CSD | CENTER FOR THE STUDY OF DEMOCRACY

Cyber Security Survey for Businesses

A toolkit for investigating incident management and cybersecurity strategies among businesses

Cyber Security Survey for Businesses

A toolkit for investigating incident management and cybersecurity strategies among businesses

CSD
CENTER FOR
THE STUDY OF
DEMOCRACY

In recent decades, the private sector's online presence has grown steadily, marked by the rise of Web 2.0 and the implementation of cloud services and mobile computing. Within this context, cybercrime has emerged as a dynamic and growing threat to European businesses, which incur high costs for preventing cyber threats and offences to their IT infrastructures.

Authors:

Dr. Atanas Rusev, Director, Security Program, Center for the Study of Democracy
Dr. Tommaso Comunale, Analyst, Security Program, Center for the Study of Democracy
Dr. Alexander Gerganov, Director, Sociological Program, Center for the Study of Democracy

CSD CENTER FOR THE STUDY OF DEMOCRACY

CYBBAR

This report was funded by the European Union's Internal Security Fund — Police. The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Cover photo: Canva

Center for the Study of Democracy, 2023.

CONTENT

GLOSSARY

Business Email Compromise (BEC)

Rather than using a very general pretext designed to fool a large number of users, this particular attack is targeted directly at an individual or small group. "A BEC attack relies upon the ability to look like someone with power within a company or a trusted external partner. An attacker can accomplish this in a few different ways, including:

Domain Spoofing: Email address verification is not built into the email protocol (SMTP) by default. This means that an attacker can fake the display name and sender address of an email to make it look like it came from inside the company or a trusted vendor.

Lookalike Domains: Lookalike domains are designed to take advantage of characters that can be easily confused" (Check Point Software, n.d.).

Distributed Denial of Service (DDoS)

A Distributed Denial-of-Service (DDoS) attack is one of the most powerful types of attacks on the internet. DDoS attacks are perpetrated by cyber criminals to "make services or resources unavailable by flooding them with more requests than they can handle" (European Court of Auditors, 2019, p. 8).

Hack-and-leak operations (hacking)

"Hack-and-leak operations include activities where a threat actor has unlawfully accessed information via a cyberattack and then leaks this information" (ENISA, 2021, p. 22).

Malware

"Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of a system" (ENISA, 2021, p. 8).

Phishing

"Aims at stealing important information like credit card numbers and passwords, through e-mails involving social engineering and deception" (ENISA, 2021, p. 56).

Ransomware

"A type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access" (ENISA, 2021, p. 8).

Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources. Phishing and Business Email Compromise (BEC) are variants of social engineering.

Business identity theft

Business identity theft can be defined as a "type of identity theft committed with the intent to defraud or hurt a business (e. g. financial business identity, extortion)" (The National Cybersecurity Society, 2018, p. 4).

INTRODUCTION

In recent decades, the private sector's online presence has grown steadily, marked by the rise of Web 2.0 and the implementation of cloud services and mobile computing (Ponemon Institute, 2012).[1] Within this context, cybercrime has emerged as a dynamic and growing threat to European businesses, which incur high costs for preventing cyber threats and offences to their IT infrastructures. As per the working definition of provided by Europol (2018, p. 3), cybercrime can be defined as:

> "*Any crime that can only be committed using computers, computer networks or other forms of information communication technology*".

The threat posed by cybercrime has also been highlighted by the European Parliament which reported that 80% of all European businesses were victims of at least one cyber-attack in 2017, with "the constantly evolving nature of the cyber threat landscape [posing] serious legal and technological challenges for all stakeholders" (European Parliament, 2017, p. 7). In addition, cybercrime can not only cause financial losses to companies but also indirect reputational or privacy damage (Anderson et al., 2019; Paoli et al., 2018; Watkins, 2014). Therefore, today cybersecurity is a crucial and strategic aspect of business development, as it is "now both a key business driver and a key threat discussed at the board level" (McMurdie, 2016, p. 87). The most relevant forms of cybercrimes against businesses include ransomware, malware, distributed denial of service (DDoS) attacks, and social engineering techniques and offences such as phishing and business email compromise (BEC) (see Glossary) (ENISA, 2021; Europol, 2020, 2021). While the prevalence of cybercrime varies across business sectors and sizes, **ransomware** has emerged as one of the greatest risks for organisations and businesses, as it can facilitate large-scale cyber-attacks which in turn can have long-term effects (ENISA, 2021; Europol, 2021; Europol & Eurojust, 2019). Ransomware attacks have strongly increased over the last years (see Nouh et al., 2019), targeting businesses in several sectors such as manufacturing, finance, energy and transport (National Coordinator for Security and Counterterrorism & National Cyber Security Centre, 2021). As forms of ransomware become more sophisticated, their industrialisation can also be observed (Wall, 2021). This resulted, for instance, in a 150% increase in ransomware attacks in the EU in 2020 compared to the previous year (ENISA, 2021). Other forms of cybercrime such as **malware** and **DDoS** attacks also remain key threats to businesses, together with **phishing** and **BEC** techniques used for the theft of sensitive information through deception (ENISA, 2021; Europol, 2020).

The exposure of businesses to cybercrime has progressively increased over the last few years, accelerated by the COVID-19 pandemic, and worsened by the war in Ukraine. Since the pandemic outbreak, most companies have

[1] The Web 2.0 refers to the development of the internet following the technological advancements made starting from the 2000s. The Web 2.0 marks the transition "from the availability of low-cost computers to the advent of home broadband and mobile connectivity. The net result is a much more 'vivid' internet with multimedia content and social media" (European Commission & Joint Research Centre, 2020, p. 113).

moved their operations online by introducing remote working. As a result, different business sectors are now more interconnected and dependent on networks and information systems, and therefore their exposure to potential cybercrimes has also increased (Europol, 2021; see also Williams et al., 2019). In addition, the ongoing conflict in Ukraine has not only been taking place on the ground, but also in the cyber field, with Ukrainian as well as other countries' IT infrastructures at risks of becoming potential targets of cyber incidents (Lewis, 2022).

CYBERCRIME REPORTING BY BUSINESSES

The transnational nature of the cyberspace and cyber offences have posed many challenges to the law enforcement agencies of countries around the world, including EU Member States. Scholars have reported a number of constraints in the investigation of cybercrime: the rapidly changing cyber threat landscape, the multiplicity of cybercriminals, as well as often outdated police digital tools for investigation (Wright et al., 2021). These issues have generally been compounded by the lack of available data on cybercrimes against businesses, mostly due to low rates of reporting cybercrimes to law enforcement agencies (Aebi et al., 2022; Wright et al., 2021; see also van de Weijer et al., 2020).[2] Overall, reporting to the police or any other organisation remains low, with 44% cybercrimes experienced by small and medium sized enterprises (SMEs) not reported to anyone, as highlighted by the Flash Eurobarometer 496 SMEs and cybercrime of the European Commission. However, when cybercrimes are reported, police are the most common organisation to which these types of offences are reported to (European Commission, 2022a, p. 51).

To enhance the knowledge of cybercrimes against businesses, recent research has investigated the factors associated with cybercrime reporting and non-reporting (Aebi et al., 2022; CBS, 2022; European Commission, 2022a; van de Weijer et al., 2020). While reporting mechanisms vary widely between Member States, common **factors for reporting** cybercrimes by businesses to law enforcement authorities can be identified. Businesses are more likely to report cybercrimes when there exist information sharing and trust-building processes, secure communication channels, standardised and centralised reporting mechanisms, and an internal "reporting culture" (Cristofori et al., 2019; Giorgi et al., 2020; Mantelero, 2020; Norwegian University of Science and Technology, 2019; Peuvrelle, 2019). In contrast, **factors for non-reporting** cybercrimes mostly include the fact that the incident was dealt with internally and the feeling that the incident was too trivial and/or not worth reporting (European Commission, 2022a), as well as fear of reputational damages, lack of trust in law enforcement authorities and the criminal justice system, the ineffectiveness of having several reporting channels, conflicts of interest with business continuity, and gaps in cybersecurity awareness (Aebi et al., 2022; Akdemi r et al., 2020; European Court of Auditors, 2019; Kertysova et al., 2018; Loohuis, 2020). Overall, central reporting processes would be favoured by the harmonisation of reporting mechanisms and well-established public-private

[2] Overall, as indicated by Alexander Seger, head of the Cybercrime Division of the Council of Europe, less than 1% of cybercrime offences that occur is reported and recorded by criminal justice authorities (see Aebi et al., 2022).

partnerships (European Cybersecurity Forum, 2021; McMurdie, 2016). On the other hand, effective cybercrime reporting and operational cooperation strategies should take into account common factors for non-reporting, among all fear of reputational damage and business continuity, which is often given a higher priority than preserving evidence for criminal investigations (Akdemi◎r et al., 2020; Brady & Heinl, 2020; Jhaveri et al., 2017).[3]

As for **global business risk reports**, different companies have mapped the risk and threat landscape faced by businesses in the cyber domain. In early 2022, Allianz published the *Allianz Risk Barometer* (Allianz, 2022), a survey reporting information on the most important global business risks, including cyber incidents, business interruption, natural catastrophes, and the COVID-19 pandemic outbreak. The survey focused on large and small-medium sized companies and was based on the insights of 2650 risk experts from 89 countries/territories and 22 industry sectors. The respondents were asked to identify the top three most important risks for their industry sector. Cyber incidents – including cybercrime, IT failure/outage, data breaches, fines and penalties – emerged as the first business risk worldwide and in Europe in 2022, with 44% and 48% of responses, respectively. Another company, PwC, surveyed 1,296 executives in 53 countries/regions and 7 industries for the *Global Economic Crime and Fraud Survey 2022* (PwC, 2022). The study, which included cybercrime among the forms of offences, reported that the most common external perpetrators cases in the previous 24 months were the result of hackers (31% of respondents). In addition, cybercrime emerged as the prevalent type of fraud in 4 industries, namely technology, media and telecommunications (50%), health industries (40%), government and public sector (36%), and industrial and manufacturing (32%). Kroll, a corporate investigation and risk consulting firm, surveyed 588 senior executives across 13 countries and 10 industries for the *2019 Global Fraud and Risk Report* (Kroll, 2019). The study provided insights on cybersecurity and cyber incidents experienced by businesses, with a focus on data breach and cyber intrusion. The results indicated that for nearly half of the respondents, data theft (49%) played a role in computer system breaches during the previous year, followed by leaks of internal information (48%) and IP theft (43%).

Ernst & Young Global Limited (EY) addressed the issues related to cybersecurity with the *Global Information Security Survey 2021*. The survey was administered to 1,010 senior cybersecurity professionals primarily via telephone, with a minority completed online (EY, 2021). The survey was combined by a qualitative in-depth discussion with cybersecurity leaders, although no further information on the methodology is specified. The survey covered Europe, Middle East, India and Africa (43% of respondents), the Americas (36%), and the Asia-Pacific region (20%). The study found that the majority of respondents (77%) had seen an increase in the number of disruptive attacks as ransomware in the previous 12 months. Moreover, the survey provided insights on the level of confidence of chief information security officers (CISOs) when faced with threat actors. Of the respondents, less than half (47%) reported to understand and be able to anticipate new strategies used by threat actors, while only one in three respondents (35%) declared to be confident in their team's ability to deal with data breaches. Data breaches and their economic impact on businesses have also been

[3] It is important to note that this section does not cover victimisation surveys investigating cybercrime against individuals. For a recent EU-level study on cybercrime against individuals, with a focus on online identity theft and identity related crime, see European Commission (2022b).

analysed by IBM Security and Ponemon Institute through the Cost of a Data Breach Report 2021 (IBM Security, 2021). The study was developed by administering a survey to 537 organisations across 17 countries and regions in 17 industries. The organisations were considered as the unit of analysis and allowed to reach nearly 3,500 individuals for interviews. Of the total global average cost of data breach (USD 4.24 millions), more than a third was due to lost business cost (38%), followed by detection and escalation costs (29%) and post breach response (27%). Regarding the type of industries and attacks, healthcare organisations experienced the highest cost of data breach on average (USD 9.23 millions), while ransomware and destructive attacks were the cyber offences causing the most economic damages on average (USD 4.62 millions). Compared to the other global risks report reviewed, this study provided more details on the analytical approach and methodology. In particular, it provided definitions of a data breach and compromised record as well as information on the data collection method, measurement of data breach costs, and matching strategies to track the same type of organisations each year (see IBM Security, 2021, p. 68).

As for **EU level studies**, to the best of the authors' knowledge, to date the recent *Flash Eurobarometer 496 SMEs and cybercrime* of the European Commission is the only existing survey to have investigated cybercrime against businesses across EU Member States (European Commission, 2022a). Through a representative sample of SMEs across four main industry sectors,[4] the Flash Eurobarometer provides insights on companies' cybercrime risks awareness, level of concern about cybercrime, cybercrime victimisation and reporting channels for reporting cybercrime incidents in the previous 12 months. Among the main findings, the study highlights that of the total respondents with a leading role in their SME, 71% are well informed about the risks posed by cybercrime. Overall, respondents were also asked about their level of concern about cybercrime. Hacking online bank account (or hacking attempts) accounts for the 32% of responses, with companies being very concerned. In terms of geographic distribution, Portugal and Spain score higher on concerns about different forms of cybercrime. On the contrary, Denmark, Estonia, and Sweden have lower levels of concern (European Commission, 2022a). When it comes to cybercrime victimisation, viruses, spyware or malware are the most recurring form of cybercrime experienced (14% of respondents). In particular, malicious software was indicated by 30% of SMEs as the most serious incident in the previous 12 months, followed by scams and fraud (28%) and exploiting software, hardware, or network vulnerabilities (23%). One of the target countries of the CYBBAR survey, Spain, scored the highest among all EU MS not only on malicious software, but also on all other forms of cybercrime, with more than half of Spanish SMEs surveyed (52%) reporting this cybercrime as the most serious incident (European Commission, 2022a, p. 94).[5] Moreover, the study investigated the most common forms of cybercrime experienced. The different types of cybercrime included are: viruses, spyware or malware (excluding ransomware); phishing, account takeover or impersonation attacks; hacking (or attempts to hack) online bank accounts; unauthorised accessing of files

[4] Manufacturing, retail, services, and industry.

[5] The only exception is Cyprus, with 52% of SMEs reporting scams and fraud as the most serious type of incident. The other types of most serous incidents included in the survey were: Exploiting software, hardware, or network vulnerabilities; Password cracking; Identity theft; Denial of service (false traffic to overwhelm website or network); and Disruption or defacing of web presence.

or networks; ransomware; denial of service attacks; unauthorised listening in to videoconferences or instant messages; any other breaches or attacks (European Commission, 2022a, p. 32). Among these cybercrimes, viruses, spyware or malware (excluding ransomware) was the most prevalent type of cybercrime (14% of SMEs), followed by phishing, account takeover or impersonation attacks (11%). In terms of impact on SMEs' business, more than half of SMEs (58%) reported to have experienced at least one type of cybercrime with such an impact in the previous 12 months. Interesting results emerge from the analysis of cybercrime reporting. 44% of SMEs declared to not have reported to anyone the cybercrime incidents they experienced. Nonetheless, when asked about hypothetical cybercrime incidents, SMEs declared that the police would be the most likely organisation they would report it to. Finally, SMEs that experienced at least one type of cybercrime in the previous 12 months, reported that they did not report it the incident because the dealt with it internally (52%), with feeling that the incident was too trivial or not worth reporting to the police as the second most common reason for not reporting (44%).

As for **national cyber victimisation surveys**, a number of studies have been implemented in European countries to highlight cybersecurity threats and cybercrime against businesses. One of the most notable studies is the *Cyber Security Breaches Survey* (CSBS), a survey conducted by the UK government on an annual basis (Department for Digital, Media, Culture and Sport).[6] The CSBS provides a qualitative and quantitative assessment of the impact and cost of cyber breaches and attacks against businesses, charities, and education institutions. Qualitative insights are obtained through in-depth interviews with organisations with IT capacity and/or online presence. The quantitative analysis relies on sampling and data collection method comprising a random probability telephone survey of UK organisation. The sample is also weighted to statistically represent businesses and charities' population, and to ensure the proportionate distribution by size and sector (through randomised iterative method). The CSBS also distinguishes between micro businesses (up to 9 employees), small businesses (10-49 employees), medium businesses (50-249 employees), and large businesses (250 or more employees). Lastly, the organisations are grouped by business sectors, with a total of 13 different sectors in the latest CSBS published in 2022 (Department for Digital, Culture, Media & Sport, 2022).[7] The CSBS 2022 investigated a representative sample of UK businesses (1,243), registered charities (424), and education institutions (420). Of business respondents, 39% identified a cyber-incident in the previous 12 months. Of those businesses, the vast majority (83%) reported to have identified phishing attempts, with the remaining forms of attacks being identified in ransomware, malware and denial of service. Interestingly, ransomware was indicated as the major cyber threat and by businesses nearly a third of victimised businesses (31%) estimated to having been attacked at least once per week. As per the economic impact of cyber-attacks, medium and large businesses suffered on average a loss of money or data of GBP 19,400, although the authors note that figures related to financial impacts may be underreported. Underreporting may also be related with the cyber maturity and size of organisations: less mature businesses may have lower ability to identify cyber-attacks, while larger businesses tend to have enhanced cyber security which in turns may result in higher level of detection and reporting.

---

[6] The CSBS has been published every year since 2017, except for 2018.

[7] For more information, see https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.

The CSBS has been further analysed by Kemp et al. (2021) to specifically investigate the factors associated to cybercrime reporting by businesses in the UK. The authors analysed the data from the CSBS 2018, 2019, and 2020 and excluded charity and public sector organisations from the sample. The sample was then proportionally stratified by regions and disproportionally stratified by the sector and size of businesses, to ensure representativeness of small, medium, and large companies. The sample was also weighted to adjust it to the population of businesses in the UK before merging the three rounds of surveys. The final sample of companies consisted of businesses reporting at least of cybersecurity incident in the previous 12 months: 708 companies (2018), 584 (2019), 673 (2020) (for more information, see Kemp et al., 2021, p. 6). The sample was analysed through binary logistic regressions to measure the effect of different independent variables on two outcome measures relating to cybercrime reporting: *likelihood of reporting to anyone outside the organisation and likelihood of reporting to public authorities*. The main results indicate that reporting decisions are associated with the type of cybercrime, the negative impact generated by the cybersecurity incident, and with high priority given by the company to cybersecurity. Moreover, reporting to public authorities is associated to having in-house cyber security teams, as they seem to be more inclined to reporting. Finally, the authors discuss the study limitations and outline suggestions for future research. Among all, surveys should include direct questions on reporting to public authorities and carefully consider potential overlap among cybercrime categories to ensure that respondents are able to identify the cyber offence leading to the incident (Kemp et al., 2021).

Previous research in the Netherlands has also devoted attention to the study of cybercrime against businesses and factors for reporting cybercrime victimisation (CBS, 2022; Veenstra et al., 2015; see also van de Weijer et al., 2020). Veenstra et al. (2015) investigated cybercrime against Dutch SMEs. The authors conducted desk research and semi-structured face-to-face interviews with representatives of SMEs, self-employed professionals, and cybersecurity professionals to further develop a business cyber victimisation survey. From the initial number of SMEs (2 to 50 employees) contacted, randomly selected from the Netherlands Chamber of Commerce, 1,203 companies completed the questionnaire. The research results indicate that almost a third of SMEs surveyed (28.5%) reported to have suffered cybercrime victimisation, with malware, online fraud, phishing and hacking being the most prevalent cyber offences. The study also revealed that SMEs were not aware or had little knowledge about how the cybercrime was committed. Furthermore, loss of time, limited access to data, and financial damage (up to EUR 240,000) were the most commonly reported types of damages (Veenstra et al., 2015, p. 13). Lastly, in terms of reporting, Veenstra and colleagues found that only 7.2% of SMEs reported to the police to have been victim of cybercrime. Statistics Netherlands (CBS), an autonomous administrative authority, has been extensively involved in the study of crime and digital security in the Dutch society,[8] including cybercrime against businesses. In this regard, the latest Cyber security monitor 2021 surveyed around 20,000 randomly selected Dutch companies of different sizes and from different sectors to assess their cyber resilience (CBS, 2022). In terms of cybersecurity measures, the study indicates that small companies (2-10 employees) tend to have fewer number of measures compared to large companies (250+ employees), with

[8] For more information, see https://www.cbs.nl/nl-nl/zoeken?q=cybercrime.

half of such companies having all the ten measures considered by the study: including, antivirus software, authentication via soft or hardware token, strong password policy, data encryption, etc. (for more information, see CBS, 2022, p. 23). Not surprisingly, overall antivirus software measure emerges as the most common measure regardless of company size, with more than 80% of companies using antivirus software (CBS, 2022).

Cybercrime and cybersecurity threats against businesses have also been investigated in other countries, as Denmark and Norway (PwC, 2021a, 2021b). However, the information on the methodological approach of such cybercrime and cybersecurity reports is often limited, as the study findings and recommendations are generally the main focus.

In conclusion, of the national business cyber victimisation surveys reviewed, the CSBS survey emerges to be the most comprehensive source in terms of detailed description of the methodology, research findings, and robustness of results. Nonetheless, its national focus is not very informative for cross-country studies as the CYBBAR survey. In addition, global or multi-national business risk reports often do not report sufficient information on the analytical approach. On the other hand, the *Flash Eurobarometer 496 SMEs and cybercrime* (European Commission, 2022a) represents the cross-country analysis most closely related to the objective of this study. For this reason, the EU level analysis was carefully reviewed to investigate cybercrime against businesses and cybercrime reporting in Bulgaria, Netherlands, and Spain.

THE CYBER SECURITY SURVEY FOR BUSINESSES METHODOLOGICAL TOOLKIT

To integrate the existing data on business cyber victimisation and contribute to enhancing the knowledge of cybercrimes against businesses in EU Member States, the following sections outline the key features of *the Methodological Toolkit for a Business Victimisation Survey on Cybercrime*.

Analytical approach

As in most victimisation surveys, the main focus of the Business Victimisation Survey on Cybercrime (henceforth CYBBAR Survey) is on measuring quantitatively the self-reported **prevalence** and **incidence** rates of the most common types of cybercrimes. **Prevalence rate** in this context is usually defined as the ratio of victims compared to a base population (in this case the universe of companies considered to be eligible for the survey), while **incidence rate** refers to the ratio between the number of incidents discovered through the survey and the same base (see Lauritsen & Rezey, 2013). Another critical aspect in measuring crime through victimisation surveys is estimating the degree to which such crime is reported to different authorities, since this provides invaluable information on **unreported crime** that does not appear in official statistics because of non-reporting or non-registering. In line with previous studies (e.g., see European Commission, 2022a), a standard period of 12 months is selected to allow for monitoring the changes of these indicators over time.

To measure these three main aspects of cybercrime through a victimisation survey, it is critical to select the types of crimes included in the survey. In addition, previous research has hinted that in victimisation studies respondents do not always differentiate between some of the cybercrime types and sometimes tend to categorise an incident incorrectly (see Junger & Hartel, 2020). In order to avoid respondents' mistakes or subjective judgement and to register only the facts, questions should be phrased very carefully, focusing on what actually happened and what could be reasonably known by the respondents, rather than what the possible goals or intentions of the perpetrators might have been. Building upon previous cyber victimisation surveys (CBS, 2022; Department for Digital, Culture, Media & Sport, 2021; European Commission, 2022a),[9] we included **ransomware** and **malware** attacks, **DDoS** attacks, **hacking**, **phishing**, and other **security breaches** or attacks (as unauthorised accessing of files or networks). In the survey, attached as Annex I, these potential crimes are described in terms of what the victims might have experienced, but the popular names of the crimes are also provided in brackets. Instructions to the interviewers provide additional information for some of the crimes in case further clarification is needed during the interview. A summary of all types of cybercrimes that should be included in the core questionnaire is also attached in Annex II. Annex II also includes a list of other potential types of cybercrime that are not currently included in the CYBBAR survey but that could be considered (as optional questions).[10]

One of the biggest advantages of victimisation surveys is the possibility to estimate **unreported crime** – crime that took place according to the victims but was not reported to the authorities and therefore was not included in any official statistics. In addition to non-reporting, sometimes crimes are reported but not registered properly for multiple reasons. Victimisation surveys allow researchers to estimate roughly the actual number of reported and non-reported crimes and to compare these numbers to official statistics. Besides its role for estimating actual prevalence and incidence rates, the third main focus of the CYBBAR Survey is the factors for reporting and/or non-reporting cybercrime to law enforcement authorities. In fact, the reasons victims provide for non-reporting crimes are very informative for potential changes that could be made in how the police (or other relevant authorities) process certain types of crimes.

---

[9] See also section "Cybercrime reporting by businesses" for further details.

[10] For example, Business identity theft can be defined as a "type of identity theft committed with the intent to defraud or hurt a business (e. g. financial business identity, extortion)" (The National Cybersecurity Society, 2018, p. 4). In addition, the 2018 Business Identity Theft in the US report distinguishes between four types of Business identity theft (The National Cybersecurity Society, 2018): Financial Fraud "obtaining new lines of credit, loans or credit cards; UCC fraudulent filings"; Tax Fraud "filing fraudulent returns using tax subsidies or obtaining refunds from federal and state governments"; Website Defacement "by manipulating a business's identity on the web"; Trademark Ransom "registering the business name as an official trademark and demanding a ransom for release of the trademarked business name". These types of crimes are currently left out since they do not fit that well the currently adopted operational definition for cybercrime.

In terms of developing the survey instrument, the main challenge regarding cybercrime reporting is to list relevant options for reporting for a particular country, while also ensuring that the questions allow cross-country comparability. To this end, a quasi-standardised question is developed to include different groups of potential organisations to which the cybercrime could be reported. An example list for Bulgaria is presented in Table 1 below, each target country is expected to add relevant options to each of the 4 categories: (1) national public authorities, (2) external financial, insurance, or IT companies (e.g., banks, insurance companies, internet providers, etc.), (3) other stakeholders like clients, suppliers, professional associations and others, and (4) international organisations dealing with cybercrime.

Table 1. Public authorities and organisations to which cybercrime offences could be reported

Answer in question Q10 "Who was the breach or attack reported to"	Coverage	Category
The Police	All countries	National public authorities
European emergency number (112)	EU countries	National public authorities
Specialised cybercrime hotline (if applicable to the country)	EU countries	National public authorities
National Cyber Security Centre (if applicable to the country)	EU countries	National public authorities
Data protection agency (if applicable to the country)	EU countries	National public authorities
Other national government agency (write down)	All countries	National public authorities
Bank or credit card company	All countries	Financial, insurance, IT
Insurance company	All countries	Financial, insurance, IT
Internet/Network Service Provider	All countries	Financial, insurance, IT
Website administrator	All countries	Financial, insurance, IT
Outsourced cyber security provider	All countries	Financial, insurance, IT
Antivirus company	All countries	Financial, insurance, IT
Professional/trade/industry association	All countries	Other
Clients/customers	All countries	Other

Suppliers	All countries	Other
Was publicly declared	All countries	Other
An international organisation (write down)	All countries	International organisations

Other topics that are often included in victimisation surveys are security and costs. To keep the length of the survey shorter, a section covering costs and cybersecurity is included with only the most important questions: the estimated overall cost an incident caused to the respondent organisation, security checks performed during the past 12 months preceding the survey, and cybersecurity policies implemented within the organisation.

Finally, a demographic section of the CYBBAR Survey provides important information for segmentations and profiling of the victimised company, such as economic sector and size of the company.

Sampling

We recommend that the CYBBAR Survey is conducted using CATI method (computer-assisted telephone interviewing) and its duration is no longer than 20 minutes on average. The CATI survey method provides a relatively fast and reliable method to reach a representative sample of companies, as usually all companies have telephone access. CATI is also suitable since the filtering of the survey is done automatically by the computer, and interviewers' mistakes with following the filters are not likely. Alternatively, CAWI (computer-assisted web interviewing) is also a viable and less expensive option.

Using online survey for this questionnaire is not recommended, as a representative sample is much more difficult to achieve and systematic sampling biases are possible in online surveys – e.g., digitally skilled invitees might be either more capable and willing or, on the contrary, are more hesitant to respond to an online survey than less digitally skilled invitees.

The universe for the CYBBAR Survey is defined as micro, small, medium and large companies/organisations. With some exceptions, we include all business sectors and organisation types in the target population for the survey to have a full picture of the businesses. In line with previous studies, we exclude charities,[11] and we also exclude public organisations and NGOs, which might be the focus of future surveys.

A national representative sample size of at least 400 effective (i.e., completed) interviews is recommended to ensure a margin of error of 5% with 95% certainty of similar outcomes in a different sample. To be able to analyse effectively different sizes of companies, it is recommended that these 400 are divided into 50 large companies (250+ employees), 80 medium-size companies (50-250 employees), 120 small companies (10-50 employees), and 150 micro companies (1-9 employees).

[11] Charities were excluded with the rationale that they are affected by different digital threats than businesses (Buil-Gil et al., 2021).

Eligible interviewees from a respondent organisation include employees directly related to cyber security or at least to IT (if no cyber security experts are available) or for smaller organisations – management staff, either senior or non-senior.

Analysis and Indicators

Five main indicators should be computed from the raw data collected through the CYBBAR Survey:

1. **Prevalence rate** (computed for each type of crime) equals the % of victims from all companies in the survey.

Prevalence rate should be computed from question Q6 (see Annex I) for every cybercrime type. Prevalence rate (for each sub-question) equals the count of "yes" answers (i.e., Q6=1) divided by the sample size N.

2. **Incidence rate** (computed for each type of crime) refers to the approximate total number of incidents mentioned in the survey divided by the number of companies in the sample (only applicable if the question is asked. Incidence rate could also be considered as the frequency of occurrence of cyber incidents, i.e., how often, see Q7 in Annex I).

3. Unreported crime rate (computed for each type of crime) is computed as the % of victims who reported a crime to the public authorities (the police or another relevant national organisation).

Unreported crime rate should be computed from question Q10 (see Annex I) for every cybercrime type. Unreported crime rate (for each sub-question) equals the count of respondents who reported to at least one public authority organisation (codes 1 to 4 in Q10) divided by the number of victims for the corresponding sub-question (count of respondents for which Q6=1).

4. **Costs** (computed for each type of crime) is computed as the average cost (standard error should also be provided) reported by the respondents for a particular crime.

Average cost (for each type of crime) is computed as the average value provided by the respondents in Q8. Since costs are provided in local currency, they should be converted to EUR first. Codes for refusals and "do not know" answers should be excluded before calculating the average.

5. **A cybersecurity index** should be computed based on the cybersecurity questions, considering the weight of different policies, measures and vulnerabilities in predicting the likelihood of a cybercrime to take place in an organisation. Methods like principal component analysis, regression analysis and relative weight analysis may be used for developing the cybersecurity index. Demographic variables like company size, economic sector and others should be included as control variables in such regression models.

Practical guidelines

Fieldwork agency selection

Procuring a fieldwork agency should follow national guidelines, but in principle at least 3 offers should be collected. A terms-of-reference document for this process should include:

- The length of the questionnaire (recommended 20 minutes)
- Whether translation into local language is needed (as well as the translation procedure required)
- Sample size (recommended at least n=400 per country)
- Sampling method – national representative, target universe (e.g., charities, self-employed, and public organisations excluded), 50-80-120-150 ratio between large, medium, small, and micro companies
- Required deliverables (usually a clean and labelled data file in SPSS format or similar, and a technical report)
- A more detailed ToR for recruiting a fieldwork agency is provided in Annex III.

Questionnaire translation

A typical approach to translating a questionnaire is having two independent forward translations (performed by different translators), reconciliation by a local expert which includes selecting the best translation in case of differences between the two forward translations and discussing issues with the survey implementation team and finally a back translation into English conducted by a different translator. The back translation is compared to the original questionnaire and any differences between the two are analysed and discussed carefully to avoid changes in the intended meaning during the translation process.

Lessons learned from piloting the CYBBAR Survey

The survey included in this document is the final version of the Business Victimisation Survey on Cybercrime (CYBBAR Survey) following its implementation in the Netherlands, Spain, and Bulgaria. The revisions made to the survey instrument (see Table 2 in Annex IV) were informed by insights gained from data analysis and the results obtained from the collected information on cybercrime against businesses, as outlined in the *Methodology guideline for producing country studies* (D4.4). The modifications focused on enhancing clarity and removing redundant or overly complex questions and/or responses.

The completion of the CYBBAR Survey now provides researchers and other interested parties with a valuable tool for investigating cybercrime targeting businesses as well as other types of organisations. As such, this instrument can be utilised to further explore and understand the dynamics of cyber threats in these contexts.

REFERENCES

Aebi, M. F., Caneppele, S., & Molnar, L. (Eds.). (2022). Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys. Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020. Eleven.

Akdemir, N., Sungur, B., & Başaranel, B. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. International Security Congress Special Issue, 111–134. https://doi.org/10.28956/gbd.695956

Allianz. (2022). Allianz Risk Barometer 2022. Allianz. https://www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html

Anderson, R., Barton, C., Bölme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. Presented at: The 2019 Workshop on the Economics of Information Security, Boston, US. https://orca.cardiff.ac.uk/id/eprint/122684/

Brady, S., & Heinl, C. (2020). Cybercrime: Current Threats and Responses. A review of the research literature. Irish Department of Justice and Equality, Research and Data Analysis Unit. http://www.justice.ie/en/JELR/Cybercrime_-_Current_Threats_and_Responses.pdf

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders, 16(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

CBS. (2022). Cybersecuritymonitor 2021. Statistics Netherlands (CBS). https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021

Check Point Software. (n.d.). Business Email Compromise (BEC)—The different types of attacks. Check Point Software Technologies Ltd. Retrieved September 12, 2022, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/

Cristofori, D., Tikanmäki, I., Räsänen, J., Simola, J., Bieze, M., & Katos, V. (2019). D3.6 ECHO INFORMATION SHARING MODELS. European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO). https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D3.6-ECHO-Information-Sharing-Models-v1.0.pdf

Department for Digital, Culture, Media & Sport. (2021). Cyber Security Breaches Survey 2021: Technical annex. UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977491/20-046099-01_CSBS_2021_quant_technical_annex_v2.4__clean__190321.pdf

Department for Digital, Culture, Media & Sport. (2022). Cyber Security Breaches Survey 2022. UK Government. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice, 42(5), 500–515. https://doi.org/10.1080/0735648X.2019.1691855

ENISA. (2021). ENISA Threat Landscape 2021. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Commission. (2022a). Flash Eurobarometer 496 SMEs and cybercrime. Publications Office of the European Union. https://data.europa.eu/doi/10.2837/14988

European Commission. (2022b). Study on online identity theft and identity-related crime: Final report. Publications Office of the European Union. https://data.europa.eu/doi/10.2837/197724

European Commission & Joint Research Centre. (2020). Cybersecurity, our digital anchor: A European perspective. Publications Office of the European Union. https://doi.org/10.2760/352218

European Court of Auditors. (2019). Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors (Review No 02/2019). https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416

European Cybersecurity Forum. (2021). Together against adversarial internet. Recommendations and takeaways. 6th European Cybersecurity Forum - Cybersec Global & 4th Cybersec Brussels Leaders' Foresight. https://ik.org.pl/wp-content/uploads/keytakeaways_CSGlobal2020_CSBXL21_v2.pdf

European Parliament. (2017). European Parliament resolution of 3 October 2017 on the fight against cybercrime. (2017/2068 (INI)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.html

Europol. (2018). Internet Organised Crime Threat Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Europol. (2020). Internet Organised Crime Threat Assessment (IOCTA) 2020. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol, & Eurojust. (2019). Common challenges in combating cybercrime, as identified by Eurojust and Europol. Joint Report Europol and Eurojust Public Information. https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol

EY. (2021). EY Global Information Security Survey 2021. Ernst & Young Global Limited. https://www.ey.com/en_vn/ey-global-information-security-survey-2021

Giorgi, G., Mari, S., Bocci, V. E., & Rieke, R. (2020). D4.1: Requirements for the ISAC Pilot. Edge enabled Privacy and Security Platform for Multi Modal Transport (E-CORRIDOR) Project. https://e-corridor.eu/wp-content/uploads/2020/12/E-CORRIDOR_D4.1_Final.pdf

I**BM Security.** (2021). Cost of a Data Breach Report. IBM Corporation. https://www.ibm.com/security/data-breach

Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Eeten, M. V. (2017). Abuse Reporting and the Fight Against Cybercrime. ACM Computing Surveys, 49(4), 1–27. https://doi.org/10.1145/3003147

Junger, M., & Hartel, P. (2020). Crime Victimisation Surveys Measuring Cybercrime. Presented at the Conference: Measuring cybercrime in the time of covid-19: the role of crime and criminal justice statistics, organised by the European Union and the Council of Europe. https://rm.coe.int/presentation-marianne-junger/1680a033ae

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. Criminology & Criminal Justice, 17488958211062360. https://doi.org/10.1177/17488958211062359

Kertysova, K., Frinking, E., van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018). Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. European Economic and Social Committee. https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

Kroll. (2019). Global Fraud and Risk Report 2019/20. Mapping the New Risk Landscape. https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019

Lauritsen, J. L., & Rezey, M. L. (2013). Measuring the Prevalence of Crime with the National Crime Victimization Survey (TECHNICAL REPORT September 2013, NCJ 241656). U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/content/pub/pdf/mpcncvs.pdf

Lewis, J. A. (2022). Cyber War and Ukraine. Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine

Loohuis, K. (2020, December 15). Cyber crime victims in the Netherlands not reporting offences. Computer Weekly. https://www.computerweekly.com/news/252493660/Cyber-crime-victims-in-the-Netherlands-not-reporting-offences

Mantelero, A. (2020). D4.2: Legal Framework. Cyber Security for Europe (CYBERSEC4EUROPE) Project. https://cybersec4europe.eu/wp-content/uploads/2020/09/CS4E-D4.2-Legal-Framework_post-rev_20200914_v1.1.pdf

McMurdie, C. (2016). The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), 85–93. https://doi.org/10.1080/23738871.2016.1168607

National Coordinator for Security and Counterterrorism, & National Cyber Security Centre. (2021). Cyber Security Assessment Netherlands (CSAN) 2021. Dutch Ministry of Justice and Security. https://english.nctv.nl/documents/publications/2021/08/05/cyber-security-assessment-netherlands-2021

Norwegian University of Science and Technology. (2019). Deliverable D2.1 State of the Art on Cybersecurity Solutions & Technologies in EPES. SDN - microgrid reSilient Electrical eNergy SystEm (SDN-microSENSE) Project. https://www.sdnmicrosense.eu/wp-content/uploads/2021/09/SDN-microsense_D2.1.State-of-the-Art-on-Cybersecurity-Solutions-Technologies-in-EPES-1.pdf

Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. Proceedings 2019 Workshop on Usable Security. https://doi.org/10.14722/usec.2019.23032

Paoli, L., van Hellemont, H., Verstraete, C., Visschers, J., De Wolf, R., & Martens, M. (2018). Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium. Belgian Research Action through Interdisciplinary Networks. https://www.belspo.be/belspo////fedra/proj.asp?l=de&COD=BR%2F132%2FA4%2FBCC

Peuvrelle, V. (2019). D8.1: Legal state of the art. Security of Air Transport Infrastructures of Europe (SATIE) Project. https://satie-h2020.eu/wp-content/uploads/2020/09/SATIE_D8.1_Legal-state-of-the-art_v1.0.pdf

Ponemon Institute. (2012). The Impact of Cybercrime on Business Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil. Ponemon Institute. https://www.security-finder.ch/fileadmin/dateien/pdf/studien-berichte/The_Impact_of_Cybercrime_on_Businesses.pdf

PwC. (2021a). Cybercrime Survey 2020. PricewaterhouseCoopers. https://www.pwc.dk/da/publikationer/2021/pwc-cybercrime-survey-2020-uk.pdf

PwC. (2021b). Cybercrime Survey 2021. PricewaterhouseCoopers. https://publikasjoner.pwc.no/cybercrime-survey-2021/executive-summary/

PwC. (2022). Global Economic Crime and Fraud Survey 2022. PricewaterhouseCoopers. https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

The National Cybersecurity Society. (2018). Business Identity Theft in the US (2018 Report). National Cybersecurity Society. https://nationalcybersecuritysociety.org/wp-content/uploads/2018/07/NCSS-2018-Biz-ID-Report-6_2018.pdf

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. Policing: An International Journal, 43(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Veenstra, S., Zuurveen, R., & Stol, W. (2015). Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden-en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland [Cybercrime among companies]. Lectoraat Cybersafety: Leeuwarden.

Wall, D. S. (2021). The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. European Law Enforcement Research Bulletin, 1–16. https://ssrn.com/abstract=3908159

Watkins, B. (2014). The impact of cyber attacks on the private sector (Briefing Paper No. 12). Association for International Affairs. http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. Deviant Behavior, 40(9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786

Wright, D., Garstka, K., & Kumar, R. (2021). Rising to the Proliferation of Cybercrime Challenging LEAs Across Europe. European Law Enforcement Research Bulletin, 21, 81–98. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/447/345

ANNEX I – FINAL CYBER SECURITY SURVEY FOR BUSINESSES

Section 1. Screening and company demographics

ASK ALL

Q1. Is your job:

(READ OUT, ONE ANSWER ONLY)

1. Directly related to cyber security
2. Directly related to IT
3. Not related to cyber security/IT – senior management level
4. Not related to cyber security/IT – non-senior management level
5. Not related to IT or management

INTERVIEWER: IF Q1=9, PLEASE ASK TO SPEAK TO AN APPROPRIATE RESPONDENT OR TERMINATE THE INTERVIEW.

ASK ALL

Q2. How familiar are you with your company's IT setup in general, including cybersecurity and potential cybersecurity threats and attacks:

(READ OUT, ONE ANSWER ONLY)

1. Very familiar
2. Somewhat familiar
3. Not very familiar
4. Not familiar at all

ASK ALL

Q3. Including yourself, how many employees does your company have?

(READ OUT, ONE ANSWER ONLY)

1. Micro (1-9 employees)
2. Small (10-49 employees)
3. Medium (50-249 employees)
4. Large (250 employees or more)

INTERVIEWER: IF THE COMPANY IS INACTIVE, PLEASE TERMINATE THE INTERVIEW.

Q4. What is the main economic activity of your company?

(READ OUT, ONE ANSWER ONLY)

A Agriculture, Forestry and Fishing
B Mining and Quarrying

C Manufacturing
D Electricity, Gas, Steam and Air Conditioning Supply
E Water Supply; Sewerage, Waste Management and Remediation Activities
F Construction
G Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles
H Transportation and Storage
I Accommodation and Food Service Activities
J Information and Communication
K Financial and Insurance Activities
L Real Estate Activities
M Professional, Scientific and Technical Activities
N Administrative and Support Service Activities
O Public Administration and Defence; Compulsory Social Security
P Education
Q Human Health and Social Work Activities
R Arts, Entertainment and Recreation
S Other activities

Q5. Does your company currently have or use?

(READ OUT, ONE ANSWER PER LINE)

Q5_1 Accounts or pages on social media sites (e.g. Facebook or Twitter)
Q5_2 A company/organisation website
Q5_3 An online bank account
Q5_4 An online ordering and payment service for customers
Q5_5 Online ordering or payment systems of suppliers, consultants or other business partners
Q5_6 Company e-wallets/accounts different from a bank account (like PayPal or crypto-wallets)
Q5_7 An industrial control system
Q5_8 Web-based applications for payroll processing, e-signature etc
Q5_9 Cloud computing or storage
Q5_10 Personal data about your clients stored electronically
Q5_11 Network-connected devices like TVs, building controls, alarms, speakers etc., sometimes called smart devices
Q5_12 A company intranet
Q5_13 Work computers connected to the Internet or other IT technologies
Q5_14 Personal devices owned by your employees such as smartphones, tablets, laptops or desktop computers that are used to carry out regular business-related activities? (This includes devices that are subsidized by your company).
Q5_88 None of the above

(RESPONSE SCALE)

1. Yes
2. No

9 Don't know / Refused (DO NOT READ OUT)

INTERVIEWER: IF Q5_88=1, PLEASE TERMINATE THE INTERVIEW.

Section 2. Cyber Victimisation

Q6. Has your company experienced any of the incidents listed below in the past 12 months (January 2022 – December 2022)?

(READ OUT, ONE ANSWER PER LINE)

1. There was a cyber-attack trying to deny you access to your company data or systems by encrypting them, in order to obtain a ransom from you for restoring your data/systems back - a ransomware attack?
2. Apart from that, have computers in your company been targeted by a virus or similar malicious software or firmware? We are asking whether you have detected any attacks with a malicious software or firmware intended to perform unauthorised processes that could have an adverse impact on the confidentiality, integrity, or availability of your systems: malware like viruses or spyware that is different from ransomware
3. Have your employees received any fraudulent emails, or visited any fraudulent websites that tried to convince them to provide important company information like credit card numbers and passwords through deception (phishing attacks)
4. Apart from all the incidents mentioned above, has anyone tried to access without authorisation your company's online bank/payment accounts?
5. Have you it experienced any cyberattacks that tried intentionally to slow or take down your company's website, applications or online services. We are talking about Denial-of-service attacks: false traffic intended to bring down your website or network. We are not talking about server issues or similar internal technical problems, but only about intentional cyberattacks.
6. Do you know of any cases when your customers or other people outside of your company received emails or other online communication that pretended to come from your company and was done for fraudulent purposes like trying to obtain money, or important information such as passwords, credit card numbers and other (business identity theft / Impersonation)?
7. Unauthorised accessing of files or networks by staff, even if accidental
8. Unauthorised accessing of files or networks by people outside your company
9. Unauthorised listening into video conferences or instant messaging
10. Takeovers or attempts to take over your website, social media accounts or email accounts
11. Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Yes
2. No
9 Don't know / Refused (DO NOT READ OUT)

ASK Q6A IF Q6_1=1.

Q6A. You mentioned that you experienced at least one ransomware attack in the past 12 months. Thinking of the last time this happened, what was the outcome of the incident?

(READ OUT, ONE ANSWER ONLY)

1. We detected the attack through our anti-virus software, but no computers were infected
2. Some computers were infected, but we managed to clean them on our own using an anti-virus program or other methods
3. Some computers were infected and we had to seek specialized help outside of our company to get back access to our data
4. We paid a ransom to get access to our encrypted data.
5. We lost our data (regardless of whether paying a ransom or not).
9 Don't know (DO NOT READ OUT)

ASK Q6B IF Q6_2=1.

Q6B. You mentioned that you experienced at least one virus/malware attack in the past 12 months. Thinking of the last time this happened, what was the outcome of the incident?

(READ OUT, ONE ANSWER ONLY)

1. We detected the attack through our anti-virus software, but no computers were infected
2. Some computers were infected, but we managed to clean them on our own using an anti-virus program or other methods
3. Some computers were infected and we had to seek specialized help outside of our company to get back access to our data
4. Don't know (DO NOT READ OUT)

ASK Q6B2 IF Q6B=2 OR Q6B=3.

Q6B2. Thinking again about the last time your company computers were infected, did you lose any money or sensitive data?

(READ OUT, MULTIPLE ANSWERS POSSIBLE)

1. Our bank accounts were attacked through stolen credentials, but we did not lose any money
2. Our bank accounts were attacked through stolen credentials and money were stolen
3. We lost important data
4. Sensitive data might have been stolen due to the incident
5. Our systems were harmed
6. No money or data were stolen and we managed to restore our computers and other systems.
9 Don't know (DO NOT READ OUT)

ASK Q6C IF Q6_3=1.

Q6C. You mentioned that you experienced at least one phishing attack in the past 12 months. Thinking of the last time this happened, what was the outcome of the incident?

(READ OUT, MULTIPLE ANSWERS POSSIBLE)

1. To the best of our knowledge, the attack was not successful and no sensitive information was leaked.
2. Our bank accounts were attacked through stolen credentials, but we did not lose any money
3. Our bank accounts were attacked through stolen credentials and money was stolen
4. Our bank accounts were not attack directly, but we lost money due to another scheme like making payments to someone who pretended to be a trusted person
5. Sensitive data might have been stolen due to the incident
6. The attack was successful, but we did not lose any money or data
7. Don't know (DO NOT READ OUT)

ASK Q6D AND Q6D2 IF Q6_4=1.

Q6D. You mentioned that you experienced at least one attack against your company's online bank/payment accounts. Thinking of the last time this happened, what was the outcome of the incident?

(READ OUT, ONE ANSWER ONLY)

1. The attack was not successful and we did not lose any money.
2. Money was stolen
9 Don't know (DO NOT READ OUT)

Q6D2. Thinking again of the last time this happened, do you have any information on how the attack was carried out?

(READ OUT, ONE ANSWER ONLY)

1. We do not know how the attack was carried out.
2. Bank/payment account information was stolen through phishing – i.e. through fraudulent emails
3. Bank/payment account information was stolen through a virus/malware/spyware
4. Bank/payment account information was stolen through other hacking methods involving using vulnerabilities in our intranet or WiFi or others
5. Automatic attempts to "guess" our password – a brute force attack
6. Other
9 Don't know (DO NOT READ OUT)

ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1.

Q7. Approximately, how often did you experience any of the following types of cybercrime in the last 12 months?

(READ OUT, ONE ANSWER ONLY)

- Q7_1 A ransomware attack
- Q7_2 Malware like viruses or spyware that is different from ransomware
- Q7_3 Phishing attacks
- Q7_4 Attempt to access without authorisation your company's online/ bank account
- Q7_5 Denial-of-service attacks: false traffic intended to bring down your website or network
- Q7_6 Business identity theft / Impersonation
- Q7_7 Unauthorised accessing of files or networks by staff, even if accidental
- Q7_8 Unauthorised accessing of files or networks by people outside your company
- Q7_9 Unauthorised listening into video conferences or instant messaging
- Q7_10 Takeovers or attempts to take over your website, social media accounts or email accounts
- Q7_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Once only
2. More than once

9 Don't know / Refused (DO NOT READ OUT)

Section 3. Direct and Indirect Costs incurred

ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1.

Q8. Thinking of the last time there was this type of attack, how much do you think this incident or incidents have cost your company financially and non-financially (indirect costs) overall during the past 12 months? What was the approximate total cost of such losses related to this incident?

(READ OUT, ONE ANSWER ONLY)

- Q8_1 A ransomware attack
- Q8_2 Malware like viruses or spyware that is different from ransomware
- Q8_3 Phishing attacks
- Q8_4 Attempt to access without authorisation your company's online/ bank account
- Q8_5 Denial-of-service attacks: false traffic intended to bring down your website or network
- Q8_6 Business identity theft / Impersonation
- Q8_7 Unauthorised accessing of files or networks by staff, even if accidental
- Q8_8 Unauthorised accessing of files or networks by people outside your company
- Q8_9 Unauthorised listening into video conferences or instant messaging
- Q8_10 Takeovers or attempts to take over your website, social media accounts or email accounts
- Q8_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Below 100 EUR
2. 100 - 1000 EUR
3. 1000 – 10 000 EUR
4. Above 10 000 EUR
5. No cost of this kind incurred

88 Refused/Don't know (DO NOT READ OUT)

Section 4. Reporting

ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1.

Q9. Thinking about the last time there was this type of attack, was this breach, attempt, or attack reported to anyone outside your company, or not?

(READ OUT, ONE ANSWER ONLY)

Q9_1 A ransomware attack
Q9_2 Malware like viruses or spyware that is different from ransomware
Q9_3 Phishing attacks
Q9_4 Attempt to access without authorisation your company's online/ bank account
Q9_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q9_6 Business identity theft / Impersonation
Q9_7 Unauthorised accessing of files or networks by staff, even if accidental
Q9_8 Unauthorised accessing of files or networks by people outside your company
Q9_9 Unauthorised listening into video conferences or instant messaging
Q9_10 Takeovers or attempts to take over your website, social media accounts or email accounts
Q9_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Yes
2. No

99 Don't know (DO NOT READ OUT)

ASK ANY Q9=1. ONLY ITEMS FOR WHICH Q9=1.

Q10. Thinking again about the last incident of this type, who was this breach or attack reported to?

(READ OUT, MULTIPLE ANSWERS PER LINE)

Q10_1 A ransomware attack
Q10_2 Malware like viruses or spyware that is different from ransomware
Q10_3 Phishing attacks
Q10_4 Attempt to access without authorisation your company's online/ bank account
Q10_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q10_6 Business identity theft / Impersonation
Q10_7 Unauthorised accessing of files or networks by staff, even if accidental
Q10_8 Unauthorised accessing of files or networks by people outside your company
Q10_9 Unauthorised listening into video conferences or instant messaging
Q10_10 Takeovers or attempts to take over your website, social media accounts or email accounts
Q10_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. The Police
2. European emergency number (112)
3. Specialised cybercrime hotline (if applicable to the country)
4. National Cyber Security Centre
5. Data protection agency (if applicable to the country)
6. Other national government agency
7. Bank or credit card company
8. Insurance company
9. Internet/Network Service Provider
10. Website administrator
11. Outsourced cyber security provider
12. Antivirus company
13. Professional/trade/industry association
14. Clients/customers
15. Suppliers
16. Was publicly declared
17. An international organisation

ASK ANY Q9=1. ONLY ITEMS FOR WHICH Q9=1.

Q10B. What were the reasons you decided to report the last incident of this type?

(READ OUT, MULTIPLE ANSWERS PER LINE)

Q10B_1 A ransomware attack
Q10B_2 Malware like viruses or spyware that is different from ransomware
Q10B_3 Phishing attacks
Q10B_4 Attempt to access without authorisation your company's online/ bank account
Q10B_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q10B_6 Business identity theft / Impersonation
Q10B_7 Unauthorised accessing of files or networks by staff, even if accidental
Q10B_8 Unauthorised accessing of files or networks by people outside your company
Q10B_9 Unauthorised listening into video conferences or instant messaging
Q10B_10 Takeovers or attempts to take over your website, social media accounts or email accounts
Q10B_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Legal obligations/mandatory reporting
2. Prevent repeated victimisation
3. Because of the insurance requirements
4. We reported to the bank in order to block stolen cards/accounts
5. To seek help with the incident/incidents in order to prevent (further) losses (e.g. ransomware attack)
6. To seek recovery of lost assets
7. To have the police punish the culprit regardless of asset recovery
8. To aid the authorities in fighting incidents like that in the future
9. It is the right thing to do
10. Other

ASK ANY Q10 IS NOT EQUAL TO 1, OR 2, OR 3, OR 4. ONLY ITEMS FOR WHICH A TYPE OF ATTACK IS NOT REPORTED TO THE AUTHORITIES. ASK ANY Q6=1.

Q10C. What were the reasons you didn't report the last incident of this type to the police or 112 or other national authorities?

(READ OUT, MULTIPLE ANSWERS PER LINE)

Q10C_1 A ransomware attack
Q10C_2 Malware like viruses or spyware that is different from ransomware
Q10C_3 Phishing attacks
Q10C_4 Attempt to access without authorisation your company's online/ bank account
Q10C_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q10C_6 Business identity theft / Impersonation
Q10C_7 Unauthorised accessing of files or networks by staff, even if accidental
Q10C_8 Unauthorised accessing of files or networks by people outside your company

Q10C_9 Unauthorised listening into video conferences or instant messaging

Q10C_10 Takeovers or attempts to take over your website, social media accounts or email accounts

Q10C_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. They cannot do anything to help
2. We dealt with the incident internally
3. It was too trivial/not worth reporting
4. We expected it would be reported by another authority (e.g. Internet provider/bank)
5. We tried to report it but police were not interested
6. We did not know the police dealt with this type of incident
7. It was too inconvenient/too much trouble
8. They would not bother to do anything about it
9. The police are not trustworthy when it comes to incidents like these
10. We reported to other more relevant organisations
11. We did not know to which agency we should report such incidents
12. Because of the complexity of reporting / burdensome / bureaucratic procedures?
13. We did not know this was a crime
14. We did not want the incident/s to be known outside of the company due to potential reputational damage
15. Because of possible interruption of business processes (e.g. servers are taken for forensic analysis, etc.)
16. We didn't know we had an incident until much later
17. Our losses from the incident were insignificant
18. Other (write down_____)

ASK IF NONE OF Q10=1. ONLY ITEMS FOR WHICH NO TYPE OF ATTACK IS REPORTED TO THE POLICE.

Q10D. What would make you more likely to report such incidents in the future?

(READ OUT, MULTIPLE ANSWERS PER LINE)

Q10D A ransomware attack

Q10D_2 Malware like viruses or spyware that is different from ransomware

Q10D_3 Phishing attacks

Q10D_4 Attempt to access without authorisation your company's online/ bank account

Q10D_5 Denial-of-service attacks: false traffic intended to bring down your website or network

Q10D_6 Business identity theft / Impersonation

Q10D_7 Unauthorised accessing of files or networks by staff, even if accidental

Q10D_8 Unauthorised accessing of files or networks by people outside your company

Q10D_9 Unauthorised listening into video conferences or instant messaging

Q10D_10 Takeovers or attempts to take over your website, social media accounts or email accounts

Q10D_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Enhanced online platforms
2. User friendly platforms
3. Better trained police offices
4. More information about channels for reporting
5. My legal rights and obligations

11 Other (write in……)

Section 5. Cyber security

Q11. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your company?

(READ OUT, MULTIPLE ANSWERS POSSIBLE)

1. A cyber security vulnerability audit
2. A risk assessment covering cyber security risks / Invested in threat intelligence
3. Used specific tools designed for security monitoring, such as Intrusion Detection Systems Penetration testing
4. Testing staff awareness and response (e.g. via mock phishing exercises)

88 None of these (DO NOT READ OUT)

99 Don't know (DO NOT READ OUT)

Q12. Have you outsourced any of your IT support services to an external company or companies:

(READ OUT, ONE ANSWER ONLY)

1. IT is completely outsourced to an external company
2. IT is partially outsourced to an external company and it is responsible for our cybersecurity
3. IT is partially outsourced to an external company, but we are responsible for our cybersecurity
4. IT is partially outsourced to an external company and both we and the external company are responsible for our cybersecurity
5. IT is not outsourced or minor aspects of it are outsources

99 Don't know (DO NOT READ OUT)

Q13. Which of the following rules or controls, if any, do you have in place?

(READ OUT, MULTIPLE ANSWERS POSSIBLE)

1. A policy to apply software security updates within 14 days
2. Up-to-date malware protection
3. Firewalls that cover your entire IT network, as well as individual devices
4. Restricting IT admin and access rights to specific users
5. Any monitoring of user activity
6. Specific rules for storing and moving personal data files securely
7. Security controls on company-owned devices (e.g. laptops)
8. Only allowing access via company-owned devices
9. Separate WiFi networks for staff and for visitors
10. Backing up data securely via a cloud service
11. Backing up data securely via other means
12. A password policy that ensures users set strong passwords
13. A two or three-step login verification for your employees or/and clients
14. A virtual private network, or VPN, for staff connecting remotely
15. Encryption techniques for data, documents, or emails
16. An agreed process for staff to follow when they identify a fraudulent email or malicious website
17. Regular cyber security trainings or awareness raising sessions specifically for staff members who are not directly involved in cyber security
18. None of these (DO NOT READ OUT)
99. Don't know (DO NOT READ OUT)

Q14. Which of the following best describes the way your company has been working in the past 12 months?

(READ OUT, ONE ANSWER ONLY)

1. Everyone works at the company premises
2. Everyone works in a co-working space
3. A Hybrid work setup: some employees come to the office, some work from home
4. Most employees work from home on their company computers
5. Most employees work from home on their personal computers
99 Don't know (DO NOT READ OUT)

Q15. There are general insurance policies that provide cover for cyber security breaches or attacks, among other things. There are also specific insurance policies that are solely for this purpose. Which of the following best describes your situation?

(READ OUT, ONE ANSWER ONLY)

1. We have a specific cyber security insurance policy
2. We have cyber security cover as part of a broader insurance policy
3. We are not insured against cyber security breaches or attacks
99 Don't know (DO NOT READ OUT)

ANNEX II – TYPES OF CYBERCRIME INCLUDED AND QUESTIONNAIRE FORMULATIONS

Question read to the respondent	Type of cybercrime	Included in the questionnaire
Q6_1 There was a cyber-attack trying to deny you access to your company data or systems by encrypting them, in order to obtain a ransom from you for restoring your data/systems back - a ransomware attack?	Ransomware	Core questionnaire
Q6_2 Apart from that, have computers in your company been targeted by a virus or similar malicious software or firmware? We are asking whether you have detected any attacks with a malicious software or firmware intended to perform unauthorised processes that could have an adverse impact on the confidentiality, integrity, or availability of your systems: malware like viruses or spyware that is different from ransomware	Malware	Core questionnaire
Q6_3 Have your employees received any fraudulent emails, or visited any fraudulent websites that tried to convince them to provide important company information like credit card numbers and passwords through deception (phishing attacks)	Phishing	National public authorities
Q6_4 Apart from all the incidents mentioned above, has anyone tried to access without authorisation your company's online bank/payment accounts?	Hacking	Core questionnaire
Q6_5 Have you it experienced any cyberattacks that tried intentionally to slow or take down your company's website, applications or online services. We are talking about Denial-of-service attacks: false traffic intended to bring down your website or network. We are not talking about server issues or similar internal technical problems, but only about intentional cyberattacks	DDoS	Core questionnaire
Q6_6 Do you know of any cases when your customers or other people outside of your company received emails or other online communication that pretended to come from your company and was done for fraudulent purposes like trying to obtain money, or important information such as passwords, credit card numbers and other (business identity theft / Impersonation)?	Business identity theft / Impersonation	Core questionnaire

Q6_7 Unauthorised accessing of files or networks by staff, even if accidental	Security breach	Core questionnaire
Q6_8 Unauthorised accessing of files or networks by people outside your company	Security breach / Hacking	Core questionnaire
Q6_9 Unauthorised listening into video conferences or instant messaging	Security breach / Hacking	Core questionnaire
Q6_10 Takeovers or attempts to take over your website, social media accounts or email accounts	Security breach / Hacking	Core questionnaire
Q6_11 Any other types of cyber security breaches or attacks	Security breach / Hacking	Core questionnaire
Bank cards owned by employees being physically copied through "skimming" while using ATMs?	Skimming	Optional
(Only for financial institutions?) Clients' bank cards issued by your organisation being physically copied through "skimming" while using ATMs?	Skimming	Optional
Card data theft through POS terminal attacks	POS terminal attacks	Optional
Financial Fraud – criminals obtaining new lines of credit, loans or credit cards using your company name; UCC fraudulent filings;	Business identity theft	Optional
Tax Fraud – criminals filing fraudulent returns using tax subsidies or obtaining refunds from federal and state governments through using your company name;	Business identity theft	Optional
Website Defacement – criminals manipulating your business identity on the web which lead to website defacement;	Business identity theft	Optional
Trademark Ransom – criminals registering your business name as an official trademark and demanding a ransom from you for release of the trademarked business name.	Business identity theft	Optional

ANNEX III – TERMS OF REFERENCE FOR RECRUITING A FIELDWORK AGENCY

Technical specifications for conducting Cyber Security Survey for Businesses

Introduction

CYBBAR Business Victimisation Survey on Cybercrime is an instrument that addresses the lack of available data on business cyber victimisation. Its goal is to enhance the knowledge on cybercrimes against businesses in EU Member States.

The questionnaire will be about 20 minutes long and will include questions about victimisation rates for various cybercrime types, questions on reporting and non-reporting, cybersecurity and cyber-practices in the organisation, and company demographics (including size and industry sector).

The Business Victimisation Survey on Cybercrime is part of the ongoing Project CYBBAR (Cyber Victimisation Barometer), a 24-month project funded by the European Commission. The project is being developed by a 3-partner Consortium: Center for the Study of Democracy (coordinator), Ecorys, and Forentec.

Technical specifications

Sample size: n=400 completed interviews per country.

Sampling method: National representative.

Interviewing mode: CATI (computer-assisted telephone interviewing). Alternatively, a combination of CATI and CAWI (computer-assisted web interviewing) due to lower implementation costs.

Length: Approximately 20 minutes.

Language: Administered in local language (with English version as reference document).

Target universe:

- All active business organisations with at least 1 employee, excluding non-profit, self-employed, and public organisations.
- 50-80-120-150 ratio between large, medium, small, and micro businesses (250+ employees, 50-249 employees, 10-49 employees, 1-9 employees).
- Businesses without IT facilities and without online presence are screened out during the screening phase and are not included in the sample size of 400.

- Eligible interviewees from a respondent organisation: employees directly related to cyber security or at least to IT (if no cyber security experts are available) or for smaller organisations – management staff, either senior or non-senior. Eligible interviewees should be familiar with the IT setup and cyber security of the organisation.

Deliverables

- 400 conducted CATI interviews
- A clean file in SPSS sent by the Contractor according to a predefined template.
- Weighting variable(s) included in the SPSS file.
- Technical report describing the methodology, fieldwork duration, response rate, fieldwork related difficulties, computation of the weighting variable(s). A template for the technical report will be provided.

Application process

In response to the call for proposal, the Tenderer should apply with:

- A price offer in EUR;
- A technical offer that describes:
- Sampling frame and methodology for drawing a representative sample of the target universe.
- Sample size (at least 400).
- Timeline for conducting the survey.
- Additional information, if applicable.

ANNEX IV – UPDATED SURVEY QUESTIONS IN THE CYBER SECURITY SURVEY FOR BUSINESSES

Table 2 provides a brief overview of the questionnaire items that were modified during the data cleaning and analysis process to enhance the presentation of the research findings.

Table 2. Updated survey questions

CYBBAR Survey	
Initial question	**Updated question**
Q3. Including yourself, how many employees does your company have? (READ OUT, ONE ANSWER ONLY) 1. only myself 2. Under 10 3. 10–49 4. 50–249 5. 250–999 6. 10 00 or more	**Q3. Including yourself, how many employees does your company have?** (READ OUT, ONE ANSWER ONLY) 1. Micro (1-9 employees) 2. Small (10-49 employees) 3. Medium (50-249 employees) 4. Large (250 employees or more)
ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1. **Q7. Approximately, how often did you experience any of the following types of cybercrime in the last 12 months?** (READ OUT, ONE ANSWER ONLY) Q7_1 A ransomware attack Q7_2 Malware like viruses or spyware that is different from ransomware Q7_3 Phishing attacks Q7_4 Attempt to access without authorisation your company's online/bank account Q7_5 Denial-of-service attacks: false traffic intended to bring down your website or network Q7_6 Business identity theft / Impersonation Q7_7 Unauthorised accessing of files or networks by staff, even if accidental Q7_8 Unauthorised accessing of files or networks by people outside your company Q7_9 Unauthorised listening into video conferences or instant messaging Q7_10 Takeovers or attempts to take over your website, social media accounts or email accounts Q7_11 Any other types of cyber security breaches or attacks	ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1. **Q7. Approximately, how often did you experience any of the following types of cybercrime in the last 12 months?** (READ OUT, ONE ANSWER ONLY) Q7_1 A ransomware attack Q7_2 Malware like viruses or spyware that is different from ransomware Q7_3 Phishing attacks Q7_4 Attempt to access without authorisation your company's online/bank account Q7_5 Denial-of-service attacks: false traffic intended to bring down your website or network Q7_6 Business identity theft / Impersonation Q7_7 Unauthorised accessing of files or networks by staff, even if accidental Q7_8 Unauthorised accessing of files or networks by people outside your company Q7_9 Unauthorised listening into video conferences or instant messaging Q7_10 Takeovers or attempts to take over your website, social media accounts or email accounts Q7_11 Any other types of cyber security breaches or attacks

(RESPONSE SCALE)

1. Once only
2. More than once but less than once a month
3. Roughly once a month
4. Roughly once a week
5. Roughly once a day
6. Several times a day

88 Refused (DO NOT READ OUT)

99 Don't know (DO NOT READ OUT)

(RESPONSE SCALE)

1. Once only
2. More than once

99 Refused/Don't know (DO NOT READ OUT)

Direct and Indirect Costs incurred

ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1.

Q8. Thinking of the last time there was a this type of attack, how much do you think this incident or incidents have cost your company financially and non-financially (indirect costs) overall during the past 12 months?

(READ OUT, ONE ANSWER ONLY)

Q8_1 A ransomware attack
Q8_2 Malware like viruses or spyware that is different from ransomware
Q8_3 Phishing attacks
Q8_4 Attempt to access without authorisation your company's online/bank account
Q8_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q8_6 Business identity theft / Impersonation
Q8_7 Unauthorised accessing of files or networks by staff, even if accidental
Q8_8 Unauthorised accessing of files or networks by people outside your company
Q8_9 Unauthorised listening into video conferences or instant messaging
Q8_10 Takeovers or attempts to take over your website, social media accounts or email accounts
Q8_11 Any other types of cyber security breaches or attacks

Direct and Indirect Costs incurred

ASK ANY Q6_1 TO Q6_11=1. ONLY ITEMS FOR WHICH Q6=1.

Q8. Thinking of the last time there was a this type of attack, how much do you think this incident or incidents have cost your company financially and non-financially (indirect costs) overall during the past 12 months? What was the approximate total cost of such losses related to this incident?

(READ OUT, ONE ANSWER ONLY)

Q8_1 A ransomware attack
Q8_2 Malware like viruses or spyware that is different from ransomware
Q8_3 Phishing attacks
Q8_4 Attempt to access without authorisation your company's online/bank account
Q8_5 Denial-of-service attacks: false traffic intended to bring down your website or network
Q8_6 Business identity theft / Impersonation
Q8_7 Unauthorised accessing of files or networks by staff, even if accidental
Q8_8 Unauthorised accessing of files or networks by people outside your company
Q8_9 Unauthorised listening into video conferences or instant messaging
Q8_10 Takeovers or attempts to take over your website, social media accounts or email accounts
Q8_11 Any other types of cyber security breaches or attacks

First, please think of all:

- external payments made **when the incident was being dealt with** (like any payments to external IT consultants or contractors to investigate or fix the problem and any payments to the attackers, or money they stole)

Q8A. What was the approximate total cost of such losses related to this incident?

(RESPONSE SCALE)

1. Below 100 EUR
2. 100 - 1000 EUR
3. 1000 – 10 000 EUR
4. 10 000 to 100 000 EUR
5. Above 100 000 EUR

77 No cost of this kind incurred
88 Refused (DO NOT READ OUT)
99 Don't know (DO NOT READ OUT)

Now please think of all:

- external payments made **in the aftermath of the incident**? (e.g. payments to external IT consultants or contractors to run audits, the cost of new or upgraded software or systems, recruitment costs if you had to hire someone new)

Q8B. What was the approximate total cost of such losses related to this incident?

(RESPONSE SCALE)

1. Below 100 EUR
2. 100 - 1000 EUR
3. 1000 – 10 000 EUR
4. 10 000 to 100 000 EUR
5. Above 100 000 EUR

77 No cost of this kind incurred
88 Refused (DO NOT READ OUT)
99 Don't know (DO NOT READ OUT)

(RESPONSE SCALE)

1. Below 100 EUR
2. 100 - 1000 EUR
3. 1000 – 10 000 EUR
4. Above 10 000 EUR

77 No cost of this kind incurred
88 Refused/Don't know (DO NOT READ OUT)

Note: After conducting preliminary data analysis, it was observed that respondents had difficulty distinguishing between costs incurred during or after the incident for the other types of questions. Furthermore, including a very similar question regarding other costs was unlikely to yield significantly different results. Consequently, the research team made the decision to focus on and retain the general question pertaining to both financial and non-financial (indirect) costs for the final version of the survey.

Finally, please think of all:

- **other costs, different from the costs mentioned above**, related to this incident (e.g. staff time dealing with the incident, the cost of any time when staff could not do their jobs, the value of lost files or intellectual property, the cost of any devices or equipment that needed replacing, any compensations to clients, etc.)

Q8C. What was the approximate total cost of such losses related to this incident?

(RESPONSE SCALE)

1. Below 100 EUR
2. 100 - 1000 EUR
3. 1000 – 10 000 EUR
4. 10 000 to 100 000 EUR
5. Above 100 000 EUR

77 No cost of this kind incurred
88 Refused (DO NOT READ OUT)
99 Don't know (DO NOT READ OUT)

Core questionnaire

CENTER FOR
THE STUDY OF
DEMOCRACY