Q&A Guide

Promoting Cybersecurity for SMEs in Europe

Global Digital Foundation
The Digital Policy Network

eit Digital

Co-funded by the European Union

HUAWEI

00 TABLE OF CONTENTS

CHAPTER 01

WHY SMEs MATTER

WHY ARE SMEs SO IMPORTANT FOR EUROPE?

SMEs contribute to the EU economy through the creation of high-quality jobs. The promotion and protection of SMEs in Europe are key political priorities for EU policymakers.

25mil

There are 25 million SMEs in Europe.

99%

SMEs represent more than 99% of all firms in Europe.

100mil

SMEs employ 100 million people in Europe.

+**50**%

SMEs contribute to over half of the EU GDP.

SMEs underpin the building of a more innovative society.

SMEs are drivers of digital transformation & economic growth.

WHY SHOULD SMEs HAVE ROBUST LEVELS OF CYBER-SECURITY?

Recent Covid-19 pandemic confinement restrictions accelerated the need for SMEs to further digitalise their operations and offerings. The digitalisation of a large share of European SMEs happened very quickly. This growth in digitalisation was unfortunately marked by an increase in cybersecurity attacks. According to the World Economic Forum (WEF), there was an increase of 667% in phishing attacks during the initial months of Covid-19 in 2020. A number of these SME businesses were unprepared for cyber attacks with many employees unaware as to how to mitigate against cyber risk. It is not correct to assume that cyber attacks target large companies only. There is clear evidence that the SME sector is being systematically targeted by cyber criminals too.

- In an ENISA survey in 2021, 57% of SMEs believe that their companies will go out of business as a result of a cyber attack. This clearly results in very negative consequences for the SME that has been attacked. In a broader sense, it also undermines business confidence and disrupts the process of digital transformation across Europe. Cyber attacks against SMEs can have a disruptive effect on the EU economy.

- The cybersecurity of SMEs is critical in securing the supply chain in Europe. Supply chain cybersecurity can be defined as the resilience of each company, product and service involved in delivering a final product or solution to the end user. The number of supply chain attacks is increasing exponentially. The ENISA Threat Landscape Report 2022 has found that supply chain attacks account for 17% of all cyber attacks in 2022, compared to only 1% in 2021. Many attacks where the networks or the information of customers is compromised relates to a security breach of a supplier.

- Higher levels of cybersecurity for SMEs will further protect EU cyber resilience. SMEs serve critical sectors of the European economy by contributing services and products to IT providers or to utility operators. As a way to penetrate otherwise secure critical infrastructure networks, cyber hackers do target SME suppliers to gain access to key networks and data.

- The cybersecurity of SMEs is an essential component in preserving the security of the people of Europe. If technology is unsecured and SMEs use it, this clearly generates vulnerabilities and poses higher risks for users.

2021

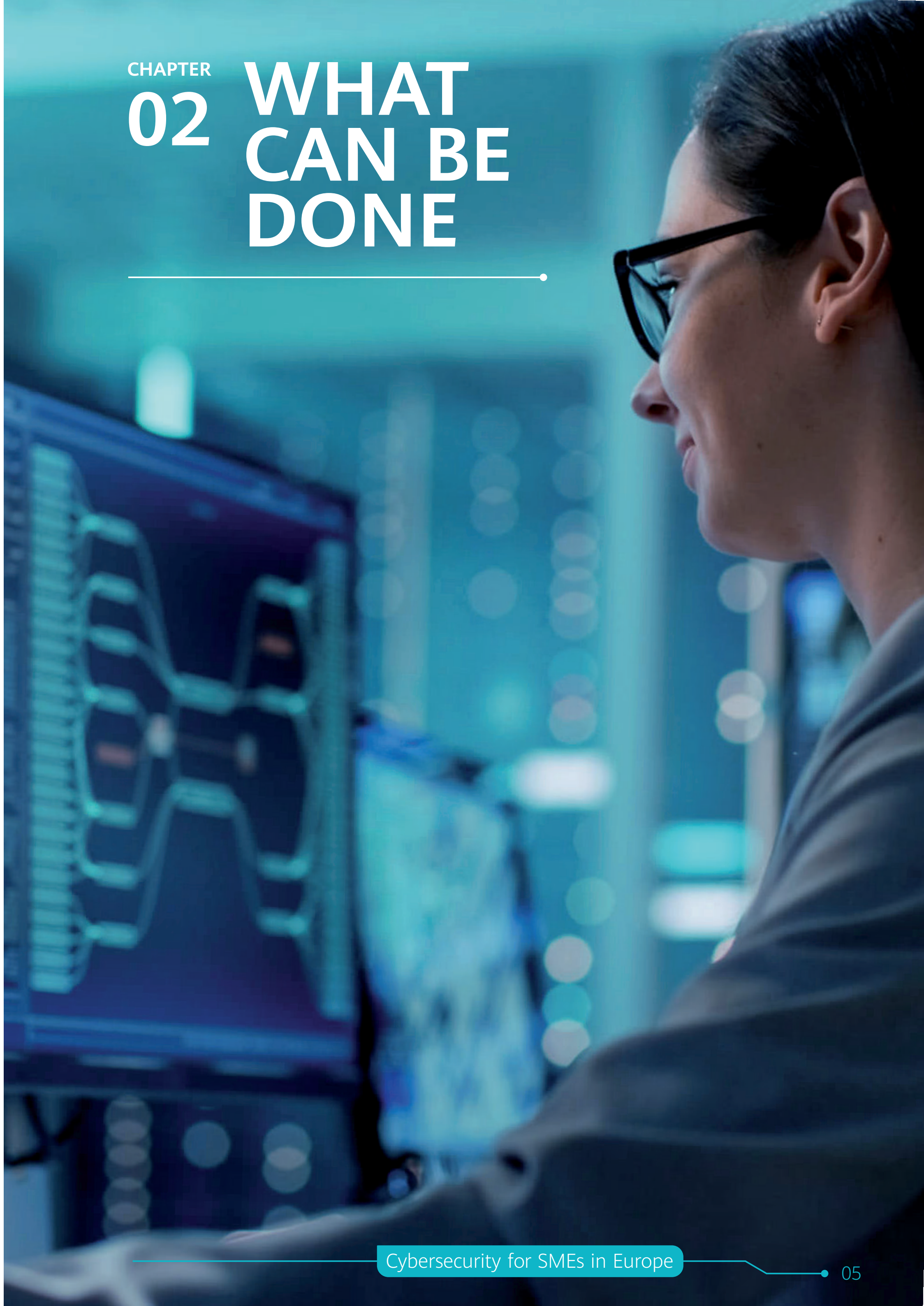
1,0%

Supply chain attacks accounted for only 1% of all cyber attacks.

2022

17,0%

Supply chain attacks accounted for 17% of all cyber attacks.



CHAPTER 02

WHAT CAN BE DONE

WHAT ARE THE KEY CHALLENGES FOR SMEs IN THE PROMOTION OF HIGHER CYBERSECURITY STANDARDS AND CYBER SKILLS?

A key concern for SMEs is the continuation or expansion of business opportunities and doing so in a safe and secure manner. To achieve this objective, SMEs need to take account of the evolving cyber threat landscape. Key challenges related to the cybersecurity of SMEs include the following:

A human element

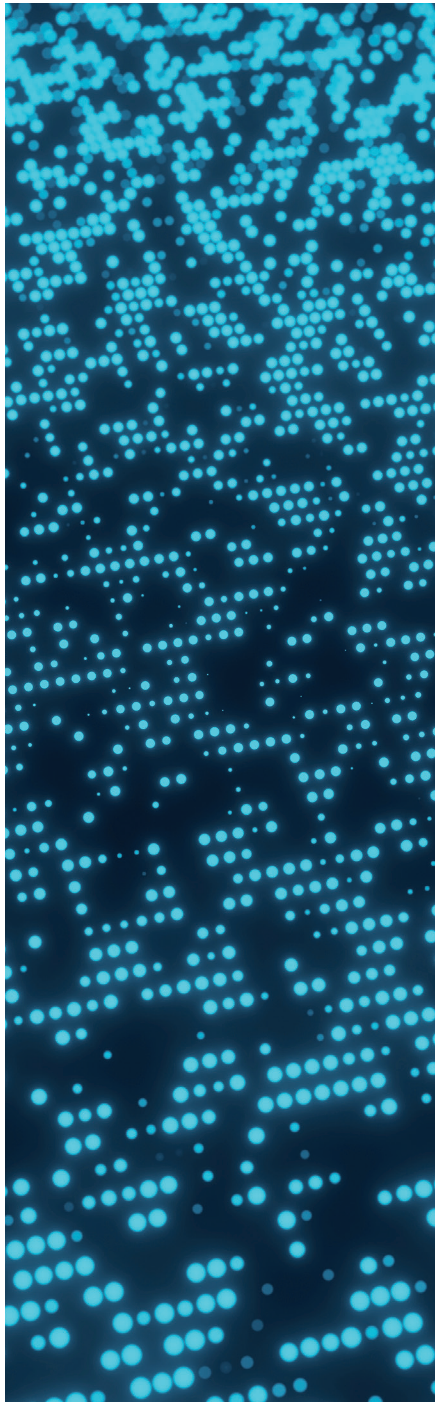
According to Verizon's 2022 Data Breaches Investigations report, 82% of data breaches involve a human element. This is linked to the lack of cybersecurity awareness of some employees and users. It is challenging to address this underlying problem – human behaviour and habits. Securing sensitive data and protecting it from theft should be an essential element of employee cyber skills training.

Investment

93% of SMEs are of a micro nature, with less than 10 employees and without any dedicated IT or security personnel. Like fire or house insurance, cybersecurity investment is critically important in protecting the products and services of SMEs. It can take time and specialist expertise to assess the cyber risk and to identify the critical processes and assets that need to be protected. We have to stop situations where companies realise the need for cybersecurity only after a significant incident – evidently when it is too late.

Lack of skills and competence

SMEs face difficulty in accessing trained security professionals for tailored advice on integrating cybersecurity into their operations. According to an ISC2 Cybersecurity Workforce Study 2021, Europe was lacking over 200,000 cybersecurity specialists. This all leads to an increased responsibility for SME managers and employees to keep up to date with an ever-changing cybersecurity landscape. The Fortinet Cybersecurity Skills Gap Report 2022 revealed that 80% of organisations have suffered one or more breaches that could be attributed to a lack of cybersecurity skills and/or to a lack of cybersecurity awareness in the workplace. The European Cybersecurity Skills Framework was published by ENISA in April 2022. This framework identifies the critical cybersecurity skills set that is required for the workplace. It also provides the appropriate tools for HR personnel to better understand what is exactly needed to recruit cybersecurity staff.



WHAT PRACTICAL MEASURES NEED TO BE TAKEN TO HELP IMPROVE CYBERSECURITY FOR SMEs IN EUROPE?

There are four key measures that should be considered in building a security strategy that can minimise the risk of operational interruptions, data compromise and data loss:

- Identifying critical enterprise processes and resources, security threats, vulnerabilities and risks.
- Implementing security measures, such as strong access control, awareness and training, vulnerability and patch management, data backup and recovery processes.
- Using up-to-date anti-malware, security incident detection and staff/user reporting procedures.
- Maintaining incident and disaster recovery plans and putting in place the appropriate communication structures to engage with stakeholders.

WHAT SHOULD SMEs DO TO REDUCE THE MOST COMMON TYPES OF CYBER THREATS?

The most common types of attacks on SMEs include malware, phishing, web based attacks, ransomware and distributed denial of service (DDoS).

Strict access control: secure password management

- Over 60% of all cybersecurity breaches involve user credentials. Poor and weak password practices pose a real risk to cybersecurity.
- Using a strong, unique password with at least 12 characters and letters, numbers and symbols. It is strongly recommended to use a password manager in order to generate, manage and store passwords in an encrypted form.
- Applying/activating multi-factor authentication (MFA) for the applications and systems that SMEs use or make available. MFA acts as a further layer of security protection for SMEs.

Managing vulnerabilities

- It is incumbent on SMEs to ensure that vulnerabilities in their products are identified and mitigated. Vulnerability patches and mitigating measures for the products/services that they use (as flagged by suppliers or national authorities) can be applied in a timely manner.
- Antivirus installation and maintenance is an essential step in protecting the operating systems and applications of SMEs from other threats.

Secure data backup

- Backing up the essential data for business activities in at least 2 locations outside a corporate network.
- Using full disk encryption to ensure that in the case a hard disk is lost or stolen, the data remains safe. Encryption keys can be securely protected.

Firewall installation and maintenance

- Installing a firewall in order to improve security by isolating a trusted network from an untrusted network. Patching and hardening the firewall. Using a whitelisting approach (default deny) to only allow for the specific traffic that is required by the services used by the business. Updating the firewall software regularly, and wherever possible automating the process.

Wireless / Wi-Fi Protected Access (WPA)

- Using WPA3 wherever possible and a strong unique password with Wi-Fi network encryption containing at least 20 letters, numbers and special characters.

Virtual Private Network (VPN) for access outside a corporate network

- A strong VPN can provide secure remote access to a network and applications.

Maintain an Incident and Disaster Recovery Plan

- Defining and maintaining an incident and disaster recovery plan to respond to security breaches so that SMEs are able to regain control over their business operations and data.

WHY IS IT SO IMPORTANT THAT MANAGERS IN SMEs CLEARLY COMMUNICATE WORK RESPONSIBILITIES CONNECTED TO CYBERSECURITY ISSUES?

- Managers in SMEs need to communicate very clearly to their staff and explain concisely what is expected from them to mitigate against cyber attacks in the workplace.
- Proper cybersecurity training should be given in password management, data back-up and in how to respond to a cyber attack. Training can emphasise that 82% of data breaches occur as a result of human error.
- It is advised that a plan is developed in how to communicate with stakeholders in the case of a cybersecurity incident.

Training can emphasise that 82% of data breaches occur as a result of human error.

82%

Result of human error

WHAT CAN SMEs DO TO STOP MALWARE BEING INSERTED INTO THEIR SYSTEMS?

The main purposes of malicious code are the following:

01

Encryption, modification or theft of information, e.g. to demand ransom or resell the data.

02

Monitoring data flows, e.g. for corporate gain.

03

Taking control of a device, e.g. to cause an incident.

Key measures for SMEs to protect themselves against malware:

- Installing and maintaining specialised anti-malware software. Such software can be installed on mobile devices, operating systems and in networks. The software scans incoming data for malware and blocks or quarantines suspicious or proven malicious code before use. There are many different anti-malware software types for sale in the marketplace.
- Users/Employees should remain alert and refrain from clicking on suspicious links in emails or open suspicious attachments.
- Data needs to be backed up.

HOW CAN FIREWALLS IMPROVE SECURITY FOR SMEs?

A firewall tries to improve security by isolating internal systems, applications and data from an untrustworthy network like the Internet.

- The rules defining network access should be specific. Company security guidelines can be defined.
- Regular audits of firewalls should be carried out. For example, any unauthorised firewall configuration change should be flagged.

HOW CAN SMEs RECOGNISE PHISHING ATTACKS?

Phishing attacks are a type of social engineering attack, i.e. targeted at people rather than at system vulnerabilities. It is, in essence analogous to traditional types of fraud. By default, phishing is not a complex technical attack. It just requires a good reason such as a fraud scenario to make the user click on a malicious link, open a malicious file or URL or type/give confidential information.

Recognising common types of fraud scenarios can prevent SMEs from falling victim to many phishing attacks. Understanding the different types of phishing attacks will help managers and employees in SMEs to develop an instinct to check email and other messages carefully before they click on links or attachments contained within them.

Questions that people working in SMEs should ask so as to stop a phishing attack:

Is the message solicited or expected? If not, all the questions below should be answered to identify a phishing attempt.

Is the sender legitimate, i.e. using the correct corporate email, profile or phone number? If not, this could be a phishing attempt.

Is there a sense of urgency in the message, a scary consequence or a great reward? If yes, this could be a phishing attempt.

Is the request claiming to come from a bank, postal services, tax administration, or from a law enforcement agency? If yes, this could be a phishing attempt and may emanate from a widespread type of a phishing attack. These types of organisations typically use secure communication channels (e.g. apps). If in doubt, go directly to the 'sender' app/web page and log in to check if any messages appear.

Is the message appearing odd, with typos or is very generic? Then this could be a phishing attempt.

WHAT CAN SMEs DO IN THE CASE OF A PHISHING ATTACK?

Phishing attacks are a reality for SMEs. They should consider the following responses:

- Never click on a link in the case of a suspected phishing attack.
- Flag the message as phishing to their IT department or to the platform used or to the impersonated organisation.
- Delete the message.
- In the case of a phishing attack, inform the security/IT team and change passwords and PINs for all important accounts (email, bank, authentication services, operating systems and cloud services).
- If the phishing attack is successful, systems and data may be compromised and become inaccessible. In that case, they could receive a ransomware message. There are some useful resources containing advice as to how to engage in the case of a ransomware incident such as the Europol No More Ransom site and working with their local CSIRT (Computer Security Incident Response Team).

WHAT CAN SMEs DO TO AVOID A WEB-BASED ATTACK?

A web-based attack exploits internet infrastructure security weaknesses in order to carry out a cyber attack against, for example a company website, an e-commerce site, a blog or a search engine. Examples of a web-based attack include the installation of malicious code to extract sensitive information such as a consumer database or a payment detail, a modification of the data on the website, the deletion of data and the sabotaging of website access.

- For protection against web-based attacks, SMEs should consider the following:
- Keeping operating systems up to date. The latest available security updates can be installed in a timely manner.
- Enabling security options, such as strong authentication for administrative access, encryption and backup.
- Controlling and monitoring websites to detect and prevent vulnerabilities and the delivery of malicious code.

CHAPTER 03

SUPPORT AT A EUROPEAN LEVEL

WHAT IS THE EU POLICY TOWARDS SUPPORTING SMEs FROM A CYBERSECURITY VIEWPOINT?

The EU approaches the improvement of cybersecurity for SMEs in 2 ways: investment and regulation.

Cybersecurity Act (2019)

- One policy instrument that promotes and supports the cybersecurity of SMEs in the EU is the Cybersecurity Act 2019. It lays the groundwork for the enhanced development of EU-wide cybersecurity certification schemes.

- Such certification schemes can benefit SMEs looking for cybersecurity assurance from their suppliers, as well as act as an instrument to promote and give a competitive advantage to SMEs that invest in cybersecurity. There are three major EU cybersecurity certification schemes in the making that are focused on Cloud Services (EUCS), 5G and the building of Common Criteria (EUCC) for trusted ICT products in the EU. Cloud and 5G are the infrastructural building blocks that will enable both a stronger digitalisation of SMEs and new services development. The Common Criteria scheme certifies the ICT security attributes of products and this may in turn be used by SMEs as part of their product and service offerings.

NIS2 / Cyber Resilience Act (CRA)

- The new **NIS2 Directive (2020)** will introduce a series of measures that will require operators of certain important services within the EU to implement security measures and carry out an assessment of the cybersecurity risk of suppliers. In exceptional cases this may include some SMEs from the EU member states.

- In September 2022, the European Commission published the **Cyber Resilience Act (CRA)** that is focused on improving cybersecurity for products with a digital element (e.g. Manufacturers of digital products). According to this CRA proposal, such products must comply with strict cybersecurity, incident and vulnerability management, risk analysis and notification requirements before being placed on the EU market. The governance and legislative approach of the CRA is based on the NLF (New Legislative Framework) process that currently is in place to certify the safety of products for the EU market.

Horizon Europe / Digital Europe

- On the investment side, the EU has allocated €10 billion for cybersecurity collaborative actions under the **Horizon Europe** research, innovation and science programme 2021-2027. Funds are available too from the **Digital Europe** programme for SMEs to promote higher levels of cybersecurity in Europe. These initiatives afford SMEs more opportunities to expand their footprint in Europe in developing new, innovative cybersecurity related products and services.

The EU has allocated €10 billion for cybersecurity collaborative actions under the Horizon Europe research, innovation and science programme 2021-2027.

InvestEU / EU Recovery and Resilience Facility

- Cybersecurity is also a part of InvestEU, a financial instrument that will support stronger cybersecurity value chains in Europe. Under the EU Recovery and Resilience Facility many EU countries are adopting plans that contain a number of additional investments in cybersecurity.

European Year of Skills 2023

- A number of new cybersecurity-related initiatives in the area of cyber skills will be developed by the European Commission and by EU member states in the context of the roll-out of activities under the European Year of Skills 2023.

HOW CAN EIT DIGITAL FURTHER SUPPORT SMEs IN DELIVERING HIGHER LEVELS OF CYBERSECURITY?

EIT Digital embodies the future of innovation by mobilising a pan-European multi-stakeholder open-innovation ecosystem of top European corporations, SMEs, start-ups, universities and research institutes. Students, researchers, engineers, business developers and investors can address the technology, talent, skills, business and capital needs of digital entrepreneurship.

EIT Digital builds the next generation of digital ventures, digital products and services. This breeds digital entrepreneurial talent, helping businesses and entrepreneurs to be at the frontier of digital innovation by providing them with technology, talent, and growth support.

EIT Digital answers specific innovation needs by, for example, finding the right partners to bring technology to the market, supporting the scale-up of digital technology ventures, attracting talent and developing digital knowledge and skills.

As the largest digital innovation ecosystem in Europe, **EIT Digital** is contributing to higher standards of SME cybersecurity in several ways. This is in order to increase the number of European cybersecurity products and services, which currently stands at around 16% of the global cybersecurity market. EIT Digital runs a variety of initiatives to support both start-up companies and the scaling up of SME enterprises:

EU European cybersecurity products & services. make up **16%** of the global cybersecurity market.

- Through its Accelerator, EIT Digital identifies and supports the scaling of new European cybersecurity startups. This further contributes to the diversity and availability of SME cybersecurity solutions.

- The EIT Digital DeepHack programme brings together digital innovators and entrepreneurs to solve critical business challenges including within the cybersecurity field.

- The EIT Digital Innovation Factory initiative brings European partners together to create the next generation of digital ventures, products and services.

- The EIT Digital Venture Programme provides financial support and training to European entrepreneurs to get new deep tech ventures started.

- The skills gap is being closed through the work of the EIT Digital Masters Cybersecurity Programme. This initiative is already taking place in a number of countries in Europe, including in the Netherlands, Italy, France, Hungary, Romania and in Finland. Issues being addressed by these courses relate to addressing skills shortages in cloud computing security, application security, cyber risk management, security analysis, cryptography, network infrastructure security, systems validation and secure data management.

HOW CAN THE EUROPEAN CYBERSECURITY COMPETENCE CENTRE AND NETWORK DELIVER HIGHER STANDARDS OF CYBERSECURITY FOR SMEs?

- One of the roles of the European Cybersecurity Competence Centre (ECCC) is to support and coordinate a number of research & innovation projects related to cybersecurity issues within Europe. This is one example of a coordinated effort across the EU to help ensure that SMEs can translate cybersecurity research activities into innovative products and solutions for the marketplace.

- The annual cybersecurity work priorities of the ECCC can give further strong support to SMEs to take part in both the Horizon Europe and Digital Europe initiatives.

- The ECCC closely engages with the Network of National Coordination Centres (NCCs) across the 27 member states of the EU. This collaboration can expand upon SME cybersecurity support programmes in individual EU member states and uniformly across the EU.

- Support capacity building across the 27 EU Member states to promote higher standards of cybersecurity and an increased uptake in cybersecurity certification.

04 USEFUL CYBERSECURITY INFORMATION AND RESOURCES FOR SMEs.

ENISA (European Union Agency for Cybersecurity)

- Cybersecurity for SMEs (2021).
  https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
- SME Cloud Security Tool (2021).
  https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security/security-for-smes/sme-guide-tool
- European Cybersecurity Month.
  https://cybersecuritymonth.eu/
- Be aware, be prepared – Cybersecurity Tips for SMEs.
  https://www.youtube.com/watch?v=epJTYOdW3sU&t=24s&ab_channel=ENISAvideos
- Cybersecurity Culture Guidelines. Behavioural Aspects of Cybersecurity (2021).
  https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/at_download/fullReport
- European Cybersecurity Skills Framework 2022.
  https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

Europol

- In the case of a ransomware attack, SMEs can find support for reaction plans and decryption keys as advised by Europol.
  https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

ETSI

- Cybersecurity for SMEs. Part 1: Cybersecurity Standardisation Essentials.
  https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf

OECD

- Digital Security in SMEs 2021.
  https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en#chapter-d1e7025

World Economic Forum

- What SMEs need to do for a Cybersecurity future 2021?
  https://www.weforum.org/agenda/2021/06/cybersecurity-for-smes-europe/

CyberWatching.eu

- SMEs Guides:
  https://cyberwatching.eu/smes-guides

CSIRT (Computer Security Incident Response Teams) in the EU27

- https://csirtsnetwork.eu/

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.