European
Commission

Digital Economy and Society Index (DESI) 2020

Cybersecurity

Table of Contents

Table of Figures

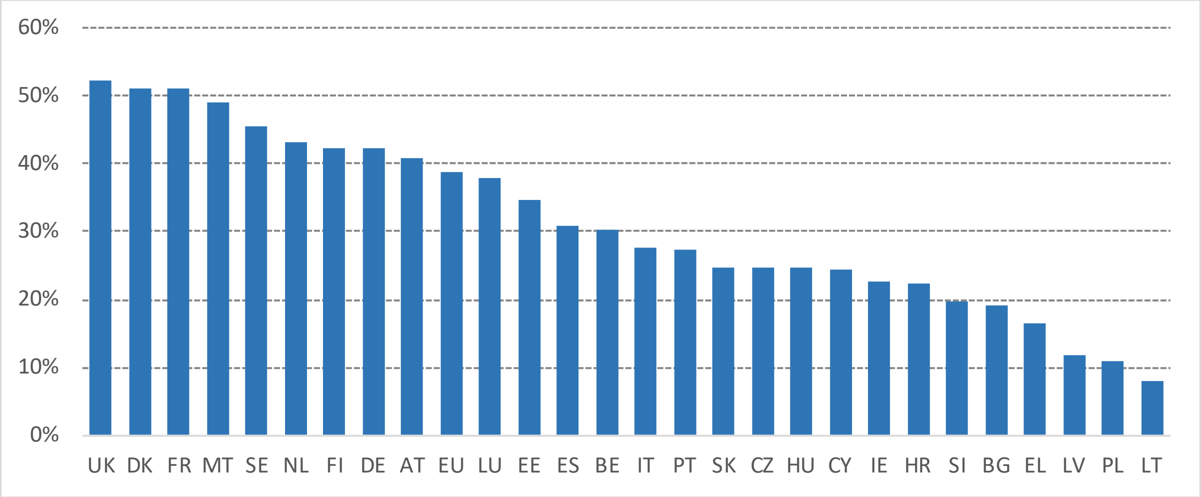
Cybersecurity

1. Internet security: incidents and concerns among EU citizens

Following the outbreak of the COVID-19 pandemic and the extensive use of digital tools, ensuring internet security and preventing cybercrime, data misuse or fraud are of paramount importance.

In 2029, 39% of EU citizens who used the internet in the last year[1] experienced security-related problems. This percentage varies greatly across Member States: from more than 50% in the UK to less than 10% in Lithuania.

Figure 1: Individuals who experienced a security-related problem (% of internet users) 2019

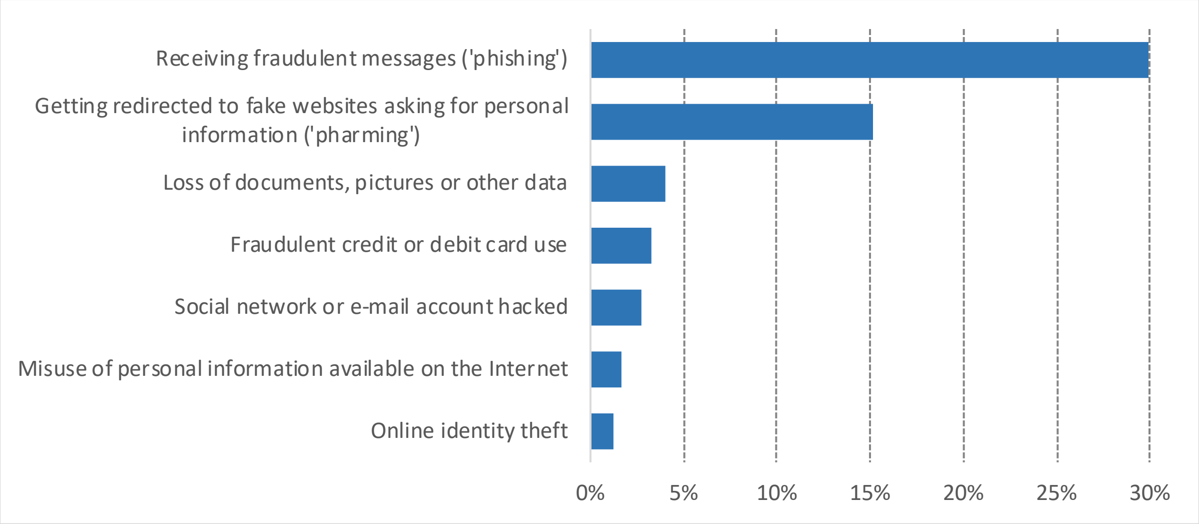


Data not available for Romania
Source: Eurostat, Community survey on ICT usage in Households and by Individuals.

Phishing and pharming are the most common security-related problems experienced. The receipt of fraudulent messages (known as 'phishing') was reported by 30% of EU internet users in 2019. Redirection to fake websites asking for personal information ('pharming') was experienced by 15% of EU internet users. Other problems are less common. For example, 3.6% of internet users lost documents, pictures or other data due to a virus or other computer infection. 1.7% of internet users experienced misuse of their personal online information resulting in issues such as discrimination, harassment, bullying, and 1.3% experienced online identity theft. Only 1.5% of internet users experienced financial losses resulting from identity theft, receiving fraudulent messages, or being redirected to fake websites.

[1] Hereafter referred as 'internet users'.

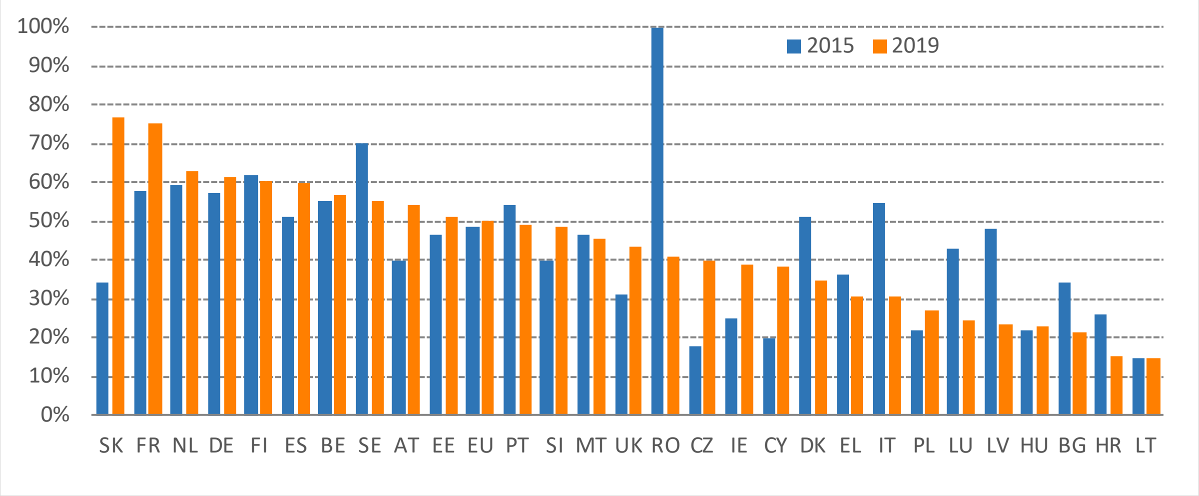
Figure 2: Type of security-related problems experienced (% of internet users) 2019



Source: Eurostat, Community survey on ICT usage in Households and by Individuals.

Security concerns remain high among internet users, and have slightly increased over the last 5 years. In 2019, security concerns limited or prevented 50% of EU internet users from performing online activities, an increase from 48% in 2015. However, there are large differences among Member States. In 2019, internet users reporting security concerns ranged from 77% in Slovakia and 75% in France, to 15% in both Croatia and Lithuania. Moreover, the comparison between 2015 and 2019 shows a scattered picture. Although the overall percentage of internet users expressing security concerns slightly increased in the EU over this period, 12 Member States recorded a decline.

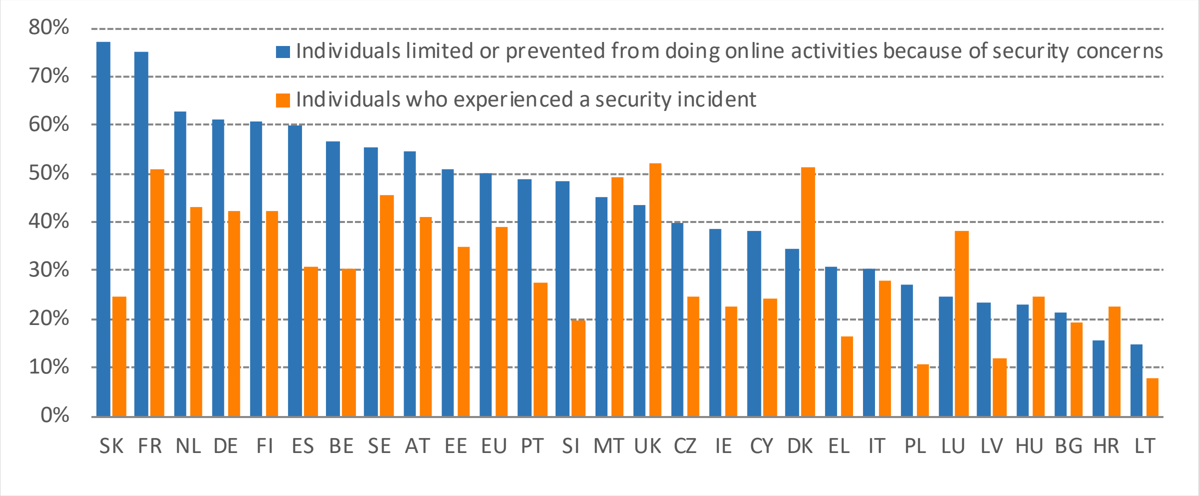
Figure 3: Individuals who were limited or prevented from performing selected online activities because of security concerns (% of internet users) 2015 and 2019



Source: Eurostat, Community survey on ICT usage in Households and by Individuals.

The incidence of security concerns among internet users does not necessarily correspond to the actual number of people experiencing security issues. In the EU as a whole and in most of the Member States, the percentage of internet users who expressed security concerns exceeded the percentage of users who actually experienced a security incident while online.

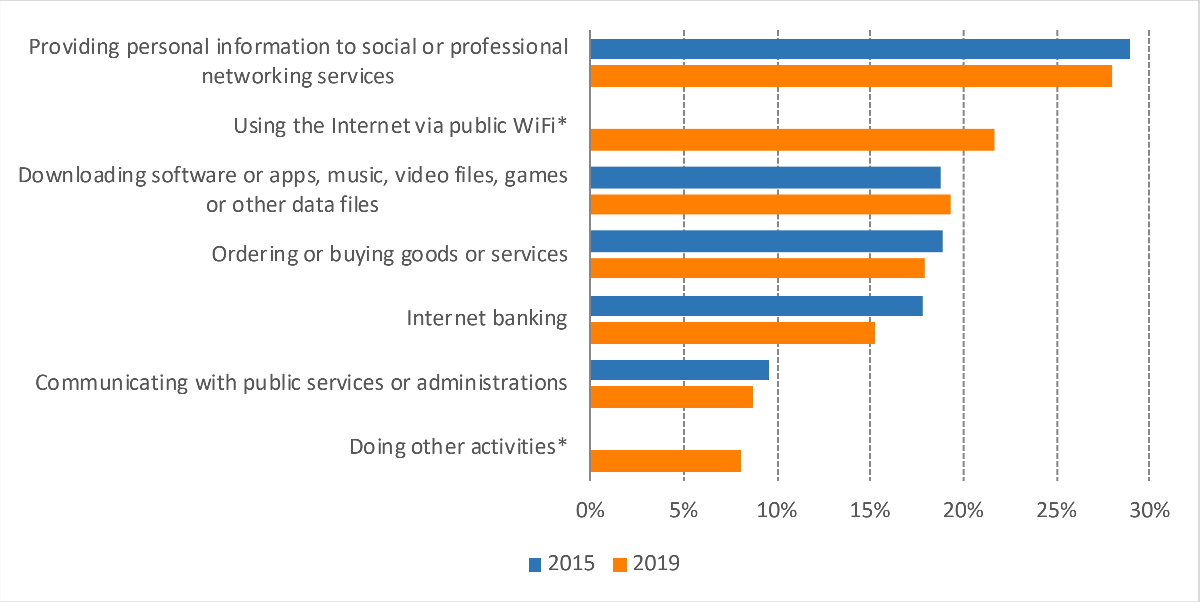
Figure 4: Security incidents and security concerns (% of internet users) 2019



Data not available for Romania
Source: Eurostat, Community survey on ICT usage in Households and by Individuals.

There is a general reluctance to provide personal information to social or professional networks: 28% of internet users expressed this concern, slightly less than in 2015. Moreover, 22% of internet users are reluctant to use public WiFi, and 17.9% to engage in ordering or buying goods or services online. Security concerns also limited or prevented 15.2% of internet users from using online banking.

Figure 5: Online activities limited or prevented because of security concerns (% of internet users) 2015 and 2019



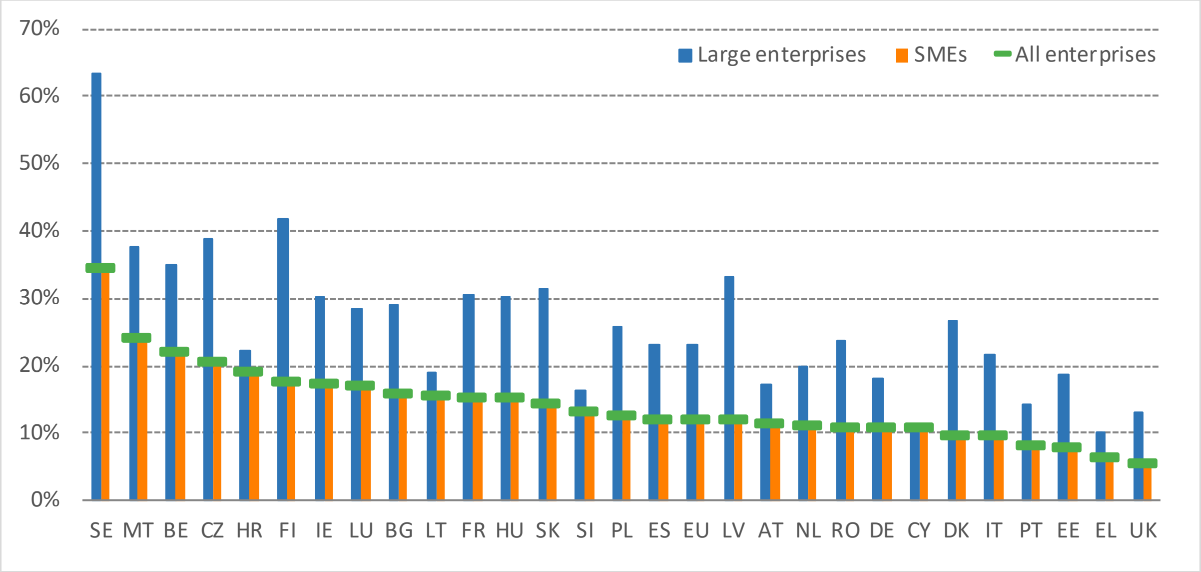
** Data not available for 2015*
Source: Eurostat, Community survey on ICT usage in Households and by Individuals.

2. ICT security: Incidents and measures taken by EU enterprises

In 2018, 12.3% of all EU enterprises experienced problems due to ICT security incidents at least once. This percentage was higher among large companies. ICT security incidents were reported by 23% of large enterprises, against 12% of SMEs. Their use of more complex digital systems and services – but also their greater capacity to register and report attacks and failures – might explain the higher rate of incidents among large enterprises.

Country-level analysis shows a mixed picture, with no clear link between the level of business digitisation in the country and the incidence of ICT security issues among enterprises. For example, although Sweden and the UK have similar levels of business digitisation, 35% of Swedish enterprises reported ICT security incidents, against only 5.7% of British enterprises.

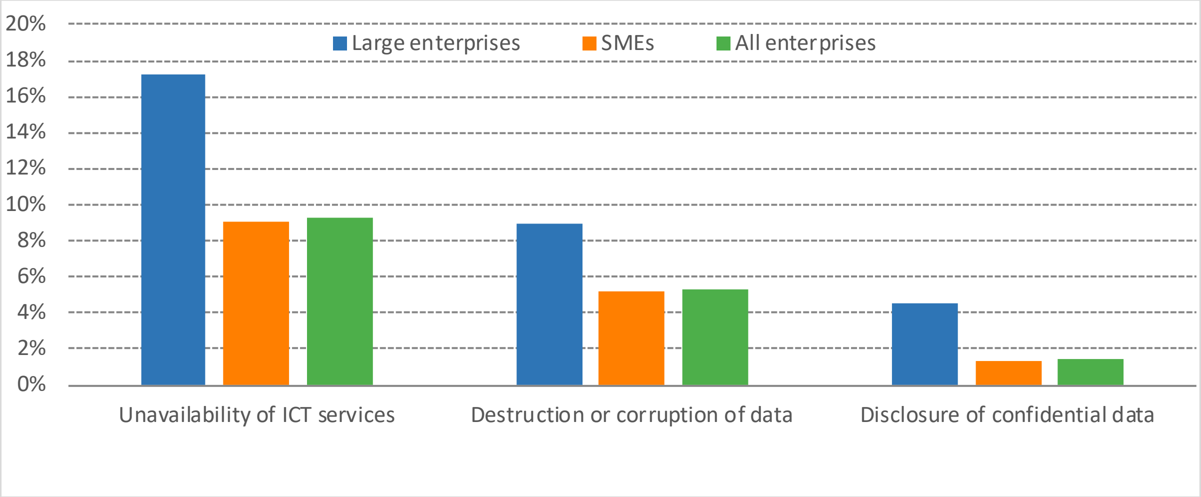
Figure 6: Enterprises that experienced at least once problems due to an ICT related security incident (unavailability of ICT services, destruction or corruption of data, disclosure of confidential data) (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

The most frequently reported problem was the unavailability of ICT services (reported by 9.3% of all enterprises in the EU), followed by the destruction or corruption of data (reported by 5.3%) and the disclosure of confidential data (reported by 1.4%).

Figure 7: Problems experienced due to ICT security incidents (% of enterprises) 2019

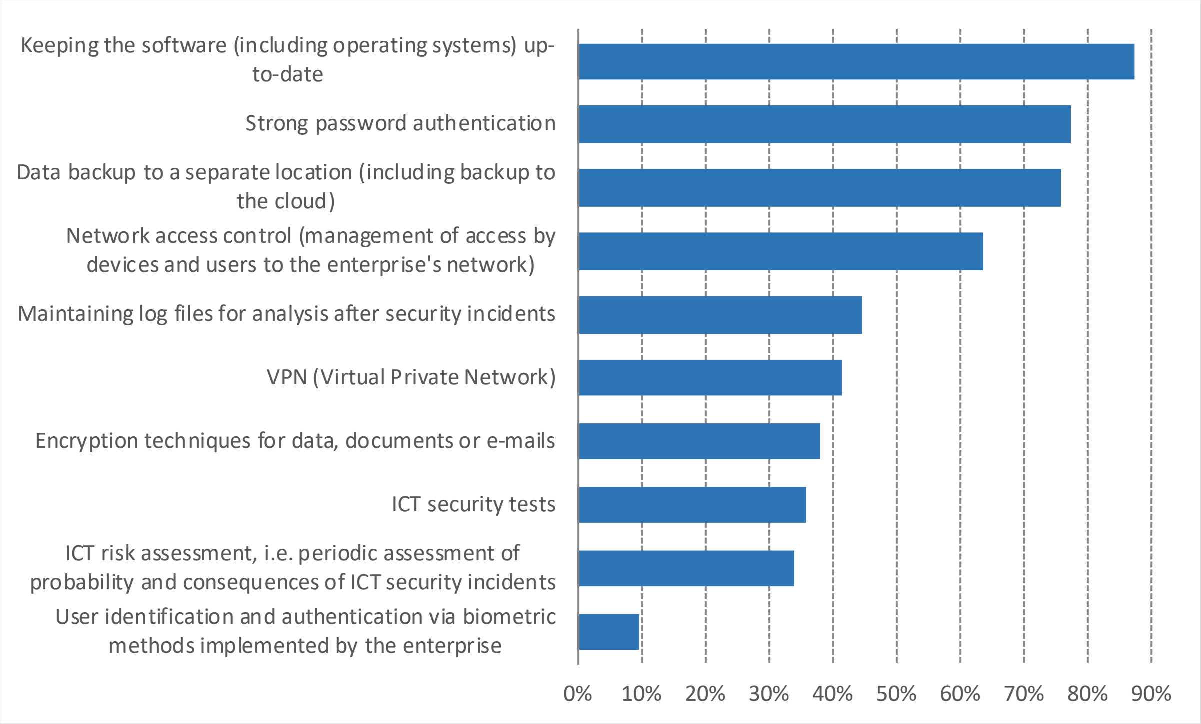


Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

One in three EU enterprises (34%) have ICT security documents setting out measures, practices or procedures. However, 93% of EU enterprises have adopted at least one ICT security measure. The adoption of ICT security measures is widespread among both large enterprises and SMEs: 99% of large enterprises and 92% of SMEs deploy some ICT security measures.

The types of security measures taken vary. Most EU enterprises have put in place basic measures such as keeping software up-to-date (87%); requiring strong password authentication (77%); and backing up data in a separate location including backing data up to the cloud (76%). A smaller percentage of enterprises use more sophisticated measures such as ICT risk assessments (34%) or ICT security tests (36%), and only a few enterprises use biometric methods for user identification and authentication (9.5%).

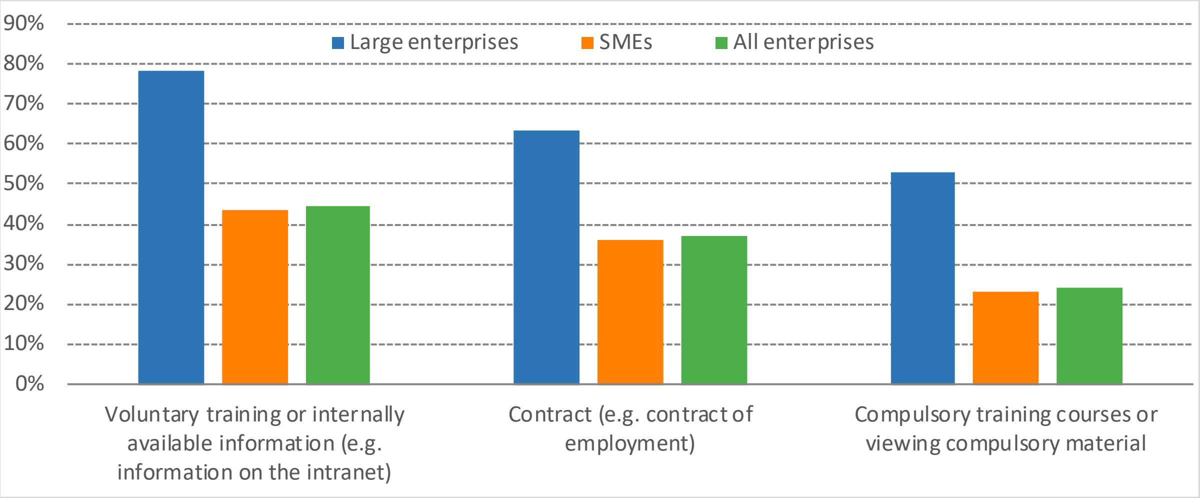
Figure 8: Type of ICT security measures adopted by EU enterprises (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

Most EU enterprises make their employees aware of ICT security obligations, but only 24.2% of enterprises plan compulsory training on this subject. 62% of EU enterprises make employees aware of their obligations in ICT security, mainly through voluntary training or internally available information (44% of enterprises do this) and by contract (37%).

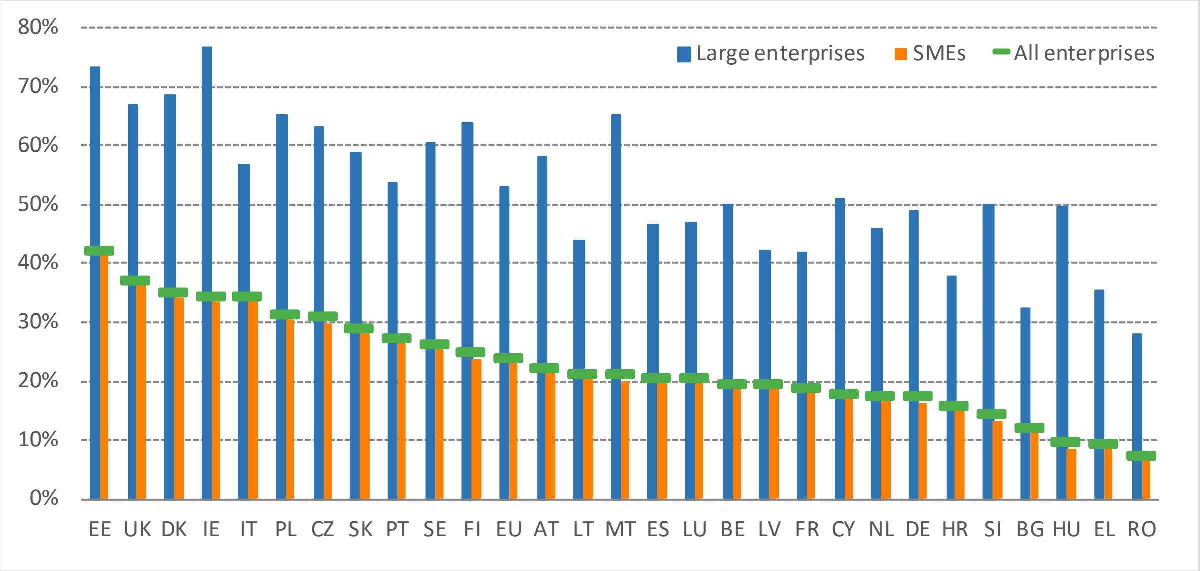
Figure 9: Enterprises that make persons employed aware of their obligations in ICT security issues (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

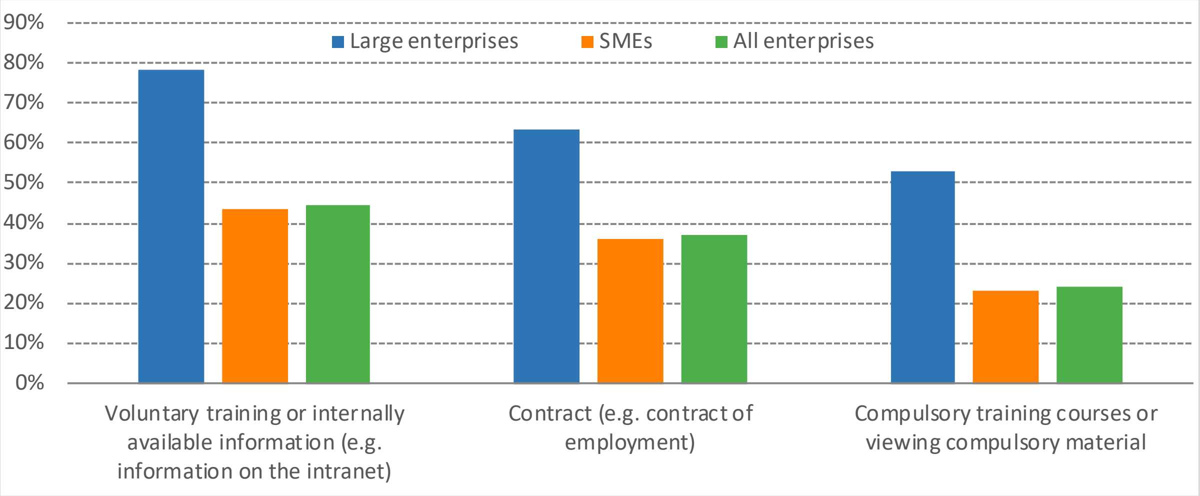
On compulsory training courses, there are significant disparities across Member States. More than 35% of enterprises provide compulsory training in Estonia, the UK and Denmark, while less than 10% of enterprises do so in Romania, Greece and Hungary.

Figure 10: Enterprises make persons employed aware of their obligations in ICT security issues by compulsory training courses or compulsory material (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

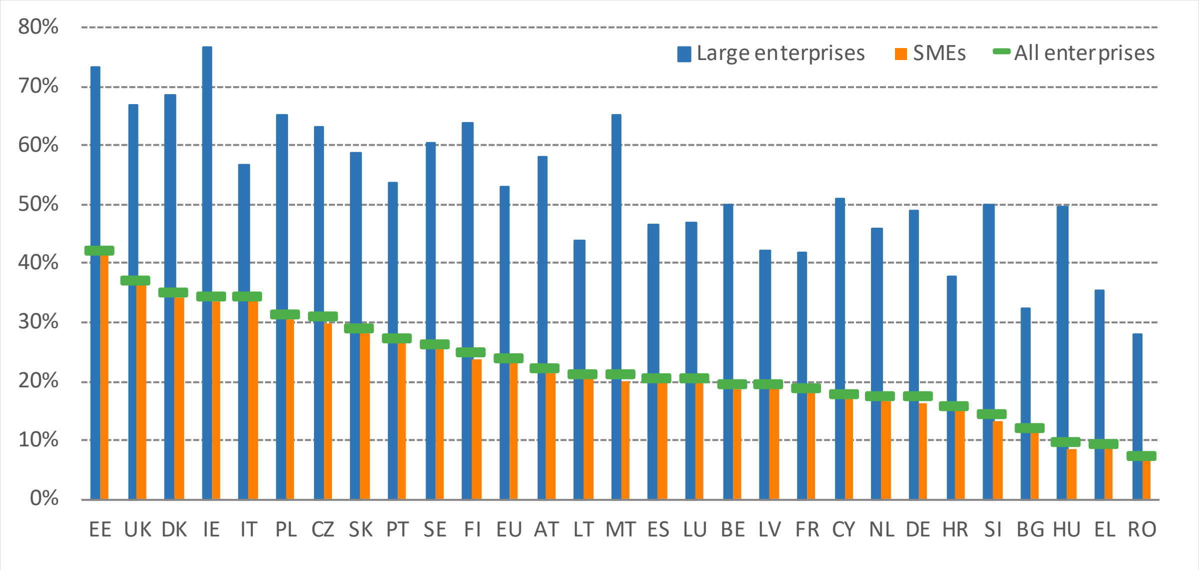
Figure 11: Enterprises that make persons employed aware of their obligations in ICT security issues (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

Regarding compulsory training courses, there are significant disparities across Member States. The percentage of enterprises providing compulsory training is above 35% in Estonia, the UK and Denmark, while it is below 10% in Romania, Greece and Hungary.

Figure 12: Enterprises make persons employed aware of their obligations in ICT security issues by compulsory training courses or compulsory material (% of enterprises) 2019



Source: Eurostat, Survey on ICT usage and e-commerce in enterprises.

ANNEX I Abbreviations

Abbreviation	Explanation
4G / 5G	Fourth/Fifth generation technology standard for cellular networks
AI	Artificial Intelligence
BCO	Broadband competence office
BERD	Business expenditure on R&D
CAGR	Compound annual growth rate
CEF	Connecting Europe Facility
CRM	Customer Relationship Management
CSA	Coordination and Support Actions
DIH	Digital Innovation Hubs
DII	Digital Intensity Index
DOCSIS	Data over cable service interface specification
DSL	Digital subscriber line
DTT	Digital terrestrial television
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
eForm	Electronic Form
EFSI	European Fund for Strategic Investments
eID	Electronic Identification
eider’s	Electronic Identification, Authentication and Trust Services
EIF	European Investment Fund
ERA-NET	European Research Area
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
Euro HPC JU	Euro High Performance Computing Joint Undertaking
FET	Future & Emerging Technologies
FTTB	Fibre-to-the-building
FTTH	Fibre-to-the-home
FTTP	Fibre-to-the-premises
FWA	Fixed wireless access
GBARD	Government Budget Allocations for R&D
GDP	Gross Domestic Product
GHz	Gigahertz
HES	Secondary and Higher Education Establishments
HPC	High Performance Computing
IA	Innovation Action
IaaS	Infrastructure as a service
ICOs	Initial Coin Offerings
ICT	Information and communication technology
IMSI	International mobile subscriber identity
IoT	Internet of Things
JRC	Joint Research Centre
LEIT	Leadership in Enabling and Industrial Technologies
LTE	Long-term evolution
Mbps	Megabits per second
MHz	Megahertz
MNO	Mobile network operator
MVNO	Mobile virtual network operator

NACE	Statistical Classification of Economic Activities in the European Community
NBP	National broadband plan
NGA	Next generation access
NRA	National regulatory authority
OTT	Over-the-top
PaaS	Platform as a Service
PCP	Pre-Commercial Procurement
PERD	R&D personnel
PPI	Public Procurement for Innovation
PPS	Purchasing Power Standards
PRC	Private for-Profit Companies
PSAP	Public safety answering point
QCI	Quantum Communication Infrastructure
R&D	Research and Development
R&I	Research and Innovation
REC	Research Organisations
SaaS	Software as a Service
SMEs	Small and Medium Enterprises
USO	Universal service obligation
VDSL	Very-high-bit-rate digital subscriber line
VHCN	Very high capacity network