actor in global cybersecurity efforts.<sup>328</sup> In the Global Cybersecurity Index 2020, the country ranked among the top ten globally, and second in ASEAN, for its commitment to cybersecurity.<sup>329</sup> Despite this, Malaysia faces substantial cyber threats. The country's cyber threat risk index stands at 43% and cyber breaches represent potentially significant economic losses, which could rise to more than 10 billion USD, representing over 4% of GDP.<sup>330/331</sup>

In Malaysia, MSMEs form the backbone of the economy but are notably vulnerable in digital space. A majority are micro enterprises, which face disproportionate cyber risks due to their limited cybersecurity awareness, inadequate resources, and less robust security measures, compared to larger businesses. Recent surveys indicate that 84% of MSMEs in Malaysia have experienced cyber threats, and in some cases repeated attacks, underscoring the urgency for more targeted support and stronger cybersecurity policies that specifically address the needs of this sector.<sup>332/333</sup>

Thus far, the strategic response of the government has included development of the National Cyber Security Policy (NCSP) and the establishment of a National Cyber Security Agency (NACSA). It was the NACSA that spearheaded efforts to draft the Malaysia Cyber Security Strategy 2020–2024.<sup>334</sup> The Strategy emphasizes the imperative to protect the vast network of MSMEs, which make up over 97% of the country's businesses and are critical to its economic fabric.<sup>335</sup> Efforts to bolster cybersecurity for MSMEs are therefore underway but must continue to be a priority, so that these businesses are shielded from escalating cyber threats and Malaysia can maintain its economic integrity and growth. Current strategies, including the implementation of tailored cybersecurity education, the provision of accessible resources for threat mitigation, and the offer of government-backed incentives designed to foster robust cybersecurity frameworks within the MSME sector, are crucial to ensuring that cybersecurity measures evolve in step with the ever-changing threat landscape and can provide continuous protection to these vital economic contributors.

## The General Cybersecurity Context In Malaysia

The advanced digital infrastructure of Malaysia allows for almost total internet penetration (97%) in the country.<sup>336</sup> Though matched by a high commitment to cybersecurity, Malaysia nonetheless faces considerable cyber threats.<sup>337/338</sup> Since the 2006 formulation of the National Cyber Security Policy (NCSP), which was developed primarily to address risks to Critical National Information Infrastructure (CNII), the government has taken a proactive stance on cybersecurity. Malaysia's data privacy law, the Personal Data Protection Act 2010 (PDPA), was passed in 2013 and applies to all commercial transactions in the country, imposing penalties for non-compliance, including fines and jail time.<sup>339</sup> And in 2017, the National Cyber Security Agency (NACSA) was established to reinforce the cybersecurity apparatus and the strategic measures used by Malaysia to combat cybercrime.<sup>340</sup> The NACSA led development of the Malaysia Cyber Security Strategy 2020–2024, in which MSMEs are clearly discussed as part of the wider cybersecurity ecosystem.<sup>341</sup> (See Malaysia-Figure 1)\*

However, these measures have not prevented Malaysia from experiencing frequent and well-documented cyberattacks and data breaches.<sup>342</sup> In 2023, there were 5,917 of these cybersecurity incidents, including 3,705 cases of fraud; exacting a significant toll on the Malaysian economy.<sup>343</sup> In 2021, in response to these cybersecurity challenges, and with the aim to prevent potentially sizable economic losses for the country, the Malaysia Digital Economy Corporation (MDEC), in collaboration with the NACSA and SME Corporation Malaysia, announced the MATRIX–Cybersecurity for SMEs initiative. Yet, this program, intended to focus on four areas of cybersecurity assistance to MSMEs, has yet to be realized.<sup>344</sup>

## The Context For MSMEs In Malaysia

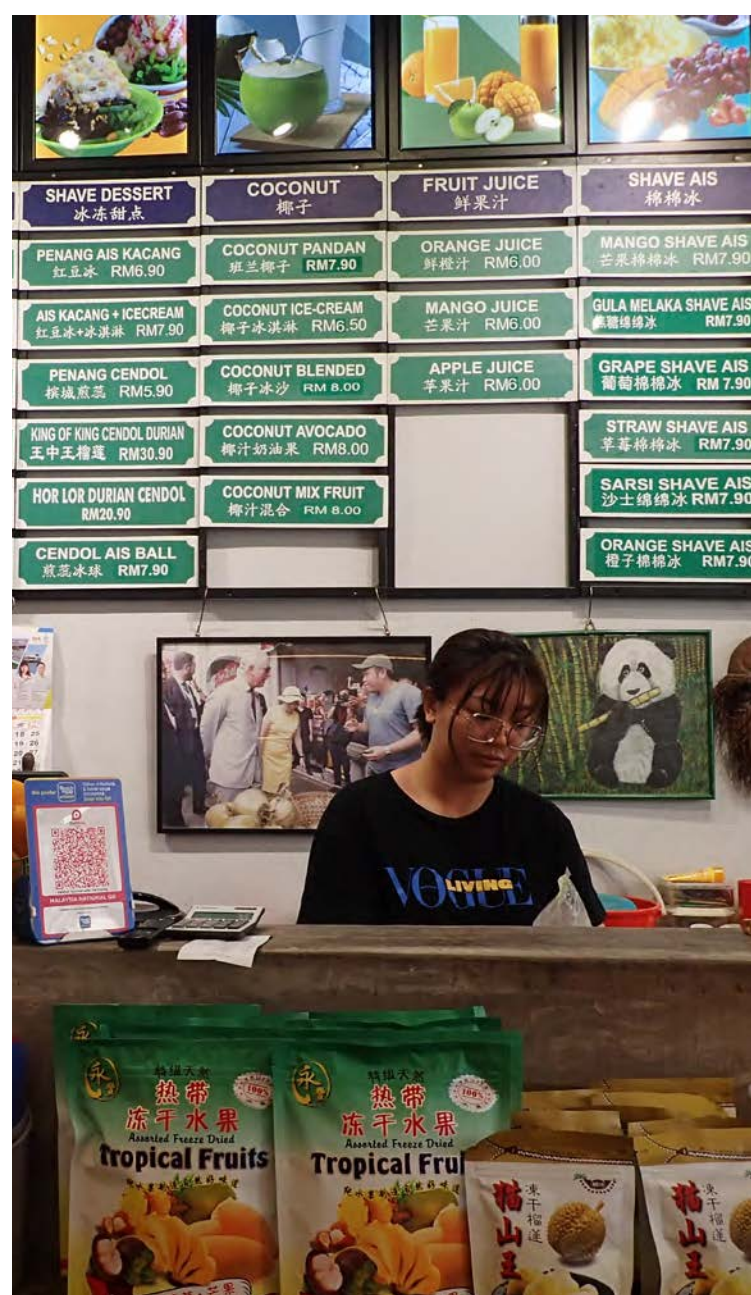
In Malaysia, MSMEs account for 97% of all enterprises, generate 38% of GDP, and provide employment for 7.3 million people.<sup>345</sup> Nearly eight in ten (78%) of these businesses are micro enterprises, and a majority are in the service sector.<sup>346</sup> Compared to small and medium businesses, micro enterprises face different and specific cybersecurity challenges, as they tend to have more limited knowledge and management capacity.<sup>347</sup> This may explain persistent gaps in cybersecurity adoption in Malaysia, despite efforts to bolster digital resilience, and highlights the need for more concerted action to mitigate the cyber threats increasingly facing MSMEs of all sizes.

Typically, MSMEs in Malaysia are family owned, small-scale operations that utilize local resources. Even informal MSMEs are likely to use some digital technology, but usually only the most affordable options, such as digital payment and e-commerce platforms. On top of these financial constraints, many informal MSMEs lack access to information, expertise, and new technology, as well as the legal protections enjoyed by formal enterprises, leaving them considerably more susceptible to cyber threats.<sup>348</sup> The sensitive personal information of MSME owners is also frequently at risk if their business is breached, because it is common for MSMEs to use personal accounts for business purposes. Cybersecurity regulations alone will not mitigate this problem, as the informal nature of many MSMEs in Malaysia puts them beyond the reach and application of formal regulations.<sup>349</sup>

Of the 84% of Malaysian MSMEs that report having been compromised by cyber incidents, an overwhelming three-quarters (76%) of these businesses have experienced repeated attacks.<sup>350</sup> Sustained efforts to bolster cybersecurity measures in this sector are clearly needed, particularly given the contribution of MSMEs to the national economy. In 2022, for example, MSMEs achieved economic growth that surpassed pre-pandemic levels, recording GDP growth of nearly 12%, exceeding overall national GDP growth of just under 9%.<sup>351</sup>

### Prevalence Of The Informal Sector

The informal sector in Malaysia (defined as employment with unregistered firms) fell marginally as a proportion of total non-agriculture employment in the decade from 2011 to 2021, from just over 9% to just under 9%, and declined overall from 38% in 2009 to 27% in 2022.<sup>352/353</sup> According to the World Bank, MSMEs remain far from realizing their full potential to contribute to the Malaysian economy, as long as they operate in low value-added industries with high informality, including informal sources of funding.<sup>354</sup> This informality is linked to the lower barrier to market entry it presents, as owners need not go through the complex process of business registration.



## High Risk Platforms And Most Used E-Commerce/Social Media Platforms

The most commonly used e-commerce platforms in Malaysia are Lazada and Shopee. In the third quarter of 2023, e-commerce income in Malaysia grew by over 5%, primarily driven by the manufacturing and service sectors.<sup>355</sup> Meanwhile, WhatsApp, Facebook, Instagram, and Telegram are the most-used social media platforms in the country.<sup>356</sup> And for micro enterprises in Malaysia, 60% of which used social media platforms for their business operations in 2022, the platforms they used for customer engagement were Whatsapp (39%), Facebook (19%), Google (14%), and Instagram (10%).<sup>357</sup>

Some of the e-commerce platforms and social media sites relied upon by Malaysian MSMEs to carry out day-to-day operations have experienced significant cybersecurity breaches. For instance, in 2022, a hacking community took credit for selling a database of 487 million WhatsApp user mobile numbers, of which 11 million belonged to Malaysian account holders.<sup>358</sup> Also that year, the e-commerce platform Carousell had a database of 2.6 million user accounts in Malaysia and Singapore stolen and sold on dark web and hacking forums, with 1.95 million user accounts affected; though, its credit and payment-related information was not compromised.<sup>359</sup> MSMEs in Malaysia also utilize secure online payment gateways like iPay88, Razer Merchant Services, eGHL, and Paypal. While this does help protect their digital transactions and lowers fraud risks, cybersecurity incidents can strike these platforms as well, such as when iPay88 suffered a data breach\* in May 2022 that potentially compromised the credit card data of customers.<sup>360</sup>

## Key Trends In Cybersecurity Among MSMEs In Malaysia

About half (51%) of MSMEs in Malaysia have implemented basic cybersecurity strategies, but a significant portion (76%) of these businesses rely on the default, built-in controls offered by providers. Notably, one-third (32%) of the 9% of businesses that lack any security solutions at all are micro enterprises. Thus, it is not surprising that 97% of these micro businesses (as well as 81% of small enterprises) have yet to adopt cloud-based solutions.<sup>361</sup>

### Case Study 1

In 2022, an employee at a small hardware store opened a file attached to an email that was, as it turned out, some kind of malware\*. The next day, the store's stock order and cash registers malfunctioned, impairing the business. The total financial impact of this network failure was 178,000 USD.<sup>362</sup>



## Case Study 2

In Malaysia, MSMEs—especially micro and small businesses—often use Facebook to market and sell items. Cyber attackers are known to make clone accounts with the goal of stealing customers from these businesses. They then engage in fake sales transactions so that payment is made to the cloner’s account. The only recourse for MSMEs is to report this to Facebook or post a public acknowledgement and apology on their seller’s page, which can damage their reputation.<sup>363</sup>

## Current Cybersecurity Measures For MSMEs

The Malaysian government has taken the increase of cyber threats seriously. It has reshuffled government entities that address cybersecurity concerns and has invested heavily in new cybersecurity and digital protection laws. The allocation of approximately 12.5 million USD for CyberSecurity Malaysia in the 2024 National Budget underscores the level of commitment of the government to fortifying national cybersecurity infrastructure, and particularly to developing a 5G Cybersecurity Testing Framework and local expertise on 5G technology, to increase preparedness vis-à-vis cyber threats.<sup>364</sup>

### Government Initiatives:

- The Ministry of Digital was formed to oversee Digital Nasional Berhad (DNB) and CyberSecurity Malaysia, previously under the (joint) Ministry of Communications and Digital.
- CyberSecurity Malaysia launched the “Cyber Security Technology Roadmap: Cybersecurity Malaysia Framework 2024-2029,” containing specific stipulations for various departments within the organization, with the aim of better fulfilling its mission; but it remains to be seen if programming will be tailored specifically to MSMEs.<sup>365</sup>
- The National Cyber Coordination and Command Centre (NC4), together with the National Cyber Security Agency (NACSA), led the drafting of a new Cybersecurity Bill in 2023. This bill was subsequently gazetted and officially released as Cybersecurity Act 854 in June 2024, marking a significant milestone in Malaysia’s efforts to strengthen its cybersecurity framework.<sup>366/367</sup>
- Program Galakan Pemerkasaan Keselamatan SIBER (PGKS), launched in 2021, is aimed at empowering and strengthening cybersecurity and safeguarding digital infrastructure in Malaysia by focusing on enhancing cybersecurity awareness, preparedness, and response capabilities. PGKS offers a suite of services to support and complement the needs of MSMEs in facing digital security challenges, designed to comprehensively assess cybersecurity by means of:

1. An Information Security Governance Risk & Compliance (ISGRiC) Assessment
  2. A Cyber Health Assessment: Malware\* Scanning
  3. Vulnerability Assessment & Penetration Testing (VAPT)
  4. Certified Information Security Awareness Manager (CISAM) training & certification
  5. A Cyber Security Awareness Session<sup>368</sup>
- The MDEC has laid out a Digital Economy Blueprint for Malaysia that outlines a clear vision for enhancing cybersecurity adoption among MSMEs, in three phases, with Phase 1 (2021–2022) now complete, Phase 2 (2023–2025) in process, and Phase 3 (2026–2030) yet to come. By the end of Phase 2, the target is for 70% of companies to have adopted cybersecurity measures, specifically MSMEs, with support from grants to bolster investment in cybersecurity products and assessments and capacity building.<sup>369</sup>

### Industry Initiatives

- Public-private partnerships developed by CyberSecurity Malaysia with LGMS Berhad, Velum Labs, Axiata, Celcom, and CTM360 support cyber resilience measures among MSMEs and are developing or have developed subscription-based solutions aimed at MSMEs.<sup>370/371</sup>
- Maxis Berhad, a communications company, and Public Bank Berhad have signed a Memorandum of Understanding to promote digital adoption among Malaysian MSMEs, paving the way for greater access to digital solutions and financial assistance for cybersecurity implementation.<sup>372</sup>
- EC-Council has partnered with the National Tech Association of Malaysia to build capacity and up-skill Malaysian MSMEs in cybersecurity education and training.<sup>373</sup>
- Blackberry launched The Cybersecurity Center of Excellence (CCoE) in March 2024, offering a range of initiatives and building an ecosystem of cybersecurity while also providing cyber threat intelligence and incident response\* teams to businesses and government.<sup>374</sup>
- Asia Pacific University now offers “Cybersecurity as a Service”, a commercial response unit specifically targeted at MSMEs as a cost-effective solution.<sup>375</sup>

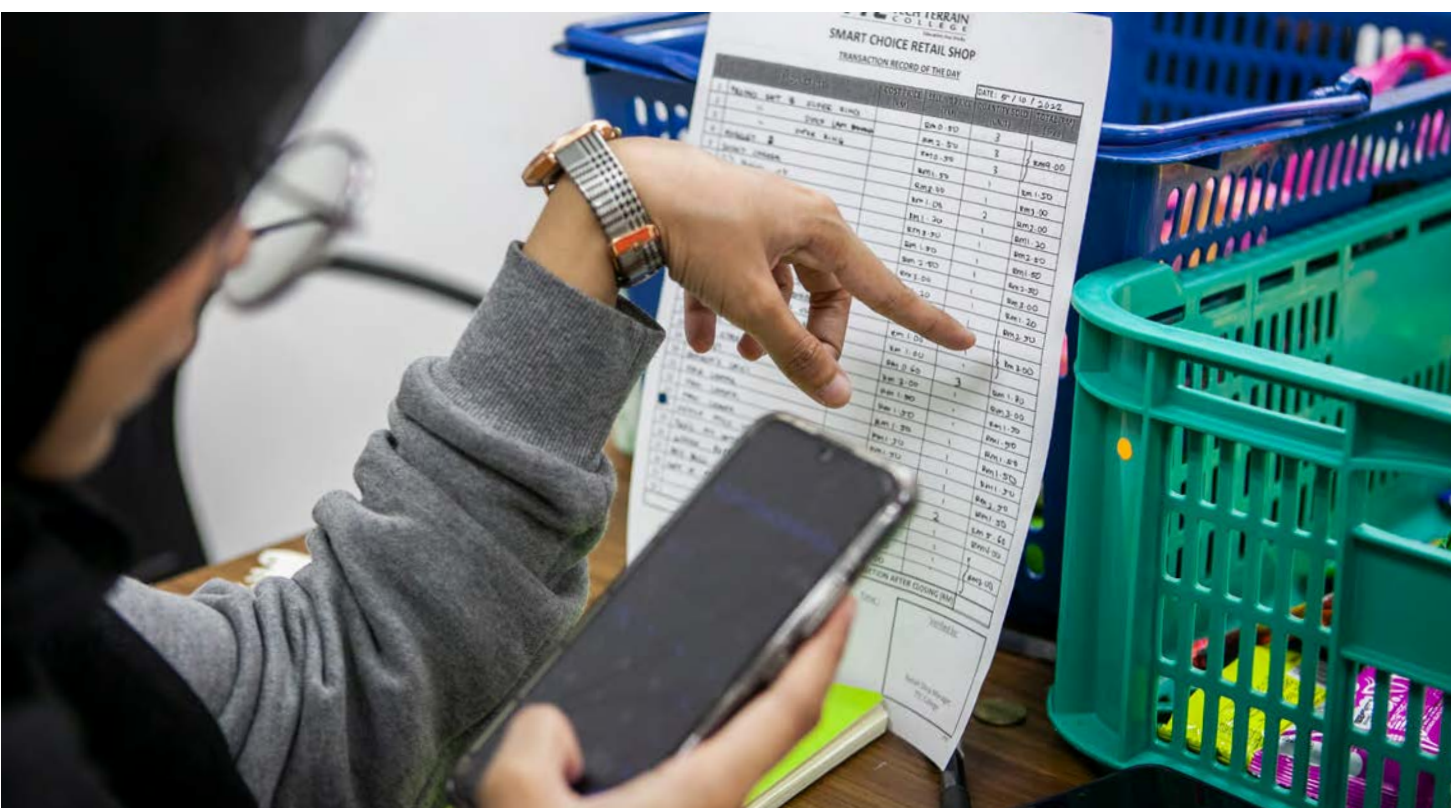
## Challenges And Barriers To Cybersecurity For MSMEs

Addressing the multifaceted challenges to cybersecurity adoption in Malaysia requires a nuanced approach. MSMEs in particular face several barriers, alongside the dynamic and growing nature of cyber risks, that complicate these efforts. Research has also found that MSMEs are often so focused on daily operations that they do not or cannot prioritize robust cybersecurity measures.<sup>376</sup> The COVID-19 pandemic did compel many Malaysian businesses to reconsider their cybersecurity strategy, to account for the heightened security risks related to remote work.<sup>377</sup> Studies have shown a strong positive correla-

tion between increased knowledge of cybersecurity and safer practices in digital marketing communications among MSME entrepreneurs in Selangor and Terengganu.<sup>378</sup> However, overall, the uptake by Malaysian MSMEs of suitable cybersecurity protection has been relatively low, which leaves them more susceptible to cyberattacks, especially as they expand their businesses by embracing technology but maintain limited budgets and resources to address cybersecurity risks.<sup>379</sup>

Additionally, existing cybersecurity frameworks are not suitable for implementation in the agile and lean technology startup products used by MSMEs. Such frameworks are typically not equipped with cyber quantification tools anyway, which are key to calculating the return of security investments for micro enterprises, allowing for better decision making and budgeting when investing in cybersecurity protection with limited resources.<sup>380</sup> This encourages MSMEs in Malaysia to take corrective actions on a case-by-case basis after a cyberattack rather than invest in a security measure with minimal apparent return on investment (ROI). Thus, the lack of in-house expertise in this sector is coupled with little funding to support in-house information systems.<sup>381</sup>

Overriding these other common barriers to maintaining cybersecurity protections in MSMEs is a general lack of understanding about the potential personal and professional impacts of cyber incidents, and an inability to identify and assess cyber risks. A 2019 report by Chubb noted for example that two-thirds (67%) of Malaysian MSMEs considered large corporations to be more at risk of cyberattacks than small businesses, and a similar rate (64%) characterized cyber risks as an IT concern rather than a shared responsibility across an enterprise.<sup>382</sup> There is also some evidence that certain stakeholders see cybersecurity as a passing trend and are skeptical about the utility of cyber insurance, which has been adopted in Malaysia at a relatively low rate.<sup>383</sup>



## Conclusion

Malaysia's impressive strides in digital competitiveness and the widespread internet access its citizens enjoy shape its proactive cybersecurity strategy. The country's digital infrastructure and cybersecurity efforts have propelled it to a significant position in global cybersecurity rankings, demonstrating the firm commitment of the government to securing its digital landscape. However, with cyber threats ever on the rise, especially those targeting MSMEs, Malaysia faces a challenge that could undermine its economic growth and digital transformation.

To combat the unceasing cyber threats experienced by MSMEs, which constitute the majority of Malaysian businesses, more comprehensive and adaptive cybersecurity measures are necessary. The Malaysian government has adopted proactive strategies (e.g., the Malaysia Cyber Security Strategy 2020–2024 and initiatives led by the NACSA), but implementation within the MSME sector remains insufficient, revealing critical gaps in the current national cybersecurity framework. Indeed, enhancing the resilience of MSMEs against cyberattacks does not merely protect individual businesses and owners but safeguards the backbone of Malaysia's economy, meaning that the nation's future success depends on its ability to secure these enterprises against the growing scale and sophistication of cyber threats. Strategic investments in cybersecurity, tailored support for MSMEs, and even stronger public-private partnerships will be essential to fortifying Malaysia's digital defenses. Malaysia must continue to innovate and adapt its cybersecurity strategies to ensure comprehensive protection for all sectors, further securing its position as a leader in digital technology and cybersecurity in the APAC region.

## Methodology

This report primarily utilized secondary research sources, including government databases, academic articles, industry white papers, and local and international news, with a focus on materials from the post-2020 period to capture the impacts of the COVID-19 pandemic on the cybersecurity of MSMEs in Malaysia. Supplementary interviews with regional cybersecurity experts and collaboration with experts on the ground in Malaysia enriched the analysis. Challenges arose in gathering data and case studies about micro and small businesses in Malaysia, as these are often overlooked in official documentation and reports, which tend to concentrate on the cybersecurity efforts of larger businesses and the government.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Pakistan | 



# PAKISTAN

4.5 million MSMEs<sup>384</sup>

## Digital Services Most Used for E-Commerce<sup>385/386</sup>



## Top Cyber Threats Faced By MSMEs<sup>387/388</sup>

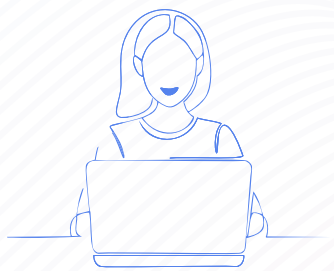


## Key Facts





In 2023, almost **24%** of Pakistan's **87.35 million** internet users were affected by online threats.<sup>389</sup>

Pakistan saw an **83%** increase in cybercrime between 2020 and 2023.<sup>390</sup>





## DEFINITION OF MSME<sup>391</sup>



### MICRO ENTERPRISE

-  Employees  
10 or less
-  Annual Turnover  
Not found

### SMALL ENTERPRISE

-  Employees  
Between 11 and 50
-  Annual Turnover  
Less than 150 million PKR

### MEDIUM ENTERPRISE

-  Employees  
51 to 250
-  Annual Turnover  
Turnover of 150 to 800 million PKR



## Executive Summary

Among the countries in this study, Pakistan is second only to Sri Lanka in its vulnerability to cyberattacks, according to the Global Cybersecurity Index 2020, published by the UN's International Telecommunication Union (ITU).<sup>392</sup> Pakistan lacks a data privacy law and sufficient regulatory frameworks, and struggles to protect its infrastructure and businesses from cyber threats. Therefore, ambitious efforts are underway to implement a data privacy law, better protect public and private enterprises from cyberattacks, and increase digitalization while improving digital literacy across the country.<sup>393</sup>

MSMEs constitute nearly 90% of all enterprises in Pakistan, the majority of which are part of the informal economy.<sup>394/395</sup> Many micro businesses, such as street vendors, home-based businesses, and domestic workers, operate in the informal sector.<sup>396</sup> And, despite a low participation rate by women in the labor force overall, approximately 12 million informal sector workers are women, many of whom use mobile devices to run home-based businesses as micro entrepreneurs.<sup>397/398/399</sup>

There are many cybersecurity challenges facing MSMEs in Pakistan, including the high number of phishing\*, malware\*, and hacking attacks directed at the country, which often use vectors such as social media, SMS, and fake or spoofed apps.<sup>400/401/402/403</sup> These smaller enterprises tend to lack cybersecurity awareness and the financial resources required to implement necessary defensive measures, much less access to expertise and training.<sup>404</sup> In addition, they operate without the protections of a comprehensive legal framework, or adequate mechanisms for the reporting of attacks.<sup>405</sup>

Special challenges to cybersecurity exist in Pakistan, including a lack of cybersecurity education and awareness in rural areas with internet connectivity, where the majority of the country lives.<sup>406</sup> This is complicated by a high illiteracy rate, and the fact that, in many regions, residents speak dialects that are not used in cybersecurity awareness campaigns and training, as the national languages are Urdu and English. On top of this, women business owners in the MSME sector may require special accommodations in order to participate in cybersecurity training, given that traditional and conservative cultural norms may make them uncomfortable with mixed-gender settings, especially outside urban areas.<sup>407/408</sup>

Data on cyberattacks and cyber threats in Pakistan is more scarce than for other countries in the APAC region. Yet, increased internet usage alongside government initiatives to expand the country's digital infrastructure are only raising its vulnerability to cybercrime, as more and more businesses and individuals connect to the internet without appropriate cybersecurity awareness. Many opportunities for a positive digital future in Pakistan exist, especially with such a young population and plans to integrate digital literacy, technology, cybersecurity, and IT education into grade school and university curricula. If digitalization is accompanied by sufficient cyber literacy and cybersecurity awareness, so that a culture of cyber hygiene\* develops in Pakistan, this growth of internet connectivity and infrastructure will provide significant economic opportunities for MSMEs across the country.

## The General Cybersecurity Context In Pakistan

Pakistan is among the most vulnerable countries to cyberattacks of those included in this study, ranking only above Sri Lanka in the Global Cybersecurity Index 2020, at 79th in the world (out of 182 rankings for 194 countries).<sup>409</sup> This reflects the fact that it lacks a data privacy law, as well as effective and cohesive cybersecurity initiatives across its government and industry. However, Pakistan has recently launched several initiatives to improve cybersecurity, including its ambitious National Cyber Security Policy 2021, which outlines goals across the government and private sector to significantly strengthen the security of its digital systems.<sup>410</sup> This builds on the Digital Pakistan Policy, introduced in 2018, aimed at bringing digital connectivity and ICT infrastructure to more citizens while educating them about cyber threats.<sup>411</sup>

Despite this forward-thinking approach to cybersecurity, cybercrime has become an increasingly serious problem in Pakistan, climbing by 83% over the three years from 2020 to 2023.<sup>412</sup> In 2023 alone, almost a quarter (24%) of Pakistan's 87.35 million internet users were affected by online threats.<sup>413/414</sup> Most commonly, these are phishing\*, malware\* (especially banking malware and spyware), trojan attacks\*, and ransomware\*.<sup>415/416</sup> And while a legal framework does exist to facilitate the reporting and investigation of cybercrime in the country, gaps in this framework make it inefficient, marked by extensive delays and a lack of cooperation among investigators and the courts, within an infrastructure ill-equipped to effectively handle the growing number of cybercrime cases.<sup>417</sup>

In 2024, internet penetration in Pakistan stands at 46%, significantly below the rates of access enjoyed by users in most of the countries in this study. However, 79% of the population has an active cellular mobile connection.<sup>418</sup> Given that the majority of Pakistan's population lives in rural areas, where they are less likely to have internet access, cybersecurity education tailored for users of mobile devices may be most effective. One advantage the country has in advancing such efforts is the young median age of the country (20 years old).<sup>419</sup> Not only do young people tend to take a greater interest in technology, but the government's plan to implement cybersecurity and digital literacy training in schools and universities has the potential to create new cultural norms around cybersecurity that will make a real difference in the future cyber health of the country and the ability of the population to participate in the digital economy.

## The Context For MSMEs In Pakistan

Some 4.5 million MSMEs operating in Pakistan constitute nearly 90% of all enterprises in the country, and account for at least 40% of GDP.<sup>420/421</sup> There is a push by the government and various industry and international partners to ensure the digitalization of these smaller businesses, to drive economic growth.<sup>422</sup> In particular, MSMEs are being encouraged to adopt responsible digital payment systems, which is likely to bring more businesses into the formal economy.<sup>423</sup>

### Prevalence Of The Informal Sector

There is no consensus on the percentage of MSMEs operating within the informal sector in Pakistan. However, recent research and surveys estimate that the sector constitutes anywhere from three-quarters to nearly all (75–97%) of the economy, and generates roughly 457 billion USD.<sup>424/425</sup> Much of the sector is made up of micro entrepreneurs, from street vendors to home-based workers, who operate without formal registration, often due to the high cost of taxation and other barriers to entry.<sup>426</sup>

There are believed to be approximately 20 million home-based workers in Pakistan, six in ten of whom are women.<sup>427</sup> This is a remarkable rate, given that only about two in ten women participate in the country's labor force overall.<sup>428</sup> In one study conducted to understand mobile phone use by female micro entrepreneurs in developing countries, it was found that mobile phones facilitated home-based work for many women in Pakistan, allowing them to circumvent some of the social norms that typically restrict them from engaging in business.<sup>429</sup> By using mobile technology like SMS and instant messaging apps to work from home, they did not have to reveal their gender, location, or identity.<sup>430</sup> But these technologies also make women owners of micro enterprises in the informal economy likely targets of cyber threats that use mobile devices as a vector.



## High Risk And Most Used E-Commerce/Social Media Platforms

In Pakistan, cyberattacks are typically executed through email, WhatsApp, and Facebook.<sup>431</sup> However, other social media platforms, including X (formerly Twitter), Instagram, TikTok, Snapchat, and more, have also seen a surge in cybercrime.<sup>432</sup> Financial fraud has become prevalent, and is increasingly perpetrated through social media.<sup>433</sup> According to an expert in cybersecurity in Pakistan, many people in the country download VPNs\* to circumvent bans on platforms like X, and fake VPN\* apps on the Google Play store serve as another vector by which cybercriminals install malware\* onto mobile phones.<sup>434</sup> As of March 2024, one such app cited by this expert, “SecureVPN”, was still available for download.

## Key Trends In Cybersecurity Among Msmes In Pakistan

The most common cyber threats to businesses in Pakistan include phishing\*, malware\* (especially spyware), hacking attacks, and ransomware\*.<sup>435/436/437</sup> These threats are frequently delivered through compromised business emails and fake apps. While there are no exact figures on the volume of these threats, the country has seen a considerable rise in cyberattacks targeting businesses since the COVID-19 pandemic.<sup>438</sup> This is exacerbated by the fact that many businesses in the country, particularly smaller MSMEs, still use legacy systems\* that are incredibly vulnerable to attack.<sup>439</sup>

Currently, the protections for MSMEs operating in digital spaces are minimal. These enterprises face the typical challenges of possessing limited awareness and funding for cybersecurity, but also have little legal recourse in the case of an attack due to gaps in Pakistan’s legislative framework. Whether reports of cybercrime are taken seriously or investigated by law enforcement or the courts is also in question.<sup>440</sup> Alone or in combination, these factors may discourage MSMEs from adopting digital tools\* for business.

With this in mind, the acting president of the Islamabad Chamber of Commerce and Industry (ICCI) highlighted in late 2023 that smaller enterprises are the backbone of the economy and called on the government to bring a greater focus to cybersecurity and cyber threat prevention now that more MSMEs are expanding their reach into online markets.<sup>441</sup> This could be supported by cooperation between the ICCI and Digital Pakistan to promote digitalization among MSMEs. One of the objectives of Digital Pakistan is to meet the digital connectivity and cyber education needs of certain groups, such as women and people in rural areas, to improve their prospects for social mobility, including through employment opportunities.<sup>442</sup>



### Case Study

Accessing credit is a particular challenge for MSMEs in Pakistan, especially those operated by lower income individuals and women, leading many business owners to fall prey to the many fake microloan apps that are easily downloaded onto any mobile device from app stores. This was the case for a woman in Lahore, who downloaded such an app and unexpectedly received a deposit in her bank account several days later. She had not applied for the loan, and although she promptly returned the money, the app persistently made contact with her and used access to the contact list in her phone to harass her friends and family. She eventually paid 145 USD as extortion money to put an end to these threats, but was still contacted by the app, eventually leading her to inform authorities.<sup>443</sup>

## Current Cybersecurity Measures For MSMEs

There are currently many changes underway in Pakistan that will affect its cybersecurity landscape and digital readiness, including attempts to develop a data privacy law and efforts to adopt more comprehensive and integrative approaches to cybersecurity, in both the public and private sectors. These extend from the government's seven-year cybersecurity strategy published in 2021, which is based on six pillars: the legal framework, cyber resilience, proactive monitoring and incident response\*, capacity building, cooperation and collaboration, and public awareness.<sup>444</sup>

### Government Initiatives

- The National Cyber Crimes Investigation Agency (NCCIA) enforces the Prevention of Electronic Crimes Act (PECA), which serves as the basis for the criminalization of cyber threats and cyberattacks.<sup>445</sup>
- The Pakistan Telecommunication Authority (PTA) regulates and polices the telecommunications sector by blocking malicious websites, securing the internet, and combating cybercrime, and also coordinates cybersecurity awareness campaigns for the public.<sup>446</sup>
- Digital Pakistan promotes the adoption of emerging digital technologies and innovative applications to enable cross-sector socioeconomic development and digital transformation, including through cybersecurity awareness building activities.<sup>447</sup>

### Industry Initiatives

- The Pakistan Computer Emergency Response Team (PakCERT) provides cybersecurity services and training for the public, the government, and the private sector, assisting in instances of security compromises, identifying cyber threat trends, and presenting workshops and seminars.<sup>448</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

MSMEs in Pakistan face a range of challenges and barriers to cybersecurity. Like most MSMEs worldwide, they tend to lack the awareness, training, funding, and expertise to deploy effective cybersecurity measures. However, they also face some challenges that are more unique to the context in Pakistan. For example, the country is experiencing a “brain drain” as talented youth with an interest in cybersecurity and IT leave the country for more competitive pay and a wider selection of job opportunities.<sup>449</sup> Further, the traditionally conservative culture of Pakistan has kept women largely out of the workforce, and that is only beginning to change through intentional gender mainstreaming, such as in the government’s 2021 cybersecurity strategy—which specifically details the inclusion of women and prioritizes increased cybersecurity awareness among women as a part of encouraging them to embrace professional IT and cybersecurity roles.<sup>450</sup>

Still, online tools and training programs to bolster the digital literacy of MSMEs are ultimately at the mercy of the country’s digital infrastructure. Although programs like Digital Pakistan seek to improve digital literacy in the country, internet penetration remains very low. This is true even in some urban areas, while there are rural areas where internet connectivity is simply nonexistent.<sup>451</sup> Furthermore, literacy rates and language are a challenge, even where infrastructure is not a barrier. In some parts of Pakistan, people are fluent in the country’s national languages of Urdu or English (or both), whereas people in other areas may only be literate in their regional dialects. In fact, the language with the highest literacy rate in Pakistan is in Punjab, at 64%. This poses a considerable obstacle to access when cybersecurity products, tools, and training for MSMEs are produced only in the national languages.<sup>452</sup>

## Conclusion

This overview of the cybersecurity landscape of Pakistan, especially as it pertains to MSMEs, highlights the unique challenges they face due to the country's weak cybersecurity capacities and lack of legal and regulatory frameworks. Low levels of literacy, limited internet penetration, budget constraints, outdated software\* and systems, and a lack of cybersecurity awareness all undermine the cybersecurity of MSMEs, and therefore of Pakistan more broadly.

The weakness of Pakistan's mechanisms for reporting cybercrime, and a lack of knowledge among the population about how to report them, means that data is lacking. The country's large informal economy further complicates data collection, making it difficult to quantify the threats MSMEs are confronting, and to what effect. Absent this data, government and industry efforts to protect private enterprises are more challenging to deploy in a tailored and targeted way. This presents opportunities for more primary research in the country, especially among MSMEs, on the question of what cyber threats are most prevalent and impactful and what will help these businesses better mitigate cybersecurity risks.

## Methodology

To explore the cybersecurity landscape for MSMEs in Pakistan, this research relied on secondary sources—including government databases, academic journals, industry white papers, and a mix of local and international news articles—especially materials published post-2020, to assess the impacts of the pandemic on MSMEs. This was supplemented by earlier data where relevant. Additional insights were garnered through an interview with a regional cybersecurity expert. The limited availability of data for MSMEs in Pakistan, especially for micro or small enterprises, proved to be a significant challenge. Data from government sources may not be accurate with respect to MSMEs due to the very high levels of informal employment in the country. And research by international NPOs has tended to focus on specific aspects or sectors of the MSME economy, but there appears to be little research on MSMEs as a whole, especially after 2020.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

The Philippines |





# THE PHILIPPINES

1.1 million MSMEs<sup>453</sup>

## Digital Services Most Used for E-Commerce<sup>454/455</sup>

facebook

YouTube



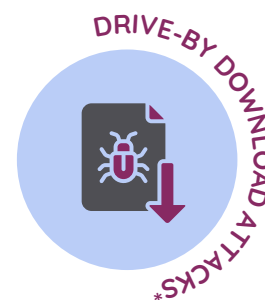
TikTok

Shopee

Lazada

carousell

## Top Cyber Threats Faced By MSMEs<sup>456/457/458</sup>



## Key Facts





The SMS capital of the world with **46%** of reported fraud cases being SMS scams in 2023.<sup>459</sup>

In 2022, the Philippines ranked **4th** worldwide for number of cyber incidents and **2nd** in web threats.<sup>460</sup>





## DEFINITION OF MSME<sup>461</sup>



### MICRO ENTERPRISE

-  Employees  
1 to 9
-  Total Assets (excluding land)  
Less than 3 million PHP

### SMALL ENTERPRISE

-  Employees  
10 to 99
-  Total Assets (excluding land)  
Between 3 and 15 million PHP

### MEDIUM ENTERPRISE

-  Employees  
100 to 199
-  Total Assets (excluding land)  
Between 15 and 100 million PHP

## Executive Summary

The cybersecurity landscape in the Philippines has become increasingly complex due to a rise in cyberattacks, and is shaped by the country's geopolitical and economic dynamics. The strategic location of the country and its close ties with the United States heighten the cybersecurity risk faced by the Philippines from state actors such as China and North Korea, both of which are known for their sophisticated cyber warfare capabilities.<sup>462</sup> In fact, data from sources like Kaspersky and the Department of Information and Communications Technology in the Philippines indicate that the country is among the top targets of cyberattacks and web threats globally.<sup>463</sup> The sectors most frequently targeted by cyber attackers have included travel, law and government, and financial services.<sup>464</sup>

The Philippines experiences a high rate of SMS scams, or smishing\*, which account for nearly half (46%) of all the reported fraud cases in the Philippines, and are matched by the same rate of phishing\* attacks.<sup>465/466</sup> These are some of the most common cyber threats targeted at MSMEs in the Philippines, along with drive-by download attacks\* and ransomware\* attacks.<sup>467/468</sup> MSMEs are essential to the country's economy, constituting over 99% of all businesses, providing 60% of employment, and helping improve the Global Innovation Index rating of the Philippines to 56 out of 132 in 2023.<sup>469/470/471</sup> These smaller enterprises operate heavily in sectors like wholesale, retail, and food and beverage, but notwithstanding their critical role in the economy, many are still in the early stages of digitalization. In 2022, only 6% of MSMEs in the Philippines were utilizing advanced digital tools\* and almost a quarter (23%) reported having initiated no digitalization whatsoever.<sup>472</sup>

In a digitalizing world, this leaves some Philippine MSMEs much more vulnerable to cybersecurity threats. To mitigate this risk, a tailored cybersecurity strategy that addresses the requirements and vulnerabilities of MSMEs in the Philippines is urgently needed. One government initiative that sets out to do this is the Market One-Stop Shop (MOSS) Portal in Quezon City, a digital platform that simplifies the booking and payment processes for vendors in markets by providing online registration and space leasing services.<sup>473</sup> The aim is to enroll thousands of vendors working in both city-owned and private markets, as well as in sanctioned temporary vending locations and in talipapas.<sup>474/475</sup> Raising awareness about cybersecurity best practices, particularly among MSMEs, is also critically important, as is the implementation of robust data protection measures. These efforts will not only safeguard key sectors but will enhance the overall economic stability and security of the country.



## The General Cybersecurity Context In The Philippines

Cybersecurity has recently become a significant concern in the Philippines as cyberattacks have increased.<sup>476</sup> In 2022, the Philippines ranked 4th worldwide for number of cyber incidents and 2nd in web threats.<sup>477</sup> The country's Cybercrime Investigation and Coordinating Center now advises the public to exercise heightened caution while shopping online, especially during the holiday season, because the country's shopping scam rate has soared to 36%.<sup>478</sup> Victims are often enticed with incentives or are over-trusting, and fall prey to scams.

In 2024, data from Imperva shows that 29% of all cyberattacks targeting the Philippines have originated from within the country, followed by attacks originating in Singapore (13%) and the United States (10%).<sup>479</sup> That said, Philippine entities have been among the hardest hit by attacks from outside, such as when Medusa ransomware\* and RedEnergy Stealer-as-a-Ransomware\* specifically targeted the country in 2023.<sup>480</sup> The sectors that most often suffer attacks are travel (34%), law and government (8%), gaming (7%), financial services (3%), and computing and IT (1%).<sup>481</sup>

A 2023 report by Cloudflare found that the most common cybersecurity incidents in the Philippines were phishing\* (68%), web attacks (64%), and business email compromise (47%).<sup>482</sup> The impact of these attacks on businesses is profound and lasting, extending beyond financial losses to include significant reputational damage (22%), loss of data or intellectual property (20%), and a loss of customers (10%).<sup>483</sup> These consequences underline the need for a comprehensive cybersecurity strategy that is customized to the distinct economic, digital, and geopolitical characteristics of the Philippines.

The government recognizes the significant role that cybersecurity plays in safeguarding the Philippine economy and protecting critical data. The country's primary regulatory framework for cybersecurity is the Data Privacy Act of 2012, or Republic Act No. 10173, which established comprehensive guidelines for the protection of personal data within both government and private sector systems.<sup>484</sup> The Act also created the National Privacy Commission as an enforcement mechanism, emphasizing the importance of transparency, consent, the rights of data subjects, the implementation of security measures, and mandatory breach notifications.<sup>485</sup>

## The Context For MSMEs In The Philippines

MSMEs represent a key component of the Philippine economy. In 2022, there were 1,105,143 MSMEs in the country, comprising over 99% of all enterprises and accounting for 60% of employment.<sup>486//487</sup> The vast majority of these businesses (90%) were micro enterprises, and nearly half (49%) were in the wholesale and retail sector, while 14% were in the hospitality and food and beverage sector, and 12% in the manufacturing sector.<sup>488</sup>

These enterprises have shown remarkable innovation, and have contributed to improving the Global Innovation Index for the country, moving it from 73rd in 2018 to 56th in 2023 (out of 132 countries).<sup>489//490</sup> However, the digitalization process for MSMEs in the Philippines is a mixed bag; these businesses have been instrumental in pushing for digitalization but only 6% have implemented advanced digital tools\* and 23% have not digitalized at all.<sup>491</sup> Many are therefore more vulnerable to cyberattacks, and yet there is no dedicated body that tracks cyber hygiene\* and security breaches among MSMEs.

### Prevalence Of The Informal Sector

In the Philippines, the informal sector forms a core part of the economy. Valued at about 514 billion USD, or 34% of the GDP, the sector encompasses street vendors, farmers, and small entrepreneurs.<sup>492//493</sup> These workers often offer essential goods and services, work in a variety of conditions, and may operate from static locations or mobile units.<sup>494</sup> According to the Philippine Department of Labor and Employment, 36% of people employed in the country work in the informal sector.<sup>495</sup> Informal workers face specific challenges such as unregulated working conditions and inadequate legal protections.<sup>496</sup> Thus, the government has introduced the Magna Carta of Workers in the Informal Economy (MACWIE), a bill filed in 2022 and still pending, aimed at addressing issues like labor rights and conditions, and equitable wages.<sup>497//498</sup>

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

MSMEs in the Philippines are heavily reliant on social media platforms like Facebook, YouTube, X (formerly Twitter), and Tiktok for their business operations and advertising.<sup>499</sup> The e-commerce sector is also growing, and is projected to achieve a gross merchandise value of 15 billion USD by 2025.<sup>500</sup> This means that MSMEs are increasingly leveraging e-commerce platforms to expand their online presence. These include Shopee (53.9 million monthly visits), Lazada PH (24.4 million visits), and Carousell PH (3.9 million visits).<sup>501</sup> Platforms like Zalora, SeaTooo, eBay PH, Temu PH, Alibaba, and Amazon Global are also popular with MSMEs.<sup>502//503</sup> The expanded reach of the Philippine e-commerce sector is impressive, but it is also a prime target for cyber threats. A 2023 survey conducted by the Global Anti-Scam Alliance and Gogolook found that more than one-third (36%) of respondents from the Philippines had been victim to or had encountered an online shopping scam.<sup>504</sup>

## Key Trends In Cybersecurity Among MSMEs In The Philippines

The cybersecurity environment for MSMEs in the Philippines is undergoing rapid change, with a notable increase in cyber threats. Among these are drive-by download attacks\*, which pose a significant and specific risk to MSMEs, and occur when users inadvertently download malware\* from compromised websites.<sup>505</sup> Phishing\* and ransomware\* attacks are common threats as well, along with malware\* and a range of scams, from fake websites to fraudulent investment schemes. Also prevalent in the Philippines are man-in-the-middle attacks\* in which cybercriminals intercept and steal data during transactions. All of these threats can and do cause financial and reputational harm to businesses.<sup>506//507</sup>

As this threat environment shifts and takes new shape, MSMEs in the Philippines are increasingly using cloud services\*. Some are using Amazon Web Services (AWS) through the AWS Lift program, designed to help smaller enterprises in Australia, New Zealand, ASEAN, Japan, and Korea by making cloud services\* more accessible and tailored to their business needs.<sup>508</sup> This kind of support is crucial to MSMEs as they face new challenges like data breaches and unauthorized access, which raises the importance of appropriate cyber hygiene\* and robust Identity and Access Management (IAM) practices\*.<sup>509</sup>



### Case Study 1

In December 2021, Girlie Jacildo, an employee at a business processing firm, received a suspicious email. The text claimed her GCash account (virtual wallet) was blocked, and urged her to click a verification link. Recognizing the potential danger, Jacildo promptly contacted GCash customer service to verify her account status. She discovered her account was active and was not in violation of any terms, which confirmed her suspicion of a phishing\* attempt. Jacildo had the benefit of being a former bank employee, and therefore understood the need to verify the legitimacy of an email before clicking any links, but she posted to Facebook to make her friends and family aware of the potential of phishing\*, and to warn them about this specific kind of attack.<sup>510</sup>

## Case Study 2

Recently, Acer Philippines experienced a supply chain attack through a third-party vendor responsible for managing its employee attendance data. This data breach, reported on March 12, 2024, resulted in unauthorized access to sensitive employee information including names, usernames, passwords, contact details, and more. Acer Philippines confirmed that no customer data was compromised and has initiated a thorough investigation, notifying the National Privacy Commission and the Cybercrime Investigation and Coordinating Center. As this case illustrates, cybercriminals are increasingly targeting the less secure components within a larger entity's network of suppliers and vendors to initiate supply chain attacks, with the objective of breaching the systems of the larger enterprise by exploiting vulnerabilities in the cybersecurity defenses of their smaller partners. As large companies enhance their own defenses, attackers are turning to these weaker links in the supply chain to gain unauthorized access.<sup>511</sup>

## Current Cybersecurity Measures For MSMEs

The cybersecurity landscape in which Philippine MSMEs are operating is, in part, the product of their choices related to technology and various socio-economic factors. A cybersecurity expert who has worked in the IT industry in the Philippines for over 25 years explained, for example, that about 80% of MSMEs use Windows operating systems, exposing them to specific vulnerabilities that impact a large number of enterprises. Additionally, the widespread use of outdated software\* is a major concern, as this leaves systems lacking the latest security updates and significantly increases their exposure to cyber threats.<sup>512</sup>

This same expert noted that the vulnerability\* Filipino MSMEs' faces are heightened by factors like widespread internet usage in the absence of adequate cybersecurity awareness, alongside underdeveloped cybersecurity infrastructure<sup>513</sup>.

These MSMEs face threats emanating from a range of external actors, calling for comprehensive and versatile cybersecurity approaches, but must also address internal threats like employee misconduct and poor cyber hygiene\* practices. In fact, these internal risks are potentially as harmful as external attacks. This highlights the need for MSMEs to implement internal security policies and regular training in cybersecurity best practices for employees.<sup>514</sup>



## Government initiatives

- The Inter-Agency Response Center (I-ARC) Hotline 1326 is a centralized, inter-agency cybercrime response collaboration of the Cybercrime Investigation and Coordinating Center (CICC), the Department of Information and Communications Technology (DICT), the National Telecommunications Commission (NTC), and the National Privacy Commission (NPC), with the Philippine National Police (PNP) and the National Bureau of Investigation (NBI) as its law enforcement arm. This 24/7 hotline is staffed by trained professionals who can help callers report a variety of scams, from investment scams, to phishing\* and smishing\* scams, to romance scams.<sup>515</sup>
- The DICT offers government-funded cybersecurity awareness and information sharing training to MSMEs.<sup>516</sup>
- The Quezon City government has launched the MOSS Portal, a digital platform that streamlines vendor bookings and payments, offering online registration and space leasing.<sup>517</sup>
- The Department of Trade and Industry (DTI) has implemented a digitalization project in the MIMAROPA district, to aid MSMEs in adopting digital technology in order to improve their business operations.<sup>518/519</sup> As part of this initiative, a one-day TikTok Content Creation Workshop was held in March 2024 for women entrepreneurs.<sup>520</sup>
- The Philippine government enacted the Subscriber Identity Module Registration Act, or SIM registration law, in 2022 to tackle SMS-based scams (smishing\*) by requiring users to register their SIM cards before activation.<sup>521</sup> As of 2023, the impact of this Act has been less potent than expected, as ongoing challenges in curbing mobile fraud and tracking SMS scammers persist, due to their use of false identities.<sup>522</sup>



## Industry Initiatives

- The DTI has partnered with Meta on the “Be Wais at Magduda: Anti-Scam Campaign,” which promotes digital literacy and raises awareness about the importance of safety and security in the digital world.<sup>523</sup>
- The Department of Science and Technology (DOST) has launched the Small Enterprise Technology Upgrading Program (SETUP), focused on aiding MSMEs in Central Luzon through advanced technologies, technical advice, and training sessions. For instance, as part of the program, an MSME in the farming sector will transition to solar technology, significantly reducing its energy costs and enhancing its operational efficiency.<sup>524</sup>
- Go Negosyo and the US Embassy co-hosted “Digital Sign Up Now 2022” to encourage MSMEs to embrace the digital transformation by sharing experiences and best practices with other entrepreneurs who have successfully and securely digitalized.<sup>525</sup>
- CyberSecurity Philippines CERT® (CSP-CERT©), a non-profit Computer Security Incident Response Team (CSIRT), is recognized as the first registered Computer Emergency Response Team (CERT®) in the Philippines. CSP-CERT© receives, reviews, and responds to computer security incident reports and activities, and collaborates with various local government entities, law enforcement, schools, and universities to raise awareness about cybersecurity, develop the cyber defense skills of Filipinos, and promote future employment in the field. It also assesses the effectiveness of security practices to improve upon them, and works closely with other CSIRTs and cybersecurity initiatives, both within the Philippines and internationally.<sup>526</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

Philippine MSMEs face significant cybersecurity challenges, particularly a lack of awareness and training. Ongoing awareness raising and capacity building is needed to help these businesses keep up with evolving threats, and thus to close the gaps exploited by cybercriminals.<sup>527</sup> The limited resources of many MSMEs, both financial and technical, leaves them to rely on outdated and unsupported operating systems and software\*, additionally increasing their vulnerability\* to cyberattacks. On top of this, internal threats from employees, such as poor cyber hygiene\*, can pose serious security risks.<sup>528</sup>

Addressing these challenges will require the cultivation of a culture of cybersecurity awareness, the implementation of internal controls, and collaboration among businesses, government, and industry experts to strengthen the resilience of MSMEs against cyber threats.<sup>529</sup>

## Conclusion

The cybersecurity landscape of the Philippines is marked by an alarming frequency of cyberattacks, placing it among the top targets globally. This vulnerability\* extends across various sectors, with MSMEs, which form the backbone of the economy, particularly at risk. These enterprises, critical for employment and innovation in the country, confront a complex array of threats from ransomware\* to phishing\* attacks.

Despite the government's efforts, through initiatives like the Data Privacy Act and the creation of the National Privacy Commission, these challenges persist, particularly in the context of widespread digitalization among MSMEs lacking sufficient cyber literacy. A large proportion of these businesses are micro enterprises, which face ever greater exposure to cyber threats due to their reliance on digital platforms for growth and customer engagement, combined with poor cybersecurity practices. This is exacerbated in the informal sector, which contributes significantly to the economy, where many business operators implement almost no cybersecurity measures at all.

To safeguard the economic stability and digital integrity of the Philippines, a comprehensive cybersecurity strategy tailored to the unique challenges facing MSMEs is crucial. This should include efforts to enhance digital literacy, expand access to secure technologies, and foster a culture of cybersecurity awareness across the entire business sector, and beyond. Strengthening the resilience of MSMEs will not only protect individual businesses in the Philippines, but will help secure the broader economic and digital landscape of the country, ensuring a safer and more prosperous future for all citizens.

## Methodology

The research for this report was drawn largely from secondary sources, including academic journals, local and international news reporting, and government databases. Additional perspectives were captured in primary interviews with representatives of local organizations. While data on the cybersecurity challenges and threats faced by Philippine MSMEs generally was readily available, it was more challenging to find detailed case studies on cyberattacks targeting smaller businesses, likely due to underreporting and the tendency of media to focus on larger-scale incidents. Despite this limitation, details of one incident involving a cyberattack on a small business provided valuable insight into the kind of cybersecurity threats that are targeted at smaller enterprises in the Philippines.







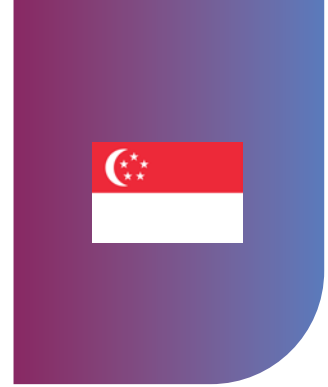
# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Singapore | 

# SINGAPORE



0.3 million MSMEs<sup>530</sup>

## Digital Services Most Used for E-Commerce<sup>531/532</sup>

facebook

Instagram

TikTok

Telegram

WeChat

Shopee

Lazada

amazon

## Top Cyber Threats Faced By MSMEs<sup>533</sup>

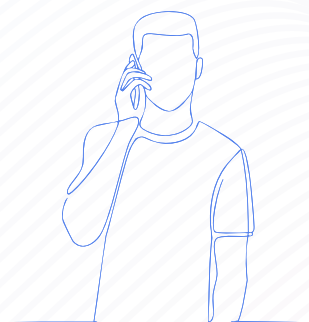


## Key Facts



In 2020, Singapore ranked **#1** in the ASEAN region, tied with Korea, in terms of good cybersecurity practices.<sup>534</sup>

In 2021 **40%** of all cyberattacks target MSMEs. **77%** of MSMEs felt exposed to cyber threats.<sup>535</sup>





## DEFINITION OF MSME<sup>536</sup>

### MICRO ENTERPRISE

-  Employees  
10 or less

### SMALL & MEDIUM ENTERPRISE

-  Employees  
200 or less
-  Annual Turnover  
100 million SGD or less

## Executive Summary

Singapore's highly digitized economy makes it particularly vulnerable to cyber threats. Despite leading the ASEAN region (in a tie with Korea) on the Global Cybersecurity Index in 2020, Singapore ranked sixth globally for exposed databases in 2021. And in 2023, over 70% of the country's large businesses reported breaches.<sup>537/538</sup> The average financial loss per phishing\* case has increased and the ransomware\* epidemic only continues to grow, with MSMEs in manufacturing and retail marked as prime targets.

In Singapore, MSMEs constitute 99% of the country's enterprises and employ 71% of its workforce. This makes them critical to the economy as well as a focal point for cyberattacks.<sup>539</sup> In fact, up to 40% of all cyberattacks in Singapore target MSMEs, many of which are not designated as essential under the Cybersecurity Act even if they are integral parts of larger networks.<sup>540</sup> Notwithstanding this high threat exposure, only 12% of Singaporean MSMEs reported in 2021 that they were extremely prepared for cybersecurity incidents, citing a lack of comprehensive cybersecurity measures, employee training, and will to improve cyber hygiene\*.<sup>541</sup>

Overcoming these challenges is particularly difficult for MSMEs, 80% of which have neither in-house cybersecurity expertise nor formal protocols for managing cybersecurity.<sup>542</sup> The mitigation strategies currently in use by some MSMEs include an increased investment in cybersecurity, scenario planning, and simulation exercises. But many smaller enterprises have yet to implement basic measures and are resistant to necessary changes, either due to the complexity of cybersecurity or to the perception that it is irrelevant to their business. Though the government offers support, MSMEs in Singapore face structural and cultural challenges to adopting cybersecurity measures.

Government investment in cybersecurity, nationally and in the MSME sector, is high in Singapore. Generous government grants are available to MSMEs to bolster their cybersecurity, and the country's robust legal and regulatory framework is recognized worldwide for its effectiveness and forward-thinking approach.<sup>543/544</sup> New cybersecurity challenges must continuously be addressed, however, to ensure the integrity of digital systems and the broader economy.



## The General Cybersecurity Context In Singapore

In 2022, Singapore's digital economy contributed 17% to its GDP, among the largest shares in the world.<sup>545</sup> This is supported by extensive internet penetration, which stood at nearly 97% in 2023.<sup>546</sup> Yet, widespread digitalization invites cybercrime, and a 2023 survey of 100 Singaporean businesses with 1,000 or more employees found that over 70% had experienced at least one cyber breach. On top of this, 5% reported facing multiple attacks daily.<sup>547</sup>

The global ransomware\* epidemic has not spared MSMEs in Singapore, which also face other cyber threats including website defacement\*, social engineering attacks\*, the exploitation of misconfigured cloud computing systems\*, infected IoT infrastructure\*, distributed-denial-of-service attacks\*, and phishing\*. These attacks were up in 2023 compared to 2022, and largely targeted MSMEs in manufacturing and retail.<sup>548</sup> Thus, it is concerning that researchers discovered 5,882 databases in Singapore had been exposed to the internet in 2021 without a proper firewall\*, or even password protection in some cases.<sup>549</sup>

Indeed, on any given day, almost 56,000 physical and virtual assets are connected to the networks of Singapore's businesses and only about half of these are monitored. Moreover, half of businesses surveyed in 2023 lack complete visibility over the assets they own and/or manage. Over one-third (39%) of the attributes of these assets could not be accounted for, including location and support status.<sup>550</sup> Sub-par internal processes like insufficiently comprehensive code reviews, incomplete documentation, and a lack of pre-launch testing are also common.<sup>551</sup>

Singapore has a robust legal and regulatory framework for data privacy and cybersecurity. Its primary legal mechanisms are the Cybersecurity Act of 2018 and the Personal Data Protection Act (PDPA), with which all businesses of any size must comply.<sup>552/553</sup> Importantly, the Cybersecurity Act was updated in 2024 to account for the use of cloud infrastructure in critical computing systems.<sup>554/555</sup>

## The Context For MSMEs In Singapore

There are roughly 289,000 MSMEs in Singapore, which make up virtually all (99%) of the country's businesses and employ 71% of its workforce. The sector accounts for nearly half (48%) of total GDP.<sup>556</sup> A majority of Singaporean MSMEs are in services, wholesale and retail trade, and manufacturing.<sup>557</sup>

## Prevalence Of The Informal Sector

The informal sector is estimated to represent around 2% of the economy in Singapore. Compared to other countries in the APAC region, this constitutes an exceptionally small informal sector. Its size is due largely to the well-regulated and structured economic system of Singapore, which incorporates almost all employment within formal arrangements.<sup>558</sup> This small sector likely includes micro enterprises in the freelance and gig economy (such as driving and food delivery apps), and domestic work.

## High Risk Platforms And Most Used E-Commerce/Social Media Platforms

According to Meltwater's 2024 Global Digital Report, the most popular social media platform in Singapore is WhatsApp, followed by Facebook, Instagram, TikTok, Telegram, Facebook Messenger, LinkedIn, X (formerly Twitter), WeChat, and iMessage.<sup>559</sup> Of these, MSMEs tend to use Facebook and LinkedIn most often.<sup>560</sup> When it comes to e-commerce platforms, Shopee is by far the most popular in Singapore, with almost 14 million users per month. Lazada trails behind at some distance, with approximately 7.1 million users per month, and then Amazon with 4.8 million monthly users and Qoo10 with 2.8 million monthly users.<sup>561</sup>

While Amazon, Lazada, Qoo10, and Shopee have all adopted the cybersecurity features recommended by the Ministry of Home Affairs, Shopee is rated as slightly less safe than the others, due to a relatively large volume of scams reported on the platform, in contrast to its closest competitor Lazada (311 versus 46, respectively, in 2022).<sup>562</sup> However, it should be mentioned that Shopee also experiences a far higher rate of user traffic than Lazada.<sup>563</sup> And notably, even LinkedIn can be the source for a potential breach. Attackers trawl the platform for career updates from potential targets, gather personal information from data-broker sites, and then pretend to be someone from within their new company to phish for desired information.<sup>564</sup>

## Key Trends In Cybersecurity Among MSMEs In Singapore

According to an audit conducted by the Cyber Security Agency (CSA) of Singapore in 2022, MSMEs are targeted in up to 40% of all cyberattacks in the country.<sup>565</sup> Ransomware\* is a particular problem for these enterprises, especially in the manufacturing and retail sectors; but successful scams are also on the rise, with 20% more reported in 2023 than in 2022.<sup>566/567</sup> These threats are clearly understood and experienced by many owners of MSMEs in Singapore, 77% of whom said in a 2021 survey that they felt exposed to cyber threats, and 40% of whom reported suffering cyberattacks in the previous year. Even so, two years later (in 2023), only 12% described their businesses as extremely prepared to handle cybersecurity incidents, compared to over a quarter (27%) of large enterprises and multi-national corporations.<sup>568</sup>

Interestingly, nearly two-thirds (65%) of the leaders of larger companies in Singapore were likely to strongly agree that cybersecurity is the responsibility of all employees, while only four in ten (42%) leaders of MSMEs said the same. These smaller enterprises were less likely to equip their employees with basic cybersecurity knowledge through interventions such as trainings, simulation exercises, and easy access to cybersecurity materials and external courses, or to hire new cybersecurity talent. At the same time, MSMEs were five times more likely to lack any cybersecurity measures at all.<sup>569</sup> While 70% of MSMEs in Singapore say they update their software\* frequently and possess incident response protocols, only 20% report the implementation of access control and malware\* protections, which means they lag behind larger businesses significantly in adopting these important measures.<sup>570</sup>

If we consider micro enterprises specifically, the situation is even more problematic. At least 80% of those surveyed said they have no in-house cybersecurity expertise, and the same rate were also very unlikely to conduct regular penetration testing.<sup>571</sup> Of all MSMEs, these micro businesses were also the most inclined to manage cybersecurity through ad hoc means instead of formal protocols, increasing their vulnerability to malicious actors.<sup>572</sup> This is concerning given that three-quarters (75%) of Singaporean MSMEs affected by cyberattacks in 2021 reported a loss of customer data, and over half reported losses of intellectual property, sensitive information, money, and customer trust.<sup>573</sup>

But the economic impact is also significant, with just over half (51%) of these businesses reporting financial losses of at least 500,000 USD. When breaches occur, the negative impacts of downtime—from the disruption of operations, to revenue loss, to legal implications—grow with every hour, and for one in ten MSMEs in Singapore, a single day of downtime would result in their closure.<sup>574</sup> Only 15% of these businesses have the capacity to detect cyber incidents within an hour, however, and a mere 10% can fix a breach within that time.<sup>575</sup> Thus, for MSMEs, the potential fallout from a serious cyber incident can be considerable. And due to the relatively smaller scale and resources of these businesses, any consequences can be much more serious than for larger businesses. In fact, a global study conducted in 2019 found that the per-employee cost from cyberattacks is 16 times higher for MSMEs than for large companies.<sup>576</sup>

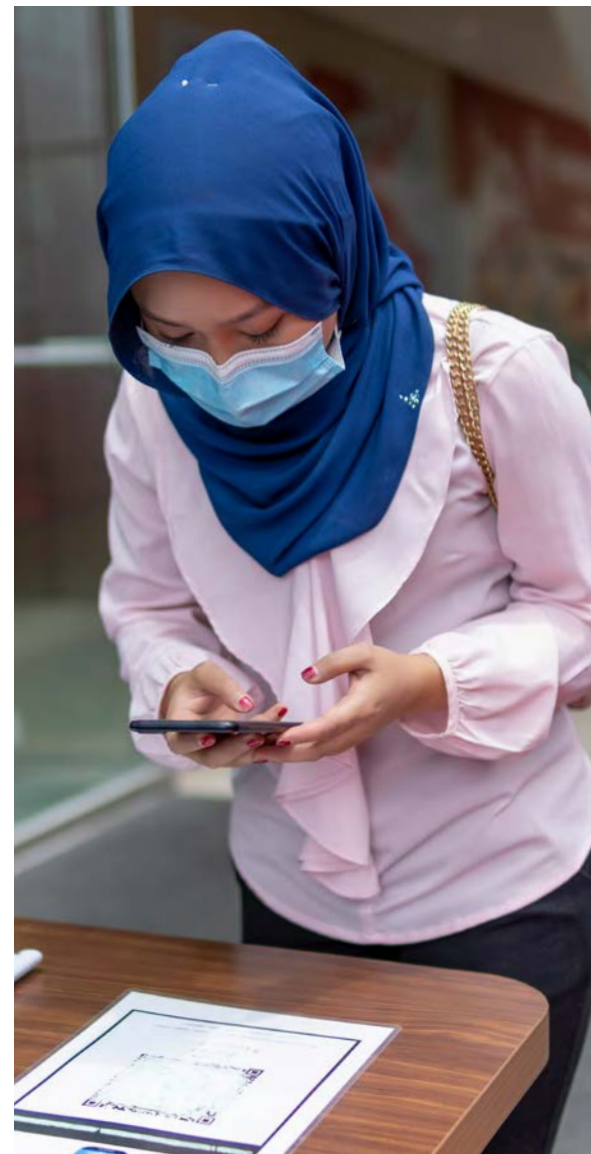


As MSMEs in Singapore increasingly recognize the critical nature of the cyber challenges they face, they are boosting investments in cybersecurity.<sup>577</sup> This has meant the implementation of solutions that scale up with the size of the enterprise, from restrictions on internet access and administrator privileges to cyber-audit services.<sup>578</sup> In addition, many have engaged in scenario planning and simulation exercises, with eight in ten (82%) finding that this helped them identify specific weaknesses, about half of which could be addressed within two weeks.<sup>579</sup>

In general, Singaporean MSMEs have not adopted artificial intelligence (AI) solutions in the cybersecurity domain, despite an overwhelming majority (90%) indicating in a recent survey that they had adopted some form of AI to boost productivity.<sup>580</sup> While there are larger companies using AI-powered extended detection and response (XDR) services that deliver powerful, enterprise-grade security with automated monitoring and a team of experts, and at a fraction of the typical cost thanks to shared-service models, this is unlikely to be a viable option for MSMEs.<sup>581</sup> By their own account, these smaller enterprises lack the financial resources to employ cutting edge cybersecurity solutions, or they see cybersecurity as overly complex and too daunting to tackle.<sup>582</sup>

### Case Study

In 2014, the Karaoke company KBox (which was in the MSME sector at the time) was breached by a cyberattack, resulting in a leak of mobile numbers, identity card numbers, and addresses for over 317,000 account holders.<sup>583</sup> An inquiry into the circumstances behind the incident revealed glaring deficiencies in the security protocols of KBox, including the use of a single-character password for access to company systems, the absence of any policy or physical/digital security system to guard against removal of customer personal data from the premises, the transmission of unencrypted customer personal data over Gmail, non-enforcement of staff password strength, and non-deletion of unused accounts.<sup>584</sup> It is plausible, if not probable, that a similar suite of vulnerabilities lie behind the bulk of cybersecurity incidents reported by MSMEs in Singapore.





# Current Cybersecurity Measures For MSMEs

## Government Initiatives

- The Cyber Security Agency (CSA) has created a raft of support measures for MSMEs in Singapore, from toolkits and cybersecurity health plans to the Cyber Essentials/Cyber Trust Marks of certification and curated lists of affordable vendors and grants.<sup>585</sup> The CSA has also embarked on community building through the SG Cyber Safe Programme, which brings businesses together to collaboratively develop cybersecurity-related training content, products and services, and community-outreach programming directed at both businesses and the public, to increase awareness and promote adoption of cybersecurity measures.
- The SMEs Go Digital Programme incorporates components aimed at helping small and medium enterprises secure their digital operations, though it is not focused specifically on cybersecurity.<sup>586</sup>
- CISO-as-a-Service, offered by the Infocomm Media Development Authority (IMDA), provides smaller businesses with access to expert cybersecurity advice and solutions to help them manage and mitigate cyber risks more effectively. This is particularly valuable for MSMEs that may not have the resources to employ a full-time Chief Information Security Officer (CISO).<sup>587</sup>
- The Singapore Police Force (SPF) Anti-Scam Center (ASC) investigates and deters scams by working with over 60 entities, including financial institutions, telecommunications companies, internet service providers, social media platforms, consumer protection agencies, and regulatory bodies.<sup>588</sup>

## Industry Initiatives

- The CyberSG Talent, Innovation and Growth (TIG) Collaboration Centre, launched by the National University of Singapore in collaboration with the CSA, supports the development of a skilled cybersecurity workforce and seeks to expand capabilities across industry sectors.<sup>589</sup>
- The Association of Information Security Professionals (AiSP) provides a platform to raise cybersecurity awareness, discuss digital risks, and share or seek knowledge about available cybersecurity solutions that are tailored to MSMEs.<sup>590</sup>
- The CyberSG R&D Programme Office (CRPO), located at Nanyang Technological University with funding from the CSA, drives research and development to build cybersecurity capacities in Singapore.<sup>591</sup>
- Singtel Cyber Security Institute (CSI) advocates cyber resilience and operational best practices and serves as a hybrid of an advanced cyber range and an educational institute, making it the first of its kind in the region to test and train companies, especially MSMEs, in dealing with sophisticated cyber threats.<sup>592</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

The dangers that MSMEs face from cyber threats in Singapore are often more severe than those faced by larger businesses. And while large enterprises are required by law to include a cybersecurity policy as part of their corporate governance practices, MSMEs may not have the resources or capacity to do the same.<sup>593</sup> Typically, MSMEs operate on slimmer margins and can allocate less of their budget to cybersecurity.<sup>594</sup> These slimmer margins can also force them to adopt lower-cost cybersecurity solutions, which may provide less safety and render them more vulnerable to supply chain attacks\*. Moreover, MSMEs may merge their IT and cybersecurity departments, if cybersecurity is not handled directly by the business owner, limiting the resources, expertise, and capacity of a business to continuously monitor for ever-evolving threats.<sup>595</sup> These limitations make regulatory compliance more challenging for MSMEs, which further increases their vulnerability\*.

When MSMEs do not invest in awareness raising and train employees in cybersecurity best practices, these businesses are more susceptible to human error as a vector for breaches as well. Combined with outdated security software\* that has not been updated due to budget constraints, MSMEs in Singapore are frequently ill-equipped, on many levels, to handle new threats. This not only makes them attractive targets for cyberattacks but also positions them as potentially fruitful gateways to larger partner networks, particularly because MSMEs may struggle to respond effectively to cyber incidents due to a lack of formal incident response plans\* and resources, including in-house cybersecurity talent.<sup>596</sup>

In a 2023 survey of 416 MSMEs in Singapore, some 39% of respondents were nonetheless ambivalent about adopting cybersecurity measures, arguing that their business did not store sensitive/personal data, that cybersecurity was too complex, or that cyber incidents were unlikely to affect them.<sup>597</sup> In some cases, MSMEs have taken a wait-and-see approach to cybersecurity, even when they are concerned about phishing\* and fraud.<sup>598</sup> This over-optimism has existed alongside a basic general awareness of cyber threats for several years.<sup>599</sup> Hence, business leaders must do more to foster a culture of cybersecurity awareness. Many senior managers continue to view cybersecurity as a primarily technical question with technology solutions like firewalls\* and antivirus software\*, instead of as an organization-wide initiative that must encompass policies, procedures, employee training, and the promotion of security awareness.<sup>600</sup>

There is also a prominent misconception among MSMEs in Singapore that adopting cloud solutions shifts the responsibility for cybersecurity onto the shoulders of providers. This suggests that these enterprises may not adequately understand cybersecurity strategies.<sup>601</sup> Indeed, in a 2021 survey, approximately 20% of MSME owners in Singapore possessed limited knowledge even of local legal re-

quirements related to cybersecurity. A lack of awareness of minimum standards and key frameworks may be linked to the deprioritization of cybersecurity in these businesses.<sup>602</sup>

On top of this, the large variety of government grants available to MSMEs to bolster their cybersecurity regimes may have the paradoxical effect of producing an “analysis paralysis” that results from this surplus of options, so that some choose none at all.<sup>603</sup> It has also been reported that the tedium and length of the administrative grant-approval process is not worth the value of the grants to many MSMEs, and that some vendors seek to exploit the opportunity to advance their business in other ways, pointing to a need to further streamline these efforts on the part of the government. The perception that cybersecurity is overly complex has also led to calls for grants that explicitly include support for implementation.<sup>604</sup>

In interviews, representatives of a regional NGO described the cybersecurity challenges facing immigrant workers, elderly individuals, and non-English speakers as multifaceted, and noted they are deeply rooted in language barriers, cultural norms, and educational levels. Many immigrant workers in Singapore, particularly women who may spend years accumulating savings, have limited English proficiency, making them particularly vulnerable to sophisticated scams that can deplete their hard-earned money. Similarly, elderly people, especially those between 70 and 80 years of age, often lack both digital literacy and English language skills, rendering them susceptible to targeted attacks such as pension fund scams. Cultural factors play a significant role in shaping individual risk in this context; for example, in many communities, the concept of retirement is unknown and older individuals work late into their lives.<sup>605</sup>



## Conclusion

Singapore's advanced digital infrastructure and widespread connectivity underpin its dynamic MSME economy, and facilitated the swift adoption of new technologies by smaller businesses in response to the challenges posed by the COVID-19 pandemic. The nation's proactive cybersecurity policies are designed to guide it into a future that increasingly depends on technological advancements. Yet, this advancement is occurring in the shadow of escalating cyber threats that specifically target the vital MSME sector, which forms the backbone of the Singaporean economy. There is an urgent need for enhanced support for MSMEs from both the government and industry, to help them meet the challenges of implementing effective cybersecurity measures and move them past a continued reliance on inadequate IT infrastructure. This will require measures to overcome financial hurdles, efforts to foster workplace cultures that value IT and cybersecurity across all age groups, and substantial investments in developing future talent in cybersecurity.

Because the digital economy of Singapore is highly developed, there is a scarcity of studies conducted by both international and domestic organizations on the unique challenges faced by micro and small businesses. Additionally, existing reports often fail to distinguish between micro and small enterprises. This makes it difficult to quantify the specific threats these businesses encounter and the barriers they face in securing their digital environments. Industry experts have also noted that many of these smaller enterprises use personal bank accounts and laptops for business transactions, leading to insufficient data on their operations. Therefore, significant opportunities exist to delve into this segment of Singapore's economy, to determine the best ways MSMEs can be supported by government and industry partners. Protecting MSMEs is not merely a matter of securing businesses in Singapore; it will reinforce the entire economy and safeguard the nation's digital future.

## Methodology

This report primarily utilized secondary research sources, including government databases, academic articles, industry white papers, and local and international news, with a focus on materials from the post-2020 period to capture the impacts of the COVID-19 pandemic on the cybersecurity of MSMEs in Singapore. Supplementary interviews with regional cybersecurity experts and consultations with a leading professor in Singapore enriched the analysis. Challenges arose in gathering data and case studies about micro and small businesses in Singapore, as these are often overlooked in official documentation and reports, which tend to concentrate on the cybersecurity efforts of larger businesses and the government.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Sri Lanka | 



# SRI LANKA

1.1 million MSMEs<sup>606</sup>

Digital Services Most Used for E-Commerce<sup>607/608</sup>

facebook

TikTok

Instagram

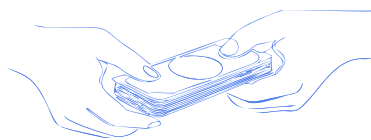
kaymu.com

Daraz

Top Cyber Threats Faced By MSMEs<sup>609</sup>



## Key Facts



Despite the growing adoption of digital payment methods, concerns about cybersecurity persist, with **79%** of the population opting for cash on delivery rather than trusting online card payments.<sup>610</sup>



In 2023, Sri Lanka was ranked **83 out of 176** countries in the National Cyber Security Index (NCSI), as compared to holding the 100th position in 2020.

Reflecting its efforts to develop cybersecurity policies, improve cybersecurity responses, and fight cybercrime.<sup>611</sup>





## DEFINITION OF MSME<sup>612</sup>



### MICRO ENTERPRISE

-  Employees  
1 to 9
-  Annual Turnover  
15 million RS

### SMALL ENTERPRISE

-  Employees  
10 to 50
-  Annual Turnover  
Between 16 and 250 million RS

### MEDIUM ENTERPRISE

-  Employees  
51 to 200
-  Annual Turnover  
Between 251 and 750 million RS



## Executive Summary

MSMEs are the foundation of Sri Lanka's economy, contributing over 50% of national economic output.<sup>613</sup> However, these enterprises have faced significant challenges as the result of disruptive events like the COVID-19 pandemic and the subsequent economic downturn, which combined to generate widespread job losses and employment contracture in approximately one-fifth of both micro and medium-sized businesses in Sri Lanka.<sup>614</sup> These crises also caused the MSME sector—which accounted for nearly all businesses and nearly half of employment in the country before the pandemic—to shrink by over 15% overall, due to the permanent closure of businesses.<sup>615/616</sup>

Many surviving MSMEs relied on digital technologies to streamline their operations, adapting low-cost digital resources such as social media platforms and personal mobile devices for business purposes. A lookback study found that the digital maturity of these enterprises was impacted by some factors outside the control of business owners, such as the condition of digital infrastructure in their province.<sup>617</sup> In response to this and other challenges, the Sri Lankan government has demonstrated a steadfast commitment to implementing economic recovery strategies, with an emphasis on reviving the MSME sector.<sup>618/619</sup> These enterprises are regarded as the cornerstone of the national economy and the key to future economic growth.<sup>620/621</sup>

The increasing reliance by MSMEs on digital technology in recent years matches a rise in access and use of the internet across Sri Lanka. At the beginning of 2023, there were 14.58 million internet users in the country, amounting to an internet penetration rate of 67% percent.<sup>622</sup> This represented a greater than 30% rise in penetration over two years (since January 2021).<sup>623</sup> While this dropped slightly in 2024, the number of social media users in the country has only grown.<sup>624/625</sup> This raises the importance of addressing serious cybersecurity challenges, which extend primarily from malicious software\*, ransomware\*, and phishing\* attacks.<sup>626</sup> In fact, spam\* emails serve as the primary vector for most cyber incidents in Sri Lanka, and pose a significant threat to its digital infrastructure and security landscape.

Several government initiatives are therefore focused on enhancing cybersecurity measures. And, crucially, the Sri Lankan government has established a Computer Emergency Readiness Team (CERT), in collaboration with the Information and Communication Technology Agency (ICTA). The role of the CERT to act as a focal point for cybersecurity in Sri Lanka includes engagement in discussions on cybersecurity legislation.<sup>627</sup>

## The General Cybersecurity Context In Sri Lanka

Sri Lanka was among the first countries in the APAC region to extensively utilize the internet in both the government and private sectors, which has made the country more susceptible to various cyber threats.<sup>628</sup> Indeed, in 2016, Sri Lanka experienced a cybersecurity incident when the official website of President Maithripala Sirisena fell victim to hacking by local youths.<sup>629</sup> This incident, which resulted from a failure to implement existing policies and regulations aimed at preventing such breaches, exposed critical vulnerabilities in the country's cyber infrastructure. But more recently, in 2023, the government was again targeted, by a significant ransomware\* attack on its cloud services.<sup>630</sup>

Six in ten people in Sri Lanka are digitally literate, and over three-quarters (77%) connect to the internet or use email on their smartphones.<sup>631/632</sup> Consequently, they are vulnerable to cybercrimes such as credit card fraud, revenge pornography, hacking, and unauthorized access to sensitive financial data.<sup>633</sup> In 2023, Sri Lanka was ranked 83 out of 176 countries in the National Cyber Security Index (NCSI), reflecting its efforts to develop cybersecurity policies, improve cybersecurity responses, and fight cybercrime. However, there is still considerable room for improvement as far as cyber threat analysis, cyber crisis management, and the development of legislation that better protects personal data.<sup>634</sup> This underscores the need for Sri Lanka to bolster some cybersecurity measures and enhance regulatory frameworks to more effectively mitigate cyber threats.

## The Context For MSMEs In Sri Lanka

Prior to the pandemic, MSMEs accounted for 99% of Sri Lankan businesses and approximately 75% of the labor force.<sup>635</sup> However, from 2020 to 2023, the economic and COVID-19 crises pushed employment in surviving firms down by 20%. This effectively moved larger enterprises into smaller enterprise categories, as their numbers of employees decreased.<sup>636</sup>

### Prevalence of the Informal Sector

Nearly three-fifths (58%) of total employment in Sri Lanka is informal.<sup>637</sup> This is especially true in micro enterprises, which account for a significant portion of informal employment.<sup>638/639</sup> Jobs in the Sri Lankan informal sector tend to be in trades, hospitality, and services, but especially in agriculture. In fact, an overwhelming majority (89%) of agricultural employment in the country is informal. This distribution of employment within the sector means that men hold considerably more informal jobs than women.<sup>640/641</sup>

## High Risk Platforms And Most Used E-Commerce/Social Media Platforms

As 2020 began, MSMEs in Sri Lanka were slow to transition to e-commerce and needed significant support to begin using digital tools\* in their businesses, but the onset of the COVID-19 pandemic brought a substantial surge in e-commerce on platforms like Daraz and Kaymu.<sup>642/643</sup> Facebook is also widely used in Sri Lanka, with nearly all online users maintaining an account. Social media use is on the rise more generally, as Sri Lankans also increasingly use platforms such as YouTube (59%), TikTok (36%), LinkedIn (17%), and Instagram (14%).<sup>644</sup>

Despite this, as well as the growing prevalence of digital payment methods, a significant portion (72%) of the Sri Lankan population opts to pay in cash upon delivery for e-commerce purchases. In nearly two-thirds of these cases (64%), buyers do not trust either the seller or the online payment process.<sup>645</sup> Online shopping is done almost entirely by smartphone in Sri Lanka, accounting for 95% of transactions.<sup>646</sup> Initiatives like LankaPay, to provide secured payments by offering QR code solutions, are meant to help Sri Lankans keep pace as the country digitalizes. Linked to the Central Bank of Sri Lanka, LankaPay aims to encourage and facilitate digital transactions in the country.<sup>647</sup>

## Key Trends In Cybersecurity Among MSMEs In Sri Lanka

According to Imperva, Sri Lanka experiences a slightly higher volume of daily inbound cyberattacks than outbound attacks, with the telecom and ISP sector particularly targeted.<sup>648</sup> One of the most common forms of cybercrime in Sri Lanka is phishing\*, wherein users are redirected by malicious emails and links to fake webpages aimed at collecting their sensitive personal information.<sup>649</sup> For MSMEs, this can lead to data breaches\*, which are the prevalent cyber threat for smaller enterprises in the country. Sri Lankans encounter a wide variety of cyber scams as well. These range from the impersonation of delivery services intended to extract fees from users, to incidents that facilitate hacking on platforms like Facebook and LinkedIn. For example, cybercriminals steal social media logins to collect personal information, in order to send fraudulent messages requesting money or advance payments for services.<sup>650</sup>

### Case Study

In 2020, when Sri Lanka Telecom (SLT) experienced a significant ransomware attack orchestrated by the REvil group, it promptly acknowledged the breach and emphasized its commitment to resolving the situation and safeguarding customer data. Despite the severity of the attack, SLT assured customers that none of their data had been compromised due to the immediate implementation of precautionary measures and the isolation of impacted servers.<sup>651/652</sup> In response to the breach, SLT recommended that their customers take all necessary precautionary measures in light of the nature of these cyber-attacks.<sup>653</sup>

# Current Cybersecurity Measures For MSMEs

## Government Initiatives

- The Computer Emergency Readiness Team (CERT) Sri Lanka was established in collaboration with the Information and Communication Technology Agency (ICTA), to enhance cybersecurity measures and support the Information Technology (IT) sector, and function as the primary policy body governing IT initiatives.<sup>654</sup>
- The government has announced that in 2024, a National Cyber Security Act will be introduced and a Cyber Security Authority will be established.<sup>655/656</sup> It is expected that the Act will establish the Authority, which would be responsible for all civilian aspects of cybersecurity, and will provide for the implementation of national information and cybersecurity strategies and policies aimed at protecting critical national infrastructure and addressing cybersecurity threats.<sup>657</sup>
- The Information and Communication Technology Agency (ICTA), the national ICT institution of Sri Lanka, provides effective and user-friendly services to streamline market procedures and government operations, enhance digital governance through knowledge sharing, implement global e-commerce and electronic payment systems, and develop updated regulations and institutional structures for data protection, cybersecurity, and intellectual property rights.<sup>658</sup>
- In June 2024, Sri Lanka hosted DigiEcon 2024, a “Digital Economy Summit” spearheaded by State Minister for Technology Kanaka Herath.<sup>659</sup> The goal was to bring together local and foreign innovators and investors, with collaboration from foreign embassies and national ministries, to facilitate investment in the Sri Lankan digital economy.<sup>660</sup>
- The government has introduced its National Digital Strategy 2030 to accelerate the country’s development by: leveraging digital technologies to enhance its economic competitiveness; drive exports and foreign exchange earnings; creating high-paying jobs for young people, women, and rural populations; and delivering trusted and inclusive public services to everyone, everywhere.

## Industry initiatives

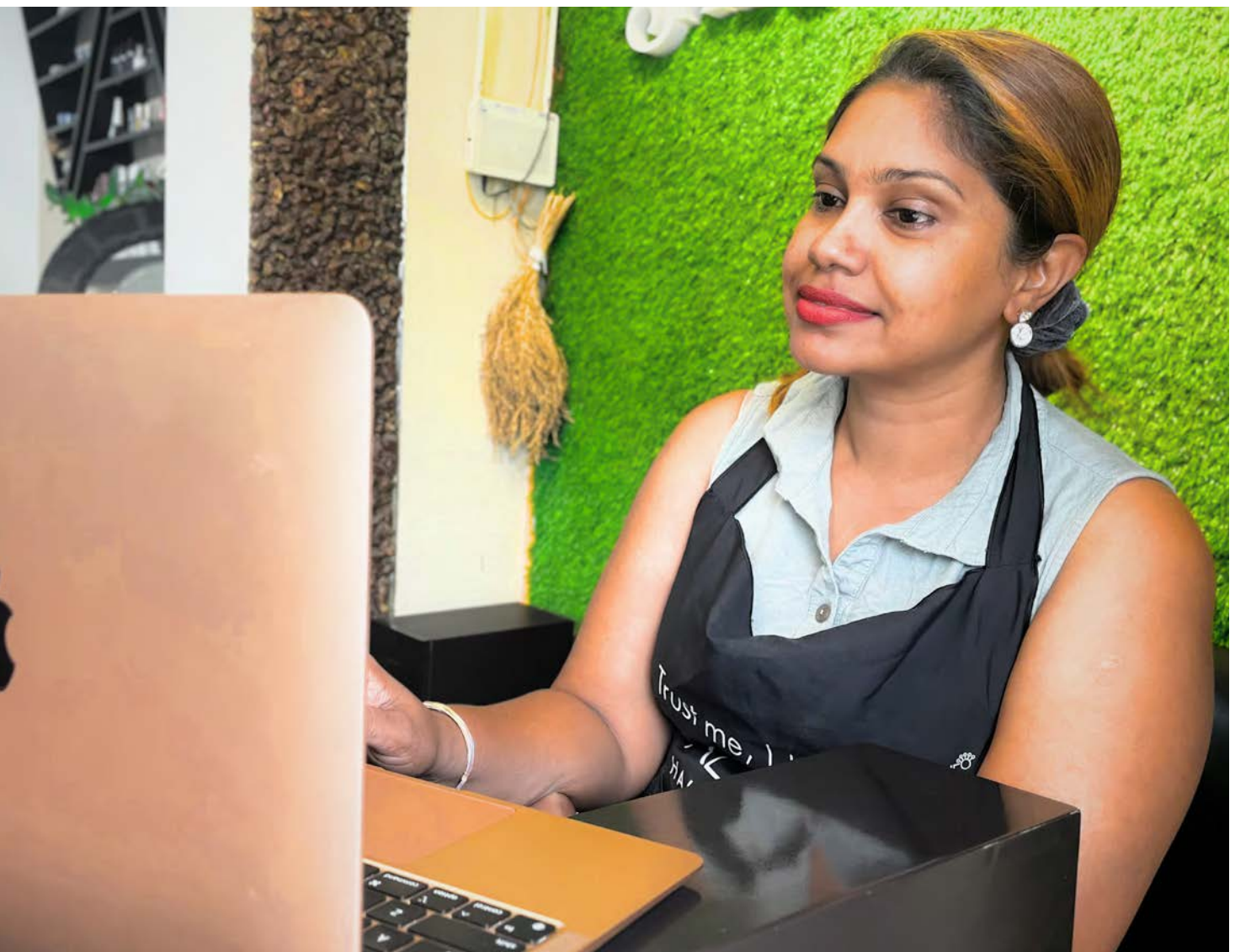
- The Cloud Security Alliance (CSA), committed to defining and promoting best practices for secure cloud computing globally, is working in Sri Lanka to strengthen cloud security standards through collaboration, education, and innovation, cultivating a network of professionals and organizations dedicated to advancing a secure and resilient cloud computing ecosystem and positioning the country as a hub for cloud security excellence.<sup>661</sup>





## Challenges And Barriers To Cybersecurity For MSMEs

Despite the significant role MSMEs play in Sri Lanka's economy, various challenges hinder their growth potential. These include financial constraints, the minimal adoption of technology, and limited connections to domestic and global value chains.<sup>662</sup> Moreover, many MSMEs in Sri Lanka face obstacles accessing formal financial services due to their low financial literacy and various bureaucratic complexities, leading them to rely on informal money lenders, who often impose high interest rates that represent a significant burden to small businesses.<sup>663</sup> The economic crisis of 2022 and the impact of the COVID-19 pandemic only exacerbated these challenges for MSMEs, over 80% of which reported decreased sales or other negative impacts to their business operations.<sup>664/665</sup>



## Conclusion

MSMEs constitute a critical segment of the Sri Lankan economy and contribute significantly to its GDP, and have shown considerable resilience, even in the face of substantial challenges stemming from disruptive events like the COVID-19 and economic crises. But as MSMEs increasingly leverage digital technologies to streamline operations and adapt to changing market dynamics, they are more vulnerable than ever to cyber threats. Sri Lanka is particularly targeted by phishing\* attacks, and the risk of data breaches requires a concerted and continued effort to strengthen cybersecurity frameworks and regulatory mechanisms. Recognizing this, and aware of the vital role played by MSMEs, the Sri Lankan government has prioritized the revival of this sector through targeted recovery strategies and support initiatives, emphasizing their importance in driving future growth and stability in a digital economy.

## Methodology

This study is based on comprehensive secondary research, utilizing sources including government databases, academic articles, industry white papers, and a range of local and international news reporting. Insights were enriched through supplementary interviews with regional cybersecurity experts. Challenges were encountered in accessing specific data and case studies related to MSMEs, which are often underrepresented in documentation, which tends to emphasize larger enterprises and government-led cybersecurity initiatives.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Thailand | 





# THAILAND

3.2 million MSMEs<sup>666</sup>

## Digital Services Most Used for E-Commerce<sup>667</sup>



facebook



Instagram

Kaidee



Shopee

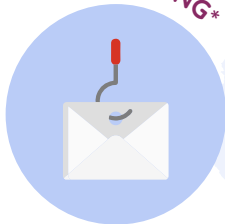


Lazada

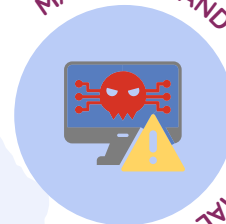
AliExpress™

## Top Cyber Threats Faced By MSMEs<sup>668</sup>

PHISHING\*



MALWARE\* AND WEB-BASED MALWARE\*



## Key Facts



According to a study in 2023, only **33%** of MSMEs said their organizations reported breaches to the relevant authorities.<sup>669</sup>

In 2021 alone, **65%** of small and medium enterprises in Thailand experienced cyberattacks.<sup>670</sup>



## DEFINITION OF MSME<sup>671</sup>

### MICRO ENTERPRISE

#### Manufacturing



Employees  
5 or less



Annual Income  
1.8 million THB or less

### SMALL ENTERPRISE

#### Manufacturing



Employees  
Between 5 and 50



Annual Income  
Between 1.8 and 150 million THB

#### Trade & Services



Employees  
Between 5 and 30



Annual Income  
Between 1.8 and 50 million THB

### MEDIUM ENTERPRISE

#### Manufacturing



Employees  
Between 50 and 200



Annual Income  
Between 150 and 500 million THB

#### Trade & Services



Employees  
Between 30 and 100



Annual Income  
Between 50 and 300 million THB

## Executive Summary

Thailand is facing challenges in data protection and cybersecurity, especially with the rapid growth of social media and e-commerce. Thailand lacks sufficient legal frameworks in these areas, prompting the government to develop new bills to address emerging issues. In 2023, the country ranked tenth in digital competitiveness in the APAC region, indicating its capacity and readiness to digitalize.<sup>672</sup> This directly affects MSMEs, which depend on adequate capacity building in cybersecurity as they transition to the digital realm with the aim of enhancing their business prospects.<sup>673</sup>

MSMEs play a pivotal role in the Thai economy. According to the Office of Small and Medium Enterprises Promotion (OSMEP), these smaller businesses contributed over one-third (35%) of the national GDP in 2022.<sup>317</sup> Still, even with MSMEs representing well over 99% of all enterprises in Thailand, large firms dominate the economy.<sup>674/675</sup> Hence, MSMEs are seeing significant benefits from an embrace of digital tools, including enhanced competitiveness, greater efficiency, and wider market reach.

Thailand's legal and regulatory frameworks for cybersecurity have evolved in recent years, with the adoption of the National Cybersecurity Act and the Personal Data Protection Act (PDPA), the latter of which resembles the EU's General Data Protection Regulation.<sup>676</sup> These measures are intended to enhance cybersecurity awareness and encourage the business sector, including MSMEs, to comply with data protection regulations and invest in cybersecurity measures. However, the large number of enterprises operating in the informal sector has made it challenging to monitor compliance with policies and legal regulations, and also makes it difficult for many MSMEs to comply.

In general, MSMEs in Thailand lack cybersecurity knowledge. Micro enterprises, which primarily use smartphones to conduct business, often have insufficient knowledge even to safeguard their accounts and manage their passwords, and cannot conceive of—much less plan for and mitigate—the risk of cyberattacks.<sup>677</sup> While small businesses may have easier access to resources and IT systems than micro businesses, they also tend to lack the necessary knowledge to effectively safeguard their devices and network.<sup>678</sup>

In January 2023, over 61 million people were accessing the internet in Thailand, representing an internet penetration rate of 85%, and 85% of these users made use of at least one social media platform.<sup>323</sup> As internet utilization increases in the country and the risk of cyberattacks grows, more digital awareness initiatives and accessible cybersecurity tools are required. Indeed, the value of the Thai cybersecurity market is projected to reach over 377 million USD by 2024.<sup>679</sup>

Policymakers in Thailand have been working to implement cybersecurity frameworks designed to target cyber threats and vulnerabilities. At the same time, regulations such as the PDPA and the Computer Crime Act, and strategic initiatives like the Thailand 4.0 economic plan, have been adopted over the last decade to increase safety and security in cyberspace\*. Thailand 4.0 envisions transforming Thailand into a high-income nation driven by innovation, technology, and creativity, including through the promotion of digitalization among MSMEs, support for start-ups and innovation ecosystems, investments in skills development, improvements to digital infrastructure, and the implementation of policy reforms.<sup>680</sup>

However, many MSMEs continue to fall victim to cyberattacks. More efforts targeting MSMEs specifically, at the community level, are therefore necessary. To achieve resilience, these small businesses must be equipped with the adequate tools and knowledge to not only overcome cyber threats but also to more effectively implement cybersecurity measures with proper monitoring.





## The Context For MSMEs In Thailand

Thailand is home to over 3 million enterprises, and MSMEs comprise nearly all of them, accounting for over 80% of the country's employment, though less than 40% of GDP.<sup>681/682</sup> Notably, Thailand has a higher concentration of large enterprises than many OECD countries, and these enterprises play a dominant role in the Thai economy.<sup>683</sup> Since the COVID-19 pandemic, however, MSMEs that transitioned to e-commerce and took advantage of new technologies have played an important part in growing the economy.<sup>684</sup>

Through e-commerce platforms, MSMEs have been able to reach bigger audiences and have successfully automated and increased their sales. Yet, this has exposed them to considerable cyber risks, and in 2021 alone, a staggering two-thirds (65%) of small and medium enterprises in Thailand experienced cyberattacks.<sup>685</sup> According to a 2021 report by Cisco, malware\* and phishing\* attacks were the threats encountered most often by these businesses.<sup>686/687</sup>

### Prevalence Of The Informal Sector

Many MSMEs in Thailand operate without formal registration, and their employees often work informally.<sup>688</sup> In fact, from 2017 to 2021, informal employment among people aged 25 to 54 consistently accounted for about two-thirds of the Thai workforce.<sup>689</sup> Thailand's informal economy is estimated to make up almost half (48%) its GDP, among the highest rates for countries in the region.<sup>690</sup> This high degree of informality limits the ability of businesses to expand, manage finances effectively, and report cyber incidents to the government. Furthermore, a FinScope survey of MSMEs in Thailand found in 2023 that less than 5% of these enterprises hold any form of insurance.<sup>691</sup> This makes it even more difficult for MSMEs to protect their assets and data, or mitigate costs, in the case of a cyber incident.

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

MSMEs in Thailand utilize mobile devices to run many aspects of their businesses, especially in the e-commerce sector. Younger business owners, who are more familiar with digital platforms and strategies, are particularly able to boost their sales this way.<sup>692</sup> To do so, Thai MSMEs rely on apps such as Line, Facebook, and Instagram, which are relatively easy to manage. This also allows them to operate without incurring any costs, and to reach a much larger audience than if they operated offline.<sup>693</sup>

Several prominent trends have emerged among MSMEs in Thailand as they move their businesses online. For instance, Facebook Messenger now stands out as a key communication tool for MSMEs.<sup>694</sup> And, as live-streaming platforms have grown in significance, Instagram, Facebook Live, and Line (which is similar to WhatsApp) have all become prime marketing channels and sites of direct sales.<sup>695</sup> These platforms cater to personal use by the general public and therefore require no tech savvy because they are designed to be user friendly. This ease of use can now be leveraged to generate profit.

## Key Trends In Cybersecurity Among MSMEs In Thailand

The use of social media platforms for online communication by MSMEs presents opportunities for growth but also heightened vulnerability\* to cyber threats.<sup>696</sup> These platforms are the primary means by which some MSMEs communicate, exposing them to significant costs if they fall prey to cyberattacks.<sup>697</sup> A 2021 study assessed that, worldwide, cyber incidents had cost MSMEs between 826 USD and 653,587 USD on average, per incident.<sup>698</sup>

### Case Study

Person A had their Facebook account compromised by a scammer, who sent a fraudulent message to a relative of Person A, asking for money and promising repayment within two hours. Unfortunately, the relative transferred the money requested to the bank account provided in the message. Upon realizing they had been deceived, this relative urged Person A to post a warning on their Facebook account, cautioning others to ignore any similar requests for funds. Subsequently, the incident was reported to law enforcement authorities and the bank, leading to the identification of the account holder, Person B. However, Person B claimed ignorance to the illegal nature of the funds received, believing them to be proceeds from legitimate sales transactions. Person B explained that they had responded to an online job advertisement promising daily earnings of 500–1,000 THB (14–27 USD), for which opening a bank account and providing the details to the employer had been a requirement of the job. The tasks of the job included receiving funds from customers, withdrawing money, purchasing a money wallet at a convenience store, and transferring the funds to the designated phone number on the employer website, for a 10% commission.<sup>699</sup>

## Current Cybersecurity Measures For MSMEs

Given the rapid pace at which Thailand is digitalizing, it has become crucial to implement various measures to enhance cybersecurity. A significant number of cyberattacks have been occurring in the manufacturing and banking sectors, with 5,789 attacks registered in these industries over just six months in 2023, along with attacks in the government and military sectors.<sup>700</sup> Additionally, Thailand ranks among the top ten countries globally in terms of daily internet usage, and boasts a large e-commerce market.<sup>701</sup> But revenues in the Thai cybersecurity market, compared to the rest of the APAC region, are among the lowest.<sup>702</sup>

This leaves certain loopholes open that make MSMEs more susceptible to phishing\* attacks and other cyber incidents, extending from the combination of their strong online presence and limited cybersecurity engagement. For example, it is common for owners of micro enterprises to use both their personal social media account and their personal mobile phone number for business purposes. Mixing their personal and business accounts makes them more vulnerable to social scams, including romance scams, which often go unreported due to the shame many victims feel and concerns about how disclosure could impact their reputation and business.

In response to this cyber threat landscape, and to maintain the integrity of the country's digital transformation, the Thai government has been developing new national strategies and initiatives. These have helped raise awareness among MSMEs of the cyber risks and threats they face and have encouraged some to invest in cybersecurity measures to protect their businesses. The government has also made strides in increasing awareness of scams, including by providing guidance on how to exercise caution when links are received from senders, the importance of verifying the sender's identity, and how to contact relevant government authorities.<sup>703</sup> For instance, this has involved promotion of the Whoscall application, which warns users of potential scammers.<sup>704</sup>

### Government Initiatives

- The Thailand 4.0 initiative, developed under the framework of a twenty-year plan to make Thailand the digital hub of Southeast Asia, is aimed at expanding digital infrastructure, and will involve the identification, analysis, and management of digital risks affecting the performance of officially registered MSMEs in the country.<sup>705/706</sup>
- The National Cybersecurity Act, adopted in 2019, created the Thailand Computer Emergency Response Team (ThaiCERT) and grants the government the authority to monitor internet activity, access data, and shut down websites without court approval.<sup>707</sup>
- The Personal Data Protection Act (PDPA) took effect in 2022 and echoes the EU's General Data Protection Regulation (GDPR), covering data processing, data collection, and data storage. The PDPA is overseen by the Personal Data Protection Committee, which is under the supervision of the Minister of Digital Economy and Society.<sup>708</sup>



## Industry Initiatives

- USAID's Digital Asia Accelerator, as a component of the Digital Connectivity and Cybersecurity Partnership announced in 2019 to enhance economic development through improved digital technology adoption and cybersecurity in the Indo-Pacific region, is organizing a contest in Thailand that invites young people to develop and share videos aimed at promoting responsible digital citizenship among the general public.<sup>709</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

There are a number of challenges to the adoption of cybersecurity measures by MSMEs in Thailand, the most significant of which is simply a lack of knowledge. Research undertaken in 2022 found a significant lack of security awareness on the part of MSMEs that were adopting new technologies, for instance.<sup>710</sup> Indeed, for some small business owners in Thailand, just the shift to digital space and online work has been overwhelming or impossible, particularly in the tourism sector, absent the skills and knowledge to take advantage of how digital devices can support their businesses.<sup>711</sup> And while some MSMEs may have more developed technological capacities, they still lack the knowledge to implement appropriate firewalls\* and security measures, putting them at risk of falling victim to security loopholes.<sup>712</sup> That said, MSMEs seem to be aware that their knowledge of cybersecurity is insufficient, with over half citing a lack of awareness as the biggest cybersecurity challenge they face.<sup>713</sup>

In a 2021 survey, respondents in the Thai tourism sector also highlighted that difficulty accessing the internet, particularly in rural areas, presents challenges to their business.<sup>714</sup> Access to technology more generally is another challenge to these smaller enterprises, many of which use outdated tools that may not meet modern requirements for safe e-commerce.<sup>715</sup> And as reliance on QR codes for payment increases, scammers are exploiting them to redirect payments intended for legitimate shop owners to other accounts, an attack known as quishing\*.<sup>716</sup> Such a heightened dependence on QR codes, especially in combination with deficient cybersecurity awareness and old technology, significantly increases the vulnerability\* of MSMEs to cyberattacks.<sup>717</sup> This has left smaller enterprises in Thailand unprepared to embrace digital assets in their business operations.<sup>718</sup>



## Conclusion

This research highlights the challenges faced by MSMEs in Thailand, as the country reaches toward new digital and economic ambitions. Despite government initiatives such as Thailand 4.0 and the passage of the PDPA, MSMEs face limited access to technology, considerable knowledge gaps, and specific cyber risks associated with social media platforms. Bridging these challenges will require collaborative efforts involving government, industry, and stakeholders in the MSME sector, to empower businesses and ensure their resilience in the digital era.

Future research on the effectiveness of these government programs in supporting MSMEs could help determine how to most meaningfully assist smaller businesses as they navigate the ongoing digital transformation and continue to strengthen their cybersecurity readiness. Exploring strategies to enhance cyber capacity building among MSMEs, especially in rural areas, could also be a valuable area of study. Additionally, research gaps exist in understanding the long-term impacts of cyber risks on the sustainability of MSMEs and the role of public-private partnerships in fostering digital resilience within these businesses.

## Methodology

This study of the cybersecurity challenges facing MSMEs in Thailand used a mixed-methods approach, combining primary and secondary research methodologies. The research relied predominantly on an extensive review of literature discussing the impact of digitalization and cybersecurity on Thai MSMEs, complemented by primary data collection through structured interviews with local stakeholders. These interviews provided critical insights into the specific cybersecurity challenges encountered by MSMEs in Thailand. Secondary sources such as government reports, industry studies, and news articles validated the findings and contextualized the research. Some challenges were encountered in sourcing data and case studies specific to the cybersecurity experiences of MSMEs.





# From Vulnerability To Resilience

Cybersecurity Challenges For MSMEs  
In The APAC Region

COUNTRY ANALYSIS

Vietnam | 



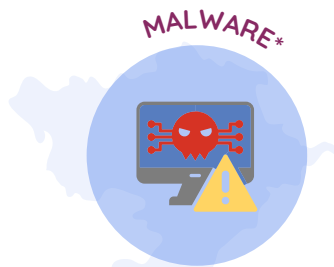
# VIETNAM

0.7 million MSMEs<sup>719</sup>

## Digital Services Most Used for E-Commerce<sup>720/721/722/723/724</sup>



## Top Cyber Threats Faced By MSMEs<sup>725</sup>



## Key Facts



MSMEs remain vulnerable due to limited awareness of cyber threats, with **70%** of small and medium enterprises operating outside the digital economy.<sup>726</sup>

Between 2022 to 2023, malware attacks on SMEs increased **20x** in Vietnam.<sup>727</sup>






## DEFINITION OF MSME<sup>728</sup>


### MICRO ENTERPRISE

#### Agriculture, Forestry, Fishing Industry, and Construction Sectors

 Employees  
10 or less

 Annual Revenue  
3 billion VND or less


#### Trade & Services Sectors


 Employees  
10 or less

 Annual Revenue  
10 billion VND or less


### SMALL ENTERPRISE


#### Agriculture, Forestry, Fishing Industry, and Construction Sectors

 Employees  
11 to 100

 Annual Revenue  
Between 3 and 50 billion VND


#### Trade & Services Sectors


 Employees  
11 to 50

 Annual Revenue  
Between 10 and 100 billion VND

### MEDIUM ENTERPRISE


#### Agriculture, Forestry, Fishing Industry, and Construction Sectors

 Employees  
101 to 200

 Annual Revenue  
Between 50 and 300 billion VND

#### Trade & Services Sectors

 Employees  
51 to 100

 Annual Revenue  
Between 100 and 300 billion VND

## Executive Summary

The cybersecurity landscape in Vietnam has been characterized by both acute challenges and significant progress. In 2023, the National Cyber Security Centre (NCSC) reported that the country faced a diverse range of cyber threats, especially phishing\*, as well as attacks exploiting software\* vulnerabilities and those targeting websites.<sup>729</sup> The NCSC is a strategic initiative aimed at sustaining Vietnam's global ranking (of between 25th and 30th) in the cybersecurity index and propelling its Information and Communications Technology (ICT) Development Index ranking into the top 50 by 2025.<sup>730/731</sup>

MSMEs are vital to Vietnam's economy, contributing over 40% to its GDP and providing employment to some 60% of the country's workforce.<sup>732/733</sup> These smaller enterprises have been central to the government's digital transformation efforts, and have leveraged platforms and tools such as KiotViet (software-as-a-service), funding societies (fintech) to enhance their operations, particularly in the retail sector.<sup>734</sup> This is not only contributing to economic growth in Vietnam but is helping to pivot these enterprises toward modern business practices in the increasingly digital marketplace.

Some government and industry initiatives have also been concentrated on raising cybersecurity awareness and building defenses against evolving threats.<sup>735/736</sup> However, many MSMEs, especially in rural areas, still face significant barriers to implementing adequate cybersecurity measures, such as a lack of digital literacy and inadequate resources. This underscores the ongoing need for comprehensive strategies that address these vulnerabilities to ensure the cybersecurity resilience of this pivotal sector in Vietnam's economy.<sup>737</sup>

## The General Cybersecurity Context In Vietnam

The digital economy contributes significantly to the overall economic performance of Vietnam, accounting for almost 17% of GDP.<sup>738</sup> To advance its digital economy further, the government is focusing on four key pillars: ICT, industry digitalization, digital management\*, and digital data\*.<sup>739</sup> As part of this effort, the prime minister approved the National Cyber Safety and Security Strategy, with the aim to ensure Vietnam's position between 25th and 30th in the Global Cybersecurity Index in 2025.<sup>740/741</sup>

This has amplified the significance of cybersecurity in Vietnam's national development strategy. The country's cybersecurity landscape has been marked by a considerable increase in incidents, totaling 13,900 in 2023.<sup>742</sup> According to the Vietnam National Cyber Security Technology Company, this represented a near 10% increase in cyberattacks compared to 2022.<sup>743</sup> These came primarily in the form of phishing\* (33% of all incidents), followed by attacks that exploit vulnerabilities in platforms and software\* on computers and servers\* (27%) and attacks directed at compromising websites (25%).<sup>744</sup> To counter these threats, the Vietnamese government has bolstered its cybersecurity measures, and the country's legal framework has been evolving to keep up with the ever-changing cybersecurity environment. A key piece of legislation in this regard is the Law on Personal Data Protection. The Law is designed to enhance legal protections for personal data and ensure that relevant agencies, organizations, and individuals fulfill their responsibilities in safeguarding that data.<sup>745</sup>

## MSMEs Context In Vietnam

MSMEs are a cornerstone of the Vietnamese economy, particularly the retail economy.<sup>746</sup> They contribute more than 40% to GDP and nearly 60% of the labor force.<sup>747</sup> As of 2021, MSMEs accounted for 97% of total enterprises in Vietnam.<sup>748</sup> In other words, MSMEs play a vital role not only in growing GDP but also in providing employment across the country.

### Prevalence of the Informal Sector

Over two-thirds (69%) of employment in Vietnam could be defined as informal in 2021.<sup>749</sup> A predominant part of the informal sector is family-run enterprises, accounting for about 70% of all businesses in Vietnam.<sup>750</sup> These are small-scale ventures operated by an individual or family—often as “business households”—who take on the full liability for operations with their own assets.<sup>751</sup> Business households such as these contribute significantly to the Vietnamese economy, in diverse activities from farming, to street vending, to seasonal work.<sup>752</sup> The informal sector also plays a vital role in providing employment; despite lower wages and greater health risks, many workers depend on jobs in this sector.<sup>753</sup> The

Vietnamese government is working to reduce the number of unregistered businesses in the country. With the adoption of Resolution 58/NQ-CP in 2023, the Ministry of Finance is now mandated to implement a tax administration reform affecting business households.<sup>754</sup> The government has set a specific target of 2025, by which it hopes to convert 8,000 to 10,000 business households into registered enterprises.<sup>755</sup>

### High Risk Platforms And Most Used E-Commerce/Social Media Platforms

Vietnamese MSMEs actively engage with social networks like Facebook, Instagram, and WhatsApp, as well as the local platform Zalo, for business purposes that include marketing and e-commerce.<sup>756/757/758</sup> Smaller businesses also use platforms like Shopee and Lazada, and Vietnamese-owned Tiki, Sendo, and VatGia, to carry out operations.<sup>759/760</sup> These platforms are pivotal to Vietnam's growing e-commerce sector, which is projected to reach export earnings of 5.5 billion USD by 2027.<sup>761</sup> This digitalization will be fueled in part by global platform expansion, improved logistics and payment infrastructure, and enhanced consumer trust in online transactions.<sup>762/763</sup>

While Vietnam's e-commerce sector is positioned for significant growth, this raises the risk of cyber vulnerabilities, including the threat of deceptive phishing\* attacks. A common threat in Vietnam extends from the creation of websites that look similar to Dropbox or Google Docs, by cybercriminals seeking to steal data.<sup>764</sup> Money lending apps also pose digital risks, and moreover, may charge excessive fees as well as interest rates that rise far above the 20% per annum ceiling stipulated by the Civil Law in Vietnam.<sup>765</sup> These interest rates can range from 35% to 69% per annum and leave many borrowers in substantial debt.<sup>766</sup> For example, apps such as Moreloan, Vaytocdo, and VDOonline—all of which are no longer operational—offered loans of up to 60 USD, of which 23 USD was deducted as a service fee; and if a borrower failed to repay their loans in a week, they were charged a daily interest of 2%.<sup>767</sup> The police arrested five suspects involved in running these three apps, which were later dismantled.<sup>768</sup> However, many similar apps are still active in the Vietnamese market.<sup>769</sup>

## Key Trends In Cybersecurity Among MSMEs In Vietnam

The first half of 2023 witnessed a sharp increase in malware\* attacks on the SME sector in Vietnam, up by 1,240 over the same period in 2022.<sup>770</sup> The uptick in use of social media by Vietnamese MSMEs, alongside the adoption of online banking, has opened these businesses to significant cybersecurity challenges.<sup>771</sup> The common threats they face include account hijacking\*, phishing\*, and malware\* installation, often via deceptive messages that mimic legitimate bank communications.<sup>772</sup>



### Case Study

Mr. Q.V. and Phan Tran Nam were both victims of separate cyber harassment incidents related to the debt owed by their employees to the financial institutions Mirae Asset Financial Company and DSP Debt Trading Company. Although Mr. Q.V and Phan Tran Nam were not themselves in debt to these institutions, they were harassed as a means of compelling them to repay the debt incurred by their employees. Mr. Q.V was bombarded with incessant phone calls, threats, and attacks on his company's Facebook page, while Phan Tran Nam and his family faced false accusations of debt made on social media. These incidents involved anonymous intimidation via fake accounts and spam\*, significantly affecting their lives and businesses. DSP Debt Trading Company has denied their role in these cyberattacks, while Mirae Asset Financial Company has not responded publicly.<sup>773</sup>

### Current Cybersecurity Measures For MSMEs

There is an urgent need for better cybersecurity measures and education for MSMEs in Vietnam. A study conducted by DAI and Ipsos in 2021 found an increase in the adoption of digital tools\* by these enterprises, with nearly three-quarters (73%) using such tools for business during the COVID-19 pandemic, up from two-thirds (67%) before the pandemic.<sup>774</sup> These tools, especially social media platforms like Facebook, WhatsApp, and Instagram, were crucial to the business operations, customer engagement, and marketing of MSMEs as they adapted to the pandemic.<sup>775</sup> However, the study also revealed barriers facing MSMEs in adopting and using digital tools\*, including a lack of knowledge and a sense that digital literacy is irrelevant to their business.<sup>776</sup> These findings underscore the importance of implementing targeted initiatives to boost digital literacy and awareness, and educate MSME owners about the business impacts of digital tools\*. This is crucial in order to harness digitalization in a way that enhances business, increases resilience, and grows the Vietnamese economy.

### Government Initiatives

- Decree 53/2022/ND-CP enhances the Law on Cyber Security 2018 with provisions for local data storage and action against illegal online activities.<sup>777</sup>
- Decree 80/2021/ND-CP enables businesses to access financing to support their digital transformation, covering 50% of the cost for certified digital platforms and solutions.<sup>778</sup>
- The Vietnamese government's Digital Transformation Plan aims to boost the country's digital economy to contribute 30% of GDP by 2030, and focuses on banking, online transactions, and consumer information access, while providing support to MSMEs in their digital transition through training and consultancy services.<sup>779</sup>

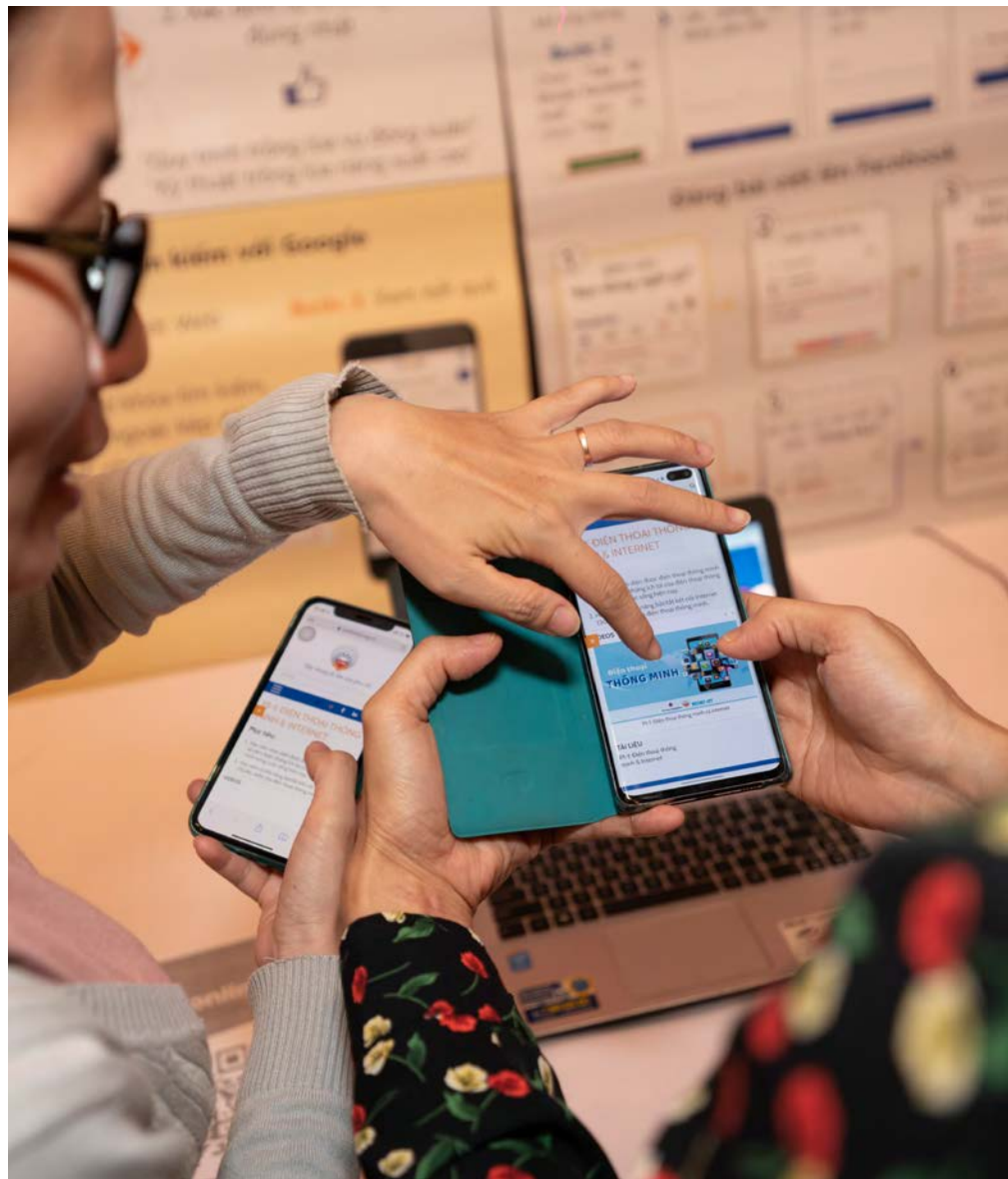
## Industry Initiatives

- RMIT University, the Vietnam Information Security Association (VNISA), and the Vietnam Association of Small and Medium Enterprises (VINASME) hosted a “Cybersecurity Awareness for SMEs in Vietnam” event in 2022, featuring participants from Vietnam and Australia, with the aim to improve cybersecurity awareness in the business sector.<sup>780</sup>

## Challenges And Barriers To Cybersecurity For MSMEs

The low levels of business development, income, education, and cyber literacy that characterize many MSMEs in Vietnam open these businesses to considerable cybersecurity challenges as digitalization accelerates.<sup>781</sup> With up to 70% of smaller enterprises operating outside the digital economy, some business owners have only a basic understanding of the internet, and this limited awareness makes them particularly vulnerable to cyber threats.<sup>782</sup> Many MSMEs also rely on outdated and insecure information systems and invest little in network defenses.<sup>783</sup> These vulnerabilities were only exacerbated by the COVID-19 pandemic.<sup>784</sup>

MSMEs also tend to employ only a few skilled cybersecurity personnel, or lack them altogether, and often utilize fragmented solutions without cohesive strategies. As they shift to digital work environments, cyber threats such as phishing\* and malware\* attacks have the potential to cause significant harm to MSMEs, through data loss, operational disruptions, and financial impacts. For this reason, these enterprises must enhance their cybersecurity measures, despite budgetary and resource constraints.<sup>785</sup>



## Conclusion

Vietnam's digital landscape is rapidly evolving as MSMEs are increasingly integrated into the digital economy. But the potential strategic advantage of this digitalization is matched by increased vulnerability, with the rise in cyber threats such as phishing\* and malware\* representing an ongoing challenge to the security and stability of these smaller enterprises. The government has taken a proactive approach, launching initiatives aimed at fortifying cybersecurity defenses and enhancing data protection in Vietnam. Nevertheless, the resilience of the country's digital infrastructure has been tested by the combined high frequency of cyber incidents and low cyber literacy of users.

A gap exists between the potential of current policies and the actual capabilities of MSMEs, and must therefore be closed. This will require efforts to reach the vast number of unregistered business households in Vietnam, which often lack the resources and knowledge to implement effective cybersecurity measures. Indeed, enhancing cybersecurity in this way is not merely about safeguarding business operations but is crucial to the growth of the Vietnamese economy.

It is imperative for both government and industry to invest in comprehensive cybersecurity education programs, develop more inclusive digital policies, and provide targeted support to bridge the digital divide in Vietnam. These efforts will not only protect but also empower the MSME sector, fostering a more secure and resilient digital economy in Vietnam. This is essential if the country is to achieve the ambition of advancing its global position in cybersecurity, and also to ensure the sustainability of its economy in an increasingly digital world.

## Methodology

To explore and understand the cybersecurity landscape for MSMEs in Vietnam, this report relied mainly on secondary research, incorporating materials including government databases, academic articles, and both local and international news sources. Additional information was gathered through interviews with representatives of local organizations. Challenges arose in finding comprehensive data and case studies on micro and small businesses, which are often overlooked in official documentation and media coverage. Despite these hurdles, the research identified a cyberattack on a small business, providing valuable insights into the cybersecurity risks facing MSMEs.







# APAC Cyber Threat Landscape For Nonprofits

## Number of NPOs

Bangladesh	at least 26,000 <sup>786</sup>
India	3.3 million <sup>787</sup>
Indonesia	appro.115,000 <sup>788</sup>
Japan	50,000 (2015) <sup>789</sup>
Korea	13,900 (2023) <sup>790</sup>
Malaysia	80,000 <sup>791/792</sup>
Pakistan	100,000 to 150,000 <sup>793</sup>
The Philippines	64,087 (2020) <sup>794</sup>
Singapore	2,379 (2022) <sup>795</sup>
Sri Lanka	at least 37,000 <sup>*796</sup>
Thailand	84,099 (2018) <sup>797</sup>
Vietnam	158,895 <sup>798</sup>

\*likely more since some organizations are unregistered

As nonprofit organizations (NPOs), non-governmental organizations (NGOs) across the APAC region increasingly embrace digital tools\* to enhance communications, extend their operational reach, and improve efficiencies, their susceptibility to cyber threats grows. This exposes them to vulnerabilities\* that can threaten their operational security, and the safety of the communities they support. Indeed, one in six NGOs in the APAC region experienced a reported cybersecurity incident in 2022 or 2023, and given the prevalence of underreporting, the rate of incidents was likely much higher than this.<sup>799</sup> The consequences of such incidents are profound, ranging from direct financial losses—such as the costs of system restoration and potential ransom payments—to non-financial impacts like reputational damage, which can irreversibly affect donor trust and volunteer engagement.

The vulnerabilities\* that put NPOs most at risk are the underfunding of cybersecurity measures and limited access to technical expertise. Despite budget constraints and a lack of prioritization for technology investments among leadership, the risk landscape for these organizations is transforming in ways that cannot be ignored, as they become ever more attractive targets for a variety of sophisticated threat actors\*. These include financially motivated cybercriminals, politically driven nation-state actors, and hacktivists\* targeting organizations based on their activities, all of which are capable of deploying destructive and disruptive attacks and those weaponizing data and disinformation, posing unique challenges to organizations that are ill-prepared to defend against such threats.

Hence, there is an urgency surrounding the need for NPOs in the APAC region to fortify their cybersecurity defenses and develop robust digital literacy frameworks to mitigate risks. The geopolitical nuances of the region complicate the cybersecurity challenges to this sector, however. Thus, it is imperative for organizations across the region to understand the specific threat landscape they face and prepare accordingly.

## The Cybersecurity Context For NPOs

Across the APAC region, NPOs are embracing technology at an unprecedented pace as they recognize the value of digital tools\* in helping enhance their communications, extend their operational reach, and improve efficiencies. According to the 2023 Influxchange Asia-Pacific NGO Digital Capability Report, half (49%) of these organizations now prioritize better utilization of digital marketing and the same rate (50%) recognize the need to improve their websites.<sup>800</sup> But as these organizations increasingly rely on digital platforms to engage with beneficiaries, attract diverse talent, or execute data-driven strategies, their attack surface increases. The vulnerabilities\* this produces are not merely technical but can have profound implications for the operational security and integrity of NPOs, and more importantly, for the security of vulnerable communities they support.



It is notable that organizations in the nonprofit sector seldom report cyber incidents publicly and may not even realize they have been attacked.<sup>801</sup> This means that, while one in six NGOs in the APAC region reported experiencing a cyber security incident in 2022 or 2023, the actual number of incidents is likely to be considerably higher.<sup>802</sup> For these donor-driven organizations, the direct and indirect financial impacts of cyberattacks can be devastating. The direct impacts include the cost of restoring systems and data, often with the help of outside cybersecurity and legal firms, as well as potential ransom payments; the indirect impacts include increased insurance premiums and a loss of donor confidence. But the non-financial consequences of cyberattacks can also be debilitating, as damage to an organization's reputation can affect the trust of beneficiaries and volunteers, which can prove fatal. That said, if NPOs survive these incidents, one of the most positive outcomes that can materialize is an organizational commitment to investing in stronger cybersecurity measures going forward, which still has a cost but also delivers clear benefits.

According to the World Economic Forum, cyber insecurity and disinformation are among the top five risks to societies globally in 2024, and for years to come.<sup>803</sup> For NPOs in the APAC region, cyber risks extend not just from the factors mentioned above but from the specific geopolitical context, particularly where these organizations operate in sensitive environments, such as in opposition to certain regimes. The risks they face can therefore be much more acute than those faced by MSMEs in the same countries. Understanding which threat actors\* are targeting NPOs in the region, and the types of cyberattacks they are carrying out, is paramount to helping these organizations navigate the complexities of their digital transformations.



## Challenges And Barriers

The cybersecurity and data protection laws in place across the region, discussed in previous chapters, apply to NPOs just as they do to MSMEs. Moreover, apart from e-commerce platforms, these organizations tend to use the same online services as MSMEs. They face similar challenges in effectively using digital technology as well, and are witnessing similar transformations in their risk profiles.

For NPOs in the region, there are two main vulnerabilities that heighten their cyber risk:

- The underfunding of cybersecurity measures, reflecting the financial constraints under which many NPOs operate. This is exacerbated by a lack of expertise, as both donors and leaders rarely come from tech backgrounds and often fail to prioritize technology and security investments for these organizations. Cultural factors in many countries in the APAC region further complicate matters, for instance where vertical power structures exist or decision-making power is held by senior employees with limited digital literacy.
- Limited technical expertise, which is not a problem only within NPOs but more widely in the APAC region, where the number of cyber professionals must increase considerably to meet demand.<sup>804</sup> Acquiring and retaining cybersecurity talent is especially hard in the non-profit sector, where salaries generally cannot compete with those in the private sector. Upskilling staff is one solution to this, but only 24% of NPOs in the region currently provide cybersecurity training to employees.<sup>805</sup>

These vulnerabilities are exacerbated by the fact that NPOs are not just cyber-poor organizations like MSMEs, they are also target-rich. By targeting these organizations, cybercriminals stand to gain access to donor information and/or very sensitive data that could have profound effects for beneficiary communities. This diversifies the threats directed at NPOs, compared to MSMEs, and puts them at a stark disadvantage when it comes to securing their digital systems.

## Specific Threat Actors

Cybercriminals are typically financially motivated and target the non-profit sector seeking monetary gain, mainly through ransomware\* or CEO fraud attacks\*. By casting a wide net, for example through the use of ransomware-as-a-service\* infrastructure rented from other criminal groups, cybercriminals can wage indiscriminate attacks. But they may also target NPOs when they are known to have received large grants, exploiting the typically weak cyber defenses of these organizations and counting on a low risk of government or police intervention. This was recently the case for the NPO Water for



People when it was targeted by a ransomware\* attack orchestrated by the Medusa gang, which used a ransomware-as-a-service\* model, threatening to release stolen information unless a 300,000 USD extortion fee was paid. The incident occurred after the nonprofit had received a 15 million USD grant.<sup>806</sup> Attacks such as this not only cause operational delays in the immediate term but can lead to longer-term data integrity issues that impact donor trust and funding.

Sometimes, it is not money that drives cybercrime, NPOs can be targeted for other reasons. While the geopolitical and national political context of countries in the APAC region vary widely, both national and foreign actors have been found to target the region's non-profit sector for reasons related to their operational activities. According to data from Microsoft, the sector is second only to the IT sector for targeting by nation-state actors worldwide.<sup>807</sup> These actors are affiliated with governments that engage in cyber operations to further national interests—whether political, economic, or military—and are known for their sophistication and persistence.

State-sponsored cyber attackers may also operate domestically with government backing while maintaining a degree of separation from formal government entities. For instance, suspected state-sponsored actors have targeted the non-profit sector in Hong Kong in search of intelligence on pro-democracy activities and activists. In 2019, Amnesty International reported that a sophisticated cyberattack was targeting its Hong Kong office, aimed at compromising organizational systems and accessing sensitive information. The attackers employed tactics commonly associated with coordinated cyber espionage, raising concerns about the safety and privacy of human rights defenders and the integrity of their work.<sup>808</sup>

Citizen journalists in the Philippines have also been targeted by suspected state-sponsored actors. Alternative outlets including Bulatlat, a small non-profit online news magazine, have experienced a series of Distributed Denial of Service (DDoS)\* attacks on several occasions.<sup>809810</sup> After initial attacks that spanned late 2018 into early 2019, IT experts from Qurium Media Foundation intervened, helping Bulatlat migrate to a secure server\* and mitigate the impacts.<sup>811</sup> But the nature and timing of these attacks, which came against a backdrop of political tension and critical reporting by the outlet, led to suspicions that they were state-sponsored.<sup>812</sup> When Bulatlat was targeted again in 2021, a forensic investigation by Qurium traced the attacks back to a group of Filipino hackers who had been publicly hailed by government officials for previously shutting down the websites of major news outlets like Rappler.<sup>813</sup> This highlights ongoing challenges to press freedom and the risks faced by journalists in the Philippines.

Beyond nation-state or state-sponsored actors, hacktivists\* may also target NPOs, often for ideological reasons. These attackers usually seek to draw public attention to a cause by disrupting the normal operations of targeted organizations or by leaking sensitive information. The resources of collectives that

engage in “hacktivism” tend to be limited and their capabilities are directly linked to the skill of their members. And though the word often has a negative connotation, many hacktivists\* are not seeking to do harm. Anonymous is the most well-known of these collectives, but there are quite a few others. In the APAC region, for example, DragonForce Malaysia is rather active and has targeted various institutions in India and elsewhere, primarily in response to what it deems as anti-Muslim rhetoric.<sup>814/815</sup>

Scammers also represent a cyber threat to the nonprofit sector. Some scammers use the websites of NPOs to test stolen credit cards, processing small payments that create a reporting headache.<sup>816</sup> And, with the growing popularity of online fundraising, there have been rising concerns about the creation of fake NPOs by scammers, used for the purpose of collecting donations from well-meaning victims who believe they are supporting a legitimate cause.<sup>817/818</sup> Scams of this sort are often shaped by local factors, such as in Thailand and the Philippines, where people forced to work for local cybercrime gangs conduct various online scams under duress, some of which likely target local NPOs.<sup>819/820</sup>

This kind of cybercrime has a significant effect on the non-profit ecosystem in the APAC region. It is common that organizations in the region are not properly registered with local authorities, in the same way that many micro enterprises are not, and often for similar reasons.<sup>821</sup> This can make it hard to distinguish these organizations from the fake NPOs of scammers. Moreover, legitimate but unregistered organizations may have little legal recourse if they are targeted by cyberattacks.

## Types Of Cyber Threats

The cyberattacks that have been directed against NPOs in the APAC region can be categorized into four main types: destructive, disruptive, data weaponization, and disinformation. Each of these carries unique implications for the non-profit sector, where organizations frequently lack robust cybersecurity defenses. Destructive cyberattacks are aimed at causing direct damage to digital infrastructure, such as by deleting critical data or disabling hardware, as in the attack targeting Water for People, mentioned above. Disruptive attacks seek to disrupt the normal operations of an organization, often using Distributed Denial of Service (DDoS)\* attacks, in which multiple compromised systems flood the bandwidth or resources of a targeted system. In 2021, for example, the Philippine human rights NGO Karapatan faced a month-long DDoS\* attack aimed at its reports on extrajudicial killings.<sup>822/823</sup>

Data weaponization happens after an attacker successfully compromises a system, and steals or manipulates data to harm an organization or its stakeholders or uses it for blackmail or espionage. Organizations that gather sensitive information, such as the personal details of vulnerable populations, are particularly at risk. After all, in many countries, activist and dissident communities are surveilled by both

domestic and foreign actors.<sup>824/825/826</sup>

Disinformation attacks may not involve efforts to compromise victims' digital defenses at all, as they rely on the spread of false information through traditional and social media. These can be especially harmful to NPOs by affecting their reputation and, with it, the effectiveness of their fundraising and outreach campaigns. In Indonesia, for instance, the UN confronted an organized disinformation campaign targeting Rohingya refugees, amplified by fake social media accounts. The campaign distorted public perceptions of the local UN agency and fueled local resistance against refugees in Aceh, leading to acts of hostility.<sup>827</sup>

## Conclusion

Across the APAC region, digitalization in the non-profit sector has undeniably brought significant operational improvements and has expanded outreach capabilities. However, it has also introduced a range of cybersecurity vulnerabilities\* that can have far-reaching consequences, not just for NPOs and themselves but also for the vulnerable communities they support. Findings from recent reports on the digital readiness of these organizations have underscored the critical and urgent need that they begin to view cybersecurity as a fundamental component of their operational strategies. In other words, the non-profit sector must move beyond the view of cybersecurity as a merely technical challenge and approach it instead as a strategic imperative that is critical to safeguarding their mission and integrity.

Threat actors\* in the APAC region are diverse and sophisticated, ranging from financially motivated cybercriminals to state-sponsored attackers to hacktivist\* groups. This exposes NPOs to a wide variety of attacks, including ransomware\*, DDoS\*, data weaponization, and disinformation campaigns. These threats can not only disrupt operations but can also compromise sensitive data and erode public trust.









# Recommendations For Cyber Hygiene Curriculum

## Recommendations For Curriculum Development

Developing a cyber hygiene curriculum for MSMEs in the APAC region presents unique challenges due to the diverse socioeconomic, political, and cultural landscapes of each country. Even so, there are common challenges faced by MSMEs across the region, and the following recommendations therefore focus on addressing these shared issues. This is meant to provide some universally applicable solutions.

To effectively combat the escalating volume of cyber threats faced by MSMEs will require a dedicated, continuously updated cybersecurity curriculum delivered in an ongoing manner. This curriculum should encompass both foundational and advanced aspects of cybersecurity and should be tailored to meet the specific challenges faced by MSMEs. Special care should be given to account for the local context in each country, to be sure that this curriculum and any training materials are culturally sensitive and relevant, and are accessible to a range of digital and language literacy abilities (including to speakers of native but not official languages) as well as to marginalized or vulnerable populations.

## Ongoing Digital Literacy And Cybersecurity Education

Digital literacy and cybersecurity education should not be first introduced in the workplace but in schools, and should then be complemented by professional development. This approach will be crucial to keeping pace with rapidly evolving cyber threats and is the only way to ensure a highly skilled future workforce. The outline below conveys the key components of an effective digital literacy curriculum.

### Basic Digital Literacy

- *Understanding digital tools\**

An introduction to computers, smartphones, and other essential digital devices

- *Using the internet*

How to efficiently and safely use the internet, including web browsing, email, and social media

- *Software\* skills*

Basic training in commonly used software\* and applications (i.e., for word processing)

### Cybersecurity Fundamentals

- *Understanding cyber threats*

An introduction to various cyber threats, including viruses, malware\*, phishing\*, ransomware\*, and social engineering attacks\*

- *Security best practices*

How to set strong passwords, recognize safe websites, use secure browsing practices, and ensure that software\* is regularly updated and is not pirated

- *Data protection principles*

The essentials of data privacy, including methods of securing personal and business data, with an emphasis on the importance of data encryption\* and secure data storage

## **Operational Security Measures**

- *Secure network setup*

How to set up and maintain a secure network, including through the use of firewalls\*, VPNs\*, and secure Wi-Fi practices

- *Endpoint protection*

Guidance on securing individual devices that connect to larger networks, such as desktops, laptops, and mobile devices

- *Email security*

Practices for securing email communications, including by spotting phishing\* attempts, using email encryption\*, and understanding email filters

## **Risk Management And Compliance**

- *Risk assessment*

How to identify, assess, and mitigate risks associated with digital operations

- *Regulatory compliance*

Information on relevant local and international data protection laws and regulations that impact operations (will especially need to be tailored to local contexts)

- *Incident response\**

Basic training on how to respond to a security breach, including steps to take immediately after discovering a breach and how to report the incident to relevant authorities (will especially need to be tailored to local contexts)

## **Advanced Cybersecurity Practices**

- *Multi-factor authentication\* (MFA)*

How to implement and manage multi-factor authentication to protect sensitive systems and data

- *Cloud security*

Cloud computing fundamentals, including the benefits and risks, and strategies to secure cloud environments

- *Cybersecurity policies*

Guidance on developing and implementing organizational cybersecurity policies and protocols to ensure the consistent application of security practices

## Ongoing Education And Training

- *Regular continuing education*

Ongoing training is necessary to help employees keep up with the latest cybersecurity trends, threats, and innovations

- *Simulated phishing\* exercises*

Drills using simulated phishing\* attempts should be used to train employees on how to recognize and react to malicious emails

- *Professional development*

Opportunities should be provided for staff to attend workshops, seminars, and courses to deepen their cybersecurity knowledge and skills

## Public-Private Partnerships And Community Engagement

- *Leveraging expertise*

Collaborations with cybersecurity firms, educational institutions, and government agencies can provide practical insights and resources

- *Community learning platforms*

The creation of forums and platforms, for example for MSMEs and NPOs, to share experiences, challenges, and solutions, to help increase knowledge sharing and problem solving related to cybersecurity

## Further Considerations

This research found that the use of mobile devices was prevalent in the APAC region, even where computer use was not. There is also a society-wide use of Facebook, WhatsApp, and other Meta applications in all 12 countries in this study, for both personal and business purposes. Any cyber hygiene curriculum should be tailored to reflect the real-world use of digital technology and platforms in any context, to make cybersecurity awareness directly applicable to people's lives and therefore most likely to be adopted.

It should be noted, too, that similar programs in the region, including USAID-supported SARDI and initiatives such as Digital India and Thailand 4.0 (mentioned in the report), have relied on community implementation as a best practice. This helps assure the relevance and appropriateness of programming to each context. Such an approach increases trust and transparency, strengthens local capacity, facilitates sustainability, and has economic benefits.



## Conclusion

This mapping of the cybersecurity landscape for MSMEs in the APAC region has produced a detailed accounting of the complex and multifaceted cyber threats confronting these enterprises as the economies in which they operate are increasingly digitalized. Paired with the complementary review of cyber threats to regional NPOs, it is clear that these threats pose a significant risk to the stability and economic prosperity of the MSME and non-profit sectors. As these businesses and organizations undergo inevitable digital transformations, they face a variety of cybersecurity challenges with the potential to endanger their operational integrity and economic viability.

Throughout the APAC region, the prevalence of phishing\*, ransomware\*, and data breaches\* highlights how critical it is that MSMEs and NPOs improve their cybersecurity to keep up with digitalization. India, for instance, is a burgeoning hub for tech startups but is also targeted by a particularly high rate of cyberattacks, as rapid digital adoption outpaces its cybersecurity readiness. Similarly, Malaysia and Indonesia have seen a surge in ransomware\* attacks targeting MSMEs. This reflects a trend seen more broadly across the region, affecting both the MSME and non-profit sectors.

Emerging cyber threats that leverage advanced technologies such as artificial intelligence are increasingly prevalent as well. This allows cybercriminals to add a layer of sophistication to attacks and exposes new vulnerabilities, especially for businesses in technologically advanced countries like Singapore and South Korea. Of course, the interconnected nature of the global economy means that attacks in any country can have serious implications in others, and this is part of why supply chain attacks are becoming more common. A recent spate of such attacks in Japan and Hong Kong has not only had a disruptive effect on local businesses but has rippled across regional and global markets. By targeting MSMEs with weaker cybersecurity mechanisms, cyberattacks can work through the supply chain to impact not just the direct targets but also their partners and stakeholders across borders.

In such a cybersecurity landscape, a robust and coordinated approach must be developed to support MSMEs, involving government intervention, private sector initiatives, and international collaboration. It is also imperative to strengthen regulatory frameworks, invest in cybersecurity solutions, and foster cultures of cybersecurity awareness. Similar initiatives for NPOs are crucial as well. For these organizations, cybersecurity is not merely a technical requirement but a critical safeguard of their mission continuity and the trust placed in them by beneficiaries and stakeholders. Yet, their tendency to make limited cybersecurity investments means that cybercriminals often see NPOs as soft targets; while coveting the valuable nature of the data these organizations handle, ranging from donor information to sensitive operational details.

In the APAC region, the ongoing resilience and economic stability of MSMEs, and the vital efforts of the non-profit sector, will depend significantly on the ability of businesses and organizations to navigate and mitigate evolving cyber threats. Ensuring that these entities are well-equipped with the necessary tools and knowledge to counteract these threats is essential to securing their operations and supporting the crucial roles the MSME and non-profit sectors play in regional development.

As the world and the region look to a digital future, investments must be made to ensure that populations feel comfortable stepping into that future and know how to do so safely and sustainably.







APAC Cybersecurity Fund



The Asia Foundation

# Appendices Glossary Endnotes

in partnership with



with support from





## Appendices

Japan Table 1 <sup>828</sup>

Category	Manufacturing and Others	Wholesale	Retail	Service
Capital (All MSME)	2.29 million USD or less	677,000 USD or less	338,000 USD or less	338,000 USD or less
Number of Employees (Medium)	300 or less	100 or less	50 or less	100 or less
Number of Employees (Small)	20 or less	5 or less	5 or less	5 or less

Japan Table 2<sup>829</sup>

### Number of firms by size in Japan, 2016

Firm size	Number of firms	%	Number of employees	%
Micro enterprises	3,048,390	84.9	10,437,271	22.3
Medium-sized enterprises	529,786	14.8	21,763,761	46.5
Large enterprises	11,157	0.3	14,588,963	31.2
Total	3,589,333	100	46,789,995	100

#### Note:

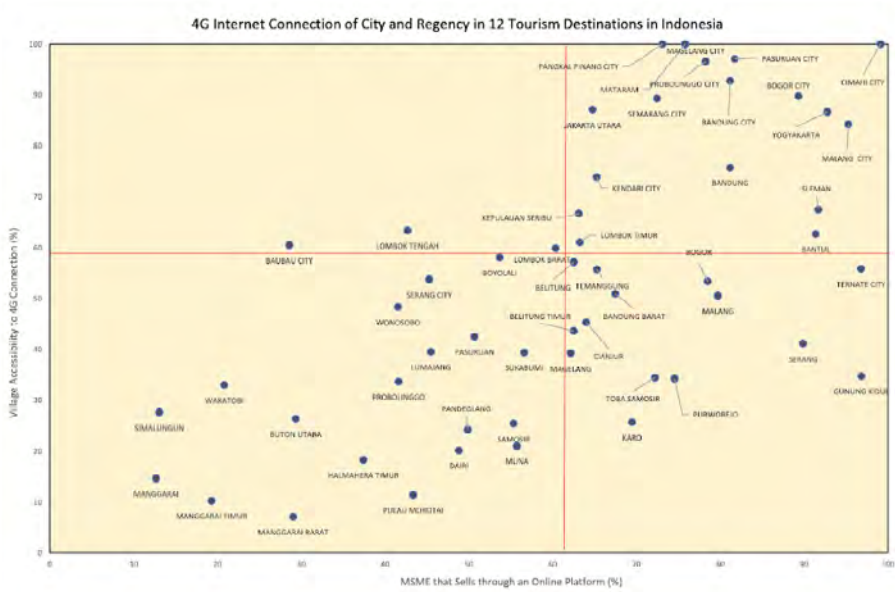
1. Number of enterprises = Number of companies + Business establishments of sole proprietors (independent establishments and head offices).
2. "Micro enterprises" refers to "micro enterprises" as defined under the Small and Medium-sized Enterprises Basic Act. "Medium-sized enterprises" refers to SMEs other than micro enterprises.

# References

Malaysia Figure 1<sup>830</sup>



Indonesia Figure 1<sup>831</sup>



**Vietnam Table 1<sup>832</sup>**

Sector / Size	Agriculture, Forestry, and Fishing Industry and Construction	Trade Services
<b>Micro</b>	Total Revenue < 121,655 USD (VND 3 billion) or Total Capital < 121,655 USD (VND 3 billion); Employees ≤ 10	Total Revenue < 121,655 USD (VND 3 billion) or Total Capital < 121,655 USD (VND 3 billion); Employees ≤ 10
<b>Small</b>	Total Revenue < 2,027,575 USD (VND 50 billion) or Total Capital < 811,030 USD (VND 20 billion); Employees 11 to 100	Total Revenue < 4,055,150 USD (VND 100 billion) or Total Capital < 2,027,575 USD (VND 50 billion); Employees 11 to 50
<b>Medium</b>	Total Revenue < 12,165,450 USD (VND 300 billion) or Total Capital < 4,055,150 USD (VND 100 billion); Employees 101 to 200	Total Revenue < 12,165,450 USD (VND 300 billion) or Total Capital < 4,055,150 USD (VND 100 billion); Employees 51 to 100

India Table 1<sup>833</sup>

**Revised Classification applicable w.e.f 1st July 2020**

**Classification of Micro, Small and Medium Enterprise (MSME) sector**

Classification	Investment in Plant & Machinery/Equipment	Annual Turnover
<b>Micro</b>	Investment in Plant and Machinery or Equipment up to Rs. 1 crore	Annual Turnover does not exceed Rs. 5 crore
<b>Small</b>	Investment in Plant and Machinery or Equipment up to Rs. 10 crore	Annual Turnover does not exceed Rs. 50 crore
<b>Medium</b>	Investment in Plant and Machinery or Equipment up to Rs. 50 crore	Annual Turnover does not exceed Rs. 250 crore

Bangladesh Table 1<sup>834</sup>

Type of Industry	Amount of Investment (Replacement cost and value of fixed assets, excluding land and factory buildings), BDT	Number of employed workers
Cottage Industry	Below 1 million	Not exceeding 15
Micro Industry	1.0 million to 7.5 million	16 to 30
Small Industry	Manufacturing: 7.5 million to 150 million	31 to 120
	Services: 1.0 million to 20 million	16 to 50
Medium Industry	Manufacturing: 150 million to 500 million	121 to 300
	Services: 20 million to 300 million	51 to 120
Large Industry	Manufacturing: More than 500 million	More than 300
	Services: More than 300 million	More than 120



## Glossary

**Angler phishing:** A type of phishing attack (see Phishing) that impersonates customer service accounts on social media to reach victims.

**APT (Advanced Persistent Threats) attacks:** Sophisticated, prolonged cyberattacks where intruders gain access to a network and remain undetected for a long period of time.

**Artificial Intelligence (AI) attacks:** Attacks involving the use of machine learning or artificial intelligence technologies to conduct malicious activities. These can include the creation of highly sophisticated phishing messages, the evasion of detection systems, the automation of the discovery of vulnerabilities, or even the manipulation of AI systems themselves to behave in unintended ways.

**Attack:** see Cyberattack

**Backup:** A copy of computer data that is kept in a safe environment, to be used in case of infrastructure failure to restore a system to a working condition.

**Baiting:** A form of social engineering that entices victims into exposing their sensitive information by offering something tempting.

**Banking malware:** Malicious software specifically designed to steal financial information, such as bank account credentials, credit card numbers, and other sensitive data related to banking and financial transactions. This type of malware often infects a user's device and monitors activities, intercepting data during transactions.

**CEO fraud attack:** A type of phishing scam where attackers impersonate a company executive (often the CEO) to trick employees, customers, or partners into transferring money or sensitive information. This scam often targets employees who have access to company finances or confidential information.

**Cloud computing systems:** Infrastructure, platforms, or software that are hosted by third-party providers and delivered over the internet.

**Cloud services:** Services made available to users on demand via the internet from the servers of a cloud computing provider.

**Cloud-based solutions:** Applications, storage, on-demand services, computer networks, or other resources that are accessed with an internet connection through another provider's shared cloud computing framework.

**Code obfuscation:** The practice of making software code more difficult to understand or reverse engineer.

**Computer Emergency Response Team (CERT):** An expert group that handles cybersecurity incidents.

**Cyberattack:** A disruptive cyber incident, data breach, or disinformation operation conducted by a threat actor using a computer network or system, with the malicious intent to cause damage (technical, financial, reputational, or other) or extract/steal data without consent.

**Cybercrime as a Service (CaaS):** The offer of cybercrime tools and services in underground markets that make cybercrime accessible to non-experts.

**Cyber hygiene:** Practices and habits that help minimize cyber risk and mitigate cyber threats.

**Cyberpeace:** a state achieved when human security, dignity, and equity are ensured in digital ecosystems.

**Cybersecurity:** The practice of protecting computer systems and networks from unauthorized information disclosure, or theft of or damage to their hardware, software, or electronic data. Through the application of technologies, processes, and controls, cybersecurity reduces the risk of cyberattack and protects systems, networks, and technologies.

**Cyberspace:** Digital systems and the online world, including everything accessible through computer networks and the internet, from corporate networks and social media platforms, to bank accounts and cloud services, to any connected appliances—video surveillance cameras, gaming consoles, TV sets, vacuum cleaners, etc.

**Cyber threat:** A circumstance or event with the potential to damage or disrupt, or otherwise adversely impact, a computer network or system.

**Data breach:** The exposure of confidential, sensitive, or protected information to an unauthorized person. This may be accidental, such as a USB drive left on a train or an email attachment sent to the wrong person, but can also be deliberate, as when malicious actors access a network and exfiltrate (target, copy, and transfer) data.

**Decryption:** Converting encrypted data (see Encryption) into its original form. This process reverses encryption to put data back into a human-readable form.

**Decryption key:** Piece of information needed for the decryption process.

**Digital data:** Information formatted in a digital mode, which can be created, stored, and processed electronically.

**Digital management:** The administration and governance of digital information and technologies.

**Digital tool:** A type of software or online resource that can be used for a specific digital process or objective.

**Disinformation:** False or misleading information spread, often covertly, with the intention to deceive.

**Distributed Denial-of-Service (DDoS) attack:** A technique used to flood a network, service, or server with excessive traffic to cause it to cease functioning normally. It is said to be distributed when the source of the attack is composed of a multitude of devices or systems.

**Drive-by download attack:** A malicious attack that automatically downloads malware to a device without consent when a compromised website is visited.

**Email spamming:** The act of sending unsolicited bulk messages via email, typically for advertising purposes.

**Encryption:** The reversible process of converting information or data into an encoded format using mathematical computation algorithms, commonly used to protect sensitive information at rest or in-transit so that only authorized parties can view it.

**Fintech:** Short for “financial technology,” describes new technology that automates the delivery and use of financial services.

**Firewall:** A part of a computer system or network, designed to block unauthorized access while permitting outward communication.

**Hactivists:** Individuals or groups that gain unauthorized access to computer files, systems, or networks to further social, political, or ideological ends.

**Identity and Access Management (IAM):** Frameworks and technologies that ensure the right individuals have the appropriate access to technological resources.

**Incident response:** The steps taken to address the short-term, direct effects of an incident, and to support short-term recovery.

**Incident Response Plan (IRP):** A document that outlines the procedures, steps, and responsibilities of a cyber incident response for an organization.

**Insider-based attacks:** Cyberattacks originating from within an organization.

**Insider threats:** Risks of data theft or damage caused by employees or associates with access to internal systems and data.

**Internet of Things (IoT):** Smart devices that are connected to the internet but are not personal computers or smartphones.

**Internet of Things (IoT) infrastructure:** The network of physical devices, vehicles, and other objects embedded with sensors, software, and connectivity that enables these objects to connect and exchange data.

**Legacy systems:** Outdated software and/or hardware that cannot resist contemporary forms of cyber-attack, presenting a risk to other applications and data that share the same infrastructure.

**Malware:** Software designed to disrupt, damage, or gain unauthorized access to computer systems.



**Man-in-the-middle attack (MitM):** A method by which an attacker secretly relays and possibly alters the communications between two parties who believe they are in direct communication.

**Medusa ransomware:** A type of ransomware (see Ransomware) that encrypts files on infected systems and demands a ransom for their decryption.

**Multi-factor authentication (MFA):** Using two or more factors to achieve authentication. These factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

**Password Stealing Ware (PSW):** Malware that searches the system files of a web browser to find sensitive data, such as credentials for online accounts and saved credit card information.

**Password targeting attacks:** Cyberattacks that aim to steal or crack passwords to gain unauthorized access to systems.

**Phishing:** A type of social engineering used to steal user data, including login credentials and credit card numbers, involving an attacker who masquerades as a trusted entity to dupe a victim into opening an email, instant message, or text message, and then induces them to provide confidential information.

**Quishing, or QR phishing:** A phishing attack that uses QR codes to redirect victims to malicious websites or prompt them to download harmful content.

**Ransomware:** A type of malware designed to extort money by encrypting or blocking access to files or an entire computer system until a ransom is paid.

**Ransomware-as-a-Service (RaaS):** The leasing of ransomware variants by cybercriminals to other attackers in exchange for a profit share.

**Risk:** The likelihood of harm or loss due to cybersecurity vulnerabilities. Cyber risk encompasses threats such as cyberattacks, data breaches, and system failures.

**Sender Policy Framework (SPF):** Used to verify sender domain authenticity by checking which IP addresses are legitimate for mail sent from an organization's domain.

**Server:** a computer or device on a network that manages network resources.

**Social engineering:** The psychological manipulation of a person to make them perform an action or give away information.

**Social engineering attacks:** Techniques that use manipulation to convince individuals to break security procedures, to gain confidential information.

**Smishing:** A type of phishing attack that involves sending fraudulent SMS messages to trick people into revealing personal information.

**Software:** a set of instructions, data, or programs used to operate computers and execute specific tasks. The opposite of hardware, which describes the physical aspects of a computer.

**Spam:** Unsolicited messages sent over the internet, typically to a large volume of users.

**SQL injection attacks:** Attacks that exploit vulnerabilities in an application's software by injecting malicious SQL statements (see Structured query language) into a database query.

**Stealer-as-a-Ransomware (StaR):** A hypothetical ransomware variant that could incorporate data theft capabilities.

**Structured query language (SQL):** A programming language used to manage data, and to access and manipulate databases.

**Supply chain attacks:** A cyberattack that seeks to damage an organization by targeting less-secure elements in its supply chain network, such as the compromise of software providers or hardware manufacturers in order to cause the distribution of malicious software updates or components.

**Threat actors:** Individuals or groups that intentionally cause harm to digital devices or systems.

**Trojan virus:** A type of malware disguised as legitimate software that tricks users into loading and executing it on their systems, enabling cybercriminals to spy on victims and steal sensitive data through backdoor access, once it is activated .

**Virtual private network (VPN):** A means of encrypting an internet connection and anonymizing an IP address by creating a secure tunnel through which internal resources are accessed.

**Virus:** Software designed to replicate itself and propagate in a computer infrastructure.

**Vulnerability:** A software error, security gap, or user weakness that may be exploited to compromise a computer system.

**Web-based malware:** Malicious software distributed through the internet and typically executed directly within a web browser, sometimes in drive-by download attacks (see Drive-by download attack).

**Web-based software:** Applications that are hosted on a web server and accessed via a web browser over a network (internet or intranet), which do not require installation on a user's personal computer and can be accessed from any device with network access.

**Website defacement:** An attack on a website that changes the visual appearance of the site or of a webpage.

**Zero-day attacks:** Cyberattacks that exploit previously unknown vulnerabilities in software or hardware, before the developer has released a fix or patch.

## Endnotes

- 1 <https://www.cnn.com/2020/11/10/southeast-asia-40-million-new-internet-users-in-2020-report-finds.html>
- 2 <https://www.ibm.com/account/reg/us-en/signup?formid=urx-51962>
- 3 <https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/>
- 4 Ibid.
- 5 <https://www.cloudflare.com/the-net/securing-future/introduction/>
- 6 <https://www.cloudflare.com/the-net/securing-future/talent-crunch/>
- 7 <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf>
- 8 [https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34\\_be4c\\_417d\\_b36c\\_ecf8db4614fc/ToR%2Ofinal%20SME.pdf](https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34_be4c_417d_b36c_ecf8db4614fc/ToR%2Ofinal%20SME.pdf)
- 9 <https://www.similarweb.com/top-apps/google/bangladesh/>
- 10 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 11 [https://unb.com.bd/category/Business/fintech-mfs-best-mobile-financial-services-in-bangladesh/43453#google\\_vignette](https://unb.com.bd/category/Business/fintech-mfs-best-mobile-financial-services-in-bangladesh/43453#google_vignette)
- 12 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
- 13 <https://www.tbsnews.net/bangladesh/92-msme-entrepreneurs-unaware-cyber-security-study-520674>
- 14 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh>
- 15 [https://www.unescap.org/sites/default/d8files/knowledge-products/MSME%20financing%20Bangladesh\\_10%20May%202021\\_share\\_0.pdf](https://www.unescap.org/sites/default/d8files/knowledge-products/MSME%20financing%20Bangladesh_10%20May%202021_share_0.pdf)
- 16 [https://www.usaid.gov/sites/default/files/2023-06/DECA\\_Bangladesh\\_Snapshot.pdf](https://www.usaid.gov/sites/default/files/2023-06/DECA_Bangladesh_Snapshot.pdf)
- 17 Ibid.
- 18 <https://datareportal.com/reports/digital-2023-bangladesh>
- 19 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 20 [https://www.usaid.gov/sites/default/files/2023-06/DECA\\_Bangladesh\\_Snapshot.pdf](https://www.usaid.gov/sites/default/files/2023-06/DECA_Bangladesh_Snapshot.pdf)
- 21 Ibid.
- 22 [https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34\\_be4c\\_417d\\_b36c\\_ecf8db4614fc/ToR%2Ofinal%20SME.pdf](https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34_be4c_417d_b36c_ecf8db4614fc/ToR%2Ofinal%20SME.pdf)
- 23 <https://documents1.worldbank.org/curated/en/172841613718788462/pdf/Business-Pulse-Survey-Impact-of-COVID-19-on-MSMEs-in-Bangladesh.pdf>
- 24 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
- 25 <https://www.dhakatribune.com/opinion/op-ed/294341/bangladesh-is-at-serious-risk-of-cyber-crimes>
- 26 <https://thefinancialexpress.com.bd/views/human-element-in-cybersecurity-training-and-awareness-in-bangladeshi-msmes>
- 27 [https://www.usaid.gov/sites/default/files/2023-06/DECA\\_Bangladesh\\_Snapshot.pdf](https://www.usaid.gov/sites/default/files/2023-06/DECA_Bangladesh_Snapshot.pdf)
- 28 <https://policyinsightsonline.com/2019/04/insights-into-the-informal-sector-in-bangladesh/#:~:text=It%20clearly%20depicts%20that%20almost,for%20female%20and%20rural%20employment>
- 29 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 30 Ibid.
- 31 <https://datareportal.com/reports/digital-2023-bangladesh>
- 32 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 33 [https://www.researchgate.net/publication/376580933\\_The\\_Landscape\\_of\\_Cyber\\_Crime\\_in\\_Bangladesh\\_Challenges\\_Trends\\_and\\_Mitigation\\_Strategies](https://www.researchgate.net/publication/376580933_The_Landscape_of_Cyber_Crime_in_Bangladesh_Challenges_Trends_and_Mitigation_Strategies)
- 34 <https://www.bssnews.net/news-flash/160354#:~:text=DHAKA%2C%20Nov%2027%2C%202023%20>
- 35 <https://www.ti-bangladesh.org/upload/files/position-paper/2024/Personal-Data-Protection-Act-Review-TIB-Article-19.pdf>
- 36 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
- 37 [https://www.usaid.gov/sites/default/files/2023-06/DECA\\_Bangladesh\\_Snapshot.pdf](https://www.usaid.gov/sites/default/files/2023-06/DECA_Bangladesh_Snapshot.pdf)
- 38 Ibid.
- 39 <https://datareportal.com/reports/digital-2023-bangladesh>
- 40 [https://www.usaid.gov/sites/default/files/2023-06/DECA\\_Bangladesh\\_Snapshot.pdf](https://www.usaid.gov/sites/default/files/2023-06/DECA_Bangladesh_Snapshot.pdf)
- 41 <https://www.dhakatribune.com/opinion/op-ed/294341/bangladesh-is-at-serious-risk-of-cyber-crimes>
- 42 [https://www.researchgate.net/publication/376580933\\_The\\_Landscape\\_of\\_Cyber\\_Crime\\_in\\_Bangladesh\\_Challenges\\_Trends\\_and\\_Mitigation\\_Strategies](https://www.researchgate.net/publication/376580933_The_Landscape_of_Cyber_Crime_in_Bangladesh_Challenges_Trends_and_Mitigation_Strategies)
- 43 <https://www.bssnews.net/news-flash/160354#:~:text=DHAKA%2C%20Nov%2027%2C%202023%20>
- 44 <https://www.ti-bangladesh.org/upload/files/position-paper/2024/Personal-Data-Protection-Act-Review-TIB-Article-19.pdf>
- 45 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 46 <https://datareportal.com/reports/digital-2023-bangladesh>
- 47 <https://documents1.worldbank.org/curated/en/172841613718788462/pdf/Business-Pulse-Survey-Impact-of-COVID-19-on-MSMEs-in-Bangladesh.pdf>
- 48 [https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34\\_be4c\\_417d\\_b36c\\_ecf8db4614fc/ToR%2Ofinal%20SME.pdf](https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34_be4c_417d_b36c_ecf8db4614fc/ToR%2Ofinal%20SME.pdf)
- 49 <https://documents1.worldbank.org/curated/en/172841613718788462/pdf/Business-Pulse-Survey-Impact-of-COVID-19-on-MSMEs-in-Bangladesh.pdf>
- 50 [https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34\\_be4c\\_417d\\_b36c\\_ecf8db4614fc/ToR%2Ofinal%20SME.pdf](https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34_be4c_417d_b36c_ecf8db4614fc/ToR%2Ofinal%20SME.pdf)
- 51 [https://files.digitalfrontiersdai.com/media/documents/Revised\\_Campaign\\_Final\\_Report\\_SARDI\\_SME\\_Cybersecurity\\_Awareness\\_Campaign.pdf](https://files.digitalfrontiersdai.com/media/documents/Revised_Campaign_Final_Report_SARDI_SME_Cybersecurity_Awareness_Campaign.pdf)
- 52 [https://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/b343a8b4\\_956b\\_45ca\\_872f\\_4cf9b-2f1a6e0/2023-10-25-07-38-4304abd7a3f3d8799fbc59ff91007b1.pdf](https://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/b343a8b4_956b_45ca_872f_4cf9b-2f1a6e0/2023-10-25-07-38-4304abd7a3f3d8799fbc59ff91007b1.pdf)
- 53 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 54 Ibid.
- 55 Ibid.
- 56 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
- 57 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 58 Ibid.
- 59 Ibid.
- 60 <https://www.tbsnews.net/bangladesh/92-msme-entrepreneurs-unaware-cyber-security-study-520674>
- 61 Ibid.
- 62 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)
- 63 <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
- 64 Ibid.



65 Ibid.

66 Interview, April 19, 2024.

67 Interview, The Asia Foundation, Bangladesh, May 25, 2024.

68 <https://www.cirt.gov.bd/>

69 <http://oldweb.lged.gov.bd/uploadeddocument/unitpublication/1/1049/vision%202021-2041.pdf>

70 <https://azi.gov.bd/azi-missions/smart-bangladesh-vision-2041/>

71 <https://www.bssnews.net/news/204847>

72 [https://www.usaid.gov/sites/default/files/2023-10/USAID\\_SARDI\\_Factsheet.pdf](https://www.usaid.gov/sites/default/files/2023-10/USAID_SARDI_Factsheet.pdf)

73 <https://inspira-bd.com/>

74 [https://www.usaid.gov/sites/default/files/2023-06/USAID\\_Bangladesh\\_DECA\\_1.pdf](https://www.usaid.gov/sites/default/files/2023-06/USAID_Bangladesh_DECA_1.pdf)

75 Ibid.

76 <https://msme.gov.in/know-about-msme>

77 <https://www.theglobalstatistics.com/india-social-media-statistics/>

78 <https://www.thehindubusinessline.com/info-tech/cyber-attacks-in-the-past-year-cost-62-smbs-in-india-over-35-crore-report/article36689903>  
ece

79 <https://www.financialexpress.com/business/sme-msme-tech-indian-small-businesses-are-at-the-highest-risk-of-cyber-attacks-report-2694417/>

80 [https://www.cisco.com/c/dam/global/en\\_hk/assets/pdfs/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_hk/assets/pdfs/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf)

81 <https://sundayguardianlive.com/top-five/surge-in-cyberattacks-on-india-linked-to-pak-officers-trained-by-italian-firm#:~:text=Last%20year%20in%20November%2C%20a,the%20highest%20share%20of%20attacks>

82 [https://msme.gov.in/sites/default/files/MSME\\_gazette\\_of\\_india.pdf](https://msme.gov.in/sites/default/files/MSME_gazette_of_india.pdf)

83 <https://timesofindia.indiatimes.com/city/ahmedabad/by-2026-digital-economy-to-contribute-20-to-gdp/articleshow/105825527.cms>

84 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

85 <https://www.newindianexpress.com/business/2023/Sep/05/83-per-centof-indian-firms-faced-cybersecurity-incident-in-past-year-report-2611905.html>

86 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

87 <https://www.forbes.com/advisor/in/business/msme-statistics/#:~:text=There%20are%20a%20total%20of,up%20to%20630.5%20lakh%20enterprises>

88 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

89 <https://www.thehindubusinessline.com/info-tech/cyber-attacks-in-the-past-year-cost-62-smbs-in-india-over-35-crore-report/article36689903>  
ece

90 <https://cuts-crc.org/pdf/briefing-paper-cybersecurity-challenges-for-indian-msmes.pdf>

91 <https://www.cloverinfotech.com/blog/small-businesses-big-problems-are-cyber-attacks-crushing-indias-msmes/>

92 <https://www.skillindiadigital.gov.in/about-us>

93 <https://www.ibef.org/industry/msme>

94 <https://kpmg.com/in/en/home/insights/2023/08/digital-personal-data-protection-act-2023-overview.html>

95 [https://npstrust.org.in/sites/default/files/inline-files/ICS\\_Policy\\_2023-NPS\\_Trust.pdf](https://npstrust.org.in/sites/default/files/inline-files/ICS_Policy_2023-NPS_Trust.pdf)

96 <https://kpmg.com/in/en/home/insights/2023/08/digital-personal-data-protection-act-2023-overview.html>

97 [https://npstrust.org.in/sites/default/files/inline-files/ICS\\_Policy\\_2023-NPS\\_Trust.pdf](https://npstrust.org.in/sites/default/files/inline-files/ICS_Policy_2023-NPS_Trust.pdf)

98 <https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/>

99 <https://timesofindia.indiatimes.com/city/ahmedabad/by-2026-digital-economy-to-contribute-20-to-gdp/articleshow/105825527.cms>

100 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

101 <https://datareportal.com/reports/digital-2023-india?rq=india>

102 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

103 <https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/>

104 <https://www.businessworld.in/article/India-5th-Most-Ransomware-Targeted-Country-Globally-Report/18-03-2024-513823/>

105 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

106 Ibid.

107 Ibid.

108 <https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/>

109 <https://kpmg.com/in/en/home/insights/2023/08/digital-personal-data-protection-act-2023-overview.html>

110 [https://npstrust.org.in/sites/default/files/inline-files/ICS\\_Policy\\_2023-NPS\\_Trust.pdf](https://npstrust.org.in/sites/default/files/inline-files/ICS_Policy_2023-NPS_Trust.pdf)

111 [https://www.dcmsme.gov.in/ssiindia/MSME\\_OVERVIEW.pdf](https://www.dcmsme.gov.in/ssiindia/MSME_OVERVIEW.pdf)

112 <https://msme.gov.in/sites/default/files/MSMEANNUALREPORT2022-23ENGLISH.pdf>

113 Ibid.

114 <https://www.ibef.org/industry/msme>

115 <https://www.smechamberofindia.com/about-msme-in-india.php>

116 <https://forumias.com/blog/indias-informal-economy-challenges-and-solutions-explained-pointwise/>

117 [https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@asia/@ro-bangkok/@sro-new\\_delhi/documents/publication/wcms\\_921154.pdf](https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@asia/@ro-bangkok/@sro-new_delhi/documents/publication/wcms_921154.pdf)

118 <https://forumias.com/blog/indias-informal-economy-challenges-and-solutions-explained-pointwise/>

119 <https://economictimes.indiatimes.com/tech/technology/75-of-indias-top-100-android-apps-contain-security-risks-report/article-show/92512490.cms?from=mdr>

120 Ibid.

121 <https://gs.statcounter.com/os-market-share/mobile/india>

122 <https://www.ibef.org/industry/ecommerce>

123 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8662980/>

124 Ibid.

125 <https://ecommerceguide.com/top/top-10-ecommerce-sites-in-india/>

126 <https://www.techinasia.com/meesho-tops-indian-ecommerce-apps-q2-downloads>

127 <https://yourstory.com/smbstory/digitisation-sme-msmes-growth-social-media>

128 <https://www.theglobalstatistics.com/india-social-media-statistics/>

129 [https://www.google.com/url?q=https://kinaracapital.com/3-digital-adoptions-to-help-msmes-scale-their-business-in-2023/&sa=D&source=docs&ust=1718057606412331&usq=AOvAw3HSx3c4axYf8jKtL\\_s6pO8](https://www.google.com/url?q=https://kinaracapital.com/3-digital-adoptions-to-help-msmes-scale-their-business-in-2023/&sa=D&source=docs&ust=1718057606412331&usq=AOvAw3HSx3c4axYf8jKtL_s6pO8)

130 <https://ccoedsci.in/blog/the-path-to-success-the-importance-of-preventing-cybersecurity-threats-for-small-businesses>

131 <https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023-report>

132 <https://www.zeebiz.com/india/news-of-all-cyberattacks-43-target-small-businesses-sme-startups-report-20795>

133 <https://www.thehindubusinessline.com/info-tech/cyber-attacks-in-the-past-year-cost-62-smbs-in-india-over-35-crore-report/article36689903>  
 134 Ibid.  
 135 <https://www.livemint.com/technology/tech-news/cyber-extortionists-intensify-attacks-on-small-indian-firms-11664307053165.html>  
 136 Ibid.  
 137 <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1519500>  
 138 <https://www.mha.gov.in/en/divisionofmha/cyber-and-information-security-cis-division>  
 139 <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/25KY010711F.pdf>  
 140 <https://www.csk.gov.in/>  
 141 <https://udyogplus.adityabirlacapital.com/>  
 142 <https://pib.gov.in/PressReleasePage.aspx?PRID=1977595>  
 143 <https://cuts-crc.org/pdf/briefing-paper-cybersecurity-challenges-for-indian-msmes.pdf>  
 144 Ibid.  
 145 Ibid.  
 146 <https://www.cloverinfotech.com/blog/small-businesses-big-problems-are-cyber-attacks-crushing-indias-msmes/>  
 147 <https://kadin.id/en/data-dan-statistik/umkm-indonesia/>  
 148 <https://www.meltwater.com/en/blog/social-media-statistics-malaysia>  
 149 <https://www.malaymail.com/news/malaysia/2022/11/28/whatsapp-data-leak-11-million-malaysian-phone-numbers-allegedly-put-on-sale-online/42267>  
 150 <https://www.thestar.com.my/business/business-news/2023/11/29/malaysia039s-3q-e-commerce-income-rises-54-y-o-y-to-rm2895bil---dosm>  
 151 <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2fb40e1d-8632-47ce-94f8-17fbe64e6f16>  
 152 <https://www.chubb.com/content/dam/chubb-sites/chubb-com/my-en/campaign/my-sme-cyber-report-2019-download/documents/pdf/chubb-my-sme-cyber-preparedness-report-2019.pdf>  
 153 <https://voi.id/en/technology/311526>  
 154 [https://www.cisco.com/c/dam/global/en\\_hk/assets/pdfs/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_hk/assets/pdfs/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf)  
 155 <https://asean.org/wp-content/uploads/2023/11/Definition-of-MSME-in-ASEAN-Member-States.pdf>  
 156 <https://www3.investindonesia.go.id/en/why-invest/indonesia-economic-update/making-indonesia-4.0-indonesias-strategy-to-enter-the-4th-generation-of-ind#:~:text=The%20implementation%20of%20Industry%204.0%20aims%20to%20achieve%20the%20great,GDP%20to%20R%26D%20and%20technology>  
 157 <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-109-the-state-of-indonesias-digital-economy-in-2022-by-si-wage-dharma-negara-and-astrid-meilasari-sugiana/>  
 158 <https://www.adb.org/sites/default/files/event/772211/files/session-1-nyoman-adhiarna-rev.pdf>  
 159 <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/consumer-business/sea-cb-indonesia-consumer-insights-2020.pdf>  
 160 <https://ugm.ac.id/en/news/cyber-attacks-on-msmes-pose-threat-to-national-economy/>  
 161 <https://www.dai.com/our-work/solutions/digital-acceleration-solutions/msme-study>  
 162 <https://www.adb.org/sites/default/files/event/772211/files/session-1-nyoman-adhiarna-rev.pdf>  
 163 <https://voi.id/fr/teknologi/315649>  
 164 <https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/>  
 165 <https://www.cyfirma.com/outofband/the-changing-cyber-threat-landscape-southeast-asia/>  
 166 <https://www.statista.com/topics/11732/cybersecurity-and-cybercrime-in-indonesia/#topicOverview>  
 167 Ibid.  
 168 <https://www.cloudflare.com/en-gb/lp/2023apjcsurvey/download/>  
 169 Ibid.  
 170 <https://www.dlapiperdataprotection.com/index.html?t=law&c=ID#:~:text=The%20PDP%20Law%20provides%20personal,data%20processor>  
 171 [https://en.mkri.id/news/details/2023-02-13/Govt:\\_Law\\_on\\_Personal\\_Data\\_Protection\\_Provides\\_Legal\\_Protection](https://en.mkri.id/news/details/2023-02-13/Govt:_Law_on_Personal_Data_Protection_Provides_Legal_Protection)  
 172 Ibid.  
 173 <https://ekon.go.id/publikasi/detail/4065/coordinating-minister-airlangga-government-continues-to-encourage-strengthening-economic-foundations-by-establishing-digital-transformation-of-msmes-as-one-of-the-priorities>  
 174 <https://www.dai.com/uploads/final-msme-reports/indonesia-country-brief.pdf>  
 175 Ibid.  
 176 <https://ugm.ac.id/en/news/cyber-attacks-on-msmes-pose-threat-to-national-economy/>  
 177 <https://opengovasia.com/indonesia-to-digitalise-one-million-msmes-thousands-of-peoples-markets/>  
 178 <https://www.adb.org/sites/default/files/event/772211/files/session-1-nyoman-adhiarna-rev.pdf>  
 179 [https://www.researchgate.net/publication/367283484\\_The\\_Effect\\_of\\_MSMEs\\_Go-Online\\_and\\_Knowledge-Based\\_Dynamic\\_Capability\\_Towards\\_MSMEs\\_Resilience\\_During\\_COVID-19\\_Pandemic\\_in\\_Indonesia](https://www.researchgate.net/publication/367283484_The_Effect_of_MSMEs_Go-Online_and_Knowledge-Based_Dynamic_Capability_Towards_MSMEs_Resilience_During_COVID-19_Pandemic_in_Indonesia)  
 180 Ibid.  
 181 <https://www.statista.com/statistics/1336051/indonesia-share-of-informal-employment/>  
 182 Expert interview, March 13, 2024.  
 183 <https://www.dai.com/uploads/final-msme-reports/indonesia-country-brief.pdf>  
 184 <https://en.dailysocial.id/post/tren-digitalisasi-umkm-di-indonesia-2023-tantangan-dan-peluang>  
 185 <https://www.statista.com/statistics/869700/indonesia-top-10-e-commerce-sites/>  
 186 <https://www.kompas.id/baca/gaya-hidup/2021/03/22/umkm-jadi-target-serangan-siber>  
 187 Ibid.  
 188 Ibid.  
 189 <https://www.liputan6.com/teknologi/read/5535580/penipuan-baru-phishing-targetkan-bisnis-kecil-dan-menengah?page=3>  
 190 <https://indonesiabusinesspost.com/risks-opportunities/ensign-infosecurity-2022-report-reveals-vulnerable-sectors-in-indonesia-amid-increasing-cyber-security-threats/>  
 191 [https://www.kompasiana.com/shadowname6142/634fec464addee6be54b0112/badai-cyber-attack-bidik-umkm-ri-bertahan-atau-ambruk?page=2&page\\_images=1](https://www.kompasiana.com/shadowname6142/634fec464addee6be54b0112/badai-cyber-attack-bidik-umkm-ri-bertahan-atau-ambruk?page=2&page_images=1)  
 192 <https://voi.id/en/technology/311526>  
 193 <https://www.cnbcindonesia.com/research/20240513235221-128-537775/modus-penipuan-sering-makan-korban-link-via-whatsapp-pinjol-illegal>  
 194 Ibid.  
 195 <https://www.liputan6.com/regional/read/5561113/modus-kejahatan-siber-mengintai-umkm-kominfo-beri-edukasi?page=2>  
 196 <https://medium.com/@asliriid/e-commerce-fraud-in-indonesia-865d0b595e8e>  
 197 Interview, The Asia Foundation, Indonesia, May 29, 2024.  
 198 <https://relawantik.or.id/>

199 <https://www.kominfo.go.id/>

200 <https://www.adb.org/sites/default/files/event/772211/files/session-1-nyoman-adhiarna-rev.pdf>

201 <https://www.bssn.go.id/edukasi-dan-literasi/>

202 <https://patrolisiber.id/en>

203 <https://relawantik.or.id/>

204 <https://www.mercycorps.or.id/program/micromentor-indonesia>

205 <https://www.cert.or.id/beranda/en/>

206 <https://voi.id/fr/teknologi/315649>

207 Expert interview, March 13, 2024.

208 <https://www.dai.com/uploads/final-msme-reports/indonesia-country-brief.pdf>

209 <https://www.statista.com/statistics/1338003/japan-number-private-small-and-medium-sized-enterprises-by-industry/#:-:text=In%202016%2C%20over%20623%20thousand,85%20percent%20were%20small%20enterprises>

210 <https://www.similarweb.com/top-apps/google/japan/>

211 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

212 [https://ebrary.net/212203/computer\\_science/japan#106845](https://ebrary.net/212203/computer_science/japan#106845)

213 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

214 <https://www.smrj.go.jp/english/about/target.html>

215 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

216 <https://www.japantimes.co.jp/news/2023/04/25/business/japan-cybersecurity-problem/>

217 <https://www.cybereason.co.jp/blog/sme/10686/>

218 <https://datareportal.com/reports/digital-2023-japan#:-:text=Japan's%20internet%20penetration%20rate%20stood,percent>

219 <https://openjicareport.jica.go.jp/pdf/12363800.pdf>

220 <https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail113>

221 Expert interview, January 30, 2024.

222 <https://www.eu-japan.eu/sites/default/files/publications/docs/Digital-Transformation-Japan-Assessing-opportunities-forEU-SMEs.pdf>

223 Expert interview, February 14, 2024.

224 [https://www8.cao.go.jp/cstp/english/society5\\_0/index.html](https://www8.cao.go.jp/cstp/english/society5_0/index.html)

225 <https://www.eu-japan.eu/sites/default/files/publications/docs/Digital-Transformation-Japan-Assessing-opportunities-forEU-SMEs.pdf>

226 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

227 <https://www.japantimes.co.jp/news/2023/04/25/business/japan-cybersecurity-problem/>

228 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

229 Ibid.

230 <https://www.dataguidance.com/jurisdiction/japan>

231 [https://ebrary.net/212203/computer\\_science/japan#106845](https://ebrary.net/212203/computer_science/japan#106845)

232 <https://www.weforum.org/agenda/2024/04/how-can-japan-navigate-digital-transformation-ahead-of-a-2025-digital-cliff/>

233 <https://www.smrj.go.jp/english/about/>

234 <https://www.oecd.org/cfe/smes/japan.pdf>

235 Ibid.

236 <https://www.worldeconomics.com/Informal-Economy/Japan.aspx#:-:text=The%20size%20of%20Japan's%20informal,billion%20at%20GDP%20PPP%20levels>

237 <https://www.imf.org/en/Blogs/Articles/2020/04/30/blog043020-a-new-deal-for-informal-workers-in-asia>

238 <https://www.jil.go.jp/english/jli/documents/2022/40-00.pdf>

239 <https://www.japanbuzz.info/social-media-in-japan/>

240 Ibid.

241 <https://www.smejapan.com/business-news/ecommerce-unleashed-fueling-growth-in-japans-smes/>

242 Ibid.

243 <https://english.kyodonews.net/news/2024/02/be5eff25bf96-police-say-no-of-cyber-scams-in-japan-up-8-in-2023-most-in-10-yrs.html>

244 <https://it-column.mjeinc.co.jp/archives/2796>

245 Ibid.

246 Ibid.

247 Expert interview, January 30, 2024.

248 <https://www.japantimes.co.jp/news/2023/04/25/business/japan-cybersecurity-problem/>

249 [https://www.meti.go.jp/english/press/2020/1228\\_001.html](https://www.meti.go.jp/english/press/2020/1228_001.html)

250 <https://www.nisc.go.jp/eng/index.html>

251 <https://www.ppc.go.jp/en/>

252 <https://www.ipa.go.jp/en/index.html>

253 <https://it-column.mjeinc.co.jp/archives/2796>

254 <https://www.ipa.go.jp/en/index.html>

255 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

256 <https://www.eu-japan.eu/sites/default/files/publications/docs/Digital-Transformation-Japan-Assessing-opportunities-forEU-SMEs.pdf>

257 <https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail113>

258 <https://www.japantimes.co.jp/news/2023/07/13/national/japan-cybersecurity-improvements-ransomware/>

259 Ibid.

260 <https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/>

261 Ibid.

262 <https://www.statista.com/statistics/1223066/south-korea-small-and-medium-enterprises-number/>

263 <https://www.similarweb.com/top-apps/google/korea-republic-of/>

264 <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=19&bbsSeqNo=94&nttSeqNo=3183831&searchOpt=ALL&searchTxt=>

265 <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>

266 <https://biz.chosun.com/it-science/ict/2022/10/13/XOXSNJWOKVBBJMEOEHMINKI23E/>

267 <https://www.mss.go.kr/site/eng/01/2010200000002019110628.jsp>

268 <https://www.law.go.kr/lsInfoP.do?lsiSeq=238565&urlMode=engLsInfoR&viewCls=engLsInfoR#0000>

269 [https://www.imd.org/wp-content/uploads/2023/12/Digital\\_2023.pdf](https://www.imd.org/wp-content/uploads/2023/12/Digital_2023.pdf)

270 <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>

271 <https://www.statista.com/topics/9530/cyber-security-in-south-korea/#topicOverview>

272 Ibid.

273 <https://www.cyberlands.io/topsecuritybreachessouthkorea>

274 <https://www.hankyung.com/article/202401263175Y>

275 <https://www.kisia.or.kr/bucket/uploads/2022/04/14/2021%EB%85%84%20%EC%AO%95%EB%B3%B4%EB%B3%B4%ED%98%B8%20%EC%8B%A4%ED%83%9C%EC%A1%BO%EC%82%AC%20%EB%B3%B4%EA%B3%AO%EC%84%9C.pdf>

276 Ibid.

277 <https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf>

278 Ibid.

279 <https://worldpopulationreview.com/country-rankings/internet-speeds-by-country>

280 <https://datareportal.com/reports/digital-2023-south-korea>

281 <https://iclg.com/practice-areas/digital-business-laws-and-regulations/korea>

282 <https://www.statista.com/topics/9530/cyber-security-in-south-korea/#topicOverview>

283 Ibid.

284 <https://iclg.com/practice-areas/digital-business-laws-and-regulations/korea>

285 <https://www.itu.int/epublications/publication/D-STR-GCl.01-2021-HTML-E>

286 [https://ccdcoe.org/uploads/2018/10/South-Korea\\_English-National-Cybersecurity-Strategy-03-April-2019\\_English-1.pdf](https://ccdcoe.org/uploads/2018/10/South-Korea_English-National-Cybersecurity-Strategy-03-April-2019_English-1.pdf)

287 <https://www.statista.com/topics/10036/smes-in-south-korea/#topicOverview>

288 <https://www.mss.go.kr/site/smba/foffice/ex/statDB/MainSubStat.do>

289 <https://www.mss.go.kr/site/eng/02/2020200000002019110610.jsp>

290 Ibid.

291 <https://www.mss.go.kr/site/smba/foffice/ex/statDB/MainSubStat.do>

292 <https://www.worldeconomics.com/Informal-Economy/Korea.aspx>

293 <https://jmagazine.joins.com/forbes/view/338788>

294 <https://pulse.mk.co.kr/news/english/10844296>

295 <https://www.reuters.com/technology/south-korea-regulator-may-sanction-meta-over-marketplace-say-media-reports-2024-03-08/>

296 Interview, The Asia Foundation, Korea, May 29, 2024.

297 [https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=d7db99ea58864ade8df2a0833672f3ab&convType=html&convLocale=ko\\_KR&contextPath=/SynapDocViewServer/](https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=d7db99ea58864ade8df2a0833672f3ab&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/)

298 [https://www.kisa.or.kr/post/fileDownload?menuSeq=201&postSeq=12065&attachSeq=1&lang\\_type=KO\\_000000\\_0000\\_000000\\_00\\_0000\\_00\\_00\\_00.pdf](https://www.kisa.or.kr/post/fileDownload?menuSeq=201&postSeq=12065&attachSeq=1&lang_type=KO_000000_0000_000000_00_0000_00_00_00.pdf)

299 <https://www.statista.com/statistics/1228659/south-korea-online-hacking-cases-by-type/>

300 <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=19&bbsSeqNo=94&nttSeqNo=3183831&searchOpt=ALL&searchTxt=>

301 <https://biz.chosun.com/it-science/ict/2022/10/13/XOXSNJWOKVBBJMEOEHMINKI23E/>

302 <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=19&bbsSeqNo=94&nttSeqNo=3183831&searchOpt=ALL&searchTxt=>

303 Ibid.

304 <https://www.m-i.kr/news/articleView.html?idxno=1041883>

305 <https://kisia.or.kr/bucket/uploads/2022/04/14/2021%EB%85%84%20%EC%AO%95%EB%B3%B4%EB%B3%B4%ED%98%B8%20%EC%8B%A4%ED%83%9C%EC%A1%BO%EC%82%AC%20%EB%B3%B4%EA%B3%AO%EC%84%9C.pdf>

306 Interview, Professor Kim Chungbuk, National University, April 18, 2024.

307 <https://www.krcert.or.kr/kr/subPage.do?menuNo=205004>

308 <https://www.krcert.or.kr/kr/subPage.do?menuNo=205007>

309 <https://www.krcert.or.kr/kr/bbs/list.do?menuNo=205021&bbsId=B000127>

310 <https://www.ncsc.go.kr:4018/eng/mainPage.do>

311 <https://www.pipc.go.kr/np/>

312 <https://www.msit.go.kr/eng/>

313 <https://www.mss.go.kr/site/eng/main.do>

314 <https://www.kbiz.or.kr/en/index/index.do>

315 <https://www.kisia.or.kr/introduction/greeting/>

316 <https://www.cyberlands.io/topsecuritybreachessouthkorea>

317 [https://dl.nanet.go.kr/search/searchInnerDetail.do?searchType=INNER\\_SEARCH&resultType=INNER\\_SEARCH\\_DETAIL&searchMethod=L&searchClass=S&controlNo=KDMT1202100005289&queryText=&zone=&fieldText=&prevQueryText=TM+620+-21-48%3ACALL\\_NO%3AAND&prevPubYearFieldText=&languageCode=&synonymYn=&refineSearchYn=&pageNum=&pageSize=&orderBy=&topMainMenuCode=&topSubMenuCode=&totalSize=3&totalSizeByMenu=3&seqNo=&hanjaYn=Y&knowPub=&isdb=&isdbsvc=&ttt=&down=&frgnLangMtrLYn=&targetLangCode=&checkedDbIdList=&baseDbId=&selectedDbIndexIdList=&caller=&asideState=&dpBranch=ALL&journalKind=&selZone=CALL\\_NO&searchQuery=TM+620+-21-48](https://dl.nanet.go.kr/search/searchInnerDetail.do?searchType=INNER_SEARCH&resultType=INNER_SEARCH_DETAIL&searchMethod=L&searchClass=S&controlNo=KDMT1202100005289&queryText=&zone=&fieldText=&prevQueryText=TM+620+-21-48%3ACALL_NO%3AAND&prevPubYearFieldText=&languageCode=&synonymYn=&refineSearchYn=&pageNum=&pageSize=&orderBy=&topMainMenuCode=&topSubMenuCode=&totalSize=3&totalSizeByMenu=3&seqNo=&hanjaYn=Y&knowPub=&isdb=&isdbsvc=&ttt=&down=&frgnLangMtrLYn=&targetLangCode=&checkedDbIdList=&baseDbId=&selectedDbIndexIdList=&caller=&asideState=&dpBranch=ALL&journalKind=&selZone=CALL_NO&searchQuery=TM+620+-21-48)

318 Expert interview, January 29, 2024.

319 <https://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/profile-and-importance-to-the-economy>

320 <https://www.meltwater.com/en/blog/social-media-statistics-malaysia>

321 <https://www.malaymail.com/news/malaysia/2022/11/28/whatsapp-data-leak-11-million-malaysian-phone-numbers-allegedly-put-on-sale-online/42267>

322 <https://www.thestar.com.my/business/business-news/2023/11/29/malaysia039s-3q-e-commerce-income-rises-54-y-o-y-to-rm2895bil---dosm>

323 <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2fb40e1d-8632-47ce-94f8-17f6e64e6f16>

324 <https://www.chubb.com/content/dam/chubb-sites/chubb-com/my-en/campaign/my-sme-cyber-report-2019-download/documents/pdf/chubb-my-sme-cyber-preparedness-report-2019.pdf>

325 <https://news.microsoft.com/en-my/2018/07/12/cybersecurity-threats-to-cost-organizations-in-malaysia-us12-2-billion-in-economic-losses/>

326 <https://www.linkedin.com/pulse/cybersecurity-smes-crucial-investment-sustainable-karuppayah-zbsqf>

327 <https://asean.org/wp-content/uploads/2023/11/Definition-of-MSME-in-ASEAN-Member-States.pdf>

328 <https://datareportal.com/reports/digital-2023-malaysia>

329 <https://www.itu.int/epublications/publication/D-STR-GCl.01-2021-HTML-E>

330 <https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomware-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insights-from-check-points-latest-security-re/>

331 <https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us175-trillion-in-economic-losses/>

332 <https://theedgemaalaysia.com/article/84-malaysia-smes-affected-cyber-incidents-past-year-%E2%80%94-chubb>

333 [https://www.mcmc.gov.my/skmmgovmy/media/General/DSRG\\_no9\\_2021/4-Track-3\\_UiTM\\_Dr-Fazlida.pdf](https://www.mcmc.gov.my/skmmgovmy/media/General/DSRG_no9_2021/4-Track-3_UiTM_Dr-Fazlida.pdf)

334 <https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf>



335 Ibid.

336 <https://datareportal.com/reports/digital-2023-malaysia>

337 <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>

338 <https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomware-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insights-from-check-points-latest-security-re/>

339 <https://www.pwc.com/my/en/services/assurance/pdpa.html>

340 <https://www.nacsa.gov.my/about-us.php>

341 <https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf>

342 <https://surfshark.com/research/study/data-breach-statistics-q3-2023>

343 <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b>

344 <https://www.kkd.gov.my/en/info-korporat/pengenalan/acts/233-kkd-news/19327-cyber-security-matrix-to-focus-on-four-areas-to-assist-smes>

345 <https://www.oecd-ilibrary.org/sites/3bc2915c-en/index.html?itemId=/content/component/3bc2915c-en>

346 <https://elibrary.worldbank.org/doi/abs/10.1596/37137>

347 Ibid.

348 [https://www.researchgate.net/publication/296700944\\_Characteristics\\_of\\_Informal\\_Micro-Entrepreneurs\\_in\\_Malaysia](https://www.researchgate.net/publication/296700944_Characteristics_of_Informal_Micro-Entrepreneurs_in_Malaysia)

349 Interview, The Asia Foundation, Malaysia, May 24, 2024.

350 <https://www.kkd.gov.my/en/public/news/19611-protecting-sme-from-cyber-attacks>

351 <https://www.oecd-ilibrary.org/sites/ea9dc78b-en/index.html?itemId=/content/component/ea9dc78b-en>

352 [https://www.krinstitute.org/assets/contentMS/img/template/editor/20201228\\_View\\_InformalityGrowth\\_FINAL2.pdf](https://www.krinstitute.org/assets/contentMS/img/template/editor/20201228_View_InformalityGrowth_FINAL2.pdf)

353 <https://documents1.worldbank.org/curated/en/099022124104025708/pdf/P1810931e39cc10471b0a511ed680a40226.pdf>

354 <https://openknowledge.worldbank.org/server/api/core/bitstreams/d2007fee-9574-5f60-9a21-b33e4a6bbd67/content>

355 <https://www.thestar.com.my/business/business-news/2023/11/29/malaysia039s-3q-e-commerce-income-rises-54-y-o-y-to-rm2895bil---dosm>

356 <https://www.meltwater.com/en/blog/social-media-statistics-malaysia>

357 <https://platform.mdec.com.my/cmscdn/v1.aspx?GUID=cf39ff90-6bd1-4884-9ac1-ca55c021c4f0&file=BDAI%20Booklet.pdf>

358 <https://www.malaymail.com/news/malaysia/2022/11/28/whatsapp-data-leak-11-million-malaysian-phone-numbers-allegedly-put-on-sale-online/42267>

359 <https://www.straitstimes.com/singapore/data-of-alleged-26m-carousell-accounts-being-sold-on-dark-web-hacking-forums>

360 [https://www.researchgate.net/publication/361865986\\_Attributes\\_impacting\\_cybersecurity\\_policy\\_development\\_An\\_evidence\\_from\\_seven\\_nations](https://www.researchgate.net/publication/361865986_Attributes_impacting_cybersecurity_policy_development_An_evidence_from_seven_nations)

361 <https://platform.mdec.com.my/cmscdn/v1.aspx?GUID=cf39ff90-6bd1-4884-9ac1-ca55c021c4f0&file=BDAI%20Booklet.pdf>

362 <https://www.chubb.com/content/dam/chubb-sites/chubb-com/my-en/campaign/my-sme-cyber-report-2019-download/documents/pdf/chubb-my-sme-cyber-preparedness-report-2019.pdf>

363 The Asia Foundation Malaysia Office (24 May 2024) Interview.

364 <https://www.malaymail.com/news/malaysia/2023/10/13/budget-2024-govt-allocates-rm60m-to-develop-5g-cyber-security-testing-framework/96094>

365 <https://opengovasia.com/2023/12/20/cybersecurity-malaysia-unveils-strategic-roadmap/>

366 <https://www.thestar.com.my/news/nation/2023/11/25/cabinet-nod-for-cybersecurity-law>

367 <https://www.nacsa.gov.my/act854.php>

368 <https://www.cybersecurity.my/pgpks/>

369 <https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf>

370 <https://www.malaysiakini.com/announcement/699999>

371 <https://gulfnews.com/business/corporate-news/cybersecurity-malaysia-partners-with-ctm360-to-fortify-cybersecurity-measures-in-malaysia-1.1709108832494>

372 <https://www.nst.com.my/business/corporate/2024/01/1006008/public-bank-maxis-jointly-promote-digital-adoption-among-smes>

373 <https://www.eccouncil.org/ec-council-in-news/ec-council-pikom-and-peoplelogy-group-spearhead-cybersecurity-skills-revolution-for-malaysian-smes/>

374 <https://www.pmo.gov.my/2024/03/the-grand-opening-of-cybersecurity-center-of-excellence-ccoe/>

375 <https://new.apu.edu.my/apu-managing-smes-cybersecurity-risks-through-cybersecurity-as-a-service-caas>

376 [https://www.researchgate.net/publication/360439361\\_The\\_role\\_of\\_cybersecurity\\_and\\_policy\\_awareness\\_in\\_shifting\\_employee\\_compliance\\_attitudes\\_Building\\_supply\\_chain\\_capabilities](https://www.researchgate.net/publication/360439361_The_role_of_cybersecurity_and_policy_awareness_in_shifting_employee_compliance_attitudes_Building_supply_chain_capabilities)

377 <https://www.pwc.com/mu/Managing-the-Impact-of-COVID-19-Mauritius-on-Cyber-security.pdf>

378 [https://www.researchgate.net/publication/357412408\\_Cyber\\_Security\\_Culture\\_towards\\_Digital\\_Marketing\\_Communications\\_among\\_Small\\_and\\_Medium-Sized\\_SME\\_Entrepreneurs](https://www.researchgate.net/publication/357412408_Cyber_Security_Culture_towards_Digital_Marketing_Communications_among_Small_and_Medium-Sized_SME_Entrepreneurs)

379 <https://ieeexplore.ieee.org/document/9703991>

380 <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9989381>

381 [https://ari.uitm.edu.my/images/2022/icfc/eProceedings\\_ICFC2022.pdf](https://ari.uitm.edu.my/images/2022/icfc/eProceedings_ICFC2022.pdf)

382 <https://www.chubb.com/content/dam/chubb-sites/chubb-com/my-en/campaign/my-sme-cyber-report-2019-download/documents/pdf/chubb-my-sme-cyber-preparedness-report-2019.pdf>

383 <https://www.sciencedirect.com/science/article/abs/pii/S0167404822002863>

384 <https://karandaaz.com.pk/blog/unlocking-micro-small-medium-enterprise-msme-potential-pakistan/>

385 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b1de7e>

386 <https://www.similarweb.com/top-websites/pakistan/e-commerce-and-shopping/>

387 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)

388 Expert interview, April 3, 2024.

389 <https://www.brecorder.com/news/40289669>

390 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b1de7e>

391 <https://msmepolicy.unescap.org/definitions-msmes>

392 [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf)

393 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)

394 <https://karandaaz.com.pk/blog/unlocking-micro-small-medium-enterprise-msme-potential-pakistan/>

395 <https://www.brecorder.com/news/40099374>

396 <https://tribune.com.pk/story/2449373/pakistans-undocumented-economy>

397 <https://smeda.org/phocadownload/Publications/SMEDA%20%20ADB%20WE%20Diagnostic%20Summary.pdf>

398 <https://library.fes.de/pdf-files/bueros/pakistan/14909.pdf>

399 <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/08/Understanding-women-micro-entrepreneurs-use-of-mobile-phones-for-business.pdf>

400 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
401 Expert interview, April 3, 2024.  
402 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)  
403 <https://www.brecorder.com/news/40289669>  
404 Expert interview, April 3, 2024.  
405 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
406 <https://datareportal.com/reports/digital-2023-pakistan>  
407 <https://tribune.com.pk/story/2449373/pakistans-undocumented-economy>  
408 <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/08/Understanding-women-micro-entrepreneurs-use-of-mobile-phones-for-business.pdf>  
409 [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf)  
410 <https://moitt.gov.pk/SitelImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>  
411 <https://www.dawn.com/news/1636817>  
412 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
413 <https://www.brecorder.com/news/40289669>  
414 <https://datareportal.com/reports/digital-2023-pakistan>  
415 Expert interview, April 3, 2024.  
416 <https://www.brecorder.com/news/40289669>  
417 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
418 <https://datareportal.com/reports/digital-2024-pakistan>  
419 Ibid.  
420 <https://karandaaz.com.pk/blog/unlocking-micro-small-medium-enterprise-msme-potential-pakistan/>  
421 <https://www.brecorder.com/news/40099374>  
422 <https://www.betterthancash.org/news/merchant-digitization-emerges-as-one-key-driver-for-pakistans-inclusive-economic-growth-in-un-report>  
423 Ibid.  
424 <https://www.brecorder.com/news/40099374>  
425 <https://tribune.com.pk/story/2449373/pakistans-undocumented-economy>  
426 Ibid.  
427 <https://library.fes.de/pdf-files/bueros/pakistan/14909.pdf>  
428 <https://smeda.org/phocadownload/Publicatoins/SMEDA%20%20ADB%20WE%20Diagnostic%20Summary.pdf>  
429 <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/08/Understanding-women-micro-entrepreneurs-use-of-mobile-phones-for-business.pdf>  
430 Ibid.  
431 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
432 Ibid.  
433 <https://aag-it.com/the-latest-cyber-crime-statistics/>  
434 Expert interview, April 3, 2024.  
435 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)  
436 Expert interview, April 3, 2024.  
437 <https://www.brecorder.com/news/40289669>  
438 Expert interview, April 3, 2024.  
439 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)  
440 <https://medium.com/@kingwillie418/enabling-internet-privacy-and-security-amidst-pakistan-cyber-threats-a6969b11de7e>  
441 <https://www.brecorder.com/news/40269072/smes-business-community-seeks-sound-cyber-security-system>  
442 <https://www.dawn.com/news/1636817>  
443 <https://www.brecorder.com/news/40269072/smes-business-community-seeks-sound-cyber-security-system>  
444 [https://pta.gov.pk/assets/media/cyber\\_security\\_strategy\\_telecom\\_sector\\_2023\\_2028\\_11-12-2023.pdf](https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_11-12-2023.pdf)  
445 <https://www.nation.com.pk/04-May-2024/national-cyber-crimes-investigation-agency-notified-to-deal-with-offences-under-peca-act>  
446 <https://www.pta.gov.pk/>  
447 <https://www.dawn.com/news/1636817>  
448 <https://www.pakcert.org/aboutus.html>  
449 <https://moitt.gov.pk/SitelImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>  
450 Ibid.  
451 <https://www.ivint.org/pakistans-cyber-woes/>  
452 Ibid.  
453 <https://www.dti.gov.ph/resources/msme-statistics/#:~:text=2022%20Philippine%20MSME%20Statistics&text=The%202022%20List%20of%20Establishments,0.41%25>  
454 Expert interview, March 13, 2024.  
455 <https://www.tmgogroup.asia/the-philippines-b2c-ecommerce-landscape/#:~:text=1,Shopee%20PH&text=With%20upwards%20of%2046%25%20of,30%20million%20visits%20over%20Lazada>  
456 <https://www.cyfirma.com/research/philippines-threat-overview/>  
457 Expert interview, March 13, 2024.  
458 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>  
459 <https://blog.semaphore.co/2023/07/17/sms-scams-philippines/>  
460 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>  
461 [https://serp-p.pids.gov.ph/feature/public/index-view?fearedtype\\_id=1&slug=micro-small-and-medium-enterprises](https://serp-p.pids.gov.ph/feature/public/index-view?fearedtype_id=1&slug=micro-small-and-medium-enterprises)  
462 <https://www.cyfirma.com/research/philippines-threat-overview/>  
463 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>  
464 <https://www.imperva.com/cyber-threat-attack-map/>  
465 <https://blog.semaphore.co/2023/07/17/sms-scams-philippines/>  
466 <https://mb.com.ph/2023/3/31/digital-fraud-attempts-in-ph-decline-18-report>  
467 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>  
468 Expert interview, March 13, 2024.  
469 <https://www.philippinesmarketresearch.com/insight/digitalization-of-msme-in-the-philippines>  
470 <https://www.dti.gov.ph/resources/msme-statistics/#:~:text=2022%20Philippine%20MSME%20Statistics&text=The%202022%20List%20of%20Establishments,0.41%25>

471 <https://www.dti.gov.ph/archives/news-archives/ph-rises-up-rank-56th-global-innovation-index-2023/>

472 <https://ycpsolidiance.com/article/msme-ecommerce-philippines>

473 <https://opengovasia.com/empowering-msme-innovation-with-tech-in-the-philippines/>

474 Talipapa: In the Philippines, a small market, usually informal, where vendors sell wet goods such as meats, vegetables, and fish.

475 <https://metromanila.politiko.com.ph/2023/02/13/qc-govt-to-open-the-countrys-first-market-one-stop-shop-system/>

476 <https://www.cyfirma.com/research/philippines-threat-overview/>

477 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>

478 <https://cicc.gov.ph/news/shopping-scam-rate-in-ph-hits-36-highest-in-11-asian-countries/>

479 <https://www.imperva.com/cyber-threat-attack-map/>

480 <https://www.cyfirma.com/research/philippines-threat-overview/>

481 <https://www.imperva.com/cyber-threat-attack-map/>

482 <https://www.cloudflare.com/en-gb/lp/2023apjcsurvey/download/>

483 Expert interview, March 13, 2024.

484 <https://www.eccinternational.com/ra-10173-data-privacy-summary/>

485 Ibid.

486 <https://www.philippinesmarketresearch.com/insight/digitalization-of-msme-in-the-philippines>

487 <https://www.dti.gov.ph/resources/msme-statistics/#:~:text=2022%20Philippine%20MSME%20Statistics&text=The%202022%20List%20of%20Establishments,0.41%25>

488 Ibid.

489 <https://www.philippinesmarketresearch.com/insight/digitalization-of-msme-in-the-philippines>

490 <https://www.dti.gov.ph/archives/news-archives/ph-rises-up-rank-56th-global-innovation-index-2023/>

491 <https://ycpsolidiance.com/article/msme-ecommerce-philippines>

492 <https://www.worldeconomics.com/National-Statistics/Informal-Economy/Philippines.aspx#:~:text=The%20size%20of%20Philippines's%20informal,billion%20at%20GDP%20PPP%20levels>

493 <https://thediplomat.com/2023/04/in-the-philippines-covid-19-is-still-taking-a-toll-on-the-informal-economy/#:~:text=The%20World%20Economics%20website%20calculates,into%20wealth%20for%20most%20vendors>

494 Ibid.

495 <https://www.philstar.com/opinion/2023/12/12/2318241/informal-workers-path-inclusive-growth-and-prosperity>

496 <https://thediplomat.com/2023/04/in-the-philippines-covid-19-is-still-taking-a-toll-on-the-informal-economy/#:~:text=The%20World%20Economics%20website%20calculates,into%20wealth%20for%20most%20vendors>

497 [https://legacy.senate.gov.ph/lis/bill\\_res.aspx?congress=19&q=SBN-338](https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-338)

498 <https://www.philstar.com/opinion/2023/12/12/2318241/informal-workers-path-inclusive-growth-and-prosperity>

499 Expert interview, March 13, 2024.

500 <https://www.philippinesmarketresearch.com/insight/digitalization-of-msme-in-the-philippines>

501 <https://www.tmogroup.asia/the-philippines-b2c-ecommerce-landscape/#:~:text=1,Shopee%20PH&text=With%20upwards%20of%2046%25%20of,30%20million%20visits%20over%20Lazada>

502 Ibid.

503 Expert interview, March 13, 2024.

504 <https://asia.nikkei.com/Business/Retail/Philippines-emerges-as-Asia-s-epicenter-for-online-shopping-scams2#:~:text=The%20shopping%20scam%20rate%20in,a%20lucrative%20market%20for%20scammers>

505 <https://www.bworldonline.com/bw-launchpad/2023/08/30/542184/tight-budgets-no-barrier-for-smes-cybersecurity-expert/>

506 Ibid.

507 Expert interview, March 13, 2024.

508 <https://manilastandard.net/?p=314315071>

509 Expert interview, March 13, 2024.

510 <https://www.sunstar.com.ph/bacolod/feature/smell-something-phishy-the-rise-of-phishing-scams>

511 <https://mb.com.ph/2024/3/12/acer-philippines-reports-data-breach-in-third-party-vendor-system>

512 Expert interview, March 13, 2024.

513 Ibid.

514 Ibid.

515 <https://www.pna.gov.ph/articles/1207775>

516 Expert interview, March 13, 2024.

517 <https://opengovasia.com/empowering-msme-innovation-with-tech-in-the-philippines/>

518 Ibid.

519 <https://www.dti.gov.ph/regions/mimaropa/profile/#:~:text=The%20name%20is%20an%20acronym,municipalities%20that%20comprise%20the%20region>

520 <https://www.dti.gov.ph/regions/mimaropa/mimaropa-news/dti-mimaropa-unleashes-power-pinay-entrepreneurs-digital-space/>

521 [https://lawphil.net/statutes/repacts/ra2022/irr\\_11934\\_2022.html](https://lawphil.net/statutes/repacts/ra2022/irr_11934_2022.html)

522 <https://opinion.inquirer.net/166179/running-circles-around-sim-card-law>

523 <https://news.abs-cbn.com/news/2024/5/11/campaign-launched-vs-fraud-scams-2354>

524 <https://www.pna.gov.ph/articles/1194126>

525 <https://gonegosyo.ph/go-negosyo-event-opens-msmes-to-the-possibility-of-technology-at-digital-sign-up-now-2022/>

526 <https://cert.ph/about>

527 Expert interview, March 13, 2024.

528 Ibid.

529 Ibid.

530 <https://www.invoiceinterchange.com/key-2021-statistics-for-singapore-smes/>

531 <https://datareportal.com/reports/digital-2024-singapore>

532 <https://www.statista.com/statistics/869701/singapore-top-10-e-commerce-sites/>

533 <https://www.statista.com/statistics/1403675/singapore-rate-of-ransomware-attacks/>

534 <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>

535 [https://www.cisco.com/c/dam/global/en\\_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf)

536 <https://asean.org/wp-content/uploads/2023/11/Definition-of-MSME-in-ASEAN-Member-States.pdf>

537 <https://www.straitstimes.com/tech/tech-news/singapore-ranked-no-6-globally-for-having-most-number-of-exposed-databases>

538 [https://www.csa.gov.sg/docs/default-source/our-programmes/support-for-enterprises/sg-cyber-safe-programme/csa-singapore-cybersecurity-health-report-2023.pdf?sfvrsn=c611e1b\\_1](https://www.csa.gov.sg/docs/default-source/our-programmes/support-for-enterprises/sg-cyber-safe-programme/csa-singapore-cybersecurity-health-report-2023.pdf?sfvrsn=c611e1b_1)

539 <https://www.singstat.gov.sg/modules/infographics/economy>

540 Ibid.

541 [https://www.cisco.com/c/dam/global/en\\_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf)

542 [https://www.linkedin.com/posts/theedgesg\\_cybersecurity-techtrends-digitaldefence-activity-7183403622850785280-2Uma](https://www.linkedin.com/posts/theedgesg_cybersecurity-techtrends-digitaldefence-activity-7183403622850785280-2Uma)

543 [https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs\\_Towards\\_Cyber\\_Security\\_Distribution\\_Copy.pdf](https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs_Towards_Cyber_Security_Distribution_Copy.pdf)

544 <https://www.crowell.com/en/insights/client-alerts/landmark-amendments-to-singapores-cybersecurity-bill-re-interpreting-cii-to-bolster-national-cyber-resilience>

545 <https://www.imda.gov.sg/-/media/imda/files/infocomm-media-landscape/research-and-statistics/sgde-report/singapore-digital-economy-report-2023.pdf>

546 <https://datareportal.com/reports/digital-2023-singapore>

547 [https://www.csa.gov.sg/docs/default-source/our-programmes/support-for-enterprises/sg-cyber-safe-programme/csa-singapore-cybersecurity-health-report-2023.pdf?sfvrsn=c611e1b\\_1](https://www.csa.gov.sg/docs/default-source/our-programmes/support-for-enterprises/sg-cyber-safe-programme/csa-singapore-cybersecurity-health-report-2023.pdf?sfvrsn=c611e1b_1)

548 <https://www.statista.com/statistics/1403675/singapore-rate-of-ransomware-attacks/>

549 <https://www.straitstimes.com/tech/tech-news/singapore-ranked-no-6-globally-for-having-most-number-of-exposed-databases>

550 <https://media.armis.com/pdfs/rp-global-attack-surface-management-trends-challenges-en.pdf>

551 Ibid.

552 <https://www.csa.gov.sg/legislation/Cybersecurity-Act>

553 <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>

554 <https://www.darkreading.com/cyber-risk/singapore-cybersecurity-update-puts-cloud-providers-on-notice>

555 [https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-\(amendment\)-bill-15-2024.pdf?sfvrsn=1bbo5508\\_1](https://www.parliament.gov.sg/docs/default-source/bills-introduced/cybersecurity-(amendment)-bill-15-2024.pdf?sfvrsn=1bbo5508_1)

556 <https://www.singstat.gov.sg/modules/infographics/economy>

557 <https://www.adb.org/sites/default/files/publication/753486/asia-sme-monitor-2021-volume-1.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.adb.org%2Fsites%2Fdefault%2Ffiles%2Fpublication%2F753486%2Fasia>

558 [https://stats.mom.gov.sg/iMAS\\_PdfLibrary/mrsd\\_2020LabourForce\\_survey\\_findings.pdf#:~:text=URL%3A%20https%3A%2F%2Fstats.mom.gov.sg%2FiMAS\\_PdfLibrary%2Fmrsd\\_2020LabourForce\\_survey\\_findings.pdf%0AVisible%3A%20O%25%20](https://stats.mom.gov.sg/iMAS_PdfLibrary/mrsd_2020LabourForce_survey_findings.pdf#:~:text=URL%3A%20https%3A%2F%2Fstats.mom.gov.sg%2FiMAS_PdfLibrary%2Fmrsd_2020LabourForce_survey_findings.pdf%0AVisible%3A%20O%25%20)

559 <https://datareportal.com/reports/digital-2024-singapore>

560 <https://asme.org.sg/article/newsroom/132/5%20must-haves%20for%20SMEs%20to%20leverage%20social%20media>

561 <https://www.statista.com/statistics/869701/singapore-top-10-e-commerce-sites/>

562 <https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>

563 Ibid.

564 <https://twitter.com/RachelTobac/status/1568656397637947392>

565 <https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022>

566 <https://www.knowbe4.com/hubfs/Singapore-Cyber-Landscape-2022.pdf>

567 <https://www.channelnewsasia.com/singapore/deepfake-artificial-intelligence-sme-association-phishing-fraud-4225386>

568 [https://www.cisco.com/c/dam/global/en\\_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cybersecurity-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf)

569 <https://www.ntuclearninghub.com/cybersecurity-2023>

570 <https://www.csa.gov.sg/News-Events/speeches/2024/opening-address-by-mrs-josephine-teo--minister-for-communications-and-information-at-the-istari-charter-asia-pacific-cyber-congress-20-mar-2024>

571 [https://www.analysismason.com/contentassets/10b656cb8b27436b8b93fe83621f08bd/analysys\\_mason\\_sme\\_cyber\\_security\\_apr2022\\_rdmzO\\_ren04.pdf](https://www.analysismason.com/contentassets/10b656cb8b27436b8b93fe83621f08bd/analysys_mason_sme_cyber_security_apr2022_rdmzO_ren04.pdf)

572 Ibid.

573 [https://www.cisco.com/c/en\\_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html](https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html)

574 Ibid.

575 Ibid.

576 [https://www.analysismason.com/globalassets/x\\_migrated-media/media/analysys\\_mason\\_survey\\_security\\_inadequate\\_sep2019\\_ren042.pdf](https://www.analysismason.com/globalassets/x_migrated-media/media/analysys_mason_survey_security_inadequate_sep2019_ren042.pdf)

577 [https://www.cisco.com/c/en\\_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html](https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html)

578 [https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs\\_Towards\\_Cyber\\_Security\\_Distribution\\_Copy.pdf](https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs_Towards_Cyber_Security_Distribution_Copy.pdf)

579 [https://www.cisco.com/c/en\\_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html](https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html)

580 [https://klse.iinvestor.com/web/blog/detail/kianweiaritcles/2024-03-27-story-h-185470550-More\\_Singapore\\_SMEs\\_falling\\_prey\\_to\\_scams\\_even\\_as\\_many\\_of\\_them\\_turn\\_to\\_](https://klse.iinvestor.com/web/blog/detail/kianweiaritcles/2024-03-27-story-h-185470550-More_Singapore_SMEs_falling_prey_to_scams_even_as_many_of_them_turn_to_)

581 <https://www.smehorizon.com/what-can-singapores-smes-do-about-cyberattacks/>

582 [https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs\\_Towards\\_Cyber\\_Security\\_Distribution\\_Copy.pdf](https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs_Towards_Cyber_Security_Distribution_Copy.pdf)

583 <https://www.todayonline.com/singapore/hackers-leak-data-over-300000-k-box-members>

584 <https://www.todayonline.com/singapore/slack-security-measures-led-leak-k-box-customers-data>

585 <https://www.gobusiness.gov.sg/gobusiness-blog/cybersecurity-for-smes>

586 <https://www.csa.gov.sg/News-Events/Press-Releases/2024/csa-releases-key-findings-from-singapore-cybersecurity-health-report-2023>

587 Ibid.

588 <https://www.police.gov.sg/Advisories/Crime/Cybercrime>

589 <https://news.nus.edu.sg/nus-and-csa-to-establish-s20-million-cybersg-talent-innovation-and-growth-collaboration-centre-to-address-growing-demand-for-robust-cybersecurity-solutions/>

590 <https://www.aisp.sg/>

591 <https://www.ntu.edu.sg/crpo>

592 <https://www.singtel.com/business/products-services/cybersecurity/cyber-education>

593 <https://rulebook.sgx.com/rulebook/mainboard-rules>

594 <https://www.experian.com.sg/insights/experian-snapshot-study-identifies-singapore-sme-sector-vulnerability-indicators-leading-into-covid-19/>

595 [https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs\\_Towards\\_Cyber\\_Security\\_Distribution\\_Copy.pdf](https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs_Towards_Cyber_Security_Distribution_Copy.pdf)

596 Ibid.

597 [https://www.qbe.com.sg//media/singapore/files/sme%20research/2023/qbe%20sme%202023%20release\\_digitalisation\\_14%20mar\\_final\\_combined\\_003.pdf](https://www.qbe.com.sg//media/singapore/files/sme%20research/2023/qbe%20sme%202023%20release_digitalisation_14%20mar_final_combined_003.pdf)

598 [https://klse.iinvestor.com/web/blog/detail/kianweiaritcles/2024-03-27-story-h-185470550-More\\_Singapore\\_SMEs\\_falling\\_prey\\_to\\_scams\\_even\\_as\\_many\\_of\\_them\\_turn\\_to\\_](https://klse.iinvestor.com/web/blog/detail/kianweiaritcles/2024-03-27-story-h-185470550-More_Singapore_SMEs_falling_prey_to_scams_even_as_many_of_them_turn_to_)

599 <https://cybersecasia.net/news/smes-lower-level-of-cyber-vigilance-takes-the-limelight-in-cybersecurity-conference/>

600 <https://insights.frost.com/hubfs/Content%20Uploads/DGT/2023/OTHER/ISACA%20Key%20Points%20IG%2020231114.pdf?hsLang=en>

601 <https://futurecio.tech/state-of-it-risk-in-singapore/>



602 [https://www.cisco.com/c/en\\_sg/products/security/cybersecurity-for-smb-in-asia-pacific/index.html](https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smb-in-asia-pacific/index.html)

603 [https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs\\_Towards\\_Cyber\\_Security\\_Distribution\\_Copy.pdf](https://communications.sgtech.org.sg/publications/CybersecurityResearch2020/SMEs_Towards_Cyber_Security_Distribution_Copy.pdf)

604 Ibid.

605 Interview, The Asia Foundation, Singapore, January 23, 2024.

606 [http://www.statistics.gov.lk/Resource/en/Industry/Other\\_Tables\\_Reports/MSMEs\\_Report.pdf](http://www.statistics.gov.lk/Resource/en/Industry/Other_Tables_Reports/MSMEs_Report.pdf)

607 <https://datareportal.com/reports/digital-2023-sri-lanka#:~:text=There%20were%2014.58%20million%20internet%20users%20in%20Sri%20Lanka%20in,percent%20between%202022%20and%202023>

608 <https://datareportal.com/reports/digital-2023-sri-lanka>

609 <https://www.igi-global.com/article/a-study-of-cyber-security-issues-in-sri-lanka/257519>

610 <https://www.slideshare.net/slideshow/2022-ecommerce-report-sri-lanka/266212902>

611 <https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1>

612 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms\\_901205.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_901205.pdf)

613 [https://www.cbsl.gov.lk/sites/default/files/cbslweb\\_documents/publications/annual\\_report/2021/en/13\\_Box\\_04.pdf](https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/2021/en/13_Box_04.pdf)

614 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms\\_901205.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_901205.pdf)

615 Ibid.

616 <https://www.industry.gov.lk/web/wp-content/uploads/2024/03/MSME-Presentation-English.pdf>

617 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms\\_901205.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_901205.pdf)

618 <https://www.adb.org/sites/default/files/publication/957856/sri-ado-april-2024.pdf>

619 [https://www.cbsl.gov.lk/sites/default/files/cbslweb\\_documents/publications/annual\\_report/2021/en/13\\_Box\\_04.pdf](https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/2021/en/13_Box_04.pdf)

620 Ibid.

621 [https://www.cbsl.gov.lk/sites/default/files/cbslweb\\_documents/publications/annual\\_report/2021/en/13\\_Box\\_04.pdf](https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/2021/en/13_Box_04.pdf)

622 <https://datareportal.com/reports/digital-2023-sri-lanka>

623 <https://datareportal.com/reports/digital-2021-sri-lanka?rq=sri%20lanka>

624 <https://datareportal.com/reports/digital-2023-sri-lanka>

625 <https://datareportal.com/reports/digital-2024-sri-lanka?rq=sri%20lanka>

626 <https://www.igi-global.com/article/a-study-of-cyber-security-issues-in-sri-lanka/257519>

627 <https://cert.gov.lk/wp-content/uploads/2023/08/Cyber-Security-Bill-13-07-2023.pdf>

628 <https://www.igi-global.com/article/a-study-of-cyber-security-issues-in-sri-lanka/257519>

629 <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1207&context=ism>

630 <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

631 <http://www.statistics.gov.lk/Resource/en/ComputerLiteracy/Bulletins/AnnualBuletinComputerLiteracy-2022.pdf>

632 <http://www.statistics.gov.lk/LabourForce/StaticalInformation/AnnualReports/2021>

633 <https://www.igi-global.com/article/a-study-of-cyber-security-issues-in-sri-lanka/257519>

634 <https://cert.gov.lk/wp-content/uploads/2024/03/NCSS-Draft-V14.pdf>

635 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms\\_901205.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_901205.pdf)

636 Ibid.

637 <http://www.statistics.gov.lk/LabourForce/StaticalInformation/AnnualReports/2021>

638 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-new\\_delhi/documents/publication/wcms\\_123348.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-new_delhi/documents/publication/wcms_123348.pdf)

639 <https://documents1.worldbank.org/curated/en/341681597688560604/pdf/Informality-Job-Quality-and-Welfare-in-Sri-Lanka.pdf>

640 Ibid.

641 <http://www.statistics.gov.lk/LabourForce/StaticalInformation/AnnualReports/2021>

642 <https://ieomsociety.org/proceedings/2021monterrey/355.pdf>

643 <https://www.diva-portal.org/smash/get/diva2:1764144/FULLTEXT02>

644 <https://datareportal.com/reports/digital-2024-sri-lanka>

645 <https://www.slideshare.net/slideshow/2022-ecommerce-report-sri-lanka/266212902>

646 Ibid.

647 <https://www.combank.lk/news/news-events/combank-breaks-new-ground-in-sri-lanka-enabling-alipay-qr-payments-for-merchants#:~:text=Commercial%20Bank%20has%20the%20distinction,Lanka%20are%20standardised%20and%20interoperable>

648 <https://www.imperva.com/cyber-threat-attack-map/>

649 <https://cybermap.kaspersky.com>

650 Interview, The Asia Foundation, Sri Lanka, January 29, 2024.

651 <https://economynext.com/sri-lanka-telecom-says-dealing-with-revil-hack-customer-data-safe-70322/>

652 <https://www.slt.lk/en/content/slt-clarifies-situation-regarding-recent-cyber-attack>

653 Ibid.

654 <https://cert.gov.lk/>

655 <https://pmd.gov.lk/news/national-cyber-security-act-anticipated-for-implementation-this-year/>

656 <https://economynext.com/sri-lanka-to-bring-national-cyber-security-act-amid-surge-in-social-network-users-state-minister-162385/>

657 <https://cert.gov.lk/wp-content/uploads/2023/08/Cyber-Security-Bill-13-07-2023.pdf>

658 <https://www.icta.lk/who-we-are/our-role>

659 <https://pmd.gov.lk/news/national-cyber-security-act-anticipated-for-implementation-this-year/>

660 <https://digieconsummit.com/about-us/>

661 <https://csasrilanka.org/>

662 [https://www.cbsl.gov.lk/sites/default/files/cbslweb\\_documents/publications/annual\\_report/2021/en/13\\_Box\\_04.pdf](https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/2021/en/13_Box_04.pdf)

663 Ibid.

664 [https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms\\_901205.pdf](https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---ilo-colombo/documents/publication/wcms_901205.pdf)

665 [https://unctad.org/system/files/official-document/BRI-Project\\_RP15\\_en.pdf](https://unctad.org/system/files/official-document/BRI-Project_RP15_en.pdf)

666 <https://www.statista.com/statistics/1337417/thailand-number-of-msmes/#:~:text=As%20of%202022%2C%20the%20number,in%20Thailand%20reached%203.2%20million>

667 <https://business.yougov.com/content/47201-charting-thailand-mobile-commerce-landscape-mobile-shopping-apps-mcommerce-purchases>

668 <https://www.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf>

669 <https://www.bangkokpost.com/business/general/2682044/report-reveals-extent-of-cybersecurity-threat>

670 [https://www.cisco.com/c/dam/global/en\\_hk/assets/pdfs/cybersecurity-for-smb-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_hk/assets/pdfs/cybersecurity-for-smb-asia-pacific-businesses-prepare-for-digital-defense.pdf)

671 <https://krungthai.com/th/financial-partner/learn-financial/1854#:~:text=%E0%B8%81%E0%B9%88%E0%B8%AD%E0%B8%99%E0%B8%88%E0%B8%Bo%E0%B8%A1%E0%B8%B2%E0%B8%94%E0%B8%B9%E0%B8%A7%E0%B9%88%E0%B8%B2,%E0%B9%81%E0%B8%A5%E0%B8%Bo%E0%B8%A7%E0%B8%B4%E0%B8%AA%E0%B8%B2%E0%B8%AB%E0%B8%81%E0%B8%B4%E0%B8%88%E0%B8%82%E0%B8%99%E0%B8%B2%E0%B8%94%E0%B8%81%E0%B8%A5%E0%B8%B2%E0%B8%87%20>

672 <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>

673 <https://www.mdpi.com/2071-1050/14/14/8476>

674 [https://www.oecd-ilibrary.org/finance-and-investment/oecd-investment-policy-reviews-thailand-2020\\_c4eeee1c-en](https://www.oecd-ilibrary.org/finance-and-investment/oecd-investment-policy-reviews-thailand-2020_c4eeee1c-en)

675 <https://msme-resurgence.uncad.org/sites/smesurge/files/documents/Thai%20Study%20SME%20-%20FINAL.1.pdf>

676 <https://www.dataguidance.com/jurisdiction/thailand>

677 <https://www.mdpi.com/2071-1050/14/14/8476>

678 <https://su.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf>

679 <https://www.statista.com/outlook/tmo/cybersecurity/thailand>

680 [https://www.boi.go.th/upload/content/Thailand,%20Taking%20off%20to%20new%20heights%20@%20belgium\\_5ab4e8042850e.pdf](https://www.boi.go.th/upload/content/Thailand,%20Taking%20off%20to%20new%20heights%20@%20belgium_5ab4e8042850e.pdf)

681 <https://msme-resurgence.uncad.org/sites/smesurge/files/documents/Thai%20Study%20SME%20-%20FINAL.1.pdf>

682 <https://www.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf>

683 Ibid.

684 <https://doi.org/10.3390/su14148476>

685 [https://www.cisco.com/c/dam/global/en\\_hk/assets/pdfs/cybersecurity-for-smb-asia-pacific-businesses-prepare-for-digital-defense.pdf](https://www.cisco.com/c/dam/global/en_hk/assets/pdfs/cybersecurity-for-smb-asia-pacific-businesses-prepare-for-digital-defense.pdf)

686 Ibid.

687 <https://www.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf>

688 <https://www.jstor.org/stable/44684451>

689 <https://documents1.worldbank.org/curated/en/099506009112325206/pdf/IDU044678b42097e804da90a85008d7c4c45b4b9.pdf>

690 <https://www.bangkokpost.com/business/general/2745121/call-for-better-integration-of-the-informal-economy>

691 [https://irff.undp.org/sites/default/files/2024-03/building-msme-resilience-in-southeast-asia\\_o.pdf](https://irff.undp.org/sites/default/files/2024-03/building-msme-resilience-in-southeast-asia_o.pdf)

692 <https://doi.org/10.3390/su14148476>

693 Ibid.

694 <https://www.trade.gov/country-commercial-guides/thailand-ecommerce>

695 Interview, The Asia Foundation, Thailand, January 25, 2024.

696 Ibid.

697 <https://www.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf>

698 Ibid.

699 Interview, The Asia Foundation, Thailand, January 25, 2024.

700 <https://www.nationthailand.com/blogs/thailand/general/40035215>

701 <https://www.statista.com/topics/11439/cybersecurity-and-cybercrime-in-thailand/#editorsPicks>

702 <https://www.statista.com/forecasts/1400787/apac-largest-cybersecurity-markets-by-revenue>

703 Interview, The Asia Foundation, Thailand, January 25, 2024.

704 Ibid.

705 [https://www.boi.go.th/upload/content/2017-07-24%20Thailand%204.0%20-%20Digital%20Economy%20\(OO2\)\\_35798.pdf](https://www.boi.go.th/upload/content/2017-07-24%20Thailand%204.0%20-%20Digital%20Economy%20(OO2)_35798.pdf)

706 [https://www.researchgate.net/publication/363430585\\_TECHNOLOGY\\_RISK\\_ASSESSMENT\\_IN\\_SMALL\\_AND\\_MEDIUM-SIZED\\_ENTERPRISES\\_SMES\\_IN\\_THAILAND](https://www.researchgate.net/publication/363430585_TECHNOLOGY_RISK_ASSESSMENT_IN_SMALL_AND_MEDIUM-SIZED_ENTERPRISES_SMES_IN_THAILAND)

707 <https://www.statista.com/topics/11439/cybersecurity-and-cybercrime-in-thailand/#topicOverview>

708 <https://www.dataguidance.com/opinion/thailand-cybersecurity>

709 <https://www.usaid.gov/document/fact-sheet-digital-asia-accelerator>

710 [https://www.researchgate.net/publication/363430585\\_TECHNOLOGY\\_RISK\\_ASSESSMENT\\_IN\\_SMALL\\_AND\\_MEDIUM-SIZED\\_ENTERPRISES\\_SMES\\_IN\\_THAILAND](https://www.researchgate.net/publication/363430585_TECHNOLOGY_RISK_ASSESSMENT_IN_SMALL_AND_MEDIUM-SIZED_ENTERPRISES_SMES_IN_THAILAND)

711 [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/06/GSMA\\_CIU\\_Thailand-MSME-Digitalisation\\_Jun2022.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/06/GSMA_CIU_Thailand-MSME-Digitalisation_Jun2022.pdf)

712 [https://www.researchgate.net/publication/363430585\\_TECHNOLOGY\\_RISK\\_ASSESSMENT\\_IN\\_SMALL\\_AND\\_MEDIUM-SIZED\\_ENTERPRISES\\_SMES\\_IN\\_THAILAND](https://www.researchgate.net/publication/363430585_TECHNOLOGY_RISK_ASSESSMENT_IN_SMALL_AND_MEDIUM-SIZED_ENTERPRISES_SMES_IN_THAILAND)

713 Ibid.

714 [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/06/GSMA\\_CIU\\_Thailand-MSME-Digitalisation\\_Jun2022.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/06/GSMA_CIU_Thailand-MSME-Digitalisation_Jun2022.pdf)

715 <https://www.mdpi.com/2071-1050/14/14/8476>

716 Interview, The Asia Foundation, Thailand, January 25, 2024.

717 Expert interview, February 5, 2024.

718 <https://www.mdpi.com/2071-1050/14/14/8476>

719 <https://data.adb.org/dataset/2023-asia-small-and-medium-sized-enterprise-monitor>

720 <https://www.dai.com/uploads/final-msme-reports/vietnam-country-brief.pdf>

721 Interview, The Asia Foundation, Vietnam, January 31, 2024.

722 <https://www.statista.com/statistics/1229529/vietnam-leading-social-media-platforms-by-generation/#:~:text=According%20to%20a%20survey%20among%20a%20channel%20among%20the%20surveyed%20respondents>

723 [https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20\(Mobile%20World\)](https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20(Mobile%20World))

724 [https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse\\_more-articles\\_related-content-card](https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse_more-articles_related-content-card)

725 <https://opengovasia.com/2024/08/28/vietnams-strategic-response-to-rising-cyber-threats/#:~:text=The%20Viettel%20report%20highlighted%20a,responding%20robustly%20to%20these%20challenges>

726 <https://mkefactsettd.maybank-ke.com/PDFS/268879.pdf>

727 <https://vietnamnews.vn/economy/1594537/cybersecurity-threats-on-the-rise-in-viet-nam-s-smb-sector-reports.html>

728 <https://asean.org/wp-content/uploads/2023/11/Definition-of-MSME-in-ASEAN-Member-States.pdf>

729 <https://ncsc.gov.vn>

730 <https://en.baochinhphu.vn/cyberattacks-in-viet-nam-plunge-as-greater-attention-paid-to-cybersecurity-111230504090705435.htm>

731 <https://www.trade.gov/market-intelligence/vietnam-cybersecurity-requirements-and-capabilities#:~:text=On%20August%2010%20C%202022%20the,overall%20cybersecurity%20market%20in%20Vietnam>

732 <https://vietnamlawmagazine.vn/digital-transformation-an-urgent-need-for-smes-59216.html>

733 <https://asean.org/wp-content/uploads/2023/07/Digitalization-of-MSMEs-in-ASEAN-and-Russia-Trends-Opportunities.pdf>

734 <https://redseer.com/newsletters/vietnam-msme-digitisation/>

735 <https://www.pwc.com/vn/en/publications/2022/220908-pwc-vietnam-legal-newsbrief-decree-53.pdf>

736 <https://www.rmit.edu.vn/news/all-news/2022/jan/small-and-medium-sized-enterprises-approach-a-cyber-secure-future>

737 [https://hkbav.org/up-to-70-of-smes-in-vietnam-operate-outside-the-digital-economy\\_news21558](https://hkbav.org/up-to-70-of-smes-in-vietnam-operate-outside-the-digital-economy_news21558)

738 <https://vir.com.vn/vietnams-ict-industry-outstanding-results-in-2023-and-new-plans-for-2024-108021.html>

739 <https://hanoicapital.chinhphu.vn/ha-noi-selects-four-pillars-for-digital-economy-development-110240227161454779.htm>

740 Ibid.

741 <https://www.trade.gov/market-intelligence/vietnam-cybersecurity-requirements-and-capabilities#:~:text=On%20August%2010%20C%20>

2022%2C%20the,overall%20cybersecurity%20market%20in%20Vietnam  
742 <https://en.vietnamplus.vn/vietnam-reports-13900-cyberattacks-in-2023/274773.vnp>  
743 <https://eastasiaforum.org/2024/03/20/vietnams-struggle-with-cyber-security/#:~:text=In%20the%20first%20half%20of,in%202023%20compared%20to%202022>  
744 <https://en.vietnamplus.vn/vietnam-reports-13900-cyberattacks-in-2023/274773.vnp>  
745 <https://baochinhphu.vn/de-nghi-xay-dung-luat-bao-ve-du-lieu-ca-nhan-102240301155959203.htm&sa=D&source=docs&ust=1718057606378253&usq=AOvVaw1Xg.BrALRaCl9lAjZRleZX>  
746 <https://redseer.com/newsletters/vietnam-msme-digitisation/>  
747 <https://vietnamlawmagazine.vn/digital-transformation-an-urgent-need-for-smes-59216.html>; <https://asean.org/wp-content/uploads/2023/07/Digitalization-of-MSMEs-in-ASEAN-and-Russia-Trends-Opportunities.pdf>  
748 <https://data.adb.org/dataset/2023-asia-small-and-medium-sized-enterprise-monitor>  
749 <https://www.gso.gov.vn/wp-content/uploads/2023/06/LAO-DONG-CO-VIEC-LAM-PHI-CHINH-THUC-O-VIET-NAM-Eg-final.pdf>  
750 [https://dangcongsan.vn/thoi-su/doanh-nghiep-gia-dinh-nhung-trinh-do-quan-tri-phai-mang-tam-quoc-gia-quoc-te-651179.html?\\_x\\_tr\\_sl=vi&\\_x\\_tr\\_tl=en&\\_x\\_tr\\_hl=en&\\_x\\_tr\\_pto=sc](https://dangcongsan.vn/thoi-su/doanh-nghiep-gia-dinh-nhung-trinh-do-quan-tri-phai-mang-tam-quoc-gia-quoc-te-651179.html?_x_tr_sl=vi&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc)  
751 <https://lingcure.org/index.php/journal/article/view/2069>  
752 Ibid.  
753 <https://www.gso.gov.vn/en/data-and-statistics/2023/06/overall-situation-of-workers-in-informal-employment-in-viet-nam/>  
754 <https://lawnet.vn/thong-tin-phap-luat/en/chinh-sach-moi/continuing-to-implement-tax-administration-reform-for-individual-business-holds-in-vietnam-115495.html>  
755 Ibid.  
756 <https://www.dai.com/uploads/final-msme-reports/vietnam-country-brief.pdf>  
757 Interview, The Asia Foundation, Vietnam, January 31, 2024.  
758 <https://www.statista.com/statistics/1229529/vietnam-leading-social-media-platforms-by-generation/#:~:text=According%20to%20a%20survey%20among%20among%20the%20surveyed%20respondents>  
759 [https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20\(Mobile%20World\)](https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20(Mobile%20World))  
760 [https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse\\_more-articles\\_related-content-card](https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse_more-articles_related-content-card)  
761 <https://www.legal500.com/developments/thought-leadership/cross-border-e-commerce-opportunities-and-challenges-for-micro-small-and-medium-enterprises-msmes-in-vietnam/>  
762 [https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20\(Mobile%20World\)](https://www.trade.gov/country-commercial-guides/vietnam-ecommerce#:~:text=Key%20e%2Dcommerce%20operators%20include,Di%20Dong%20(Mobile%20World))  
763 [https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse\\_more-articles\\_related-content-card](https://www.linkedin.com/pulse/vietnams-digitalization-push-aims-empower-msmes-e-commerce-santosh-g-f8phc?trk=article-ssr-frontend-pulse_more-articles_related-content-card)  
764 <https://vccinews.com/news/49452/cybersecurity-crucial-element-to-boost-business-development.html>  
765 <https://vietnamnet.vn/en/black-credit-leading-people-to-dead-end-with-no-escape-from-debt-687814.html>  
766 <https://vccinews.com/news/49452/cybersecurity-crucial-element-to-boost-business-development.html>  
767 <https://fulcrum.sg/navigating-vietnams-lending-app-maze/>  
768 <https://vietnamnews.vn/society/715595/five-people-arrested-in-hcm-city-loan-shark-apps-bust-worth-42-million.html>  
769 <https://www.vietnam.vn/en/chong-tin-dung-den-lua-dao-qua-app/>  
770 <https://vietnamnews.vn/economy/1594537/cybersecurity-threats-on-the-rise-in-viet-nam-s-smb-sector-reports.html>  
771 Interview, The Asia Foundation, Vietnam, January 31, 2024.  
772 <https://vietnamnews.vn/economy/1594537/cybersecurity-threats-on-the-rise-in-viet-nam-s-smb-sector-reports.html>  
773 [https://laodong.vn.translate.google.com/translate/gooq/tien-te-dau-tu/doanh-nhan-khon-kho-bi-tan-cong-mang-can-tim-ra-ke-nem-da-giau-tay-939074.ldo?\\_x\\_tr\\_sl=vi&\\_x\\_tr\\_tl=en&\\_x\\_tr\\_hl=en&\\_x\\_tr\\_pto=sc](https://laodong.vn.translate.google.com/translate/gooq/tien-te-dau-tu/doanh-nhan-khon-kho-bi-tan-cong-mang-can-tim-ra-ke-nem-da-giau-tay-939074.ldo?_x_tr_sl=vi&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc)  
774 <https://www.dai.com/uploads/final-msme-reports/vietnam-country-brief.pdf>  
775 Ibid.  
776 Ibid.  
777 <https://www.pwc.com/vn/en/publications/2022/220908-pwc-vietnam-legal-newsbrief-decree-53.pdf>  
778 <https://vneconomy.vn/gdp-se-tang-them-30-ty-usd-neu-chuyen-doi-so-cho-doanh-nghiep-sme.htm>  
779 <https://redseer.com/newsletters/vietnam-msme-digitisation/>  
780 <https://www.rmit.edu.vn/news/all-news/2022/jan/small-and-medium-sized-enterprises-approach-a-cyber-secure-future>  
781 Interview, The Asia Foundation, Vietnam, January 31, 2024.  
782 [https://hkbav.org/up-to-70-of-smes-in-vietnam-operate-outside-the-digital-economy\\_news21558](https://hkbav.org/up-to-70-of-smes-in-vietnam-operate-outside-the-digital-economy_news21558)  
783 <https://vnexpress.net/ly-do-doanh-nghiep-nho-de-bi-tan-cong-mang-4454610.html>  
784 Ibid.  
785 Ibid.  
786 <https://www.intechopen.com/chapters/84563> (NB: This number accounts for organizations registered with the NGO Affairs Bureau but not local voluntary organizations registered with the Department of Social Services.)  
787 <https://timesofindia.indiatimes.com/readersblog/maximizing-contributions-of-ngos-for-larger-goods/leveraging-ngos-51372/>  
788 <https://www.icnl.org/resources/civic-freedom-monitor/indonesia>  
789 <https://www.jnpoc.ne.jp/en/nonprofits-in-japan/>  
790 <https://www.statista.com/statistics/1227922/south-korea-number-of-ngos/>  
791 <https://asiaphilanthropycircle.org/supporting-the-third-sector-in-malaysia/>  
792 [https://dspace.stir.ac.uk/bitstream/1893/31170/1/nap\\_final\\_20200515.pdf](https://dspace.stir.ac.uk/bitstream/1893/31170/1/nap_final_20200515.pdf)  
793 <https://link.springer.com/content/pdf/10.1007/s11266-022-00554-8.pdf>  
794 <https://mb.com.ph/2024/1/25/ng-os-in-the-philippines-third-estate-in-nation-building>  
795 <https://www.charities.gov.sg/PublishingImages/Resource-and-Training/Publications/COC-Annual-Reports/Documents/Commissioner%20of%20Charities%20Annual%20Report%202022.pdf>  
796 <https://www.icnl.org/resources/civic-freedom-monitor/sri-lanka#:~:text=In%20an%20email%20interview%20in,groups%20operating%20in%20Sri%20Lanka>  
797 <https://www.icnl.org/resources/civic-freedom-monitor/thailand>  
798 <https://sdg.iisd.org/commentary/guest-articles/advancing-csos-role-in-sdgs-to-protect-marginalized-communities-in-viet-nam/> (NB: Vietnam has no official definition for “non-profit organizations” (NPOs) and “non-governmental organizations” (NGOs); instead, the government uses the terms non-profit enterprise and social enterprise.)  
799 <https://www.infoxchange.org/au/news/2023/04/infoxchange-launches-digital-capabilities-program-asia-pacific>  
800 Ibid.

801 <https://geneva.cyberpeace.ngo/>  
802 <https://www.infoxchange.org/au/news/2023/04/infoxchange-launches-digital-capabilities-program-asia-pacific>  
803 [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2024.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf)  
804 <https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals?queryID=22129e5799b268613eed147a5e30bc07>  
805 [https://digitaltransformation.nonprofit/sites/default/files/IX\\_APACReport23\\_FA3-Screen.pdf](https://digitaltransformation.nonprofit/sites/default/files/IX_APACReport23_FA3-Screen.pdf)  
806 <https://therecord.media/water-for-people-medusa-ransomware>  
807 [https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-nation-state-attacks#:~:text=Pie%20chart%20detailing%20industry%20sectors,%2C%20and%20Government%20\(10%25\)](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-nation-state-attacks#:~:text=Pie%20chart%20detailing%20industry%20sectors,%2C%20and%20Government%20(10%25))  
808 <https://www.amnesty.org/en/latest/press-release/2019/04/state-sponsored-cyber-attack-hong-kong/?stream=technology>  
809 <https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/>  
810 <https://www.bulatlat.com/2022/03/15/cyberattacks-traced-to-ph-hackers-hailed-by-govt-as-computer-geniuses-probe-shows/>  
811 <https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/>  
812 [Ibid.](#)  
813 <https://www.bulatlat.com/2022/03/15/cyberattacks-traced-to-ph-hackers-hailed-by-govt-as-computer-geniuses-probe-shows/>  
814 <https://www.dragonforce.io/>  
815 <https://www.radware.com/security/ddos-knowledge-center/ddospedia/dragonforce-malaysia/>  
816 <https://www.propertycasualty360.com/2021/02/24/how-nonprofits-can-prevent-card-testing-fraud/?slreturn=20240311174625>  
817 <https://www.freemalaysiatoday.com/category/nation/2023/11/03/ngos-collecting-donations-must-be-regulated-by-govt-say-cops/>  
818 <https://www.straitstimes.com/singapore/experts-warn-of-charity-scams-amid-middle-east-conflict>  
819 <https://cyberpeaceinstitute.org/news/trafficked-cybercriminals-in-southeast-asia/>  
820 <https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report>  
821 <https://www.adb.org/sites/default/files/publication/912361/civil-society-brief-philippines.pdf>  
822 <https://restofworld.org/2021/philippines-human-rights-cyberattack/>  
823 <https://www.bulatlat.com/2022/03/15/cyberattacks-traced-to-ph-hackers-hailed-by-govt-as-computer-geniuses-probe-shows/>  
824 [https://monitor.civicus.org/globalfindings\\_2023/asiapacific/](https://monitor.civicus.org/globalfindings_2023/asiapacific/)  
825 <https://www.amnesty.org/en/latest/news/2022/07/pegasus-thailand-activists-protests/>  
826 <https://www.reuters.com/article/china-southeast-asia-surveillance/feature-activists-fear-rising-surveillance-from-asias-digital-silk-road-idUSL8N1WDoDP/>  
827 <https://unsdg.un.org/latest/stories/rising-above-hate-indonesia-tackles-disinformation-against-rohingya-refugees>  
828 <https://www.smrj.go.jp/english/about/target.html>  
829 <https://www.oecd-ilibrary.org/sites/a4e7ef59-en/index.html?itemId=/content/component/a4e7ef59-en>  
830 <https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf>  
831 <https://www.adb.org/sites/default/files/event/772211/files/session-1-nyoman-adhiarna-rev.pdf>  
832 <https://www.oecd-ilibrary.org/sites/1359290e-en/index.html?itemId=%2Fcontent%2Fcomponent%2F1359290e-en>  
833 <https://msme.gov.in/know-about-msme>  
834 [https://www.unescap.org/sites/default/d8files/knowledge-products/MSME%20financing%20Bangladesh\\_10%20May%202021\\_share\\_O.pdf](https://www.unescap.org/sites/default/d8files/knowledge-products/MSME%20financing%20Bangladesh_10%20May%202021_share_O.pdf)





12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28			