**Training Fiche**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | Keep your data safe: Cybersecurity for MSMEs | | | |
| **Keywords** | Data security, Cybersecurity, Data protection, Information security, Cyber threats, Data breaches, Network security, Risk management, Security best practices, Cyber awareness | | | |
| **Provided by** | IT Solutions for All | | | |
| **Language** | English | | | |
| **Training area** | **Fundamentals of digital entrepreneurship in microenterprise settings**  **Digital communication and branding**  **Digital finance**  **Cybersecurity** | | | |
| **Learning outcomes** | **EntreComp** | | | |
| Ideas & opportunities  Resources  Into action  **Specific competences addressed:**  Mobilising resources, mobilising others, planning & management, coping with uncertainty, ambiguity & risk, learning through experience | | | |
| **DigComp** | | | |
| Information and data literacy  Communication and collaboration  Digital content creation  Safety  Problem solving  **Specific competences addressed:**  Protecting devices, protecting personal data and privacy, identifying needs and technological responses | | | |
| **Proficiency level** | | | |
| Level 1  Level 2 | Level 3  Level 4 | Level 5  Level 6 | Level 7  Level 8 |
| **Foundation** | **Intermediate** | **Advanced** | **Expert** |
| **Description** | In today's digital age, data is a valuable asset for every organization, including Micro, Small, and Medium Enterprises (MSMEs). However, with the increasing reliance on technology, the risk of cyber threats and data breaches has never been higher.  Our training course, "Keep Your Data Safe: Cybersecurity for MSMEs," is specifically designed to empower MSME owners, managers, and employees with the knowledge and skills needed to protect their valuable data and sensitive information. | | | |
| **Learning objectives** | * To gain a comprehensive understanding of cybersecurity threats and the necessary measures to protect their MSMEs. * To be equipped with the knowledge and skills to establish a secure IT infrastructure. * To be able to manage information security and respond effectively to cybersecurity incidents. | | | |
| **Index (3 levels: Module-Unit-Section)** | **Module: Keep your data safe: Cybersecurity for MSMEs**  **Unit 1**: Introduction to cybersecurity for MSMEs  Section 1.1. Understanding cybersecurity: definition and importance of security policies  Section 1.2. Common cybersecurity threats faced by MSMEs  **Unit 2**: Establishing a secure ICT infrastructure  Section 2.1. Assessing cybersecurity vulnerabilities  Section 2.2. Effective use of antivirus and antimalware solutions  **Unit 3**: Managing information security  Section 3.1. Practices and guidelines | | | |
| **Content developed** | **Module: Keep your data safe: Cybersecurity for MSMEs**  **Unit 1: Introduction to cybersecurity for MSMEs**  **Section 1.1.** Understanding cybersecurity: definition and importance of security policies  A security policy for Micro, Small, and Medium Enterprises (MSMEs) is a formal document that outlines the organization's approach to information security. It sets the rules, guidelines, and responsibilities for protecting the company's assets, data, and systems from potential threats and unauthorized access. The policy should be comprehensive, clear, and tailored to the specific needs and risks faced by the MSME. Understanding cybersecurity and the importance of security policies for Micro and Small medium enterprises after COVID is crucial for several reasons:  **Awareness of Cyber Threats**: Understanding cybersecurity allows individuals **to be aware of the various cyber threats and risks that exist in the digital landscape.** It **helps them recognize potential vulnerabilities** and weaknesses in their systems, networks, and practices.  **Protection of Sensitive Data**: Cybersecurity measures protect sensitive and confidential data from unauthorized access, theft, or misuse. This is especially **vital for MSMEs, as they often handle valuable customer information,** financial data, and intellectual property.  **Prevention of Data Breaches**: Security policies play a significant role in preventing data breaches and cyber attacks. They **outline procedures and guidelines to ensure that data is handled securely** and that potential entry points for attackers are minimized.  **Maintaining Business Continuity**: Cybersecurity is essential for the **smooth functioning of an MSME**. Security policies **help in identifying potential risks** that could disrupt business operations and aid in developing strategies to maintain continuity in the face of cyber incidents.  **Compliance and Legal Requirements**: Many industries have specific regulations and legal requirements concerning data protection and cybersecurity. **Understanding cybersecurity helps MSMEs adhere to these regulations, avoid penalties,** and maintain the trust of customers and partners.  **Building Customer Trust**: Demonstrating a commitment to cybersecurity and having robust security policies in place **can enhance customer trust and confidence in an MSME**. Customers are more likely to do business with organizations that prioritize the protection of their data and privacy.  **Preventing Financial Loss: Cyber attacks can result in significant financial losses for MSMEs**. Understanding cybersecurity and implementing effective security policies **can help mitigate financial risks associated with data breaches and other cyber incidents**.  **Reputation Management**: A successful cyber attack can **damage an MSME's reputation**, leading to **a loss of customers and opportunities**. Security policies help prevent incidents and demonstrate the organization's dedication to safeguarding information.  **Crisis Preparedness**: Cybersecurity awareness and security policies help MSMEs **be prepared for potential crises** reducing the recovery time.  **Employee Training and Awareness**: Understanding cybersecurity allows organizations to provide appropriate training to their employees. **Educating staff** about best practices, potential threats, and security policies **helps create a strong security culture** within the organization.  **Competitive Advantage**: Emphasizing cybersecurity and having effective security policies in place can **provide an MSME with a competitive edge**. **Customers and partners often prioritize security** when choosing business partners, making cybersecurity a valuable differentiator.  In conclusion, understanding cybersecurity and the importance of security policies is fundamental for MSMEs to protect their data, maintain business continuity, comply with regulations, and build trust with customers and stakeholders. By proactively addressing cyber threats, MSMEs can strengthen their resilience and ensure a secure digital environment for their operations.  **Section 1.2.** Common cybersecurity threats faced by MSMEs  Micro, Small, and Medium Enterprises (MSMEs) are increasingly becoming targets for cybercriminals due to their valuable data and potentially weaker cybersecurity defenses compared to larger organizations. Some common cybersecurity threats faced by MSMEs include:  **Phishing Attacks**: Phishing is a technique where cybercriminals send deceptive emails, messages, or websites to trick employees into divulging sensitive information like login credentials, financial data, or personal information.  **Ransomware**: Ransomware is a type of malware that encrypts an organization's data, rendering it inaccessible until a ransom is paid. MSMEs may be targeted due to perceived weaker security measures.  **Malware Infections**: MSMEs are susceptible to various types of malware, including viruses, Trojans, and spyware. These malicious programs can disrupt operations, steal data, or gain unauthorized access to systems.  **Insider Threats**: Insider threats involve malicious actions or unintentional mistakes made by employees or individuals with access to an organization's systems, data, or networks.  **Social Engineering Attacks**: Social engineering involves manipulating individuals into revealing confidential information, such as passwords or login credentials. This could occur through phone calls, in-person interactions, or social media.  **Unsecured IoT Devices**: Many MSMEs utilize Internet of Things (IoT) devices, such as smart cameras or sensors. If not properly secured, these devices can become entry points for attackers to infiltrate the network.  **Weak Passwords and Authentication**: Inadequate password practices, such as using easily guessable passwords or reusing them across multiple accounts, can make MSMEs vulnerable to brute force attacks or credential stuffing.  **Data Breaches**: MSMEs often collect and store valuable customer data. If not adequately protected, a data breach could lead to reputational damage, financial loss, and legal consequences.  **Denial of Service (DoS) Attacks**: DoS attacks overwhelm an organization's systems or network with a flood of traffic, causing disruptions and downtime.  **Lack of Regular Software Updates and Patches**: Failing to apply timely updates and security patches to software and operating systems can leave MSMEs exposed to known vulnerabilities.  **Cloud Security Concerns**: Storing data and applications in the cloud can be convenient for MSMEs but may also introduce security risks if not appropriately configured and managed.  **Supply Chain Attacks**: Cybercriminals may target MSMEs as a means to gain access to larger organizations by exploiting vulnerabilities in the supply chain.  **Misconfigured Security Settings**: Incorrectly configured security settings on systems, applications, or network devices can create unintentional security gaps.  **Lack of Employee Cybersecurity Awareness**: Insufficient cybersecurity awareness and training among employees can increase the likelihood of falling victim to various cyber threats.  To mitigate these threats, MSMEs should invest in cybersecurity measures, such as regular employee training, robust access controls, strong authentication methods, secure ICT infrastructure, information security management, up-to-date security software, and a well-defined incident response plan. Proactive cybersecurity practices can significantly reduce the risk of falling victim to cyber attacks and protect the organization's valuable assets and reputation.  **Unit 2: Establishing a secure ICT infrastructure**  **Section 2.1.** Assessing cybersecurity vulnerabilities  Assessing cybersecurity vulnerabilities is essential for MSMEs to identify potential weaknesses in their systems, ICT infrastructures, networks, and practices. Here are steps that an MSME can take to assess its cybersecurity vulnerabilities:  **Identify Assets and Data**: Start by identifying all the assets, ICT infrastructure, systems, devices, and data that your MSME uses or stores. This includes hardware, software, servers, network devices, cloud services, and sensitive information.  **Conduct a Risk Assessment**: Perform a comprehensive risk assessment to identify potential threats, vulnerabilities, and the potential impact of a cyber incident on your organization. This assessment will help prioritize efforts to address the most critical risks first.  **Penetration Testing**: Consider conducting penetration testing (ethical hacking) to simulate real-world cyber attacks on your systems and networks. This helps identify potential entry points and weak areas in your security defenses.  **Review Network Security**: Assess the security of your network infrastructure, including firewalls, routers, switches, and wireless networks. Ensure that these devices are appropriately configured, and access controls are in place.  **Evaluate Software and Applications**: Regularly check for security updates and patches for all software and applications used in your organization. Outdated software can create vulnerabilities that cyber attackers may exploit.  **Assess Endpoint Security**: Evaluate the security measures on endpoint devices (e.g., laptops, smartphones, tablets) used by employees. Implement antivirus software, encryption, and enforce policies for accessing company data on personal devices.  **Check Physical Security**: Don't overlook physical security. Assess the physical access controls to your office premises, server rooms, and sensitive areas where data and equipment are stored.  **Examine Employee Awareness**: Evaluate the level of cybersecurity awareness among your employees. Conduct training and workshops to educate them about common cyber threats and best practices for data security.  **Review Password Policies**: Ensure that strong password policies are in place, including requiring complex passwords, regular password changes, and not reusing passwords across multiple accounts.  **Secure Cloud Services**: If using cloud services, assess their security features and ensure they meet your organization's requirements. Implement multi-factor authentication and encryption for sensitive data stored in the cloud.  **Analyze Security Policies**: Review and update security policies regularly. Ensure they align with industry standards and compliance requirements. These policies should cover areas like data protection, access controls, incident response, and acceptable use.  **Audit Third-Party Vendors**: If you work with third-party vendors or service providers, assess their cybersecurity practices and data protection measures to ensure they don't introduce additional risks.  **Incident Response Readiness**: Evaluate your organization's incident response plan to ensure it is comprehensive and covers the appropriate steps to take in case of a cyber incident.  **Regular Security Audits**: Conduct periodic security audits and assessments to maintain an ongoing understanding of your organization's cybersecurity posture.  **Ensuring wi-fi network security:** Securing Wi-Fi networks is crucial for preventing unauthorized access and protecting sensitive data.  It can be achieved by:   * changing default credentials * using strong encryption * enabling wi-fi protected access 3 (WPA3) or WPA2 with AES (advanced encryption standard) for strong encryption * avoiding using outdated and vulnerable encryption methods like WEP (wired equivalent privacy) * modifying the default service set identifier (SSID) to a unique name that doesn't reveal information about your business or organization * turning off SSID broadcasting to make your network less visible to potential attackers * setting up a separate guest network for visitors or customers that isolates them from your main internal network, using strong passwords * enabling mac address filtering to allow only specific devices with pre-approved mac addresses to connect to your wi-fi network * keeping firmware updated * disabling remote management on router to prevent unauthorized access from outside your network * enabling firewall and network encryption * disabling universal plug and play (UPNP) on your router, as it can be exploited by attackers to open ports and expose your network to potential threats * monitoring network activity * securing physical access * educating employees.   **Section 2.2.** Effective use of antivirus and antimalware solutions:  Effective use of antivirus and antimalware solutions is critical for Micro, Small, and Medium Enterprises (MSMEs) to protect their ICT infrastructure, systems, networks, and data from various cyber threats.  Here are some best practices for using antivirus and antimalware solutions effectively:  **Choose a Comprehensive Solution**: Select a reputable and comprehensive antivirus and antimalware software that offers real-time protection, regular updates, and frequent scans to detect and remove malicious software.  **Keep Software Updated**: Ensure that the antivirus and antimalware software is up to date with the latest virus definitions and database updates. This is essential to detect and protect against new and emerging threats.  **Enable Real-Time Scanning**: Activate real-time scanning features in the antivirus software to automatically check files, downloads, and email attachments for malware as they are accessed.  **Schedule Regular Scans**: Set up scheduled scans to run at convenient times when the system is least likely to be in heavy use, such as outside of business hours.  **Enable Automatic Updates**: Enable automatic updates for both the antivirus software and the operating system to ensure continuous protection against the latest threats.  **Perform Full System Scans**: Conduct full system scans periodically to thoroughly check all files, including those in less frequently accessed areas.  **Quarantine and Isolate Threats**: Configure the antivirus software to quarantine or isolate detected threats, preventing them from spreading or causing further harm.  **Scan External Devices**: Scan all external devices, such as USB drives or external hard drives, before accessing the files to prevent malware from being introduced into the network.  **Educate Employees**: Educate employees about the importance of antivirus and antimalware protection and train them to be cautious with email attachments, downloads, and links to avoid inadvertently introducing malware.  **Implement Endpoint Protection**: Consider using endpoint protection solutions that provide a multi-layered defense against various types of threats, including ransomware and zero-day exploits.  **Centralized Management**: If managing multiple systems, use centralized management tools to monitor and control antivirus and antimalware software across all devices from a single interface.  **Regular System Maintenance:** Regularly perform system maintenance tasks, such as disk cleanup and defragmentation, to optimize system performance and improve the effectiveness of antivirus scans.  **Monitor and Respond to Alerts**: Configure the antivirus software to send alerts for detected threats, and promptly respond to and investigate any alerts to take appropriate action.  **Periodic Security Assessments**: Conduct periodic security assessments and audits to evaluate the effectiveness of the antivirus and antimalware solutions and identify areas for improvement.  **Data backup and recovery strategies:** Implement a regular data backup strategy to ensure that important files are safe in the event of a severe malware infection or ransomware attack. Establish a routine backup schedule to ensure that critical data is backed up regularly. Depending on the volume of data and frequency of changes, daily, weekly, or monthly backups may be appropriate. Moreover, MSME can use automated backup solutions to reduce the risk of human error and ensure that backups are consistently performed without manual intervention. Don’t forget to store backup data in multiple physical locations to mitigate the risk of data loss due to theft, fire, or other disasters affecting a single location. Consider cloud-based backups in addition to on-site backups as a cost-effective and reliable solution. Cloud backups provide easy scalability, accessibility, and data redundancy.  Remember that cybersecurity is an ongoing process. Regular assessments, continuous monitoring, and prompt action to address vulnerabilities are essential to keep your MSME protected from evolving cyber threats.  **Unit 3: Managing information security**  **Section 3.1.** Practices and guidelines  Managing information security is crucial for Micro, Small, and Medium Enterprises (MSMEs) to **protect their sensitive data**, **maintain customer trust**, and **safeguard their business operations**.  Here are some key guidelines and practices that MSMEs can follow to effectively manage information security:  **Risk Assessment**: Conduct a thorough risk assessment to identify potential vulnerabilities and threats to information security. Understand the types of data the organization handles, the risks associated with each type, and the impact of a security breach.  **Security Policies and Procedures**: Develop and implement comprehensive information security policies and procedures that cover areas such as data handling, access controls, password management, data backup, and incident response.  **Employee Training**: Train all employees on information security best practices, data protection protocols, and how to recognize and respond to security threats like phishing attacks. Educating employees about cybersecurity is vital for a comprehensive defense strategy. Social engineering attacks and phishing are prevalent threats targeting MSMEs, employees need to be able to identify and mitigate their risks by recognizing phishing emails, handling suspicious attachments, and implementing email authentication protocols. In this sense, password security plays a crucial role in protecting sensitive data. Employees need to be aware of practices for creating strong passwords, implementing multi-factor authentication (MFA), and managing password policies within the organization.  **Access Controls**: Implement access controls to ensure that only authorized personnel have access to sensitive data. Use role-based access control to restrict access based on job roles and responsibilities.  **Secure Data Handling**: Establish guidelines for secure data handling, both in digital and physical formats. This includes proper storage, encryption, and secure disposal of sensitive information.  **Regular Software Updates and Patches**: Keep all software, including operating systems, applications, and security tools, up to date with the latest patches and updates to address known vulnerabilities.  **Firewalls and Antivirus Software**: Deploy firewalls and reputable antivirus/anti-malware software to protect against external threats.  **Secure Network Configuration**: Configure networks securely, including Wi-Fi networks, to prevent unauthorized access and data interception.  **Data Backup and Recovery**: Regularly backup critical data and test the data restoration process to ensure business continuity in the event of data loss or a cyberattack.  **Incident Response Plan**: Develop a clear incident response plan that outlines the steps to be taken in case of a security breach or data breach. Assign roles and responsibilities to key personnel for effective incident management. Preparing for and effectively responding to cybersecurity incidents is essential for minimizing damage and mitigating risks.  **Vendor Management**: If the MSME uses third-party vendors or service providers, conduct due diligence to ensure their information security practices align with your organization's standards.  **Continuous Monitoring and Auditing**: Implement continuous monitoring and periodic security audits to detect and address potential security issues proactively.  **Data Privacy Compliance**: Stay updated with relevant data privacy laws and regulations that apply to the MSME's operations. Comply with data protection requirements and inform customers about data handling practices.  **Security Awareness and Culture**: Foster a culture of security awareness and responsibility among employees. Encourage reporting of security incidents and concerns.  **Regular Security Reviews**: Conduct regular security reviews and risk assessments to identify emerging threats and potential areas for improvement.  By proactively managing information security, MSMEs can reduce the risk of data breaches, protect sensitive information, and build trust with customers and partners, ultimately contributing to the long-term success of the business. | | | |
| **5 glossary entries** | **Internet of Things (IoT).** The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.  Source: TechTarget <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>  **Denial of Service (DoS).** Denial of service (DoS) is a type of cyber attack designed to disable, shut down or disrupt a network, website or service. Typically, a malware is used to interrupt or inhibit the normal flow of data into and out of a system to render the target useless or inaccessible for a certain period. An example of a DoS attack: when a website is accessed massively and repeatedly from different locations, preventing legitimate visitors from accessing the website.  Source: Trend Micro <https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos>  **Multi-factor authentication.** Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.  Source: Onelogin <https://www.onelogin.com/learn/what-is-mfa>  **Service Set Identifier (SSID).** (Service Set IDentifier) The name assigned to a Wi-Fi (wireless) network. All devices in the network must use this case-sensitive name to communicate over Wi-Fi, which is a text string up to 32 bytes long. Out of the box, wireless routers and access points have a default SSID, which may be the manufacturer's name, such as "linksys" or "netgear" or simply "default." Some devices use their model number as the SSID. Using a Web browser, the SSID (and password) can be manually changed in the device's configuration settings.  **Source: PcMag** [**https://www.pcmag.com/encyclopedia/term/ssid**](https://www.pcmag.com/encyclopedia/term/ssid)  **Universal Plug and Play (UPnP).** UPnP (Universal Plug and Play) is a networking protocol that enables devices to discover each other and connect without the need for manual configuration or user intervention. The protocol automates all the steps necessary for recognition and communication between devices on the same network.  Source: **PhoenixNap** <https://phoenixnap.com/blog/what-is-upnp>  **Zero-day exploits**: A zero-day (0day) exploit is a cyber attack targeting a software vulnerability which is unknown to the software vendor or to antivirus vendors. The attacker spots the software vulnerability before any parties interested in mitigating it, quickly creates an exploit, and uses it for an attack. Such attacks are highly likely to succeed because defenses are not in place. This makes zero-day attacks a severe security threat.  Source: **Imperva** <https://www.imperva.com/learn/application-security/zero-day-exploit/>  **Ransomware**: Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. More modern ransomware families, collectively categorized as cryptoransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key.  Source: **Trend Micro** [**https://www.trendmicro.com/vinfo/us/security/definition/ransomware**](https://www.trendmicro.com/vinfo/us/security/definition/ransomware) | | | |
| **5 multiple-choice self-assessment questions** | **Question 1. What is a security policy?**  Option a: It is an informal document that outlines the organization’s approach to  information security  Option b: It is a formal document that sets the rules, guidelines, and responsibilities  for protecting the company’s assets, data, and systems from potential threats and  unauthorized access  Option c: A policy to protect only the company’s assets  Option d: The tree options are correct  **Correct option: b**  **Question 2. Why it is important to understand the cybersecurity and the security**  **policies?**  Option a: Understanding cybersecurity allows individuals to be aware of the various  cyber threats and risks that exist in the digital landscape  Option b: Cybersecurity measures protect sensitive and confidential data from  unauthorized access, theft, or misuse  Option c: Security policies play a significant role in preventing data breaches and  cyber-attacks  Option d: The three answers are correct  **Correct option: d**  **Question 3. Please, indicate which answer is true:**  Option a: Cyber-attacks can cause negligible financial losses to MSMEs  Option b: A successful cyber-attack can damage an MSME’s reputation, leading to a  loss of customers and opportunities  Option c: Educating staff about best practices, potential threats, and security  policies help create a strong security culture within the organization  Option d: Customers and partners often do not prioritise security when choosing  business partners, making cyber security a valuable differentiator  **Correct option: b & c**  **Question 4. Please, point out the common cybersecurity threats to MSMEs**  Option a: Insider treats, Infections and Well-configured security settings  Option b: Data Breaches, Weak Passwords and Authentication, Malware Infections  Option c: Phishing Attacks, Supply Chain Attacks, Unsecured IoT Devices  Option d: All answers are incorrect  **Correct option: b & c**  **Question 5. What steps an MSME can take to assess its cyber security**  **vulnerabilities?**  Option a: Check Physical Security, Examine Employee Awareness and Review  Password Policies  Option b: Identify Assets and Data, Conduct a Risk Assessment and Check Physical  Security  Option c: Ensuring wi-fi network security, Penetration Testing and Evaluate  Software and Applications  Option d: The three answers are correct  **Correct option: d** | | | |
| **Bibliography and further references** | Forbes Tech Council. (2023, May 25). Small But Mighty: Cybersecurity Best Practices for SMEs. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/?sh=44510c371a33>  Devonshire Green (n.d.). The Importance of Cybersecurity for SMEs. Devonshire Green. <https://www.devonshiregreen.uk/the-importance-of-cybersecurity-for-smes/>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity for SMEs: Challenges and Recommendations. ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes/@@download/fullReport>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity Guide for SMEs. ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport>  Ministry of Economy and Competitiveness (Spain). (2021). Digitalisation Plan for SMEs [PDF]. Government of Spain. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210902-digitalisation-smes-plan.pdf>  Yerik Afrianto Singgalen. (2021, August). Exploring MSMEs' Cybersecurity Awareness and Risk Management: Information Security Awareness. ResearchGate. <https://www.researchgate.net/publication/353622348_Exploring_MSMEs_>  Cybersecurity\_Awareness\_and\_Risk\_Management\_Information\_Security\_Awareness | | | |
| **Related material** | DREAM\_WP3\_Cybersecurity\_ITSFA\_EN | | | |
| **Video (if any)** | [link] | | | |