



CENTER FOR
THE STUDY OF
DEMOCRACY

Cybercrime and Businesses

A closer look at reporting behaviour, associated costs and incident management in Bulgaria, the Netherlands and Spain

Cybercrime and Businesses

**A closer look at reporting behaviour, associated costs
and incident management in Bulgaria,
the Netherlands and Spain**

The Cyber Security Survey for Businesses provides significant insights into the prevalence of cybercrime victimisation, reporting behaviors, and associated costs among businesses in Bulgaria, the Netherlands, and Spain. The results shed light on shared trends and distinctions among these countries, underscoring the importance of tailored cybersecurity strategies and effective incident management.

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

Editorial Board:

Dr. Ognian Shentov

Ruslan Stefanov

Dr. Todor Galev

The authors would like to thank Jan Van Dijk, Mike Levi, Rutger Leukfeldt, Fernando Mirò, and Steven Kemp for their valuable expertise and contributions, which significantly enriched the preparation of this report. The authors also wish to express their appreciation to Ecorys for its continuous support throughout the research and investigation process.



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

EXECUTIVE SUMMARY	4
INTRODUCTION	7
METHODOLOGY OF THE CYBER SECURITY SURVEY FOR BUSINESSES	8
RESULTS	9
Cybercrime victimisation	10
Prevalence of cybercrime victimisation	12
Outcomes of cybercrime attacks and financial costs	12
Reporting of cybercrime	14
Reasons for Reporting of cybercrime	17
Reasons for not reporting cybercrime to the police or other national authorities	20
Cybersecurity measures	21
REFERENCES	24
ANNEX I:	
Survey tables	26
ANNEX II:	
Final Cyber Security Survey for Businesses	46

LIST OF TABLES

Table 1.	Does your company currently have or use? (multiple answers)	26
Table 2.	What is the main economic activity of your company?	27
Table 3.	Is your job:	28
Table 4.	Has your company experienced any of the incidents listed below in the past 12 months (January 2022 – December 2022)? (multiple answers)	28
Table 5.	Approximately, how often in the last 12 months did you experience any of the following cybercrimes?	29
Table 6.	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?.....	30
Table 7.	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?.....	30
Table 8.	Thinking again about the last time your company computers were infected, did you lose any money or sensitive data? (multiple answers)	31
Table 9.	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?	31
Table 10.	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?	32
Table 11.	You mentioned that you experienced at least one attack against your company's online bank/payment accounts. Thinking again of the last time this happened, do you have any information on how the attack was carried out?	32
Table 12.	Thinking of the last time there was any of the following types of cybercrime, 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?.....	33
Table 13.	Thinking about the last time there was any of the following types of cybercrime, was this breach, attempt, or attack reported to anyone outside your company, or not?.....	34
Table 14.	Thinking again about the last incident of this type, who was this breach or attack reported to? (multiple answers) – continues next page.....	35
Table 15.	Continued table - Q10 Thinking again about the last incident of this type, who was this breach or attack reported to? (multiple answers)	36

Table 16.	What were the reasons you decided to report the last incident? - Bulgaria (multiple answers)	37
Table 17.	What were the reasons you decided to report cybercrimes? - Netherlands and Spain (multiple answers)	38
Table 18.	What were the reasons you didn't report the last incident of this type to the police or 112 or other national authorities? (multiple answers) - continues next page	39
Table 19.	What would make you more likely to report such incidents in the future? (multiple answers).....	42
Table 20.	Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your company? (multiple answers)	42
Table 21.	Have you outsourced any of your IT support services to an external company or companies:	43
Table 22.	Which of the following rules or controls, if any, do you have in place? (multiple answers).....	43
Table 23.	Which of the following best describes the way your company has been working in the past 12 months?	44
Table 24.	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?	45

LIST OF FIGURES

Figure 1.	Size of companies surveyed	8
Figure 2.	Type of cybercrime experienced in the past 12 months (%)	10
Figure 3.	Cybercrime victimisation among companies in the Netherlands, Spain, and Bulgaria (%).	11
Figure 4.	Share of companies reporting any of the following cybercrimes (%)	14
Figure 5.	Reporting of cybercrimes among companies in the Netherlands, Spain, and Bulgaria – multiple answers (%)	16
Figure 6.	Reasons for reporting cybercrime among companies in Bulgaria – multiple answers (%)	17
Figure 7.	Key factors for reporting cybercrime in the Netherlands and Spain (%)	18

EXECUTIVE SUMMARY

The Cyber Security Survey for Businesses findings provide valuable insights into the prevalence of cybercrime victimisation, reporting behaviours, and associated costs among businesses in the Netherlands, Spain, and Bulgaria. The results highlight both commonalities and differences among the three countries, emphasising the need for tailored cybersecurity strategies and effective incident management.

Notably, there are variations in the prevalence of different cybercrime types across the three countries, but also similar trends. **Phishing attacks are by far the most frequently encountered cyber threats** by companies in the Netherlands, Spain, and Bulgaria. Over half of Dutch companies and more than 40% of Spanish and Bulgarian companies indicated to have suffered from phishing during the past 12 months. **The second most prevalent cybercrime is malware** like viruses or spyware that is different from ransomware. In each country, more than one in six companies reported to have experienced this cyber offence, making the prevalence of malware relatively consistent across all countries. Similarly, recent studies on cybercrime against small and medium-sized enterprises have revealed that phishing and malware (excluding ransomware) are the two most prevalent cyber offenses across the EU27 countries (European Commission, 2022). Diverse cyber threats were observed across the three countries, with DDoS attacks and business identity theft being more prevalent in the Netherlands and Spain, while unauthorised accessing of files or networks by staff was a significant concern in Bulgaria. Overall, these findings align with global trends and highlight the need for robust cybersecurity measures, including employee training on cybercrime awareness and network security protocols, to mitigate the risks associated with such malicious activities.

Further analysis of the frequency of cybercrime incidents reveals that **many companies experience repeated victimisation**. Malware and phishing stand out as the most frequently reported cybercrimes across all three countries, with a majority of companies reporting multiple occurrences. Almost any other crime exhibits a pattern of repeated victimisation, with half of the companies in each country declaring to have suffered from cyber offences more than once in the previous 12 months. The two most notable exceptions regard Bulgaria, the majority of the companies (approximately 70%) victim of attempt to access without authorisation the company's online/bank account and takeovers declaring to have suffered from it only once.

The outcomes of **cybercrime incidents and associated costs** highlight the potential impact on businesses. While many companies were able to detect malware and virus attacks without significant harm, a relevant proportion reported system damage and loss of important data. Ransomware attacks resulted in notable financial losses, particularly in the Netherlands and Spain. These findings emphasise the need for businesses to invest in robust cybersecurity measures, including regular backups, secure data storage, and incident response plans.

The analysis of reporting behaviours revealed variations among the three countries, with the Netherlands demonstrating higher reporting rates for most types of cybercrime, when compared to Spain and Bulgaria. Overall, reporting rates indicate that on average approximately one in three companies reported cyber victimisation, indicating the need for increased awareness and support for companies to report cybercrime incidents to external entities. Legal obligations, prevention of repeated victimisation, and reporting because “it is the right thing to do” emerged as prominent motivations for reporting cybercrime incidents. These factors suggest that companies recognised their responsibility to comply with legal requirements, contribute to preventing future incidents, and fulfil their ethical obligations. Nonetheless, addressing companies’ distrust in authorities remains crucial, as a significant proportion of companies expressed a belief that authorities would not provide sufficient assistance. Clearer reporting channels and awareness campaigns can help bridge this gap and foster trust in the reporting process.

The preference for **handling cybercrime incidents internally emerged as a significant factor contributing to underreporting**. Many companies chose to manage incidents within their own resources, indicating a desire for greater control over incident resolution and suggesting concerns about potential reputational damage. Across the three countries, this self-handling approach was particularly prominent for business identity theft and malware incidents but was also observed across various other types of cybercrime, such as unauthorised accessing of files or networks by staff and takeovers. The perception that incidents are too trivial or not worth reporting was another prevalent reason for underreporting. This perception was particularly evident for certain types of cybercrime, including malware, phishing, and DDoS attacks. Notably, this factor for underreporting raises concerns about the level of awareness and understanding among businesses regarding the potential risks and implications associated with these incidents. Efforts to educate businesses about the significance of reporting even seemingly minor incidents and the potential impact on overall cybersecurity therefore are crucial. In addition, providing more information about reporting channels, complemented by the implementation of user-friendly platforms, would positively impact the likelihood of companies of reporting cyber incidents. Tailored strategies, supported by effective police training to encourage reporting, should therefore be developed to address specific country contexts and promote a culture of reporting cybercrime among businesses.

As for cybersecurity practices, while some companies have implemented measures such as cyber security vulnerability audits, risk assessments, and the use of specific security monitoring tools, there are still a significant share of companies that have not taken any specific actions to identify cyber security risks. This highlights the need for increased awareness and adoption of proactive measures to address potential vulnerabilities. Moreover, the diverse approaches taken by companies in outsourcing their IT support services underscore the importance of considering the potential risks and benefits associated with such decisions, particularly with regards to ensuring the adequate protection of sensitive information and mitigating cyber security risks.

The range of rules and controls implemented by companies to enhance their cyber security practices also varies, indicating different approaches taken to mitigate cyber security risks and protect sensitive information. It is evident

that companies have varying levels of compliance with important security measures such as software security updates, malware protection, firewalls, and data encryption. These findings underscore the need for consistent and comprehensive policies and controls to ensure robust cyber security practices across organizations. Moreover, the diverse work arrangements adopted by companies and the varying levels of cyber security insurance coverage highlight the need to understand different approaches taken in terms of work setups and insurance coverage to address cyber security risks and ensure adequate protection against cyber threats. Policy considerations should take into account the varying needs and circumstances of companies, promoting flexible work arrangements that accommodate hybrid models while ensuring the implementation of robust cyber security measures. Additionally, efforts should be made to raise awareness about cyber security insurance options and encourage companies to assess their coverage needs and consider appropriate policies to safeguard against potential cyber security breaches.

This study sheds light on the reporting behaviours of businesses regarding cybercrime incidents. The findings underscore the need for enhanced collaboration between businesses and law enforcement agencies, as well as improved support systems to address the perceived limitations of authorities in resolving cybercrime incidents. Encouraging businesses to report incidents through awareness campaigns and providing resources for internal incident resolution can help address the preference for handling incidents internally. Furthermore, efforts to educate businesses about the significance of reporting and the potential risks associated with underreporting are crucial in combating cybercrime effectively. Addressing underreporting and promoting a culture of reporting cybercrime incidents are crucial steps towards enhancing cybersecurity and protecting businesses from the growing threat of cybercrime. Businesses, law enforcement agencies, as well as policymakers should carefully consider such factors when formulating strategies to address underreporting and foster a more resilient and secure digital environment.

INTRODUCTION

The increasing presence of businesses in the online sphere, fuelled by technological advancements as cloud services and mobile computing, has opened new opportunities but has also exposed them to the pervasive threat of cybercrime. Within this framework, cybercrime—intended as offences reliant on computers, computer networks, and information communication technology—has been posing increasing challenges for European businesses (European Commission, 2022; Europol, 2018).

Beyond financial losses, cybercrime also carries the risk of reputational damage and privacy violations, amplifying the risks for businesses (Anderson et al., 2019; Paoli et al., 2018; Watkins, 2014). Consequently, cybersecurity has become a critical strategic consideration, prompting discussions at the highest levels of business governance (McMurdie, 2016). Ransomware, malware, distributed denial of service (DDoS) attacks, as well as phishing and business email compromise rank among the most prevalent cybercrimes targeting businesses (ENISA, 2022a; Europol, 2021). Of these threats, ransomware poses a particularly significant risk, capable of facilitating large-scale and enduring cyber-attacks that can profoundly impact organisations and businesses (ENISA, 2022b; Europol, 2021; Europol & Eurojust, 2019). The industrialisation and increasing sophistication of ransomware attacks have resulted in a sharp rise in their occurrence, particularly affecting sectors such as heavy industry, information service, government, and health (ENISA, 2022b). Meanwhile, malware, DDoS attacks, phishing, and business email compromise techniques continue to pose significant threats to businesses (ENISA, 2022a; Europol, 2020).

Over the past years, the exposure of businesses to cybercrime has been further exacerbated by the COVID-19 pandemic, the ongoing conflict in Ukraine, as well as the harmful and illegal use of artificial intelligence (AI), whose recent development has provided new opportunities to cybercriminals. The pandemic necessitated a widespread shift to remote working, increasing businesses' reliance on networks and information systems and consequently leaving businesses potentially more vulnerable to cybercrimes (Europol, 2021; Williams et al., 2019). The cyber realm has also become a new battleground in the Ukraine conflict, with Ukrainian and other countries' IT infrastructures at risk of becoming targets for cyber incidents (Lewis, 2022). Furthermore, the misuse of new AI technologies has become prevalent in propagating cyberattacks and disseminating disinformation and misinformation against governments, public authorities, and private sector entities (Velasco, 2022).

These developments call for comprehensive and adaptive cybersecurity measures to safeguard businesses against the escalating threats of cybercrime. Effective incident response plans, employee training programs, and robust infrastructure security are indispensable for protecting sensitive information and mitigating potential risks. Such actions should also address the evolving nature of cyber threats, promoting information sharing and collaboration between businesses and law enforcement agencies, and incentivising investments in cybersecurity measures. Additionally, efforts to raise awareness among businesses about the significance of cybersecurity and the importance of reporting cyber incidents are crucial for fostering a resilient and secure digital environment. It is vital to acknowledge that the exposure to

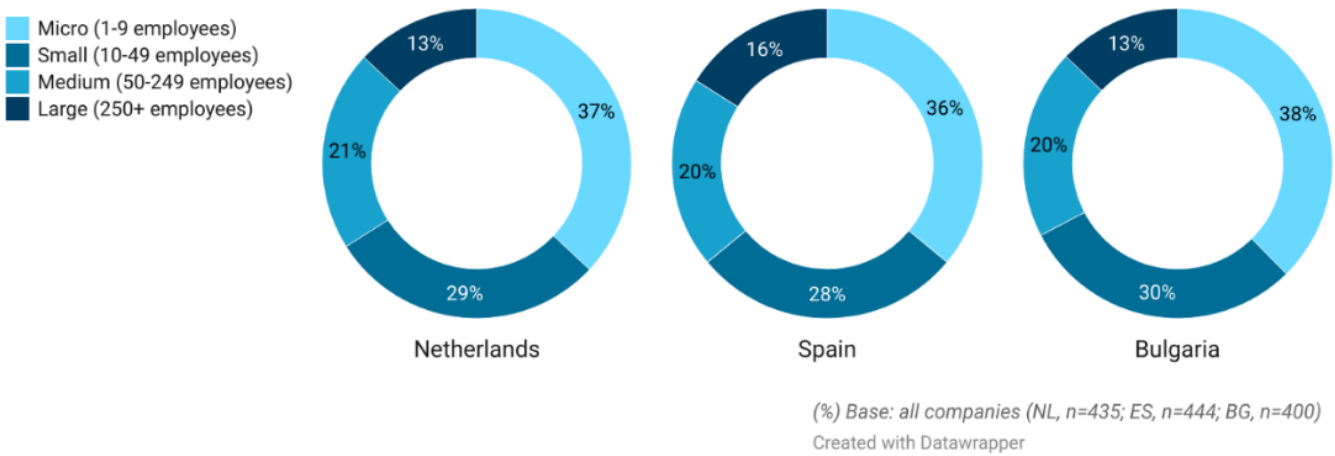
cybercrime continues to evolve, necessitating ongoing research and vigilance to proactively address emerging threats. By tackling the challenges posed by cybercrime and cultivating a culture of cybersecurity, businesses can enhance their resilience and fortify themselves against the ever-expanding threat landscape.

METHODOLOGY OF THE CYBER SECURITY SURVEY FOR BUSINESSES

We conducted the Cyber Security Survey for Businesses (henceforth the CYBBAR Survey) in the Netherlands (NL), Spain (ES), and Bulgaria (BG) using the computer-assisted telephone interviewing (CATI) method. The interviews had an average duration of 20 minutes across all three countries. We surveyed a total of 1,279 companies, including representative samples of 435 companies in the Netherlands, 444 companies in Spain, and 400 companies in Bulgaria. Notably, we made adjustments to the survey administration approach due to increased costs. Therefore, in the Netherlands and Spain, we adopted a hybrid CATI/online method. The use of online data collection (CAWI) facilitated the fieldwork agencies in collecting approximately 28% of the sample in the Netherlands and 25% in Spain.¹ Regarding the response rate, within the CATI sample, response rates were recorded at 5.50% in the Netherlands, 5.75% in Spain, and 12.28% in Bulgaria.

The CYBBAR Survey targeted micro, small, medium, and large companies (Figure 1).² To provide a comprehensive overview of the companies, we included all business sectors and organisation types in the survey, with a few exceptions. The national representative sample of around 400 completed interviews ensured a margin of error below 5% with 95% certainty of obtaining similar outcomes in a different sample.

Figure 1. Size of companies surveyed



¹ Fieldwork period: Netherlands and Spain (CATI: 6/01/2023 – 03/02/2023; CAWI: 11/01/2023 – 31/01/2023); Bulgaria (CATI: 03/01/2023 – 25/01/2023).

² In this and the subsequent sections, the percentages provided may not sum up to 100% precisely due to rounding.

The CYBBAR survey targeted companies with an online presence, as indicated by various factors such as the existence of social media accounts, websites, and online bank accounts (see Table 1 in Annex I – Survey tables). This criterion allowed us to capture a representative sample of companies actively engaged in online activities. As for the type of sector, the Information and Communication Sector accounted for the majority of sampled companies, comprising 24% of the total sample. This was followed by Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles, which represented 16%, and Professional, Scientific and Technical Activities, which accounted for 12% (see Table 2 in Annex I – Survey tables). Consistent with prior research, we excluded charities,³ public organisations, and NGOs, as these entities may be the focus of future investigations. In terms of the composition of eligible interviewees within respondent organisations, the survey predominantly included employees directly involved in cyber security or IT, comprising 75% of the total sample. Among respondents with job roles unrelated to cybersecurity or IT, senior employees accounted for 20% of the sample, while non-senior employees constituted 4% (see Table 3 in Annex I – Survey tables).

The CYBBAR data allowed us to calculate the following key indicators: prevalence rates of different cybercrimes among businesses, the unreported crime rates and the average cost incurred by companies - victims of cybercrimes. The **prevalence rate** represents the percentage of victims among all companies surveyed. The **unreported crime rate** indicates the percentage of companies that reported a crime to the public authorities, such as the police or another relevant national organisation. The **costs** related to different types of cybercrime are determined as the proportion of companies experiencing costs ranging from below 100 EUR to above 10,000 EUR. The findings by country and type of cybercrime are presented in the results section.

RESULTS

The results of the CYBBAR Survey shed light on the extent of victimisation, reporting to law enforcement and other authorities, as well as underreporting, and the associated costs incurred by the surveyed companies in Bulgaria, Spain and the Netherlands. Particular attention is devoted to the reasons for reporting and not reporting cybercrimes, alongside the cybersecurity regulations, controls, and measures implemented by victimised companies to identify and mitigate cybersecurity risks.

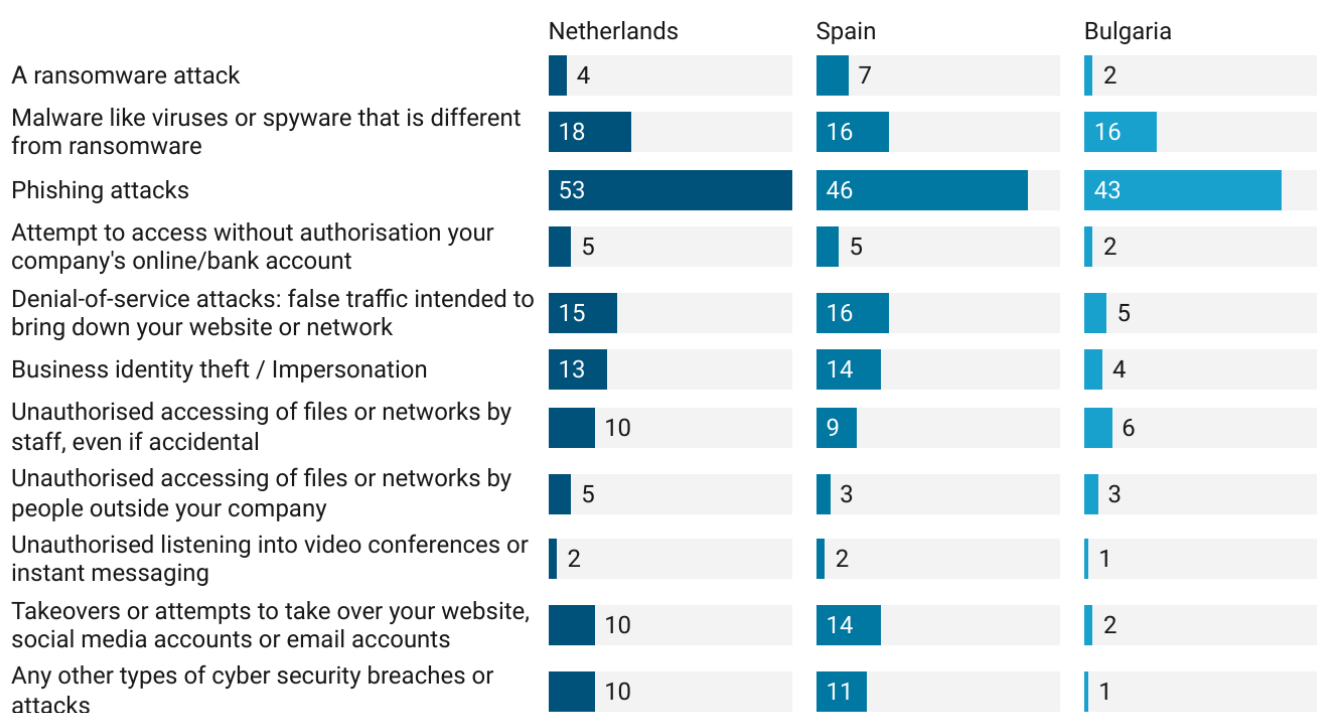
The implications of these findings are twofold: they enhance our understanding of the cybersecurity landscape in the targeted countries and offer valuable insights to policymakers, researchers, and stakeholders. By addressing cyber threats faced by businesses and formulating effective preventive measures, these insights contribute significantly to the overall cybersecurity framework.

³ Charities were excluded with the rationale that they are affected by different digital threats than businesses (Buil-Gil et al., 2021).

Cybercrime victimisation

The CYBBAR survey aimed to investigate cybercrime against businesses and reveal the extent of cyber victimisation among companies in the Netherlands, Spain, and Bulgaria over the past 12 months. In terms of the **most prevalent types of cybercrime experienced**, the analysis of the specific types of cybercrime on the total sample indicates that, on average, **phishing (47%) was the most prevalent, followed by malware (17%), DDoS attacks (11%) and business identity theft / impersonation (9%)**. In the Netherlands, over half of the companies (53%) fell victim to phishing attacks, whereas in Spain (46%) and Bulgaria (43%), the victimisation rates were slightly lower, though phishing remained the most frequently encountered type of cybercrime (Figure 2). The prevalence of malware was relatively consistent across the three countries, ranging from 16% in Bulgaria and Spain to 18% in the Netherlands. DDoS attacks were more prevalent among companies in Spain (16%) and the Netherlands (15%). In Bulgaria, the third most commonly encountered type of cybercrime was unauthorised accessing of files or networks by staff, even if accidental (hereafter referred to as unauthorised accessing by staff) (see also Table 4 in Annex I – Survey tables). In the Netherlands, one in ten companies reported experiencing takeovers or attempts to take over their website, social media accounts, or email accounts (henceforth referred to as takeovers), along with other types of cybersecurity breaches. In Spain, more than one in ten companies experienced takeovers (14%) and other types of cybersecurity breaches (11%).

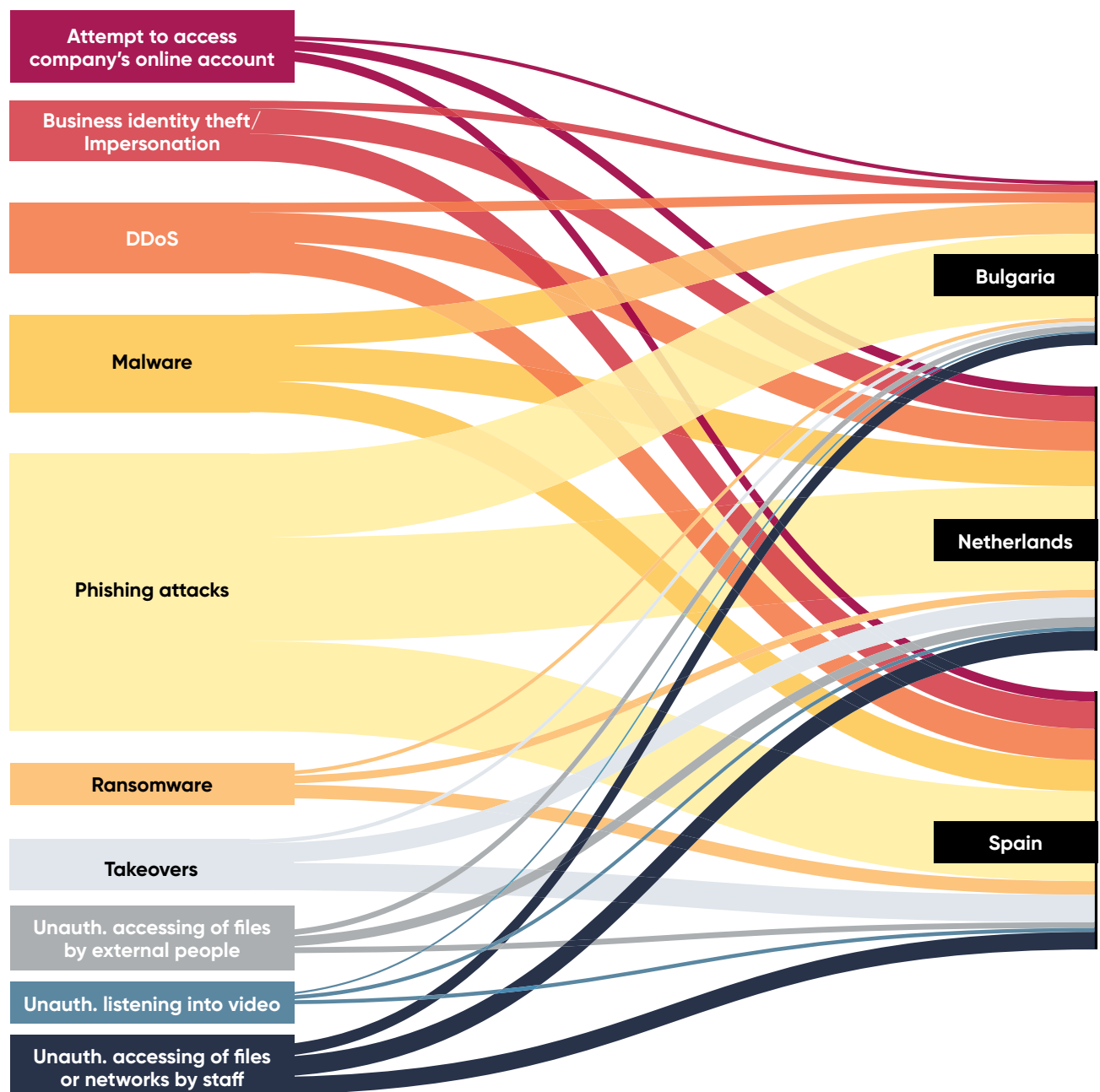
Figure 2. Type of cybercrime experienced in the past 12 months (%)



(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400)

In terms of **less prevalent types of cybercrime**, the proportion of companies that suffered from **unauthorised listening into video conferences or instant messaging** varies between 1% in Bulgaria to 2% in Spain and the Netherlands. **Unauthorised accessing of files or networks by external individuals** affected 3% of companies in Bulgaria and Spain, and 5% of companies in the Netherlands. Similarly, 5% of companies in both the Netherlands and Spain reported **attempts to access their company's online/bank accounts without authorisation**, compared to 2% of companies in Bulgaria. Ransomware was also relatively less prevalent among the surveyed companies, with Spain being the most affected country (7%), followed by the Netherlands (4%) and Bulgaria (2%) (see also Figure 3).

Figure 3. Cybercrime victimisation among companies in the Netherlands, Spain, and Bulgaria (%)



Prevalence of cybercrime victimisation

When analysing the frequency of different types of cybercrime incidents across the three countries, a notable finding emerges. **Most companies reported experiencing cyber victimisation of any crime more than once** (see Table 5 in Annex I – Survey tables). Malware incidents stand out as one of the most frequently reported cybercrimes across all three countries. In the Netherlands, 83% of companies reported experiencing malware more than once, followed by 82% in Spain and 70% in Bulgaria. Similarly, phishing attacks were prevalent, with high reporting rates for multiple occurrences. The range of reporting percentages varied from 61% in Bulgaria to 93% in Spain. Notably, 88% of companies in the Netherlands reported being targeted by phishing attacks more than once. Regarding DDoS attacks, a similar pattern emerged, although repeated victimisation was predominantly reported by companies in the Netherlands and Spain. Both countries exhibited a significant proportion, with 69% of companies reporting suffering from DDoS attacks more than once. In terms of business identity theft/impersonation incidents, half of the companies in Bulgaria reported experiencing it only once, while in the Netherlands (53%) and Spain (60%), companies encountered such cyber incidents more than once. There were variations in the prevalence of other types of cybercrime between the Netherlands, Spain, and Bulgaria. Unauthorised accessing by staff occurred more than once for 57% of companies in the Netherlands and 78% in Spain, whereas only 30% of companies in Bulgaria reported repeated victimisation. Similarly, unauthorised accessing of files or networks by external individuals occurred more than once for 79% of companies in Spain and 52% in the Netherlands, with a lower prevalence of repeated victimisation in Bulgaria (46% of companies). Another notable finding is the high prevalence of takeovers in the Netherlands (70% of companies reporting more than once) and Spain (71% of companies reporting more than once), while in Bulgaria, it was encountered as a single incident by 67% of companies. Finally, in Spain, half of the companies reported suffering from ransomware attacks only once, while the other half reported multiple occurrences. In Bulgaria, ransomware was more prevalent as a single incident, reported by 63% of companies, whereas in the Netherlands, more than half of the companies (53%) reported suffering from multiple ransomware incidents.

Outcomes of cybercrime attacks and financial costs

Among the companies that have experienced at least one ransomware attack, the majority of companies in the Netherlands (58%) and Bulgaria (50%) reported detecting the attack through their anti-virus software without any computer infection being detected. In Spain, the most common outcome of a ransomware attack was the infection of some computers (43%), but the companies managed to clean the devices on their own (see Table 6 in Annex I – Survey tables). In Spain and Bulgaria, 13% of companies sought specialised external assistance to regain access to their data, while no companies in the Netherlands reported seeking such support. Loss of data following a ransomware attack was reported by only a small proportion of companies in the Netherlands (5%) and Spain (3%).

Similarly, the vast majority of companies experiencing at least one malware or virus attack detected it through their anti-virus software, with no infection detected on their computers. This outcome was reported by 74% of companies in the Netherlands, 70% in Bulgaria, and 62% in Spain. Compared to malware, more companies sought external help, with 10% of companies in Bulgaria, 6% in Spain, and 3% in the Netherlands (see Table 7 in Annex I – Survey tables). Among the companies that have had their computers infected, more than one in ten companies (11%) in the Netherlands reported that their systems

were harmed by the attack, with this outcome reported by 22% of companies in Bulgaria and 7% in Spain. Among other outcomes of infected computers, 6% of companies in both the Netherlands and Bulgaria reported the loss of important data, while in Spain, 14% of companies experienced such a loss. Lastly, in Spain, 18% of companies reported that sensitive data may have been stolen as a result of the incident, compared to 11% of companies in the Netherlands and 6% of companies in Bulgaria (see Table 8 in Annex I – Survey tables).

Furthermore, the CYBBAR survey included questions regarding the outcomes of phishing attacks and attacks targeting company's online bank/payment accounts, as well as information on the methods employed in the latter form of cybercrime. Phishing attacks were predominantly reported as unsuccessful across all three countries, in terms of no instances of sensitive information loss or leakage. In the Netherlands and Spain, 89% of companies indicated unsuccessful attempts with no leakage of sensitive information, while in Bulgaria, 97% of companies reported the same outcome. Regarding successful attacks, 3% of companies in both the Netherlands and Spain reported financial losses despite their bank accounts not being directly targeted, and 2% of companies in these countries reported the loss of sensitive data due to such incidents. However, no companies in Bulgaria reported these outcomes. Instead, 2% of companies in Bulgaria acknowledged successful attacks without any loss of money or data, while 1% of companies reported money being stolen through bank accounts compromised by stolen credentials (see Table 9 in Annex I – Survey tables). The majority of companies experienced unsuccessful attempts when their bank/payment accounts were targeted. However, in Spain, one in ten companies reported actual monetary theft. Similar instances of loss were also reported in the Netherlands and Bulgaria, with 14% of companies in both countries reporting such incidents (see Table 10 in Annex I – Survey tables). Regarding the method of attack, around 29% of companies in both Bulgaria and the Netherlands stated that they were unaware of how the attacks were carried out. In Spain, 24% of companies reported a lack of knowledge regarding the specific method used. Almost one in five companies (19%) in each country reported that their bank/payment accounts were stolen through phishing attempts, such as fraudulent emails. Additionally, 14% of companies in both the Netherlands and Spain experienced losses due to viruses, malware, or spyware. Notably, in Bulgaria, 29% of companies had their bank/payment account information stolen through other hacking methods that exploited vulnerabilities in their intranet. This vulnerability was reported by 10% of companies in the Netherlands and 5% of companies in Spain (see Table 11 in Annex I – Survey tables).

The survey findings on cybercrime against businesses reveal significant variations in the **financial and non-financial incurred costs** across the three countries. In general, the most common responses were either no costs incurred or costs below 100 EUR (see Table 12 in Annex I – Survey tables). Notably, the Netherlands reported the highest financial costs due to ransomware attacks, with 32% of companies experiencing costs exceeding 10,000 EUR, followed by 17% of companies in Spain. The financial impact of malware attacks was most pronounced in Spain and the Netherlands. In Spain, 23% of companies reported costs ranging from 1,000 to 10,000 EUR. In the Netherlands, 12% of companies reported costs above 10,000 EUR. As for phishing attacks, the majority of companies in all three countries reported no financial costs. In the Netherlands, 39% of companies, in Spain, 47%, and in Bulgaria, a substantial

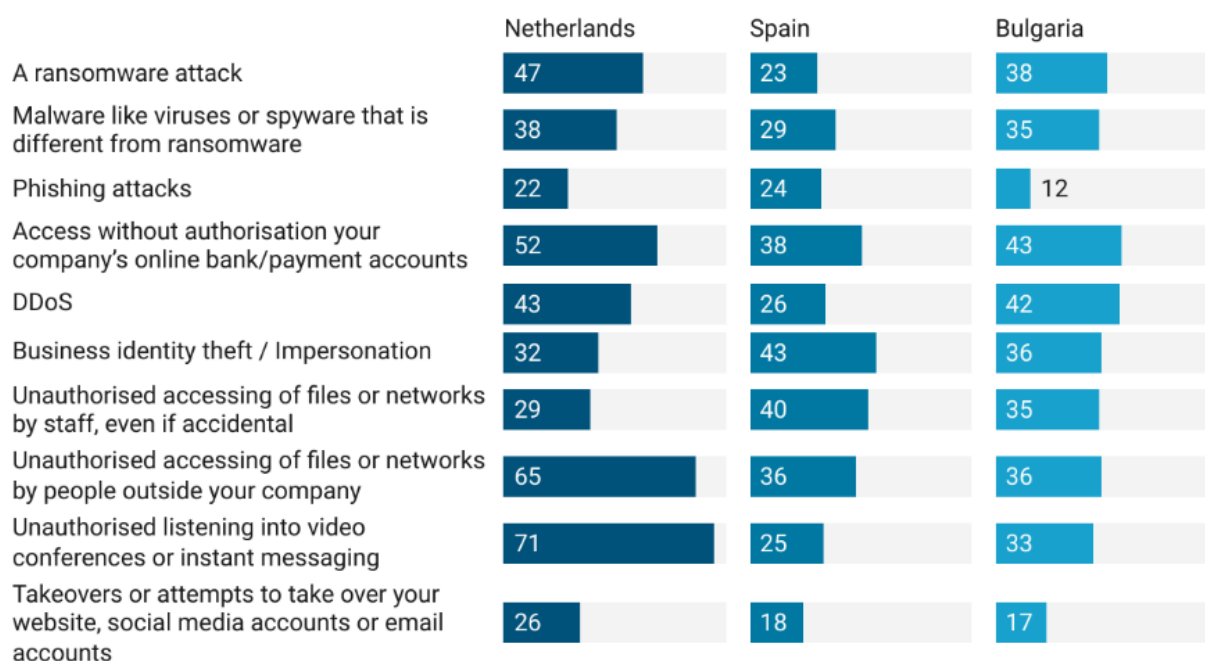
95% reported no financial impact. However, when costs were reported below 100 EUR, the Netherlands and Spain had higher percentages compared to Bulgaria.

Regarding unauthorised access to company online/bank accounts, the survey indicated that companies in the Netherlands and Spain predominantly reported costs below 100 EUR, with 43% of companies in both countries falling into this category. In contrast, in Bulgaria, 14% of companies reported costs ranging from 1,000 to 10,000 EUR. The Netherlands had a higher proportion of companies, 14%, reporting costs exceeding 10,000 EUR for this type of cybercrime. The costs associated with Distributed Denial-of-Service (DDoS) attacks were most significant in the Netherlands and Spain, with 12% of companies in the Netherlands and 9% of companies in Spain incurring costs exceeding 10,000 EUR. Finally, examining very high costs incurred, that is, above 10,000 EUR, unauthorised accessing by external individuals resulted were reported by 13% companies in the Netherlands and 14% in Spain.

Reporting of cybercrime

Examining the reporting of cybercrime incidents to law enforcement agencies or other authorities, Figure 4 provides valuable insights into the reporting behaviours of companies concerning various types of cybercrime incidents to external entities (see also Table 13 in Annex I – Survey tables).

Figure 4. Share of companies reporting any of the following cybercrimes (%)



Regarding specific types of cybercrime, the highest reporting rates were observed for unauthorised listening into video conferences or instant messaging, predominantly among companies in the Netherlands (71% of companies), while only 25% in Spain and 33% in Bulgaria reported such incidents. Similarly, a significant proportion of Dutch companies (65%) reported unauthorised accessing of files or networks by individuals outside the company, compared to 36% in both Spain and Bulgaria. In the case of ransomware attacks, nearly half (47%) of Dutch companies reported such incidents, while the reporting rates for Bulgaria and Spain were 38% and 23%, respectively. Likewise, the proportion of Dutch companies reporting unauthorised access to their company's online bank/payment accounts to 52%, compared to 38% in Spain and 43% in Bulgaria. Business identity theft/impersonation incidents prompted reporting by 32% of companies in the Netherlands, 43% in Spain, and 36% in Bulgaria. DDoS attacks were reported almost equally reported by companies in the Netherlands and Bulgaria, 43% and 42% respectively, with a lower reporting rate of companies in Spain (26%). In contrast, **phishing attacks and takeovers were the least frequently reported types of cybercrime among the three countries**. Phishing incidents prompted reporting by 22% of companies in the Netherlands, 24% in Spain, and 12% in Bulgaria. Takeovers also had low reporting rates, with 26% in the Netherlands, 18% in Spain, and 17% in Bulgaria reporting such incidents. These findings indicate that, on one hand, companies in the Netherlands reported cybercrime incidents more frequently than their counterparts in Spain and Bulgaria for almost all types of cybercrime. On the other hand, the overall reporting rates among the three countries were relatively lower compared to rates found in previous studies. For instance, the Eurobarometer 496 (European Commission, 2022) reported average reporting rates ranging between 54% and 60% for most types of cybercrime.

Among the companies that reported the cybercrime incidents to external organisations or authorities, respondents were asked to specify to whom they made the reports during the previous 12 months. Overall, across the three countries and for all types of cybercrime experienced, the two organisations/experts most commonly reached out for reporting were website administrators and internet/network service providers, followed by antivirus companies, clients/customers, and bank or credit card companies (see Figure 5). On the other hand, the European emergency number, other national government agencies, professional/trade/industry associations, and international organisations were among the least frequently reported means of reporting, along with publicly declaring the incident.

Figure 5. Reporting of cybercrimes among companies in the Netherlands, Spain, and Bulgaria – multiple answers (%)



Each square in the figure represents the average share of companies across the three countries (Netherlands, Spain, and Bulgaria) that reported each type of cybercrime to the police or other national authorities.

Country-specific analysis reveals that companies in Bulgaria frequently sought assistance from website administrators for various crimes, including malware (68% of companies reported contacting website administrators), attempts to access their company's online/bank accounts (67%), DDoS attacks (88%), and business identity theft/impersonation (80%) (see Table 14 and Table 15 in Annex I – Survey tables). Internet/network service providers were also frequently contacted by companies in Bulgaria, with 67% of companies affected by ransomware reporting reaching out to them. In the Netherlands, these providers were mainly contacted by companies affected by DDoS attacks (48%), business identity theft (44%), and unauthorised listening to video conferences (80% of companies that reported cyber incidents to external organisations). Notably, the police were most frequently contacted by companies in Spain, with 71% of companies declaring to have turned to the police to report ransomware incidents, 50% for unauthorised listening to video conferences, and 48% for business identity theft. To a lesser extent, companies in the Netherlands also contacted the police, with 39% reporting seeking their assistance for business identity theft and 33% for ransomware, followed by malware (21%), takeovers (18%), and phishing (16%). It is not surprising that companies in all three countries contacted bank or credit card companies in case of attempts to access their company's online accounts. However, only slightly more than half (55%) of companies in the Netherlands sought assistance from such companies, while in Spain, three out of four companies reached out to bank or credit card companies for this type of cybercrime, and 67% of companies in Bulgaria did the same. Lastly, other external experts and outsourced cybersecurity providers were infrequently contacted, with less than half of the companies affected by any cybercrime and reporting it stating that they sought assistance from them, except in Spain, where 60% of companies reported turning

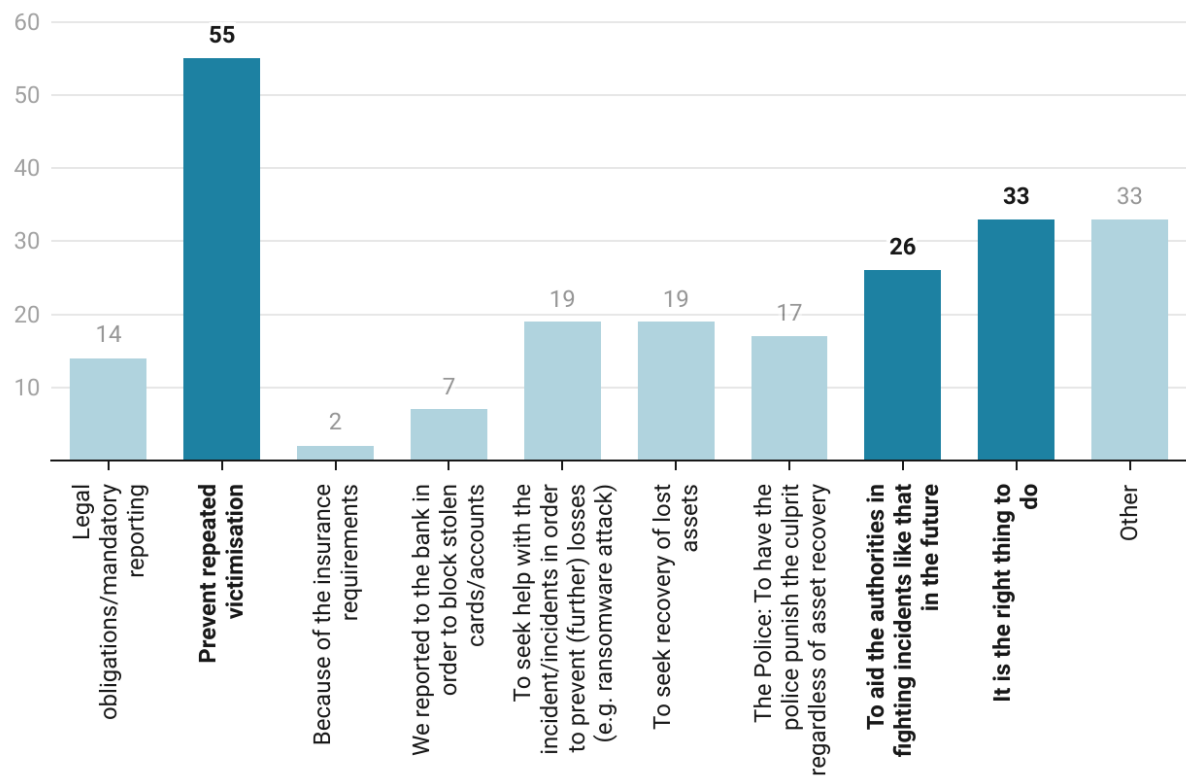
to outsourced cybersecurity providers for incidents involving unauthorised access by individuals outside the company.

Reasons for reporting
cybercrime

The reasons for reporting the last incident among Bulgarian companies are presented in Figure 6 (see also Table 16 in Annex I – Survey tables).⁴

Among the respondents, the three most frequent reasons for reporting were to prevent repeated victimisation (55%), to aid the authorities in fighting incidents like that in the future (26%), and the belief that it is the right thing to do (33%). These findings indicate that a significant share of companies in Bulgaria reported cyber incidents not only for their own protection but also to contribute to the prevention of future incidents and to fulfil their ethical responsibility. Other reasons mentioned include legal obligations/mandatory reporting (14% of companies), seeking help with the incident to prevent further losses (19%), seeking recovery of lost assets (19%), and reporting to the police for the purpose of punishing the culprit regardless of asset recovery (17%). Additionally, a small percentage of companies reported the involvement of insurance requirements (2%) and reporting to the bank to block stolen cards/accounts (7%). These findings emphasise the importance of multiple factors influencing companies’ decisions to report cyber incidents, with the prevention of repeated victimisation, collaboration with authorities, and ethical considerations being the primary motivations.

Figure 6. Reasons for reporting cybercrime among companies in Bulgaria – multiple answers (%)

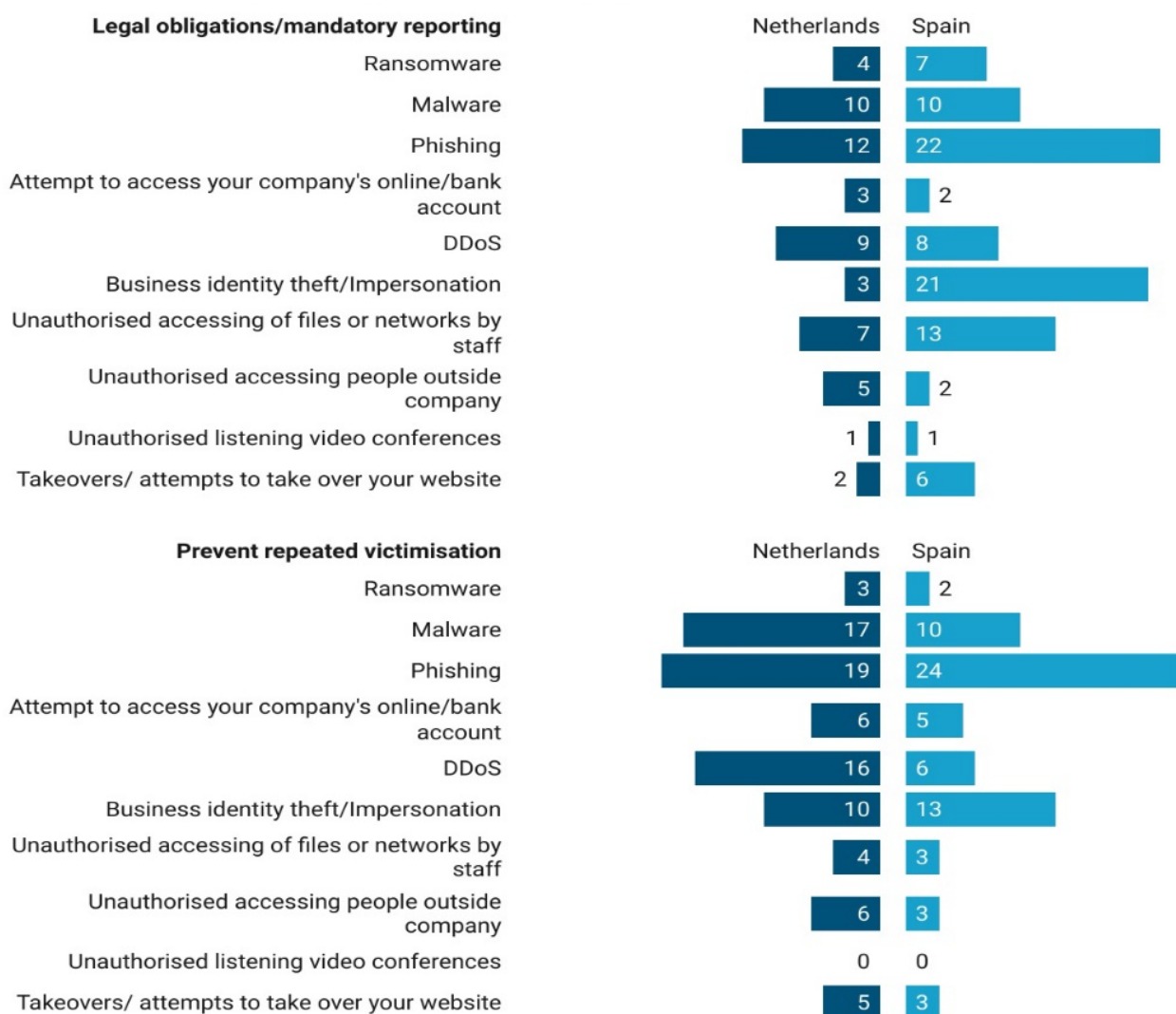


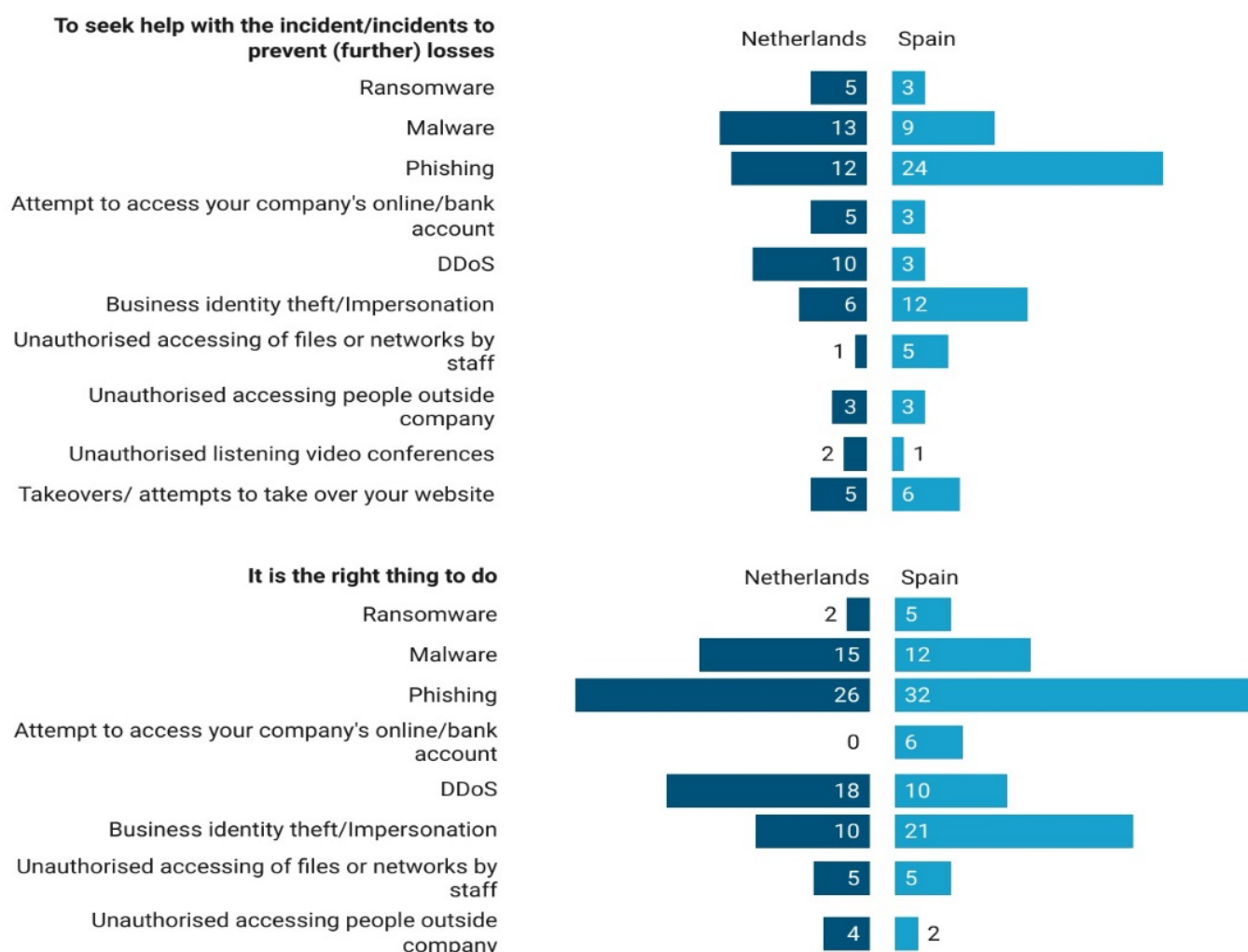
(%) Base: all Bulgarian companies providing a reason to report cybercrimes (n=42)
Created with Datawrapper

⁴ The reasons for reporting cybercrime among Bulgarian companies do not differentiate between different types of cybercrime, while in the Netherlands and Spain, the item was asked for each type of cybercrime (due to a deviation from the initial survey provided).

The analysis of reporting reasons in the Netherlands and Spain comprised also various types of cybercrime incidents to shed light on the motivations behind reporting each type of cyber incident. Overall, across the two countries and among all types of cybercrime, **legal obligations/mandatory reporting and preventing repeated victimisation, seeking help with the incident to prevent (further) losses, and the moral obligation to report as “it is the right thing to do” emerged as prominent reasons for reporting** (Figure 7, see also Table 17 in Annex I – Survey tables).

Figure 7. Key factors for reporting cybercrime in the Netherlands and Spain (%)





As for legal obligations, this reason was mostly reported among companies in the Netherlands having experienced phishing (12%), malware (10%), and DDoS attacks. Phishing attacks were also among the type of cybercrime most commonly experienced by companies in Spain declaring this factor as a reason for reporting (22%), followed by business identity theft (21% of companies), and unauthorised accessing of files by staff, for which 13% of the companies suffering from such cybercrime declared legal reasons for reporting as a factor for reaching out to someone outside their organisation (Figure 7). Similarly, preventing repeated victimisation emerged as a significant motivation for reporting phishing (19% of companies), malware (17%), and DDoS attacks (16%) in the Netherlands. In Spain, it constituted a motivation for nearly one company in five (25%) who had encountered phishing attacks, followed by business identity theft (13%) and malware attacks (10%) (Figure 7).

Among the reasons for reporting cybercrime incidents, companies in the Netherlands and Spain consistently highlighted two other key motivations: seeking help to prevent further losses and reporting because it was the right thing to do. These reasons were particularly prominent in the context of specific cybercrime types. In Spain, approximately one in four companies (24%) who experienced phishing attacks reported seeking external help to

prevent further losses. This motivation was also indicated by companies affected by business identity theft, with 12% reporting the same reason. In the Netherlands, companies targeted by malware (13%), phishing (12%), and DDoS attacks (10%) indicated that they sought external assistance to mitigate and prevent potential future losses. Furthermore, a relevant proportion of companies in Spain reported cybercrime incidents because they believed it was the right thing to do. This motivation was particularly pronounced among companies victimised by phishing (32%) and, to a lower extent, business identity theft (21%). As for Dutch companies, they emphasised the importance of doing the right thing by reporting incidents of phishing (26%), DDoS attacks (18%), and malware (15%).

Reasons for not reporting cybercrime to the police or other national authorities

Companies that have experienced cybercrime incidents within the previous 12 months but chose not to report them to the police or other national authorities were surveyed to understand the motivations behind their decision. The analysis of the responses offers valuable insights into the reasons for underreporting cybercrime in the Netherlands, Spain, and Bulgaria, highlighting variations in relation to specific cybercrime types and within each country (see Table 18 and in Annex I – Survey tables).

Among the most recurring **reasons for not reporting to the authorities**, three key factors emerged: **“they cannot do anything to help”, “we dealt with the incident internally”, and “it was too trivial/not worth reporting”**.

Firstly, a significant proportion of companies across all three countries expressed a belief that authorities would not aid in resolving the cybercrime incidents. This sentiment was particularly prevalent among companies affected by ransomware and takeovers, with 100% of companies in the Netherlands indicating this reason for both crimes. For malware incidents, approximately one in three companies in the Netherlands (31%) and a third of companies in Spain (33%) cited this as a factor. Regarding phishing, it was the most commonly reported reason for not reporting among companies in the Netherlands (50%), followed by Spain (27%) and Bulgaria (15%). DDoS attacks also prompted this reason for underreporting, especially among Dutch companies (67%), with lower percentages for companies in Spain (27%) and Bulgaria (25%). Moreover, distrust in authorities was evident among victims of business identity theft, with 78% of companies in the Netherlands, half of the companies in Bulgaria, and one in four companies in Spain citing this as a reason.

Secondly, a substantial share of companies opted to handle the incidents internally without involving external authorities. This self-handling approach was particularly prevalent for malware incidents, with 77% of companies in the Netherlands, 67% in Spain, and 56% in Bulgaria choosing to address the situation internally. Similar patterns emerged for other types of cybercrime, including phishing (71% in the Netherlands, 50% in Spain, and 70% in Bulgaria), attempts to access the company’s online/bank accounts (50% of companies in both Spain and Bulgaria, and 75% in the Netherlands), DDoS attacks (67% in the Netherlands, 64% in Spain, and 50% in Bulgaria), and business identity theft (75% of companies in Spain and Bulgaria, and 67% in the Netherlands). This suggests a preference for managing cyber-related issues within the company’s resources, possibly driven by a desire for greater control over incident resolution and concerns about potential reputational impact.

Thirdly, a common reason for not reporting cybercrime incidents was that they were considered too trivial or not worth reporting. More than half of the companies victimised by malware in the Netherlands (54%) and Spain (56%), and half of the companies affected by attempts to access their online/bank accounts in Spain and Bulgaria, cited this reason. For DDoS attacks, the prevalence of this factor was highest among companies in the Netherlands (67%) and Spain (45%). A similar trend was observed for takeovers, with 60% of Dutch companies and 57% of Spanish companies indicating this reason for not reporting. This highlights a potential lack of awareness or understanding of the risks and implications associated with these incidents, as well as the importance of reporting them.

Lastly, other reasons for not reporting cybercrime incidents included insignificant losses, which were primarily mentioned in the case of malware incidents. Additionally, some companies reported opting to report to other more relevant organisations, particularly in the Netherlands and Spain for ransomware incidents. The reason “they would not bother to do anything” also emerged, especially among Dutch companies affected by business identity theft (78%) and takeovers (60%). Other reasons, such as “we tried to report but the police were not interested”, were rarely mentioned as factors for not reporting, with few exceptions, such as Spanish companies affected by unauthorised accessing by people outside the company, with 50% of them citing this reason.

Businesses in the Netherlands, Spain, and Bulgaria were also asked about factors that would make them more likely to report cybercrime incidents in the future. Across the three countries, **having more information about reporting was the most indicated factor** that would increase the reporting of cybercrime (see Table 19 in Annex I – Survey tables). In the Netherlands and Bulgaria, 50% of respondents expressed that having more information about channels for reporting would increase their likelihood of reporting. In Spain, a higher percentage of respondents (66%) indicated that more information about reporting channels would positively influence their reporting behaviour. User-friendly platforms were also highlighted as significant in all three countries, with 36% of businesses in the Netherlands, 65% in Spain, and 39% in Bulgaria expressing that this would increase their likelihood of reporting. Enhanced online platforms were deemed important by 37% of businesses in the Netherlands, 60% in Spain, and 47% in Bulgaria, while the presence of better trained police officers was identified as a factor that would encourage reporting by 36% of businesses in the Netherlands, 54% in Spain, and 25% in Bulgaria. Lastly, businesses in the Netherlands (49%) and Spain (52%) emphasised the importance of knowledge about their legal rights and obligations as a factor that would make them more inclined to report cybercrime incidents, while in Bulgaria, only 6% of businesses considered this as a relevant factor.

Cybersecurity measures

The last section of the CYBBAR survey comprised questions about respondent's cybersecurity practices regarding cyber security risk identification and outsourcing of IT support services to external companies. The analysis provides insights into the measures taken by companies in the Netherlands, Spain, and Bulgaria to identify cyber security risks (see Table 20 in Annex I – Survey tables). The investigation reveals variations among the three countries. A considerable proportion of companies in all three countries have undertaken various actions to identify cyber security risks. For example, a cyber security vulnerability audit was conducted by 49%

of companies in the Netherlands and 47% in Spain, although by only 12% in Bulgaria. Similarly, 46% of companies in the Netherlands, 44% in Spain, and 34% in Bulgaria reported conducting a risk assessment covering cyber security risks or investing in threat intelligence. In addition, the use of specific tools designed for security monitoring was reported by a significant number of companies, with 55% in the Netherlands, 61% in Spain, and 27% in Bulgaria using such tools, while testing staff awareness and response to cyber security risks emerged as a common practice mostly among Dutch (47%) and Spanish (39%) companies, with a much lower prevalence among companies in Bulgaria (9%). Overall, a noteworthy proportion of companies in Bulgaria (51%) reported not undertaking any of these risk identification measures, therefore indicating the absence of such practices among one in two companies surveyed in the country.

Turning to the **outsourcing of IT support services**, the majority of companies in all three countries indicated that their IT services were either not outsourced or only minor aspects were outsourced (Table 21 in Annex I – Survey tables). Specifically, 40% of companies in the Netherlands, 51% in Spain, and 43% in Bulgaria reported that IT services were not outsourced, or only minor aspects were outsourced. Among the other responses, approximately one in three companies in Bulgaria reported having external companies responsible for their cybersecurity, while this prevalence was lower among companies in the Netherlands and Spain (7% in both countries). In contrast, a higher percentage of companies in the Netherlands (29%) and Spain (17%) reported a partial outsourcing arrangement where both the company and the external service provider shared responsibility for cybersecurity.

In the context of **implementing rules and controls for cyber security**, the majority of companies in all three countries reported having up-to-date malware protection, with percentages ranging from 74% in Bulgaria to 83% in the Netherlands (see Table 22 in Annex I – Survey tables). Similarly, a high percentage of companies in the Netherlands (80%) and Spain (79%) indicated the implementation of firewalls that cover their entire IT network, as well as individual devices. Restricting IT admin and access rights to specific users was also reported by a significant share of companies in the same two countries, with percentages ranging from 74% in Spain to 80% in the Netherlands.

In addition, a considerable proportion of companies reported to have specific rules for storing and moving personal data securely, with 64% in Spain, 70% in the Netherlands, and 39% in Bulgaria implementing such measures. Security controls on company-owned devices, including laptops, were reported by 71% of companies in both the Netherlands and Spain, while the percentage was slightly lower in Bulgaria at 47%. A notable proportion of companies in the Netherlands (74%) and Spain (59%) reported having a separate WiFi network for staff and visitors, while this prevalence accounts to less than one in ten companies (7%) in Bulgaria. Other rules and controls implemented by companies included enforcing a password policy for setting strong passwords, implementing a two or three-step login verification for employees or clients, and using encryption techniques for data, documents, or emails. Lastly, it is worth noting that less than half of the companies across the three countries reported to hold regular cyber security trainings or awareness raising sessions specifically for staff members who are not directly involved in cyber security, with the lowest share found among Bulgarian companies (14%).

The working arrangements adopted by companies varied, with different work setups implemented across the three countries (see Table 23 in Annex I –

Survey tables). In the Netherlands, the majority of companies (68%) reported having a hybrid work setup, where some employees come to the office while others work from home. Similarly, in Spain, 53% of companies followed a hybrid work setup, while in Bulgaria, this percentage was significantly lower at 10%. On the other hand, a considerable proportion of companies in Bulgaria (80%) reported that everyone works at the company premises, whereas in Spain, 30% of companies followed this approach. The use of co-working spaces was less prevalent, with only a small percentage of companies across the three countries (ranging from 1% to 7%) reporting this working arrangement for all of their employees.

Finally, the survey inquired about companies' cyber security insurance policies (see Table 24 in Annex I – Survey tables). A notable proportion of companies in Bulgaria (83%) reported not having any cyber security insurance, whereas in the Netherlands and Spain, the percentages were lower (40% for both countries) although still significant. Moreover, in the Netherlands, 14% of companies reported having a specific cyber security insurance policy, while 26% reported having cyber security cover as part of a broader insurance policy. Similar patterns were observed in Spain, with 17% of companies having a specific cyber security insurance policy and 26% having cyber security cover as part of a broader insurance policy. In Bulgaria, the percentages were significantly lower, with only 3% of companies having a specific cyber security insurance policy and 10% having cyber security cover as part of a broader insurance policy.

REFERENCES

- 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/>
- 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>
- ENISA. (2022a). *ENISA Threat Landscape 2022*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
- ENISA. (2022b). *ENISA Threat Landscape for Ransomware Attacks*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>
- European Commission. (2022). *Flash Eurobarometer 496: SMEs and cybercrime*. Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/00fcf078-d19d-11ec-a95f-01aa75ed71a1/language-en/format-PDF>
- 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>
- Lewis, J. A. (2022). *Cyber War and Ukraine*. Center for Strategic and International Studies. <https://www.csis.org/analysis/cyber-war-and-ukraine>
- 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>
- 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>

- Velasco, C.** (2022). *Cybercrime and Artificial Intelligence*. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23(1), 109–126. <https://doi.org/10.1007/s12027-022-00702-z>
- 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>

ANNEX I – SURVEY TABLES

Table 1. Does your company currently have or use? (multiple answers)

	NL	ES	BG
Accounts or pages on social media sites (e.g. Facebook or Twitter)	84	82	49
A company/organisation website	96	95	70
An online bank account	89	76	83
An online ordering and payment service for customers	33	34	59
Online ordering or payment systems of suppliers, consultants or other business partners	38	39	48
Company e-wallets/accounts different from a bank account (like PayPal or crypto-wallets)	27	34	25
An industrial control system	25	29	17
Web-based applications for payroll processing, e-signature etc	67	59	55
Cloud computing or storage	87	84	35
Personal data about your clients stored electronically	84	82	59
Network-connected devices like TVs, building controls, alarms, speakers etc., sometimes called smart devices	72	65	54
A company intranet	54	70	55
Work computers connected to the Internet or other IT technologies	96	98	96
Personal devices owned by your employees such as smartphones, tablets, laptops or desktop computers that are used to carry out regular business-related activities	74	72	86

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 2. What is the main economic activity of your company?

	NL	ES	BG	Total
Agriculture, Forestry and Fishing	2	2	5	3
Mining and Quarrying	0	0	1	0
Manufacturing	14	13	8	12
Electricity, Gas, Steam and Air Conditioning Supply	1	1	0	1
Water Supply; Sewerage, Waste Management and Remediation Activities	0	1	1	0
Construction	3	5	6	5
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles	8	9	33	16
Transportation and Storage	3	2	5	3
Accommodation and Food Service Activities	0	2	7	3
Information and Communication	41	25	3	24
Financial and Insurance Activities	4	2	2	3
Real Estate Activities	2	2	7	3
Professional, Scientific and Technical Activities	6	22	10	13
Administrative and Support Service Activities	6	6	3	5
Public Administration and Defence; Compulsory Social Security	1	1	0	1
Education	1	2	1	1
Human Health and Social Work Activities	4	1	4	3
Arts, Entertainment and Recreation	3	3	1	2
Other activities	0	0	6	2

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 3. Is your job:

	NL	ES	BG	Total
Directly related to cyber security	20	23	17	20
Directly related to IT	61	54	19	45
Not related to cyber security/IT – senior management level	14	15	64	30
Not related to cyber security/IT – non-senior management level	4	8	0	4

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 4. Has your company experienced any of the incidents listed below in the past 12 months (January 2022 – December 2022)? (multiple answers)

Type of cybercrime	NL	ES	BG
A ransomware attack	4	7	2
Malware like viruses or spyware that is different from ransomware	18	16	16
Phishing attacks	53	46	43
Attempt to access without authorisation your company's online/ bank account	5	5	2
Denial-of-service attacks: false traffic intended to bring down your website or network	15	16	5
Business identity theft / Impersonation	13	14	4
Unauthorised accessing of files or networks by staff, even if accidental	10	9	6
Unauthorised accessing of files or networks by people outside your company	5	3	3
Unauthorised listening into video conferences or instant messaging	2	2	1
Takeovers or attempts to take over your website, social media accounts or email accounts	10	14	2
Any other types of cyber security breaches or attacks	10	11	1

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 5. Approximately, how often in the last 12 months did you experience any of the following cybercrimes?

		NL	ES	BG
A ransomware attack	Once only	42	50	63
	More than once	53	50	38
	Refused/Don't Know	5	0	0
Malware like viruses or spyware that is different from ransomware	Once only	11	18	27
	More than once	83	82	70
	Refused/Don't Know	7	0	3
Phishing attacks	Once only	9	5	9
	More than once	88	93	61
	Refused/Don't Know	3	2	31
Attempt to access without authorisation your company's online/ bank account	Once only	43	24	71
	More than once	52	71	29
	Refused/Don't Know	5	5	0
Denial-of-service attacks	Once only	28	30	63
	More than once	69	69	32
	Refused/Don't Know	3	1	5
Business identity theft / Impersonation	Once only	46	35	50
	More than once	53	60	36
	Refused/Don't Know	2	5	14
Unauthorised accessing of files or networks by staff, even if accidental	Once only	29	20	65
	More than once	57	78	30
	Refused/Don't Know	14	3	4
Unauthorised accessing of files or networks by people outside your company	Once only	44	21	55
	More than once	52	79	46
	Refused/Don't Know	4	0	0
Unauthorised listening into video conferences or instant messaging	Once only	29	25	0
	More than once	43	75	100
	Refused/Don't Know	29	0	0
Takeovers or attempts to take over your website, social media accounts or email accounts	Once only	26	23	67
	More than once	70	71	17
	Refused/Don't Know	5	7	17

(%) Base: companies that have experienced at least one type of cybercrime in the last 12 months – Ransomware (NL, n=19; ES, n=30; BG, n=8); Malware (NL, n=76; ES, n=73; BG, n=63); Phishing attacks (NL, n=232; ES, n=205; BG, n=172); Attempt to access without authorisation your company's online/bank account (NL, n=21; ES, n=21; BG, n=7); Denial-of-service attacks (NL, n=67; ES, n=70; BG, n=19); Business identity theft /Impersonation (NL, n=57; ES, n=63; BG, n=14); Unauthorised accessing of files or networks by staff, even if accidental (NL, n=42; ES, n=40; BG, n=23); Unauthorised accessing of files or networks by people outside your company (NL, n=23; ES, n=14; BG, n=11); Unauthorised listening into video conferences or instant messaging (NL, n=7; ES, n=8; BG, n=3); Takeovers or attempts to take over your website, social media accounts or email accounts (NL, n=43; ES, n=61; BG, n=6).

Table 6. 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?

	NL	ES	BG
We detected the attack through our anti-virus software, but no computers were infected	58	40	50
Some computers were infected, but we managed to clean them on our own using an anti-virus program or other methods	37	43	38
Some computers were infected and we had to seek specialized help outside of our company to get back access to our data	0	13	13
We lost our data (regardless of whether paying a ransom or not).	5	3	0

(%) Base: companies that have experienced at least one ransomware attack in the last 12 months (NL, n=19; ES, n=30; BG, n=8).

Table 7. 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?

	NL	ES	BG
We detected the attack through our anti-virus software, but no computers were infected	74	62	70
Some computers were infected, but we managed to clean them on our own using an anti-virus program or other methods	21	33	19
Some computers were infected and we had to seek specialized help outside of our company to get back access to our data	3	6	10
Don't know	3	0	2

(%) Base: companies that have experienced at least one virus/malware attack in the last 12 months (NL, n=76; ES, n=73; BG, n=63).

Table 8. Thinking again about the last time your company computers were infected, did you lose any money or sensitive data? (multiple answers)

	NL	ES	BG
Our bank accounts were attacked through stolen credentials, but we did not lose any money	6	25	0
Our bank accounts were attacked through stolen credentials and money were stolen	11	0	6
We lost important data	6	14	6
Sensitive data might have been stolen due to the incident	11	18	6
Our systems were harmed	11	7	22
No money or data were stolen and we managed to restore our computers and other systems	72	61	89

(%) Base: companies that have had their computers infected in the last 12 months (NL, n=18; ES, n=28; BG, n=18).

Table 9. 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?

	NL	ES	BG
To the best of our knowledge, the attack was not successful and no sensitive information was leaked	89	89	97
Our bank accounts were attacked through stolen credentials, but we did not lose any money	3	3	1
Our bank accounts were attacked through stolen credentials and money was stolen	1	0	1
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	3	3	0
Sensitive data might have been stolen due to the incident	2	2	0
The attack was successful, but we did not lose any money or data	1	2	2
Do not know	1	0	0

(%) Base: companies that have experienced at least one phishing attack in the last 12 months (NL, n=237; ES, n=211; BG, n=172).

Table 10. 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?

	NL	ES	BG
The attack was not successful and we did not lose any money	81	91	86
Money was stolen	14	10	14
Don't know	5	0	0

(%) Base: companies that have experienced at least one attack against your company's online bank/payment accounts in the last 12 months (NL, n=21; ES, n=21; BG, n=7).

Table 11. You mentioned that you experienced at least one attack against your company's online bank/payment accounts. Thinking again of the last time this happened, do you have any information on how the attack was carried out?

	NL	ES	BG
We do not know how the attack was carried out	29	24	29
Bank/payment account information was stolen through phishing – i.e. through fraudulent emails	19	19	29
Bank/payment account information was stolen through a virus/malware/spyware	14	14	0
Bank/payment account information was stolen through other hacking methods involving using vulnerabilities in our intranet	10	5	29
Automatic attempts to “guess” our password – a brute force attack	0	0	14
Other	24	38	0
Don't know	5	0	0

(%) Base: companies that have experienced at least one attack against your company's online bank/payment accounts in the last 12 months (NL, n=21; ES, n=21; BG, n=7).

Table 12. Thinking of the last time there was any of the following types of cybercrime, 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?

	Ransomware			Malware			Phishing			Attempt to access your company's online/bank account			DDoS			Business identity theft/Impersonation		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
No cost of this kind incurred	16	33	50	26	29	70	39	47	95	19	24	86	25	31	79	28	35	57
Below 100 EUR	21	17	13	28	29	16	35	30	4	43	43	0	30	27	11	46	38	21
100 - 1000 EUR	11	10	25	15	10	8	13	10	1	5	14	0	16	14	11	11	8	14
1000 – 10,000 EUR	11	20	13	13	23	3	5	7	0	10	14	14	12	14	0	5	8	7
Above 10,000 EUR	32	17	0	12	4	2	3	2	0	14	5	0	12	9	0	9	2	0
Refused/Don't know	11	3	0	7	6	2	5	4	1	10	0	0	5	4	0	2	10	0

	Unauthorised accessing of files or networks by staff			Unauthorised accessing people outside company			Unauthorised listening video conferences			Takeovers or attempts to take over your website			Any other types of cyber security breaches or attacks		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
No cost of this kind incurred	41	25	61	44	14	64	14	13	100	26	25	67	30	27	100
Below 100 EUR	19	30	30	9	21	9	29	38	0	30	41	17	21	35	0
100 - 1000 EUR	7	15	4	9	7	9	14	25	0	23	16	17	16	17	0
1000 – 10,000 EUR	14	20	4	17	43	9	14	25	0	12	7	0	7	10	0
Above 10,000 EUR	7	8	0	13	14	0	14	0	0	7	5	0	14	6	0
Refused/Don't know	12	3	0	9	0	9	14	0	0	2	7	0	12	4	0

(%) Base: companies that have experienced at least one type of cybercrime – Ransomware (NL, n=19; ES, n=30; BG, n=8); Malware (NL, n=76; ES, n=73; BG, n=63); Phishing attacks (NL, n=232; ES, n=205; BG, n=172); Attempt to access without authorisation your company's online/bank account (NL, n=21; ES, n=21; BG, n=7); Denial-of-service attacks (NL, n=67; ES, n=70; BG, n=19); Business identity theft / Impersonation (NL, n=57; ES, n=63; BG, n=14); Unauthorised accessing of files or networks by staff, even if accidental (NL, n=42; ES, n=40; BG, n=23); Unauthorised accessing of files or networks by people outside your company (NL, n=23; ES, n=14; BG, n=11); Unauthorised listening into video conferences or instant messaging (NL, n=7; ES, n=8; BG, n=3); Takeovers or attempts to take over your website, social media accounts or email accounts (NL, n=43; ES, n=61; BG, n=6); Any other types of cyber security breaches or attacks (NL, n=43; ES, n=48; BG, n=5).

Table 13. Thinking about the last time there was any of the following types of cybercrime, was this breach, attempt, or attack reported to anyone outside your company, or not?

	NL	ES	BG
	Yes	Yes	Yes
A ransomware attack	47	23	38
Malware like viruses or spyware that is different from ransomware	38	29	35
Phishing attacks	22	24	12
Attempt to access without authorisation your company's online/ bank account	52	38	43
DDoS	43	26	42
Business identity theft / Impersonation	32	43	36
Unauthorised accessing of files or networks by staff, even if accidental	29	40	35
Unauthorised accessing of files or networks by people outside your company	65	36	36
Unauthorised listening into video conferences or instant messaging	71	25	33
Takeovers or attempts to take over your website, social media accounts or email accounts	26	18	17

(%) Base: companies that have experienced at least one type of cybercrime in the last 12 months – Ransomware (NL, n=19; ES, n=30; BG, n=8); Malware (NL, n=76; ES, n=73; BG, n=63); Phishing attacks (NL, n=232; ES, n=205; BG, n=172); Attempt to access without authorisation your company's online/bank account (NL, n=21; ES, n=21; BG, n=7); Denial-of-service attacks (NL, n=67; ES, n=70; BG, n=19); Business identity theft / Impersonation (NL, n=57; ES, n=63; BG, n=14); Unauthorised accessing of files or networks by staff, even if accidental (NL, n=42; ES, n=40; BG, n=23); Unauthorised accessing of files or networks by people outside your company (NL, n=23; ES, n=14; BG, n=11); Unauthorised listening into video conferences or instant messaging (NL, n=7; ES, n=8; BG, n=3); Takeovers or attempts to take over your website, social media accounts or email accounts (NL, n=43; ES, n=61; BG, n=6).

Table 14. Thinking again about the last incident of this type, who was this breach or attack reported to? (multiple answers) – continues next page

	Ransomware			Malware			Phishing			Attempt to access your company's online/bank account			DDoS		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
The Police	33	71	0	21	14	14	16	25	5	9	25	33	7	11	0
European emergency number (112)	22	0	0	0	5	0	0	4	0	9	13	0	3	6	0
Specialised cybercrime hotline (if applicable to the country)	22	29	33	24	19	5	26	25	5	9	0	33	14	11	0
National Cyber Security Centre	33	43	0	28	38	0	22	20	0	9	38	0	7	22	0
Data protection agency (if applicable to the country)	0	43	0	21	24	9	6	18	5	18	25	33	3	22	0
Other national government agency	22	14	0	7	0	0	6	0	0	0	0	0	3	6	0
Bank or credit card company	44	29	0	24	19	23	14	33	10	55	75	67	14	11	0
Insurance company	22	57	0	3	24	0	8	14	0	18	25	0	14	17	0
Internet/Network Service Provider	11	29	67	21	29	50	26	22	43	18	0	33	48	28	50
Website administrator	33	43	33	21	29	68	22	29	29	36	13	67	48	22	88
Outsourced cyber security provider	44	43	0	38	43	18	28	33	10	18	13	0	21	44	25
Antivirus company	22	29	0	31	24	36	18	20	67	27	0	33	10	11	50
Professional/trade/industry association	11	0	0	3	0	5	2	8	5	0	0	0	0	0	13
Clients/customers	11	43	0	21	29	27	12	16	19	0	13	33	41	22	13
Suppliers	11	29	0	10	19	14	2	27	19	9	0	33	14	22	13
Was publicly declared	22	43	0	3	0	0	0	6	0	0	0	33	7	0	0
An international organisation	11	14	0	3	0	0	0	4	0	0	0	0	3	6	0

Table 15. continued table – Q10 Thinking again about the last incident of this type, who was this breach or attack reported to? (multiple answers)

	Business identity theft/Impersonation			Unauthorised accessing of files or networks by staff			Unauthorised accessing people outside company			Unauthorised listening video conferences			Takeovers or attempts to take over your website		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
The Police	39	48	20	17	19	0	13	40	0	20	50	0	18	18	0
European emergency number (112)	0	4	0	8	6	0	20	20	0	20	0	0	18	0	0
Specialised cybercrime hotline (if applicable to the country)	17	26	0	8	0	0	13	0	0	0	0	0	27	0	0
National Cyber Security Centre	6	30	0	8	19	0	13	0	0	40	50	0	18	18	0
Data protection agency (if applicable to the country)	17	30	0	25	25	0	13	40	0	40	0	0	46	18	0
Other national government agency	6	0	0	33	6	0	27	0	0	0	0	0	0	0	0
Bank or credit card company	11	30	0	8	19	0	20	20	0	40	0	0	36	18	0
Insurance company	11	15	0	17	13	0	27	20	0	20	0	0	36	27	0
Internet/Network Service Provider	44	19	80	17	6	38	20	40	50	80	50	0	27	46	100
Website administrator	44	30	80	17	25	38	20	20	50	40	50	100	64	27	100
Outsourced cyber security provider	44	26	0	8	13	6	20	60	0	0	0	0	18	9	0
Antivirus company	33	22	60	8	6	25	7	0	50	20	0	0	18	0	0
Professional/trade/industry association	0	7	0	0	19	0	13	0	0	20	0	0	0	9	0
Clients/customers	17	41	0	8	19	0	13	40	0	20	0	100	18	46	0
Suppliers	17	41	0	0	19	0	7	20	0	0	0	0	9	46	0
Was publicly declared	0	0	0	8	6	0	0	0	25	0	0	0	0	9	0
An international organisation	6	4	0	0	0	0	7	0	0	20	0	0	9	0	0

(%) Base: companies that have experienced at least one type of cybercrime in the last 12 months and have reported to anyone – Ransomware (NL, n=9; ES, n=7; BG, n=3); Malware (NL, n=29; ES, n=21; BG, n=22); Phishing attacks (NL, n=51; ES, n=49; BG, n=21); Attempt to access without authorisation your company's online/bank account (NL, n=11; ES, n=8; BG, n=3); Denial-of-service attacks (NL, n=29; ES, n=18; BG, n=8); Business identity theft / Impersonation (NL, n=18; ES, n=27; BG, n=5); Unauthorised accessing of files or networks by staff, even if accidental (NL, n=12; ES, n=16; BG, n=8); Unauthorised accessing of files or networks by people outside your company (NL, n=15; ES, n=5; BG, n=4); Unauthorised listening into video conferences or instant messaging (NL, n=5; ES, n=2; BG, n=1); Takeovers or attempts to take over your website, social media accounts or email accounts (NL, n=11; ES, n=11; BG, n=1).

Table 16. What were the reasons you decided to report the last incident? - Bulgaria (multiple answers)

Reasons for reporting among Bulgarian companies	%
Legal obligations/mandatory reporting	14
Prevent repeated victimisation	55
Because of the insurance requirements	2
We reported to the bank in order to block stolen cards/accounts	7
To seek help with the incident/incidents in order to prevent (further) losses (e.g. ransomware attack)	19
To seek recovery of lost assets	19
The Police: To have the police punish the culprit regardless of asset recovery	17
To aid the authorities in fighting incidents like that in the future	26
It is the right thing to do	33
Other	33

(%) Base: companies in Bulgaria that have experienced at least one type of cybercrime in the last 12 months and have reported it to anyone outside their organisation (n=42).

Table 17. What were the reasons you decided to report cybercrimes? – Netherlands and Spain (multiple answers)

	Ransomware		Malware		Phishing		Attempt to access your company's online/bank account		DDoS		Business identity theft/Impersonation		Unauthorised accessing of files or networks by staff		Unauthorised accessing people outside company		Unauthorised listening video conferences		Takeovers/ attempts to take over your website	
	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES	NL	ES
Legal obligations / mandatory reporting	4	7	10	10	12	22	3	2	9	8	3	21	7	13	5	2	1	1	2	6
Prevent repeated victimisation	3	2	17	10	19	24	6	5	16	6	10	13	4	3	6	3	0	0	5	3
Because of the insurance requirements	3	3	4	9	3	8	1	1	3	3	3	7	1	5	5	2	3	1	2	3
We reported to the bank in order to block stolen cards/accounts	2	3	3	6	8	10	5	7	2	1	4	12	5	3	6	1	3	1	4	2
To seek help with the incident to prevent (further) losses	5	3	13	9	12	24	5	3	10	3	6	12	1	5	3	3	2	1	5	6
To seek recovery of lost assets	1	2	3	3	5	9	3	3	0	2	3	8	2	2	3	1	0	0	4	3
The Police: To have the police punish the culprit regardless of asset recovery	1	5	3	2	2	12	1	2	2	1	5	12	2	2	2	1	1	0	2	1
To aid the authorities in fighting incidents like that in the future	1	5	6	7	8	17	1	2	3	6	4	15	2	3	1	2	1	0	1	1
It is the right thing to do	2	5	15	12	26	32	0	6	18	10	10	21	5	5	4	2	0	0	2	7
Other	0	0	0	2	3	6	0	0	5	5	4	0	1	2	0	0	1	0	2	1

(%) Base: companies that have experienced at least one type of cybercrime in the last 12 months and have reported it to anyone outside their organisation (NL, n=96; ES, n=87).

Table 18. What were the reasons you didn't report the last incident of this type to the police or 112 or other national authorities? (multiple answers) – continues next page

	Ransomware			Malware			Phishing			Attempt to access your company's online/bank account			DDoS		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
They cannot do anything to help	100	0	0	31	33	6	50	27	15	38	0	50	67	27	25
We dealt with the incident internally	0	100	100	77	67	56	71	50	70	75	50	50	67	64	50
It was too trivial/not worth reporting	100	0	0	54	56	17	57	42	15	50	50	50	67	45	13
We expected it would be reported by another authority (e.g. Internet provider/bank)	0	0	0	8	0	0	14	38	0	13	50	0	38	18	0
We tried to report it but police were not interested	0	0	0	8	0	0	4	0	0	13	0	0	0	0	0
We did not know the police dealt with this type of incident	0	0	50	23	22	28	21	8	15	50	0	0	24	36	13
It was too inconvenient/too much trouble	0	0	0	23	0	6	7	0	0	13	0	0	33	0	13
They would not bother to do anything about it	100	0	50	31	11	17	32	8	5	25	25	0	29	0	13
The (Country) police are not trustworthy when it comes to incidents like these	0	0	0	0	22	6	7	4	0	13	25	0	10	0	13
We reported to other more relevant organisations	100	100	0	38	11	11	21	8	5	0	25	50	38	18	38
We did not know to which agency we should report such incidents	0	0	0	15	33	17	25	8	5	38	25	0	19	0	13
Because of the complexity of reporting / burdensome / bureaucratic procedures	100	0	0	8	22	6	14	8	0	25	0	0	10	9	0
We did not know this was a crime	0	0	0	15	22	0	4	4	10	13	25	0	19	9	0
We did not want the incident/s to be known outside of the company due to potential reputational damage	0	0	0	8	11	6	0	0	10	0	0	0	14	0	0

Because of possible interruption of business processes (e.g. servers are taken for forensic analysis, etc.)	0	0	0	8	11	6	4	8	5	0	0	0	5	0	0
We didn't know we had an incident until much later	0	0	0	0	33	6	0	4	0	0	0	0	0	9	0
Our losses from the incident were insignificant	100	0	50	46	56	11	36	27	5	38	50	0	48	36	13
	Business identity theft/Impersonation			Unauthorised accessing of files or networks by staff			Unauthorised accessing people outside company			Unauthorised listening video conferences			Takeovers or attempts to take over your website		
	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG	NL	ES	BG
They cannot do anything to help	78	25	50	33	22	25	22	0	0	50	0	0	100	29	0
We dealt with the incident internally	67	75	75	33	78	88	67	50	50	50	0	100	40	57	100
It was too trivial/not worth reporting	56	38	50	17	22	38	44	0	25	0	0	0	60	57	0
We expected it would be reported by another authority (e.g. Internet provider/bank)	11	13	0	33	0	13	0	100	0	0	0	0	0	14	0
We tried to report it but police were not interested	11	0	25	0	0	13	11	50	25	0	0	0	0	0	0
We did not know the police dealt with this type of incident	11	25	25	0	0	13	11	0	25	0	0	0	20	0	0
It was too inconvenient/too much trouble	33	0	0	17	0	0	0	0	0	0	0	0	20	14	0
They would not bother to do anything about it	78	13	0	33	0	0	11	50	0	50	0	0	60	0	0
The (Country) police are not trustworthy when it comes to incidents like these	11	25	0	17	0	0	22	0	0	50	0	0	20	14	0
We reported to other more relevant organisations	44	0	0	17	0	13	22	0	50	0	0	0	20	14	0
We did not know to which agency we should report such incidents	33	13	0	0	0	0	11	0	0	0	0	0	20	0	100
Because of the complexity of reporting / burdensome / bureaucratic procedures	33	0	0	17	0	0	22	50	0	50	0	0	20	0	0

We did not know this was a crime	0	13	0	0	11	25	0	0	0	0	0	0	20	0	100
We did not want the incident/s to be known outside of the company due to potential reputational damage	0	13	0	17	11	25	11	0	0	0	0	0	20	14	0
Because of possible interruption of business processes (e.g. servers are taken for forensic analysis, etc.)	0	0	25	0	0	25	0	0	0	0	0	0	20	0	0
We didn't know we had an incident until much later	0	0	0	0	11	13	0	0	0	0	0	0	0	14	0
Our losses from the incident were insignificant	44	25	0	0	33	0	22	0	25	0	0	0	40	43	0

(%) Base: companies that have experienced at least one type of cybercrime in the last 12 months, but did not report the incident to the police or other national authorities – Ransomware (NL, n=1; ES, n=1; BG, n=2); Malware (NL, n=13; ES, n=9; BG, n=18); Phishing attacks (NL, n=28; ES, n=26; BG, n=20); Attempt to access without authorisation your company's online/bank account (NL, n=8; ES, n=4; BG, n=2); Denial-of-service attacks (NL, n=9; ES, n=8; BG, n=4); Business identity theft / Impersonation (NL, n=6; ES, n=9; BG, n=8); Unauthorised accessing of files or networks by staff, even if accidental (NL, n=9; ES, n=2; BG, n=4); Unauthorised accessing of files or networks by people outside your company (NL, n=2; ES, n=0; BG, n=1); Unauthorised listening into video conferences or instant messaging (NL, n=5; ES, n=7; BG, n=1); Takeovers or attempts to take over your website, social media accounts or email accounts (NL, n=21; ES, n=11; BG, n=8).

Table 19. What would make you more likely to report such incidents in the future? (multiple answers)

	NL	ES	BG
Enhanced online platforms	37	60	47
User friendly platforms	36	65	39
Better trained police offices	36	54	25
More information about channels for reporting	50	66	50
My legal rights and obligations	49	52	6
Enhanced online platforms	37	60	47

(%) Base: companies providing reasons making them more likely to report in the future
(NL, n=335; ES, n=391; BG, n=36).

Table 20. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your company? (multiple answers)

	NL	ES	BG
A cyber security vulnerability audit	49	47	12
A risk assessment covering cyber security risks / Investment in threat intelligence	46	44	34
Used specific tools designed for security monitoring	55	61	27
Testing staff awareness and response	47	39	9
None of these	18	16	51
Don't know	2	3	1

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 21. Have you outsourced any of your IT support services to an external company or companies:

	NL	ES	BG
IT is completely outsourced to an external company	7	7	31
IT is partially outsourced to an external company and it is responsible for our cybersecurity	11	9	8
IT is partially outsourced to an external company, but we are responsible for our cybersecurity	11	14	11
IT is partially outsourced to an external company and both we and the external company are responsible for our cybersecurity	29	17	7
IT is not outsourced or minor aspects of it are outsourced	40	51	43
Don't know	2	3	1

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 22. Which of the following rules or controls, if any, do you have in place? (multiple answers)

	NL	ES	BG
A policy to apply software security updates within 14 days	57	52	16
Up-to-date malware protection	83	79	74
Firewalls that cover your entire IT network, as well as individual devices	80	79	11
Restricting IT admin and access rights to specific users	80	74	19
Any monitoring of user activity	56	48	15
Specific rules for storing and moving personal data files securely	70	64	39
Security controls on company-owned devices (e.g. Laptops)	71	71	47
Only allowing access via company-owned devices	50	57	32
Separate WiFi networks for staff and for visitors	74	59	7
Backing up data securely via a cloud service	70	68	22

Backing up data securely via other means	60	69	38
A password policy that ensures users set strong passwords	74	70	36
A two or three-step login verification for your employees or/and clients	72	48	9
A virtual private network, or VPN, for staff connecting remotely	58	64	4
Encryption techniques for data, documents, or emails	59	53	16
An agreed process for staff to follow when they identify a fraudulent email or malicious website	47	59	30
Regular cyber security trainings or awareness raising sessions specifically for staff members who are not directly involved in cyber security	37	43	14
None of these	1	0	4
Do not know	3	2	0

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 23. Which of the following best describes the way your company has been working in the past 12 months?

	NL	ES	BG	Total
Everyone works at the company premises	17	30	80	41
Everyone works in a co-working space	2	1	7	3
A Hybrid work setup: some employees come to the office, some work from home	68	53	10	45
Most employees work from home on their company computers	7	9	1	6
Most employees work from home on their personal computers	3	5	2	4
Don't know	2	2	1	1

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

Table 24. 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?

	NL	ES	BG	Total
We have a specific cyber security insurance policy	14	17	3	11
We have cyber security cover as part of a broader insurance policy	26	26	10	21
We are not insured against cyber security breaches or attacks	40	40	83	53
Don't know	19	18	5	14

(%) Base: all companies (NL, n=435; ES, n=444; BG, n=400).

ANNEX II – 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
9. 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 Victimization

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
- 9 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
- 9 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
- 77 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_1 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. I T 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
- 88 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)

