CYBBAR

CSD CENTER FOR THE STUDY OF DEMOCRACY

Cybercrime against businesses in the EU:
Challenges to Reporting

Policy Brief

Over the last decades, digital technologies have permeated the daily lives of EU citizens and businesses. Digital innovation has fostered socio-economic development across EU Member States but has also resulted in increased exposure of our societies to cyber threats and cyber-attacks. Cybersecurity has emerged as a fundamental asset to a digital and interconnected Europe, whose prosperity and technological progress have become increasingly dependent on cyber resilience.

New challenges have emerged since the outbreak of the COVID-19 pandemic which has accelerated digitalisation not only in Europe but around the globe. On top of this, the ongoing conflict in Ukraine has further accentuated the potential exposure of individuals, businesses, and public institutions to cybercrime. Lockdowns and teleworking have, and continue to constitute, an opportunity for cybercriminals.[1] Between 2021 and 2022, the most prevalent cyber threats have been identified as ransomware, malware, social engineering threats, threats against data and data availability (as DDoS attacks),[2] as well as data compromise – including high-profile attacks against non-profit and humanitarian institutions.[3] The conflict between Russia and Ukraine has further raised cybersecurity concerns in the EU. Cyberwarfare has been an integral part of the Russian invasion, with alleged attacks on computer networks and information systems of public and private institutions.[4] The frequent interlink between cyber- and traditional (offline) offences has heightened the criminal threat, as criminals are increasingly using the internet to scale up their

Key Points

- The two most common types of cybercrimes against SMEs in the EU27 are **viruses, spyware or malware** (excluding ransomware), followed by **phishing, account takeover or impersonation attacks.**
- In 2021, **44% of cybercrimes** experienced by SMEs in the EU27 were **not reported to anyone.**
- The main **factors for underreporting** include **the fact that the incident was dealt with internally**, the incident was not worth reporting (too trivial), and the **lack of trust in the police** and its digital competence. Other relevant factors are the **lack of a single reporting mechanism**, conflicts of interest with **business continuity**, and gaps in cybersecurity awareness.
- **Public-private cooperation** is essential. Can be fostered through the **harmonisation** and centralisation of **reporting mechanisms** and **trust-building** public-private partnerships.

[1] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.

[2] ENISA. (2022). ENISA Threat Landscape 2022.

[3] ICRC. (2022, January 19). Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people.

[4] CSIS. (2022, June 16). https://www.csis.org/analysis/cyber-war-and-ukraine.

This publication is funded by the European Union’s Internal Security Fund – Police.
The content of the publication represents the views of the athors only and is their sole responsibility.
The European Commission does not accept any responsibility for use that may be made of the information it contains.

operations to find new methods and tools for criminal behaviour.

Despite the increasing threat posed by cyber-attacks and cybersecurity threat actors, to date still little information is available on the real extent and impact of cybercrime in the EU – particularly with regard to businesses and private entities. The lack of knowledge is mostly due to underreporting, that is, a very small proportion of cyber offences come to the attention of the criminal justice system. Under-reporting is among the key obstacles to having an accurate picture of cybercrime against businesses, contributes to the lack of effective public-private cooperation, and ultimately leads to limited criminal justice outcomes.

Factors for Underreporting of Cybercrime

Underreporting remains one of the main challenges to understanding the real extent of cybercrime. Limited reporting impacts the recording of cyber offences and, therefore, the availability of accurate cybercrime data. A recent investigation of cybercrime against small and medium-sized enterprises (SMEs) in EU Member States confirms that reporting to the police remains low, with 44% of cybercrimes experienced by SMEs not reported to anyone.[5]

Several factors have been argued to play a role in underreporting among businesses. One of the most recurring factors is related to the perception that the incident was too trivial and/or not worth reporting, or that the incident was dealt with internally. Other factors include fear of reputational damage and lack of trust in the police. Regarding the former, businesses are concerned that cyber incidents become public when authorities begin the investigation, with potential negative effects on the trust of customers and investors. As for the latter factor, businesses' often lack of trust in digital competence of police authorities and therefore do not report the cyber incident.

Another important factor, especially for small companies or those not often interacting with the police is the lack of a single reporting mechanism. According to an Interpol cybercrime expert, it would be beneficial to have a centralised cyber office involved in specialised cyber reports. This would reduce the large number of reporting channels and obligations existing in many countries, which are perceived as decreasing the efficiency of the reporting mechanism.

Cybercrime reporting can also be hindered by a conflict of interest with business continuity, relating to differences between the priorities of businesses and law enforcement authorities after a cyber-attack. From the perspective of businesses, the priority after a cyber incident is to keep the business running. This implies recovering from the attack, which includes regaining access to (encrypted) data as well as avoiding extensive loss of time and financial damage. For instance, in 2021 lost business was the largest portion of the costs following a data breach for businesses worldwide.[6] Notifying private security companies, solving technical issues, and recovering assets are therefore often given a higher priority than preserving criminal evidence.

Lastly, gaps in cybersecurity awareness and reporting obligations to upper-level management and competent authorities can result in underreporting to the police. Some businesses, particularly SMEs, are often not aware of having been victimised, as they lack trained staff or resources to detect incidents and even if an incident is detected, companies may not report the attack because they underestimate its severity.[7]

Factors for underreporting as a challenge on EU level

The cybercrime and overall business environment in the different Member States seem to have limited impact on reasons for underreporting. A closer look into three different EU countries, namely Bulgaria, the Netherlands, and Spain, provides a good example. The three countries have very different business landscape in terms of share of large and SME companies and digital literacy. While the Netherlands is a home to a relatively high number of large enterprises, Spain and Bulgaria have a business population

[5] *Ibid.*

[6] IBM Seurity. (2021). Cost of a Data Breach Report.

[7] Williamson, J. (2016, February 10). Cyber-attack impact severely underestimated by SMEs. The Manufacturer.

consisting of a high number of SMEs.[8] In addition, the three target countries have different levels of business digitisation and transformation maturity, including policy instruments for digital privacy and security. However the three countries face similar challenges in terms of factors for underreporting by companies. For instance, approximately one in ten companies in each Member State reported lack of awareness that the police dealt with cybercrime incidents as a common reason for not reporting such type of offences.[9]

Bulgaria

The information on cybersecurity incidents and cybercrimes in the country is gathered by the national Computer Emergency Response Team (CERT) and Bulgaria's General Directorate for Combatting Organised Crime (GDBOP). CERT Bulgaria reported that approximately 2,100 cyber incidents were recorded in 2020, most of which consisted of phishing and malware attacks. Moreover, as reported by the Bulgarian Cybersecurity Association, in 2021 there was a 70% increase in cyber-attacks against SMEs in Bulgaria compared to the previous year. As for GDBOP, expert interviews pointed out that the unit receives about ten signals for cybercrimes or cybercrime attempts daily on its phone number. The most prevalent types of cybercrimes against businesses reported to GDBOP are Business Email Compromise (BEC), phishing attacks, ransomware, DDoS attacks (mostly for governmental sites), and cyberattacks by former employees. In particular, BECs often affect companies operating in the field of foreign trade.

As for factors for underreporting, the most prevalent ones include a lack of knowledge of cybersecurity regulations requiring the reporting of cyber-attacks (Cyber Security Act), low trust in law enforcement authorities, and lack of cybersecurity awareness - also relating to the role that businesses can play in preventing and reporting cybercrime. Bulgarian businesses are often unprepared for cyber-attacks due to a lack of expertise in cybersecurity, investments in IT, training of employees and cyber protection measures. Fear of reputational damage, especially for large companies, is another key factor.[10]

The Netherlands

The Dutch Central Bureau of Statistics (CBS) indicates that the number of cybercrime incidents in the country decreased over the period 2016-2020. In 2016, almost 40% of Dutch companies experienced some type of cybersecurity incident; in 2019 such figure accounted for less than 20% for large companies.[11] In addition, incidents related to DDoS attacks accounted for 1,610 in 2020, a 75% increase compared to 2019.

According to the recent study by the European Commission, Dutch SMEs surveyed mostly reported having experienced – in the past 12 months – phishing, account takeover or impersonation attacks (21% of SMEs), followed by viruses, spyware or malware (excluding ransomware) (17%), and unauthorized accessing of files or networks (6%). The most serious incident was carried out through scams and fraud (34%) and malicious software (21%).[12] Such findings are in line with previous studies, pointing out malware, e-fraud, phishing, and hacking as the most prevalent forms of cybercrime against SMEs in the Netherlands.[13]

As for cybercrime reporting, roughly 5-10% of Dutch companies falling victim to an external cyber-attack actually report it.[14] In this regard, there are different factors for not reporting cybercrime. The most frequent reasons for underreporting are related to the fact that the company dealt with the incident internally, the feeling that the police could not do anything about it – hence, limited trust in the police and its cyber competence – and the fact that the cyber incident or attack was not that important and/or not worth reporting.[15]

[8] Eurostat. (n.d.). Structural business statistics overview.

[9] European Commission. (2022). *Op. cit.*

[10] Interviews with experts from law enforcement, CERT centre, cybersecurity associations, and academia.

[11] CBS. (2021). Cybersecuritymonitor 2020. Central Bureau of Statistics.

[12] European Commission. (2022). Op. cit.

[13] Veenstra et al. (2015). Cybercrime among companies. Lectoraat Cybersafety: Leeuwarden

[14] CBS. (2021). Op. cit.; see also Veenstra et al. (2015). Op. cit.

[15] European Commission. (2022). Op. cit.; van de Weijer, S. et al (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized

Spain

In Spain, information on cybercrime and cybersecurity attacks is mainly available through statistics reported by the Spanish National Cybersecurity Institute (INCIBE) to the Ministry of Interior. The latest figures on private entities indicate that INCIBE-CERT managed a total of 109,126 cybersecurity incidents in Spain in 2021. The two most common forms of cybercrime were malware (29.88%) and fraud (28.60%), followed by attacks on vulnerable systems (18.9%) and intrusion (6.5%).[16] Regarding underreporting of cybercrime in Spain, two main reasons have been recently outlined: the fact that the SMEs dealt with the incident internally (57% of respondents), followed by the incident being considered too trivial and/or not worth reporting (33%).[17]

What's Next

Cyber security awareness is among the key aspects that private entities (and individuals) must acquire, with the active support of public authorities, including law enforcement agencies. Such advancements are not only needed to **increase digital literacy** but also to **enhance the businesses' knowledge** of the relevant and competent authorities in case of cyber incidents. Effective cybercrime reporting and operational cooperation strategies should:

- Address common factors for not reporting, among all lack of trust in the police, **the complexity of reporting mechanisms**, as well as business continuity, which is often given a higher priority than preserving criminal evidence.
- Turn to existing initiatives to build synergies and further implement best practices. Current initiatives and forms of collaboration include the No More Ransom Portal, launched in 2016 by Europol and other partners to support victims in the decryption of their devices or electronic files. Such a platform and its set of decryption tools are aiming at **disrupting potential business-like relationships** between affected businesses and the attackers, that is, cybercriminals offering victims discounts for using specific decryption services.
- Promote cybercrime reporting as fundamental in the fight against offences occurring in cyberspace, to **shed light on the real extent of cybercrime** and ultimately limit its (economic) impact on private entities.

Cybercrime reporting would also be favoured by the introduction of **single centralised reporting process**. The first step to introduction of a single reporting mechansim could be the harmonisation of existing reporting mechanisms and well-established **public-private partnerships** (PPPs) to facilitate information-sharing. In addition, such mechanism would benefit from trust-building processes developed via PPPs, secure and centralised communication channels as well as standardised protocols and data formats. Trust between businesses and law enforcement authorities is critical to promote existing and new partnerships and trusted information-sharing mechanisms (including secured platforms) that can ultimately enhance mutual collaboration among different actors in the fight against cybercrime.

Enterprises in the Netherlands. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing (pp. 303–325). Springer.*

[16] López Gutiérrez et al. (2022). *Informe sobre la cibercriminalidad en España 2021*. Ministry of Interior: Government of Spain.

[17] European Commission. (2022). *Op. cit.*