CYBERSECURITY IN EUROPE

Challenges and Solutions for Small Businesses

JUNE 2025

EUROPEAN MICROFINANCE NETWORK

This focus paper was prepared by the European Microfinance Network with support from the Mastercard Center for Inclusive Growth. The views and insights presented are those of the author and are intended to inform discussion; they do not reflect the official position or policies of supporting partners.

This focus paper explores the growing cybersecurity challenges facing Europe's Micro and Small Enterprises (MSEs), which play a vital role in economic growth but are increasingly vulnerable due to rapid digitalisation and limited resources. While digital transformation has helped MSEs remain competitive (particularly during crises such as the COVID-19 pandemic) it has also exposed them to a broad spectrum of cyber threats, including ransomware, phishing, malware, DDoS attacks, and supply chain breaches. These threats are intensified by a lack of cybersecurity expertise, dependence on costly or ill-suited technology solutions, and constrained budgets, all of which can result in significant operational and financial consequences.

The paper underscores the urgent need for comprehensive policy measures and targeted support from EU authorities and National Coordination Centres (NCCs). It recommends expanding access to practical training, increasing funding, and developing user-friendly cybersecurity tools to foster a strong cybersecurity culture and safeguard both individual businesses and the broader digital ecosystem.

Introduction

Context

Micro and Small Enterprises (MSEs) are the backbone of the EU economy, representing 99% of all businesses, around 24.3 million entities in total[1]. They play a key role in job creation, innovation, and economic growth, making their support and protection a priority for EU policymakers.

The COVID-19 crisis accelerated the digital transition among MSEs, with many adopting tools like cloud services, teleworking, and online sales[2] to stay operational. However, this rapid shift increased their exposure to cyber threats[3], **leading to a 667% surge in phishing attacks during the early months of the pandemic[4].** The World Economic Forum's (WEF) 2021 Global Risks Report[5] ranks cybersecurity failure as the fourth highest global risk, just behind climate disasters and infectious diseases.

Policy landscape snapshot

The Digital Decade programme[6] launched in 2022 by the European Commission and Member States set up common commitments to achieve a high level of digitalisation by 2030. The ambitious programme plans for **more than 90% of MSEs to reach at least a basic level of digital intensity[7] (in 2023, 58%[8] of EU MSEs reached this level)**. Yet, such ambitious digital transformations inevitably come with increased cybersecurity risks.

---

[1] European Commission, Annual report on European SMEs 2023/2024

[2] Cybersecurity for SMEs, Challenges and Recommendations, ENISA 2021

[3] ENISA, Cybersecurity for SMEs, Challenges and Recommendations, 2021

[4] WEF What Europe's SMEs need to do for a cyber-secure future, 2021

[5] World Economic Forum (WEF), Global Risks Report, 2021

[6] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, 2022

[7] To measure the digital intensity of a business, Eurostat has developed the Digital Intensity Index (DII): broadband connection, social media usage, website presence, cloud computing, availability of ICT specialists, ERP software usage, electronic information sharing, online sales engagement, AI usage, big data analytics, CRM software usage, and advanced digital tool/technology integration. A basic level of digital intensity means that a business covers at least 4 of the 12 indicators.

[8] European Commission, Eurostat Data Towards Digital Decade targets for Europe, 2023

The EU has established a cybersecurity policy framework to protect public and private sectors and citizens which is implemented through the **European Union Agency for Cybersecurity** (ENISA), the **European Cybersecurity Competence Centre** (ECCC) and 27 **National Coordination Centres** (NCCs).

Among the latest legislative texts, the **NIS 2 Directive**[9] focuses on medium and large businesses, requiring stronger cybersecurity practices and broader reporting. While not directly targeting MSEs, it may affect them indirectly through **supply chain** demands. The **Cybersecurity Resilience Act** (CRA)[10] sets cybersecurity standards for digital products, aiming to boost security but potentially placing additional burdens on MSEs, **impacting their resources and competitiveness**.

While the topic of cybersecurity has been the subject of many legislative and non-legislative initiatives these past few years, this paper calls on EU and national policy makers to better integrate the need of small businesses in the implementation of cybersecurity measures.

Drawing on the findings and expertise from mentees of the Mastercard Strive EU Programme[11] , this focus paper will examine the key cyber threats, their impacts, and the challenges faced by MSEs, while also offering **innovative solutions** and **policy recommendations**.

I. Cybersecurity landscape for MSEs

1. Overview of MSEs cyberthreats

Cybersecurity for European MSEs is becoming increasingly treacherous, with attacks intensifying in frequency and complexity as Artificial Intelligence (AI) emerges. Understanding the primary threat vectors is essential for these businesses.

Ransomware attacks: Ransomware remains one of the most damaging threats[12]. These attacks increased from 112 in 2022 to 175 in 2023, with MSEs accounting for 87% of victims in early 2023[13]. Many lack the resources to recover from such attacks.

Phishing & Social Engineering: Phishing and Social Engineering tactics take advantage of human error and lack of cybersecurity training. A 667% increase in phishing was reported during the COVID-19 pandemic[14].

Malware & Advanced Threats: Malware continues to evolve, with trojans, viruses, and advanced variants targeting MSEs[15]. According to a recent study, only 28% of small businesses rate their threat mitigation capabilities as strong[16].

Web-Based Attacks & Credential Theft: Poor password hygiene and weak authentication expose MSEs to data breaches[17]. The shift to digital platforms has been found to increase these risks.

Supply Chain Vulnerabilities: According to ENISA, supply chain attacks jumped from 1% in 2021 to 17% in 2022[18]. MSEs are often used as an entry point to larger companies, amplifying the risk.

Distributed Denial of Service (DDoS): DDoS attacks can shut down online operations damaging both revenue and reputation.

---

[9] Directive (EU) 2022/2555 Of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[10] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

[11] Mastercard Strive programme: Mastercard Strive is a portfolio of philanthropic programs supported by the Mastercard Center for Inclusive Growth and funded by the Mastercard Impact Fund. With programs in more than 20 countries around the world, Mastercard Strive aims to reach 18 million small businesses to go digital, get capital, and access networks and know-how

[12] UK National Cyber Security Centre, Definition of ransomware: "Ransomware is a type of malware which prevents a business of individual from accessing their device and the data stored on it, usually by encrypting your files. The hacker will then demand a ransom in exchange for decryption".

[13] DIGITAL SME Alliance, The Ransomware landscape in Europe, 2023

[14] Promoting Cybersecurity for SMEs in Europe, 2022, EIT Digital, the Global Digital Foundation & Huawei

[15] Promoting Cybersecurity for SMEs in Europe, 2022, EIT Digital, the Global Digital Foundation & Huawei

[16] Cybersecurity and Data Protection for Small, Medium and Micro Enterprises (CYSSME), Why is cybersecurity essential for SMEs?

[17] ENISA, Web-based attacks, 2020

[18] ENISA, Web-based attacks, 2020

Many **MSEs underestimate their risks**, leaving them particularly vulnerable due to limited cybersecurity resources and expertise.

2. *The consequences of cyber-attacks for MSEs*

The vulnerability of small businesses to cyber threats stems from several interrelated factors. Many MSEs owners operate under the misconception that cyberthreats primarily target larger organisations with more valuable data. They fail to recognise that smaller enterprises often represent easier targets precisely because of their limited security measures, according to ENISA[19].

This **perception gap** is problematic considering that cybersecurity incidents can have catastrophic consequences for small businesses, potentially leading to **operational disruption**, **financial losses**, **reputational damage**, and even **business failure**[20].

A new Mastercard survey of over 5,000 small and medium-sized business owners from four continents found **that 46% have faced a cyberattack in their current business**. Of those affected, **nearly one in five were forced to file for bankruptcy** or shut down entirely as a result[21].

Additionally, a survey of MSEs experiencing cyberattacks within the past year revealed that a significant **58% suffered tangible business impacts**, with the most prevalent being the burden of additional time to identify and respond to the attack (35%), and incurring repair or recovery costs (24%). **Disruption to daily operations**, including employee productivity and resource availability, affected 20% of these businesses. While revenue loss and discouragement of planned activities were noted by a smaller percentage, **reputational damage** and loss of partners were also observed[22].

This digital transformation, while essential for businesses continuity, has exposed MSEs to unprecedented levels of cyber risks. According to recent surveys, more than 85% of European MSEs acknowledge that cybersecurity incidents would have serious negative impacts on their operations within just one week of occurrence, with **57% believing they would likely become bankrupt or cease operations entirely following a significant cyber event**[23].

The economic impact of cyber incidents on small businesses extends beyond individual enterprises to affect the broader European economy. As essential components of complex supply chains, small businesses that suffer security breaches can introduce **vulnerabilities that impact larger organisations and critical infrastructure**[24].

This **interconnected nature of the digital ecosystem** means that the cybersecurity challenges facing MSEs represent a systemic risk that requires coordinated attention from policymakers, industry associations, and security professionals.

The **costs of cybersecurity attacks for MSEs** can be significant, often beyond their available cash reserves. Resilience and adaptability are key to the survival and growth of any business, regardless of its size. By addressing these challenges, the European Union can strengthen its overall cybersecurity posture while enabling small businesses to thrive in an increasingly digital landscape.

3. *MSEs and their challenges towards cybersecurity*

MSEs are becoming increasingly digitalised, as evidenced by the survey data from the European Commission[25]. On average, 41% of MSEs in the EU use five or more digital tools which significantly increase their exposure to

---

[19] ENISA, Cybersecurity for SMEs, Challenges and Recommendations, 2021

[20] WEF, What Europe's SMEs need to do for a cyber-secure future, 2021

[21] Mastercard, Too small to be ignored? Not anymore. Why shoring up cyber defenses is crucial for small businesses,2025

[22] European Commission, Flash Eurobarometer 496 SMEs and cybercrime – November-December 2021 Report

[23] ENISA, Cybersecurity for SMEs, Challenges and Recommendations, 2021

[24] WEF, What Europe's SMEs need to do for a cyber-secure future, 2021

[25] Eurostat, Flash barometer 496, SMEs and cybercrime report, May 2022: *Online bank account (76%), Website for the business (71%), Internet-connected "smart" devices (55%), Online ordering or payment systems of suppliers, consultants or other business partners (39%), Cloud computing or storage (38%), Web-based applications for payroll processing, e-signature (35%), A company intranet (32%), An internet-based video or voice call system (31%), An online ordering and payment service for customers (30%).*

cyberthreats and with **80% of MSEs handling critical information**[26], they make an easy target for cyberattacks. In 2022, the European Commission[27] reported that **28% of MSEs experienced at least one type of cyberthreat** within a 12-month period.

ENISA has identified several key factors contributing to the cybersecurity vulnerabilities of MSEs, **including low awareness of cyber threats among management level, limited budgets for cybersecurity, a lack of specialized IT security personnel**, and **the absence of tailored guidelines for the MSE sector**[28]. These findings match the observations reported by experts on the ground and small businesses as part of the Mastercard Strive EU programme.

a) Lack of cyber-literacy

Low level of awareness

The lack of cybersecurity knowledge and digital literacy is one of the primary vulnerabilities facing MSEs. ENISA, along with other national cybersecurity authorities, have consistently observed low levels of cybersecurity awareness and expertise among MSEs across the EU.

Cybersecurity is often seen as a topic only concerning ICT experts in the enterprise, but experience shows that it concerns all employees since part of the cyber-attack is the result of employees' online activities: **weak or reused passwords, unlocked devices, absence of back up policy and obsolete software** are proof of the **limited digital awareness among MSEs' management and employees**.

High costs associated with training and expertise

Due to limited resources, most MSEs lack in-house cybersecurity experts, leaving decisions to management[29]. However, low employee and management awareness[30] raises concerns about the quality of these decisions.

Despite **cybersecurity being a priority for 71% of EU businesses**[31], 74% do not provide training and 68% believe it to be unnecessary. Among MSEs, only **19% have offered any cyber awareness initiatives**[32], highlighting a significant gap in efforts to improve employees' cyber skills.

Lack of tailored solution/advice

At the national level, **National Coordination Centres (NCCs)** have developed **guidelines**, **advisory services**, **training**, and **technical support** tailored to the needs of small businesses. While many MSEs recognize the value of these resources, they often find the content too generic and not widely promoted among the broader business community, which limits its overall impact.

b) Lack of existing tools designed for MSEs, affordable for them or not easy to understand

Today, the cybersecurity market offers a wide range of software and hardware solutions to protect businesses from cyberattacks. However, experts on the ground (such as NCCs and providers of cybersecurity solutions for small businesses) point out that **these tools are often not technically suited to the needs of MSEs**. Many are too complex to install and configure without the help of specialized professionals, making them **less accessible to MSEs** with limited resources.

This observation is reinforced by findings from the **Mastercard Strive EU programme**, which highlights that many small businesses in the EU struggle to access **cybersecurity solutions that are truly aligned with their needs and capabilities**. In most cases, implementing these solutions also requires external expertise, adding to the cost and complexity for MSEs.

---

[26] ENISA defines "critical information" as information that if it is stolen or lost, the organisation would face serious legal repercussion and the owners of the personal information could encounter significant or even irreversible consequences such as: misappropriation of funds, blacklisting by financial institutions, property damages, loss of employment, subpoena, worsening of health , inability to work, long-term psychological or physical ailments.

[27] Eurostat, Flash barometer 496, SMEs and cybercrime report, May 2022

[28] Cybersecurity for SMEs, Challenges and Recommendations, ENISA 2021

[29] ENISA, Cybersecurity for SMEs -Challenges and recommendations, 2021

[30] Eurostat, Flash barometer 496, SMEs and cybercrime report, May 2022

[31] European Commission, Flash Eurobarometer 547 Cyber skills, 2023

[32] Eurostat, Flash barometer 496, SMEs and cybercrime report, May 2022

However, this issue is not without solutions. The Strive EU programme demonstrated by the solutions proposed by the innovations fund winners shows that MSEs can build a strong cybersecurity infrastructure without relying on the most advanced or technical solutions. By taking a **proactive approach, training their employees, setting up firewalls, antimalware programmes and updating software regularly, MSEs can significantly enhance their cybersecurity infrastructure**.

c) Insufficient internal funding to enhance cybersecurity

Cost is a major barrier to improving cybersecurity in MSEs, as **protection measures** (training of employees, setting up of hardware and software[33]) and **expert support** are expensive. However, investing in **cybersecurity is crucial to avoid far greater financial and reputational losses from cyberattacks**. Moreover, ongoing updates and employee training are essential to keep up with evolving threats.

There is currently **no consolidated data** on the average cost of cybersecurity for MSEs, as it varies depending on the size and nature of the business. Opinions also differ on whether and how these costs can be reduced. Nonetheless, some commonly suggested solutions include **training employees** and using simple, affordable tools such as **firewalls and anti-malware software**, provided they are kept regularly updated[34].

Despite the support mechanisms available for small businesses at the national level, representatives of MSEs emphasize that cybersecurity remains costly for smaller actors: not only financially, but also in terms of the time and expertise required to implement and maintain it.

When it comes to public funding from national and EU authorities, feedback from the ground indicates that relatively **few opportunities are specifically targeting MSEs**. Under the Digital Skills EU programme, experts have called for increased financial support for these small entities, particularly in light of the new NIS2 Directive, which may introduce additional compliance challenges for small businesses.

IN A NUTSHELL

European MSEs face growing cyber threats like ransomware, phishing, and supply chain attacks due to digital transformation. Despite often thinking they're too small to be targeted, most recognize that a cyber incident could seriously impact them, 57% of them are even fearing bankruptcy. Their biggest challenges in building cyber resilience include lack of awareness, inadequate tech solutions for their size, and high costs.

[33] ENISA, Cybersecurity for SMEs -Challenges and recommendations, 2021

[34] ENISA, Cybersecurity for SMEs -Challenges and recommendations, 2021

II. Supporting MSEs with their cybersecurity: actionable policy recommendations

To meet the challenges of cybersecurity, MSEs will need further support from the EU and national level to stay competitive and contribute to the overall EU cybersecurity. As mentioned, MSEs are faced with the following **cybersecurity challenges**:

- Lack of expertise and awareness on cybersecurity issues
- Lack of tools specifically designed for MSEs that are either affordable or easy to install and update
- Insufficient internal funding to enhance cybersecurity and the need for additional EU and national funding specifically allocated for MSEs

Mastercard and Recorded Future are partnering to deliver scalable cybersecurity by combining global infrastructure with AI-driven threat intelligence protecting all digital interactions, not just payments. Their approach gives MSEs faster threat detection, actionable insights, and stronger response capabilities.

How can we enhance the cybersecurity of MSEs?

At the national level, various training programmes, advisory services, and guidelines have been specifically launched by NCCs, some of them tailored to MSEs' needs. With 25,597,185[35] MSEs in the EU, further efforts will have to be deployed to ensure that all **MSEs can access the appropriate technical and financial support to enhance their cybersecurity.** To do that, the following recommendations should be considered at the EU and national policy level.

1. Providing the tools and solutions to create a cybersecurity culture within each MSE

Cyberliteracy is the first key element in combating cyberthreats. Well-trained employees and CEOs will be better equipped to identify threats, respond effectively to cyberattacks, ensure the compliance of their activities with cybersecurity rules and take a more proactive approach to securing their business.

Through **ethical hacking**, **Cresco** provides support to MSEs by first evaluating their cybersecurity vulnerabilities and based on this create a cybersecurity plan tailored to the business.

CRESCO

Cresco Cybersecurity is a company specialising in ethical hacking to assess and strengthen organisations' security systems. By replicating the methods of hackers, they provide in-depth security assessments and develop tailored protection plans. Committed to long-term collaboration, Cresco works with leading IT companies to improve cybersecurity in Belgium and France while ensuring transparency, confidentiality, and service excellence.

Its 360° approach to cybersecurity includes four key steps. First, they assess security by simulating cyberattacks to identify vulnerabilities and strengths to provide a comprehensive risk assessment. Then they implement safeguards measures based on their findings, creating a security plan and the necessary countermeasures. Recognising that most security breaches are due to human error, they educate employees through training programmes to help them protect themselves against cyber threats. Finally, because cybersecurity is an ongoing process, they provide ongoing monitoring, support, and emergency response to ensure long-term protection.

[35] European Commission, Annual report on European SMEs - 2023/2024

At the national level, NCCs have already developed training and awareness raising programs and published guidelines for MSEs. These first steps must be taken further to (1) **reach more MSEs**, (2) **provide more practical/hands-on information** and (3) **offer individualised advisory services.** To ensure that these services reach MSEs, awareness campaigns should also be organised.

RECOMMENDATIONS

1.1 Ensure that the training, advisory services, and guidelines offered by NCCs are **practical and hands-on**, enabling MSEs to become more self-sufficient in implementing cybersecurity measures (such as developing in-house knowledge and installing software and hardware) and fostering a genuine cybersecurity culture within the business.

1.2 Launch **awareness campaigns** at the national and regional levels to effectively promote cybersecurity initiatives tailored to MSEs.

1.3 Create **sector-specific training modules** and facilitate **peer-to-peer learning** and **knowledge sharing** through MSE networks and industry associations, in collaboration with NCCs.

1.4 Encourage MSEs to consistently report cyberattacks to their IT providers and NCCs: the lessons learned from these incidents can contribute to strengthening cybersecurity resilience for both businesses and citizens across the EU.

2. *Provide easy and affordable IT solutions fit for MSEs*

MSEs need solution adapted to their size, needs and financial/technical capacities. The solutions developed under the Strive EU programme are a good example of accessible solutions for small entities and should be replicated at the national level.

Redamp.io: An all-in-one Software as a Service (SaaS) platform for small businesses

Redamp.io is a cybersecurity company dedicated to providing small businesses with simple, intuitive, and cost-effective protection. The company has developed cybersecurity solutions for mobile operators and insurance companies, including in-network security against phishing, malware, and ransomware. Their expertise spans software development, data analytics, big data processing, and threat hunting.

Recognising the complexity and high cost of cybersecurity for SMEs, Redamp.io launched a cloud-based platform in 2021 designed specifically for small office and home office (SOHO) environments. Unlike traditional cybersecurity solutions that require multiple complex tools from different vendors, Redamp.io offers an all-in-one Software as a Service (SaaS) platform that simplifies security and remote management. Businesses can set up an account in less than five minutes with no additional software or hardware and get comprehensive protection across devices, applications, and networks. Notably, the platform also includes employee education with security tips, interactive quizzes and threat alerts.

Lupasafe is a cybersecurity platform built specifically to meet the needs of small businesses, offering a simple, effective, and affordable solution to manage cyber risks. Recognizing that many small businesses lack the time, resources, and expertise to address cybersecurity proactively, Lupasafe delivers a streamlined, AI-driven platform that makes cyber protection accessible and manageable for small teams.

At the core of Lupasafe's offering is the **Lupasafe Cyber Monitor**, an intelligent tool that continuously scans and assesses cyber risks across key business areas such as endpoints, websites, emails, cloud storage, and software systems. The platform provides a real-time, personalized dashboard that helps businesses understand their vulnerabilities and take informed action.

Lupasafe goes beyond detection by offering ongoing risk insights and clear actions to tackle threats like phishing, fraud, and outdated systems. With support from **Mastercard Strive**, it includes built-in cybersecurity training to boost employee awareness. The platform also helps small businesses stay compliant with evolving regulations like the **European Union's NIS2**.

RECOMMENDATIONS

2.1 Through NCCs, ensure that MSEs are directed towards **simple and affordable technical solutions** that can be managed internally.

2.2 Through NCCs, **expand advisory services** to support the technical implementation of tools.

3. *Increase cybersecurity budget at the EU and national level to finance dedicated initiatives for MSEs cybersecurity*

The "Digital Skills EU Programme" has allocated **€8.1 billion for 2021–2027**[36], involving NCCs, research centers, and MSEs in funding calls to advance cybersecurity tools. However, experts from the ground call for more dedicated funding opportunities for MSEs.

Under the next **Multiannual Financial Framework** (MFF), the European Commission and Member States should further **boost the budget allocated to cybersecurity**, with a particular focus on increasing funding for NCCs. Currently, NCCs receive funding through the ECCC, the Digital Europe Programme, and Horizon Europe but additional resources are needed.

NCCs are an excellent example of collaboration between the EU and national level to ensure the implementation of EU level rules and guidelines. With further resources, public and private partnership could be developed to build tailored solutions for MSEs.

RECOMMENDATIONS

3.1 Increase the EU and national **cybersecurity budgets** to support more initiatives led by NCCs on MSEs cybersecurity: providing **more funding to NCCs** will allow them to expand and reinforce their activities tailored for MSEs.

3.2 Continue to support and expand the **Digital Europe and Horizon programmes** by increasing and diversifying funding for initiatives specifically aimed at MSEs.

3.3 Create more **cascading opportunities** from Digital Europe and Horizon programmes to support the development of IT solutions by small innovators in the EU such as Cresco and Redamp.io

3.4 Develop **financial incentives** for MSEs adopting EU-certified cybersecurity solutions.

[36] European Commission, Digital European Programme, Digital country profile , consulted on March 11th

Glossary

- **COVID-19 (Coronavirus Disease 2019):** A global pandemic that emerged in late 2019.
- **Credential Theft:** A cyberattack method where hackers steal usernames, passwords, and other authentication details, often through phishing, keylogging, or data breaches.
- **Cyberliteracy:** The ability to understand, recognize, and respond to digital threats such as phishing, malware, and data breaches.
- **Cybersecurity**: As defined by ENISA, cybersecurity refers to the security of cyberspace, including the protection of digital systems, data, and networks from cyber threats, ensuring confidentiality, integrity, availability, and resilience.
- **Cybersecurity Resilience Act**: EU legislation establishing cybersecurity requirements for digital products and services to enhance security by design.
- **Cybersecurity Vulnerabilities vs. Cybersecurity Weaknesses:**
    - ***Vulnerabilities*** refer to specific flaws in software, hardware, or processes that can be exploited by attackers.
    - ***Weaknesses*** encompass broader deficiencies, such as lack of awareness, poor security practices, or inadequate funding for cybersecurity measures.
- **Data Breach:** An intentional cyber-attack brought by a cybercriminal with the goal of gaining unauthorised access and release sensitive, confidential or protected data.
- **DDoS (Distributed Denial of Service) Attack:** A cyberattack that overwhelms a website or network with excessive traffic, causing disruptions or shutdowns.
- **Digital Security Risk:** Risks associated with the use of digital technologies that can lead to data breaches, financial losses, or operational disruptions, as defined by the OECD[37].
- **ENISA (European Union Agency for Cybersecurity):** The EU agency responsible for improving cybersecurity across Europe through policy recommendations, research, and awareness initiatives.
- **Incident**: An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.
- **Malware:** Malicious software designed to infiltrate, damage, or disable computer systems, including viruses, trojans, and spyware.
- **NCCs (National Coordination Centres):** National-level cybersecurity agencies within EU Member States that provide guidance, training, and support to businesses, including MSEs, to enhance cybersecurity resilience.
- **NIS (Network and Information Security) 2 Directive:** A European Union directive aimed at enhancing cybersecurity resilience, particularly for medium and large enterprises, with potential implications for MSEs in supply chains.
- **OECD (Organisation for Economic Co-operation and Development):** An international organization that provides policy guidance on economic and social issues.
- **Phishing:** A form of social engineering where attackers deceive people into revealing sensitive information often via fraudulent emails or messages.
- **Ransomware:** A type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability or in exchange for publicly exposing the target's data.

[37] OECD, *The Digital Transformation of SMEs*, OECD Studies on SMEs and Entrepreneurship, 2021

- **Ransomware:** A type of malware that encrypts a victim's data and demands payment in exchange for restoring access.
- **MSEs (Micro and Small Enterprises)[38]:** Businesses with a limited number of employees and turnover, typically classified as:
    - **Micro-enterprises:** Micro enterprises are businesses which do not exceed the limit of at least two of the three following criteria: 1) a balance sheet total of € 350 000, 2) a net turnover of € 700 000 and 3) an average number of employees during the financial year of 10.
    - **Small enterprises:** Small enterprises are businesses which on their balance sheet dates do not exceed the limits of at least two of the three following criteria: 1) a balance sheet total of € 5 000 000, 2) net turnover of € 10 000 000 and 3) average number of employees during the financial year of 50.
- **Social engineering:** Activities that attempt to exploit human error or human behavior with the objective of gaining access to information or services.
- **Supply Chain Attack:** A method of cyberattack targeting vulnerabilities within an organization's supply chain, often exploiting smaller businesses to gain access to larger entities.
- **Web-Based Attacks:** Cyberattacks that exploit vulnerabilities in web applications, websites, or online services to gain unauthorized access, steal data, or disrupt operations.
- **WEF (World Economic Forum):** An international organization that engages leaders from business, politics, and academia to address global challenges.

[38] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) (OJ L 124, 20.5.2003, pp. 36–41)

ABOUT

The European Microfinance Network (EMN) is a member-based not-for-profit organisation based in Brussels, which promotes microfinance as a tool to fight social and financial exclusion in Europe through self-employment and the creation of microenterprises. It is the Network's mission to facilitate capacity building and to advocate on behalf of the sector.

Mastercard Strive is a portfolio of philanthropic programs supported by the Mastercard Center for Inclusive Growth and funded by the Mastercard Impact Fund. With programs in more than 20 countries around the world, Mastercard Strive aims to reach 18 million small businesses to go digital, get capital, and access networks and know-how.

SHARE YOUR THOUGHTS WITH US