Survey on the Experience of SMEs with Cybercrime

Anna Pingen

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 12 May 2022, a Eurobarometer survey about the impact of cybercrime on small and medium sized enterprises (SMEs) was published. Between 26 November and 17 December 2021, nearly 13,000 interviews with SME representatives in all 27 EU countries were conducted by Ipsos European Public Affairs. The survey covered four main topics:

- The extent to which SMEs' staff members are aware of cybercrime risks and the level of training and awareness raising of staff regarding cybersecurity risks: Here, the survey established that about seven in ten respondents (with a leading role in their SME) feel well informed about the risks of cybercrime. About one in five SMEs (19%) has provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months.
- The level of concern about cybercrime among SMEs: The survey showed that the most prevalent type of cybercrime experienced during the last 12 month are viruses, spyware or malware (experienced by 14% of SMEs in the last 12 months), followed by phishing, account takeover or impersonation attacks (11%).
- The SMEs' experiences with cybercrime over the last 12 months: More than half (58%) of SMEs, which have experienced at least one type of cybercrime, also suffered from some kind of impact on their business – the most prevalent impact mentioned is "additional time required to respond to the cybercrime incidents" (35%), followed by repair or recovery costs (24%).
- SMEs' preferred channels for reporting cybercrime, both in general and for actually experienced incidents, and SMEs' reasons for not reporting cybercrime incidents to the police: In this context, the survey observed that SMEs are most likely not to have reported these incidents because 44% of cybercrimes experienced were not reported to anyone. If cybercrime incidents were reported, they were most often reported to the police (18% of all incidents) or to the seller or service provider (17%). More than the half of SMEs (52%) responded that they did not report the incident to the police because they dealt with it internally, while 44% felt the incident was too trivial / not worth reporting to the police.

The survey is an important yardstick for future cybercrime challenges in view of the EU's planned digital transformation. The COVID-19 crisis led to an increased digital transformation for small and medium sized enterprises and at the same to a higher exposure to activities by cybercriminals.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union