Industry, trade and services

eurostat
Statistics in focus
7/2011

Konstantinos GIANNAKOURIS, Maria SMIHILY

ICT security in enterprises, 2010

The 2010 Community survey questionnaire on 'ICT usage and eCommerce in enterprises' comprised a set of questions specific to Information and Communications Technologies (ICT) security. In this context, ICT security refers to relevant incidents as well as measures, controls and procedures applied by enterprises in order to ensure integrity, confidentiality and availability of data and ICT systems.

Highlights

In January 2010, 27 % of enterprises in the EU27 had a formally defined **ICT security policy with a plan for regular review**; the corresponding shares in Sweden, Norway and Denmark were over 40 %.

The highest percentage of enterprises with a formally defined ICT security policy **addressing the risks** of destruction or corruption of data due to an attack or some other unexpected incident was reported in Norway (42 %).

Voluntary training or use of generally available information was the approach most commonly reported by enterprises for **making their staff aware** of their obligations in relation to ICT security. The highest proportions of enterprises which have adopted this approach were registered in Cyprus and Finland with 77 % and 74 % respectively.

In the majority of EU27 Member States, **the disclosure of confidential data due to intrusion, pharming or phishing attacks** was reported by 1 % or less of enterprises in 2009.

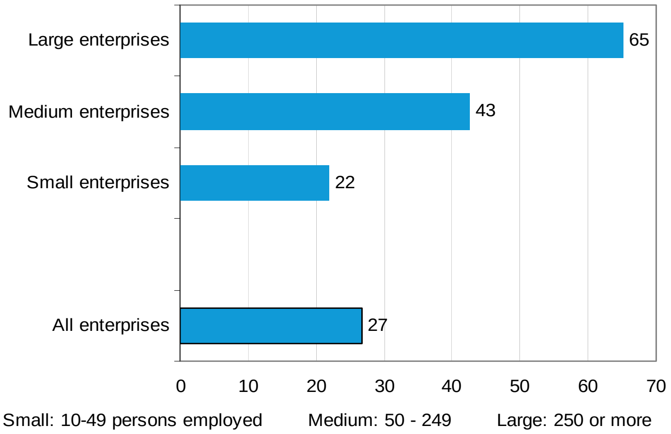
In January 2010, **the use of strong password authentication** was the most commonly reported procedure used by enterprises for internal ICT security, with the highest share registered in Italy (64 %).

The share of large enterprises that had a formally defined ICT security policy was three times more than the share of small ones.

The existence of an ICT security policy in an enterprise means that the enterprise is aware of the importance of its ICT and the related risks. The survey focus was on policies which were actually applied, hence regularly reviewed and accordingly adapted. In January 2010, almost three out of ten enterprises in the EU27 had a formally defined ICT security policy with a plan for regular review.

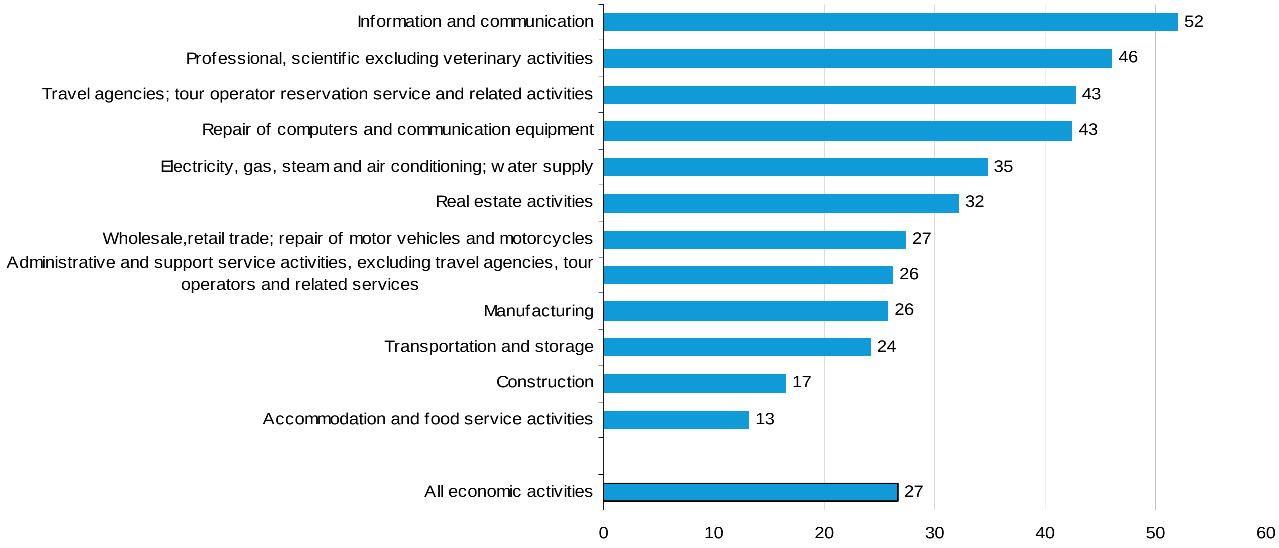
Figure 1 shows that the share of large enterprises that had a formally defined ICT security policy was three times more than the share of small ones. The highest proportion of enterprises having such a policy (52 %) in the EU27 was reported within the sector Information and communication activities (Figure 2). The lowest proportions — less than one out of four enterprises — were registered in the sectors Transportation and storage, Construction and Accommodation and Food service activities.

Figure 1: Enterprises having a formally defined ICT security policy, by size class, EU27, January 2010 (% of enterprises)



Source: Eurostat (online data code : isoc_cisce_ra)

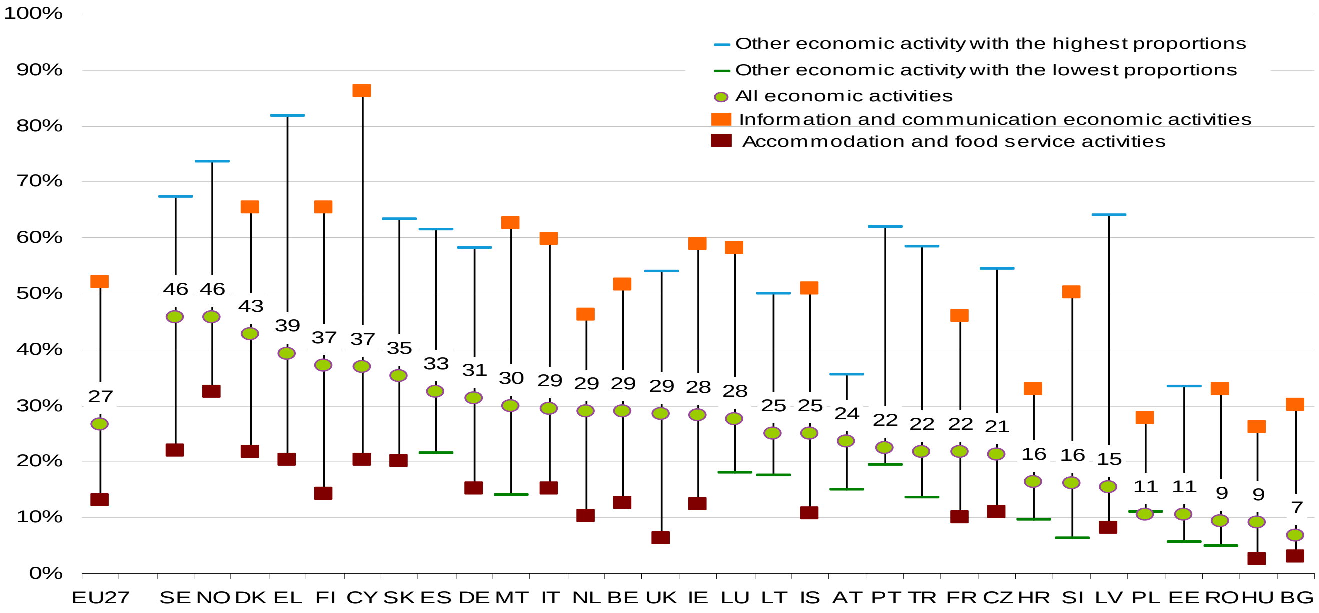
Figure 2: Enterprises having a formally defined ICT security policy with a plan for regular review, by economic activity, EU27, January 2010 (% of enterprises)



Source: Eurostat (online data code : isoc_cisce_ra)

As Figure 3 shows, in January 2010, the highest proportions of enterprises having a formally defined ICT security policy with a plan for regular review were registered in Sweden and Norway (both 46 %) followed by Denmark (43 %). In more than half of the countries, Information and communication activities had the highest percentages of enterprises with an ICT security policy. The lowest percentage for enterprises with such a policy was reported in Accommodation and Food service activities in a majority of the countries. Less than 10 % of the enterprises in Romania, Hungary and Bulgaria reported that they had a formally defined ICT security policy. It should be noted that unreliable data for specific economic activities (highest/lowest) are not shown in Figure 3 but are included in the totals (EU27 and All economic activities aggregates) of Figures 2 and 3.

Figure 3: Range of the highest/lowest proportions of enterprises having a formally defined ICT security policy with a plan for regular review, by country and economic activity, January 2010 (% of enterprises)



Source: Eurostat (online data code: isoc_cisce_ra)

The risk of destruction or corruption of data due to an attack or some other unexpected incident is the risk mostly addressed by enterprises' ICT security policies

The three types of risks addressed by enterprises having a formally defined ICT security policy with a plan for regular review correspond essentially to the core elements of the ICT security definition, i.e. integrity, confidentiality and availability of data and systems.

Three types of risks that an enterprise's ICT security policy addresses:
Type 1: Destruction or corruption of data due to an attack or some other unexpected incident
Type 2: Disclosure of confidential data due to intrusion, pharming, phishing attacks
Type 3: Unavailability of ICT services due to an attack from outside

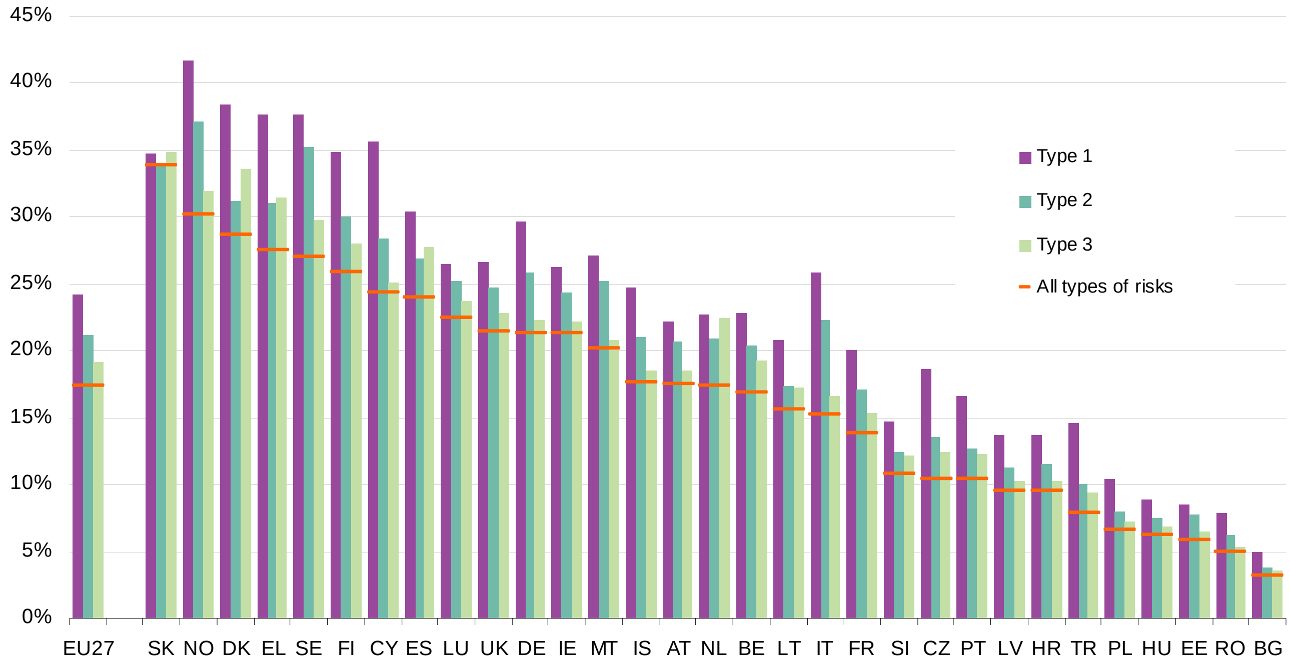
In January 2010, the highest percentage of enterprises which addressed the Type 1 risk was reported in Norway (42 %), followed by Denmark, Greece and Sweden with 38 % respectively.

Similarly, 37 % of enterprises in Norway had a formally defined ICT security policy which addressed the Type 2 risk, followed by Sweden and Slovakia with 35 % and 34 % respectively.

Slovakia reported the highest percentage of enterprises (35 %) which addressed the risk of unavailability of ICT services due to an attack from outside (Type 3).

Additionally, as Figure 4 shows, Slovakia reported the highest percentage of enterprises (34 %) having a formally defined ICT security policy which addressed all three types of risks, followed by Norway and Denmark with 30 % and 29 % respectively.

Figure 4: Enterprises having a formally defined ICT security policy with a plan for regular review which addresses specific security risks, by country and type of risk, January 2010, (% of enterprises)



Source: Eurostat (online data code : isoc_cisce_ra)

Voluntary training or use of generally available information was the approach reported by most of the enterprises to make staff aware of their ICT-related security obligations

Enterprises adopt various approaches aiming at raising awareness of ICT security policy and the relevant risks. The three approaches adopted by enterprises differ in their obligatory character and the legally binding obligations for the staff concerned.

Three approaches for raising awareness of staff's obligations in relation to ICT security:
Approach 1: Compulsory training or presentations
Approach 2: Contracts, e.g. contract of employment
Approach 3: Voluntary training or generally available information (intranet, news letters, paper documents)

In January 2010, the approach most commonly reported by enterprises for making their staff aware of their obligations in relation to ICT security was voluntary training or generally available information (Approach 3).

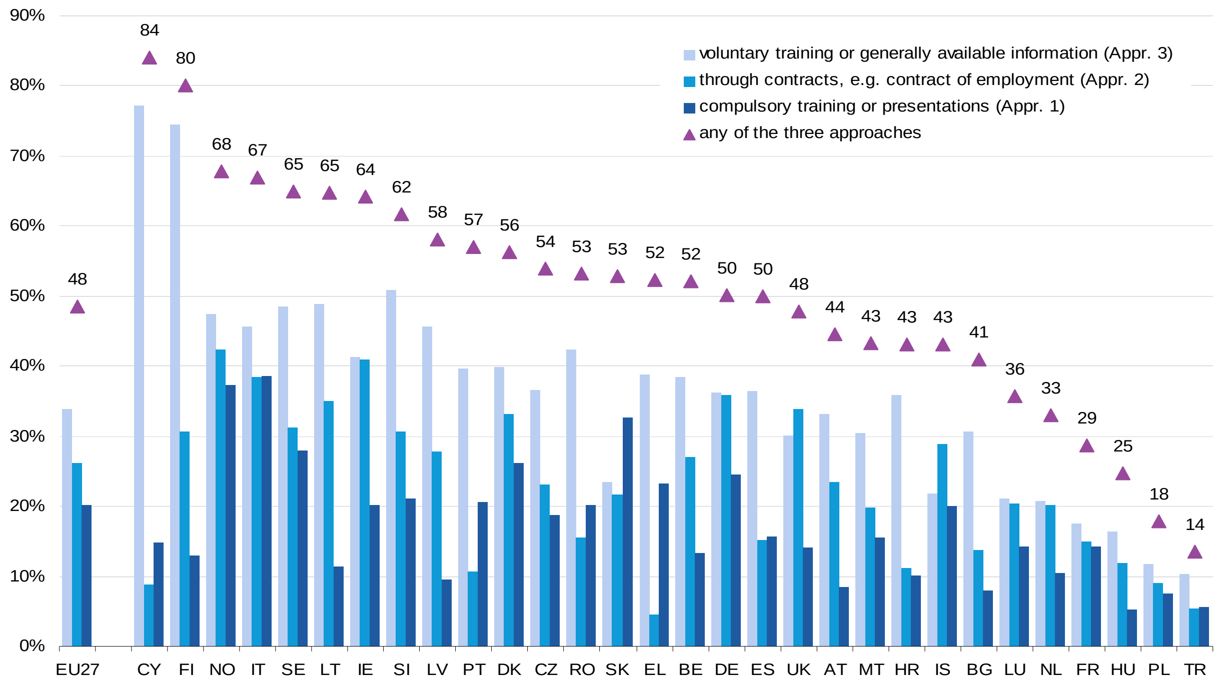
As Figure 5 shows, the highest proportions of enterprises adopting this approach were registered in Cyprus and Finland with 77 % and 74 % respectively.

The second favourite approach reported by enterprises for making staff aware of their obligations in relation to ICT security was through contractual agreements e.g. contracts of employment (Approach 2). The share of enterprises reporting this approach was highest in Norway and Ireland with more than 4 out of 10 enterprises.

Italy reported the highest percentage of enterprises (39 %) which adopted compulsory training or presentations (Approach 1) followed by Norway and Slovakia with 37 % and 33 % respectively.

Almost two thirds of EU-Member States reported a higher percentage of enterprises having used at least one of the approaches than the EU27 average (48 %). Moreover, Cyprus (84 %) and Finland (80 %) reported the highest proportions of enterprises that have adopted at least one of the three specific approaches.

Figure 5: Approach adopted by enterprises to make staff aware of their obligations in relation to ICT security, by country, January 2010 (% of enterprises)

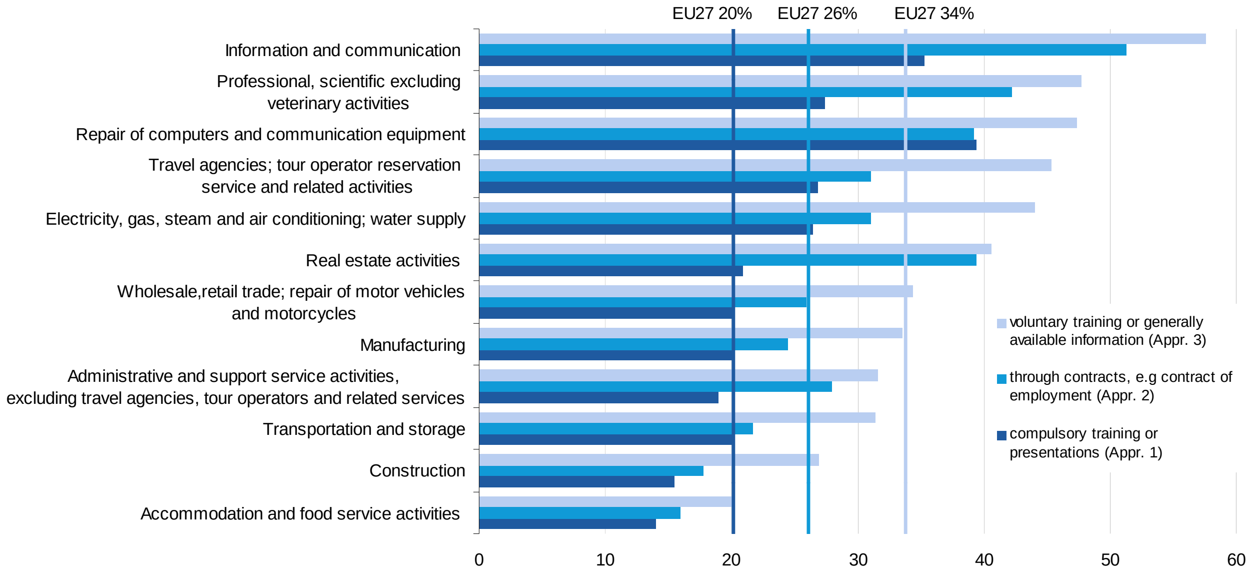


Source: Eurostat (online data code : isoc_cisce_ra), EU27 without EE

Figure 6 shows that Approaches 3 and 2 are most commonly adopted by enterprises in the EU27 in the sector Information and communication (58 % and 51 % respectively) followed by those in Professional and scientific activities (48 % and 42 % respectively).

Compulsory training and presentations (Approach 1) was recorded mostly by enterprises in Repair of computers and communication equipment (39 %) and in Information and communication (35 %) activities.

Figure 6: Approach adopted by enterprises to make staff aware of their obligations in relation to ICT security, by economic activity, EU27, January 2010 (% of enterprises)



Source: Eurostat (online data code : isoc_cisce_ra), EU27 without EE

In 2009, three out of 20 enterprises experienced an ICT-related security incident

ICT-related security incidents concern the core elements of Information Security, integrity, confidentiality and availability of the data and the IT systems.

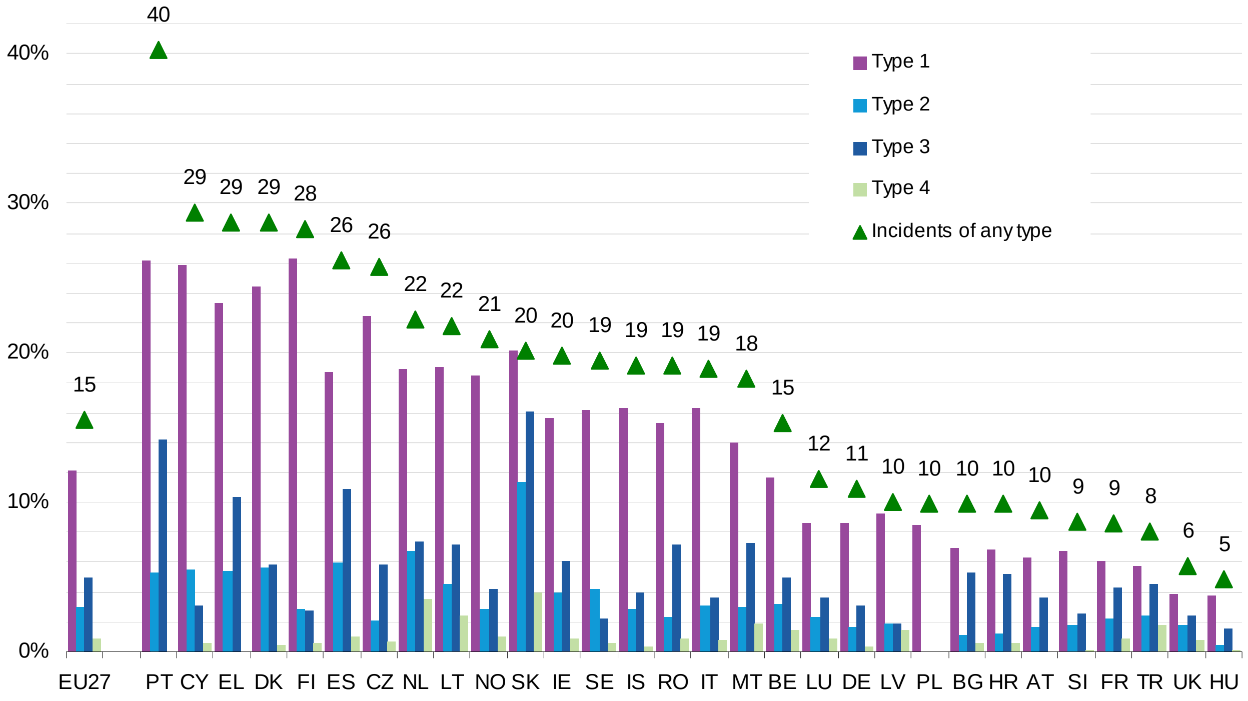
There are four types of ICT security-related incidents that result in:
Type 1: Unavailability of ICT services, destruction or corruption of data due to hardware or software failures
Type 2: Unavailability of ICT services due to attacks from outside e.g. denial of service attack
Type 3: Destruction or corruption of data due to infection or malicious software or unauthorised access
Type 4: Disclosure of confidential data due to intrusion, pharming, phishing attacks

In 2009, as Figure 7 shows, the incidents most commonly reported by enterprises were those resulting in unavailability of ICT services, destruction or corruption of data due to hardware or software failures (Type 1), with shares above 20 % registered in Cyprus, Portugal and Finland (26 % of enterprises respectively), Denmark (24 %), Greece (23 %), the Czech Republic (22 %) and Slovakia (20 %).

In 2009, the highest proportion of enterprises reporting ICT incidents resulting in the destruction or corruption of data due to malicious software infection or unauthorised access (Type 3) was registered in Slovakia (16 %), Portugal (14 %), Spain (11 %) and Greece (10 %).

The share of enterprises reporting unavailability of ICT services due to an attack from outside (Type 2) was highest in Slovakia (11 %) and the Netherlands (7 %). In the majority of EU27 Member States, the disclosure of confidential data due to intrusion, pharming or phishing attacks was reported by 1 % or less of enterprises in 2009.

Figure 7: ICT security incidents affecting the ICT systems of enterprises, by country and type of incident, 2009 (% of enterprises)



Source: Eurostat (online data code: isoc_cisce_ic), EU27 without EE

Offsite data backup and strong password authentication were the most common internal security procedures applied

Identification refers to the ability to identify and distinguish between individual users. User identification is considered as common practice in enterprises and usually complemented by authentication procedures. In general, identification and authentication of users are part of the authorisation process. Authorisation defines access and usage rights related to specific information or services.

In January 2010, strong password authentication was the most commonly reported procedure used for internal ICT security, with the highest shares registered in Italy (64 %), Ireland (63 %) and Spain (61 %).

As Figure 8 shows, among all countries, the highest proportions of enterprises reporting the use of hardware tokens for user identification and authentication were registered in Croatia (49 %) and Slovenia (48 %).

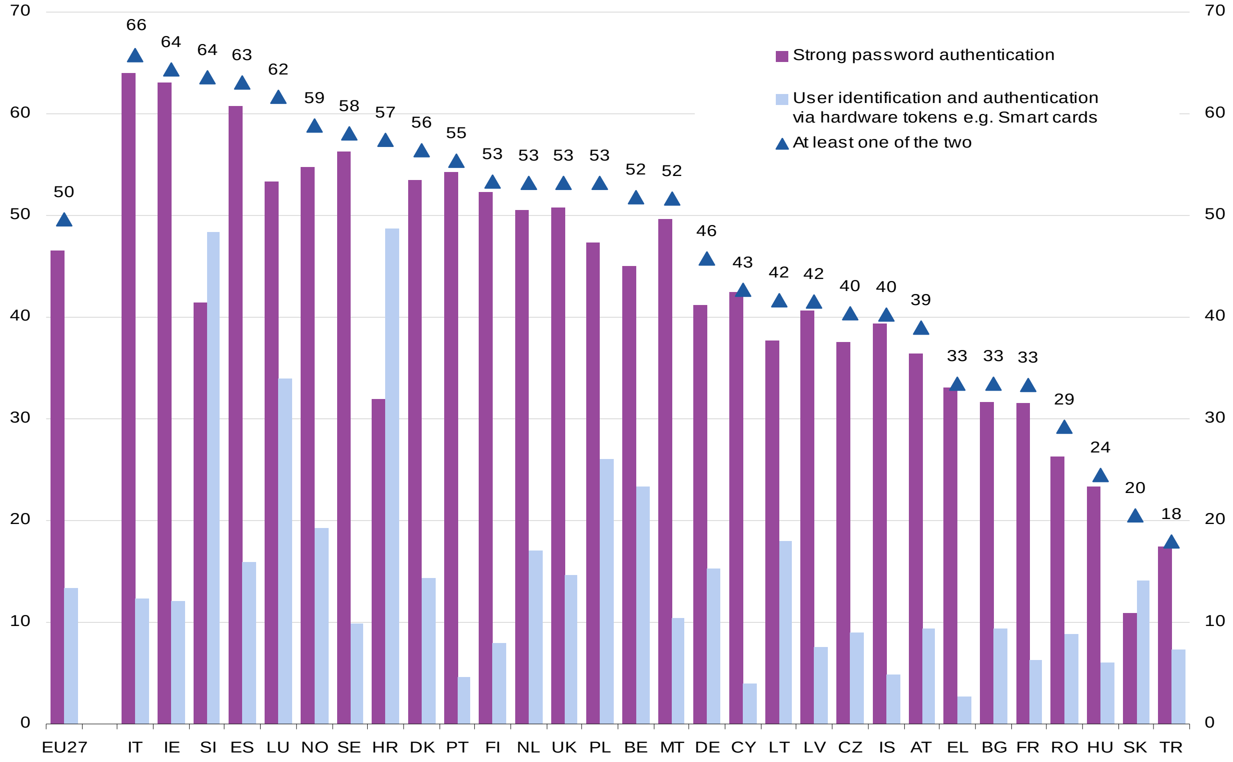
At the same time, Italy (66 %), Ireland and Slovenia (both 64 %) reported the highest proportions of enterprises that had used at least one of these internal ICT security facilities.

Offsite data backup is part of the data protection strategy of sending critical data from the main site to another location by means of removable storage media, e.g. magnetic type, external hard-disks, or electronically via remote backup services.

As Figure 9 shows, the highest proportions of enterprises using offsite backup among all countries were registered in Denmark and Norway (both 76 %) followed by Sweden (69 %) and Iceland (73 %).

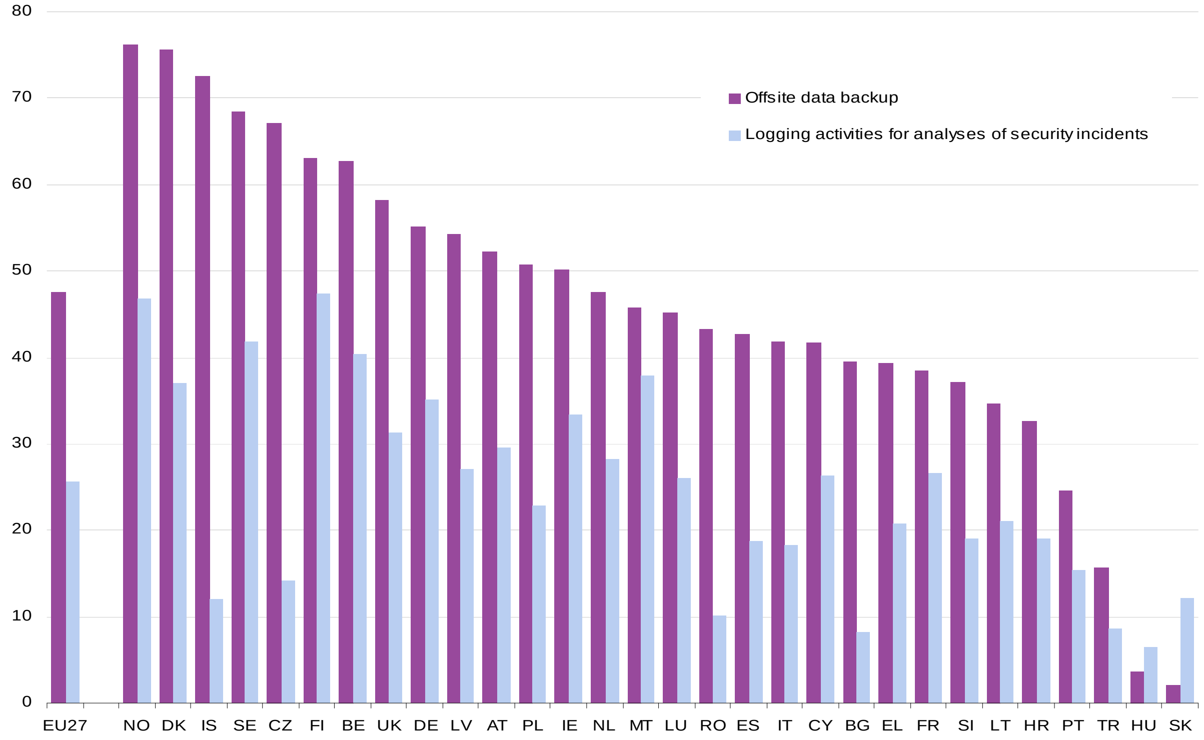
One out of four enterprises in the EU27 had used logging activities for analyses of security incidents, with the highest proportions of enterprises registered in Finland, Norway (both 47 %), Sweden (42 %) and Belgium (40 %).

Figure 8: Enterprises using identification/authentication methods, by type and country, January 2010 (% of enterprises)



Source: Eurostat (online data code: isoc_cisce_fp), EU27 without EE

Figure 9: Enterprises using offsite data backup, logging activities for analyses of security incidents, by country, January 2010 (% of enterprises)



Source: Eurostat (online data code: isoc_cisce_fp), EU27 without EE

Table 1: Enterprises having a formally defined ICT security policy with a plan for regular review, by economic activity, January 2010 (% of enterprises)

	Economic activities													
Country	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**	**(12)**	**(13)**	**(14)**
EU27	27	26	35	17	27	24	13	52	32	46	26	43	43	55
BE	29	27	:	18	31	26	13	52	:	40	30	40	:	53
BG	7	5	12	3	7	9	3	30	10	21	7	21	14	34
CZ	21	22	25	13	24	14	11	49	21	29	19	27	54	52
DK	43	47	:	26	45	40	22	65	:	57	34	:	:	68
DE	31	28	43	17	30	29	15	58	37	52	31	51	58	64
EE	11	10	10	6	10	11	6	24	13	18	13	21	33	29
IE	28	33	22	25	26	27	12	59	21	46	35	32	47	63
EL	39	:	47	38	46	45	20	59	:	58	37	:	82	66
ES	33	31	37	21	38	30	33	54	46	54	25	62	54	57
FR	22	22	22	11	23	17	10	46	29	41	20	17	:	48
IT	29	32	44	19	30	25	15	60	39	52	27	48	:	58
CY	37	28	41	25	41	54	20	86	36	66	56	76	:	92
LV	15	13	26	11	15	12	8	35	18	25	16	64	63	38
LT	25	20	39	17	27	23	18	48	27	34	36	50	43	56
LU	28	29	24	18	30	22	:	58	:	43	:	:	:	62
HU	9	9	19	4	9	9	3	26	11	15	8	9	26	28
MT	30	28	38	14	29	33	22	63	:	39	36	40	:	72
NL	29	31	43	18	30	30	10	46	30	43	23	38	46	52
AT	24	24	:	15	24	24	:	:	:	36	:	:	:	:
PL	11	:	18	:	11	12	:	28	:	:	12	16	17	30
PT	22	19	35	:	30	:	:	50	41	35	:	32	62	49
RO	9	8	13	5	9	5	5	33	22	23	9	15	11	31
SI	16	14	15	6	20	16	11	50	31	20	18	:	50	45
SK	35	33	55	28	39	31	20	57	34	47	25	63	38	55
FI	37	37	57	16	45	25	14	65	42	60	:	:	:	68
SE	46	50	67	33	49	42	22	67	62	54	39	63	:	70
UK	29	32	40	20	28	25	6	51	18	48	32	50	54	56
IS	25	19	42	14	27	32	11	51	:	45	23	23	:	64
NO	46	42	74	35	51	39	32	60	52	66	40	63	62	62
HR	16	15	:	10	18	21	16	33	:	18	:	:	14	35
TR	22	21	40	14	24	25	21	42	30	31	14	36	58	43

Source: Eurostat (online data code : isoc_cisce_ra)

Column	**NACE Rev. 2 economic activities (Tables 1, 2, 3, 4)**	**Column**	**NACE Rev. 2 economic activities (Tables 1, 2, 3, 4)**
(1)	All economic activities	(8)	Information and communication
(2)	Manufacturing	(9)	Real estate activities
(3)	Electricity, gas, steam and air conditioning; water supply	(10)	Professional, scientific excluding veterinary activities
(4)	Construction	(11)	Administrative and support service activities, excluding travel agencies, tour operators and related services
(5)	Wholesale,retail trade; repair of motor vehicles and motorcycles	(12)	Travel agencies; tour operator reservation service and related activities
(6)	Transportation and storage	(13)	Repair of computers and communication equipment
(7)	Accommodation and food service activities	(14)	ICT sector

Table 2: Enterprises having a formally defined ICT security policy with a plan for regular review addressing all security risks, by economic activity, January 2010 (% of enterprises)

	Economic activities													
Country	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**	**(12)**	**(13)**	**(14)**
EU27	17	15	25	10	18	17	7	39	23	32	18	29	35	42
BE	17	15	:	9	18	17	6	37	:	24	19	33	:	37
BG	3	2	9	0	3	4	0	17	3	16	5	1	:	22
CZ	10	9	13	5	13	6	5	29	12	17	12	12	27	28
DK	29	29	:	20	29	27	15	50	:	34	25	:	:	52
DE	21	18	36	9	20	20	11	44	27	38	20	26	50	52
EE	6	5	7	1	5	5	2	20	8	12	9	17	33	21
IE	21	25	22	15	20	21	8	45	16	32	30	28	47	54
EL	27	:	:	25	:	38	13	46	:	39	21	:	:	51
ES	24	22	28	15	29	24	15	46	32	43	19	43	52	50
FR	14	14	16	7	16	11	6	29	21	26	13	12	:	34
IT	15	15	26	9	16	16	7	40	19	27	14	27	:	37
CY	24	12	22	15	25	47	16	72	24	46	50	67	:	76
LV	10	7	12	7	9	8	4	26	12	18	11	40	:	27
LT	16	12	30	9	16	16	11	37	17	22	23	29	39	43
LU	22	22	19	13	25	19	:	52	:	37	:	:	:	55
HU	6	6	14	3	6	6	2	20	8	10	5	1	26	21
MT	20	20	25	6	20	19	12	51	:	31	20	34	:	60
NL	17	17	29	10	17	19	5	32	18	27	15	27	41	36
AT	18	18	:	10	18	17	:	:	:	28	:	:	:	:
PL	7	5	11	4	7	8	3	20	11	13	8	10	13	22
PT	10	8	:	:	16	6	:	31	:	:	:	:	:	31
RO	5	5	7	2	5	2	1	21	10	12	7	8	5	21
SI	11	8	10	3	16	10	6	36	25	11	13	:	50	40
SK	34	32	47	26	38	29	18	53	34	47	25	63	35	51
FI	26	22	39	10	33	19	:	52	36	42	:	:	:	54
SE	27	28	47	15	29	27	10	49	34	35	25	47	:	52
UK	21	23	29	17	21	21	4	44	13	34	25	40	47	48
IS	18	13	15	7	20	24	6	43	:	28	21	23	:	54
NO	30	26	60	17	36	28	17	48	34	40	30	58	62	46
HR	9	8	:	5	11	16	10	20	:	8	:	:	14	29
TR	8	7	17	5	8	9	7	18	9	17	4	11	27	20

Source: Eurostat (online data code : isoc_cisce_ra)

Table 3: Enterprises which have adopted any approach to make staff aware of their obligations in relation to ICT security, by economic activity, January 2010 (% of enterprises)

	Economic activities													
Country	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
EU27	48	49	58	39	49	47	31	75	54	67	46	61	69	77
BE	52	52	:	38	53	50	28	82	:	64	59	53	:	84
BG	41	36	42	39	43	37	36	76	44	70	33	35	71	76
CZ	54	55	63	46	56	48	38	82	59	66	47	68	96	84
DK	56	58	:	36	62	50	31	81	:	78	54	:	:	84
DE	50	47	66	30	51	46	36	80	57	71	47	65	65	82
EE	:	:	:	:	:	:	:	:	:	:	:	:	:	:
IE	64	69	66	63	65	69	41	92	61	82	65	78	100	89
EL	52	50	52	52	60	55	31	70	:	60	54	50	100	83
ES	50	46	56	43	53	51	53	69	59	66	41	72	78	76
FR	29	29	24	18	28	25	16	54	39	50	28	42	:	59
IT	67	69	79	64	69	65	45	86	68	81	62	81	:	83
CY	84	81	92	80	89	82	75	92	84	92	93	88	:	89
LV	58	53	60	55	61	68	41	69	58	66	60	49	63	75
LT	65	60	74	64	68	60	52	87	65	77	62	76	74	90
LU	36	40	43	28	34	35	:	66	:	50	:	:	:	71
HU	25	22	34	21	25	27	15	50	25	36	23	22	54	50
MT	43	32	38	24	45	57	44	71	:	60	46	42	:	85
NL	33	35	44	18	35	27	9	60	44	52	28	45	64	65
AT	44	45	:	31	47	37	:	76	:	66	:	:	:	83
PL	18	16	26	12	19	19	10	43	22	31	19	28	41	46
PT	57	49	64	51	64	86	53	81	74	69	57	73	85	64
RO	53	51	63	51	54	53	40	77	61	71	45	67	78	76
SI	62	61	77	43	69	58	50	92	90	73	64	100	83	95
SK	53	48	56	44	59	52	49	76	57	63	38	73	51	72
FI	80	79	92	73	85	72	57	96	91	93	:	:	:	97
SE	65	66	86	54	68	56	46	89	82	75	62	77	100	91
UK	48	54	59	37	47	46	11	80	52	72	53	56	69	83
IS	43	35	62	33	43	65	16	74	:	78	51	69	:	87
NO	68	62	83	54	78	57	48	87	87	79	70	83	100	90
HR	43	38	:	33	44	59	39	68	:	57	:	:	89	69
TR	14	12	29	7	15	16	11	34	20	21	12	26	49	33

Source: Eurostat (online data code: isoc_cisce_ra); EU27 without EE

Table 4: Enterprises which have used strong password authentication or user identification and authentication via hardware tokens, by economic activity, January 2010 (% of enterprises)

	Economic activities													
Country	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
EU27	50	51	56	42	50	47	37	70	50	60	49	59	61	72
BE	52	48	:	38	57	48	38	70	:	72	47	56	:	78
BG	33	30	37	29	36	31	31	63	35	53	20	24	71	67
CZ	40	40	51	37	42	40	23	66	39	50	33	52	75	64
DK	56	54	:	49	59	51	43	74	:	64	63	:	:	74
DE	46	44	53	35	46	40	42	67	48	56	45	48	71	70
EE	:	:	:	:	:	:	:	:	:	:	:	:	:	:
IE	64	72	66	60	66	64	49	88	68	64	71	78	100	89
EL	33	:	35	35	38	44	18	51	:	45	26	37	9	61
ES	63	62	67	55	68	62	61	78	66	79	57	72	80	84
FR	33	33	38	23	37	28	27	56	30	48	30	25	:	59
IT	66	70	75	61	67	62	43	80	72	83	62	80	:	79
CY	43	48	50	29	33	50	48	78	52	69	60	67	:	93
LV	42	37	45	38	43	44	33	58	45	54	37	45	52	64
LT	42	39	62	35	41	40	37	65	46	54	44	41	39	67
LU	62	61	67	54	65	62	:	82	:	73	:	:	:	84
HU	24	21	35	18	25	28	14	53	26	43	22	38	43	52
MT	52	48	38	29	56	53	53	77	:	54	50	60	:	85
NL	53	56	65	42	55	51	27	74	59	66	50	75	74	78
AT	39	38	:	28	44	32	:	:	:	56	:	:	:	:
PL	53	52	55	49	54	53	41	73	65	61	54	70	74	75
PT	55	53	78	44	62	88	46	79	84	65	40	67	82	83
RO	29	26	43	25	31	23	22	65	35	42	23	33	43	62
SI	64	63	62	47	71	70	56	92	69	68	61	:	83	82
SK	20	20	23	16	21	21	16	35	16	28	19	46	22	32
FI	53	49	69	36	58	50	52	77	76	70	:	:	:	83
SE	58	55	61	56	64	53	41	73	61	62	54	58	:	76
UK	53	55	63	49	50	53	33	76	58	64	62	72	74	76
IS	40	35	83	25	41	52	27	69	:	53	48	62	:	86
NO	59	53	71	50	64	55	49	69	68	72	59	81	60	73
HR	57	54	:	49	62	62	48	73	:	64	:	:	44	75
TR	18	17	35	10	20	21	15	38	27	27	12	32	45	38

Source: Eurostat (online data code: isoc_cisce_fp); EU27 without EE

Column	ICT security policy and relevant risks addressed (Table 5)
(1)	Enterprises that had a formally defined ICT security policy
(2)	Destruction or corruption of data due to an attack or by unexpected incident
(3)	Disclosure of confidential data due to intrusion, pharming, phishing attacks
(4)	Unavailability of ICT services due to an attack from outside
(5)	Addressed all risks; (2), (3) and (4)

Table 5: Enterprises with a formally defined ICT security policy with a plan for regular review addressing specific security risks, January 2010 (% of enterprises)

	ICT security policy and relevant risks addressed				
Country	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
EU27	27	24	21	19	17
BE	29	23	20	19	17
BG	7	5	4	4	3
CZ	21	19	14	12	10
DK	43	38	31	34	29
DE	31	30	26	22	21
EE	11	9	8	6	6
IE	28	26	24	22	21
EL	39	38	31	31	27
ES	33	30	27	28	24
FR	22	20	17	15	14
IT	29	26	22	17	15
CY	37	36	28	25	24
LV	15	14	11	10	10
LT	25	21	17	17	16
LU	28	26	25	24	22
HU	9	9	7	7	6
MT	30	27	25	21	20
NL	29	23	21	22	17
AT	24	22	21	19	18
PL	11	10	8	7	7
PT	22	17	13	12	10
RO	9	8	6	5	5
SI	16	15	12	12	11
SK	35	35	34	35	34
FI	37	35	30	28	26
SE	46	38	35	30	27
UK	29	27	25	23	21
IS	25	25	21	19	18
NO	46	42	37	32	30
HR	16	14	12	10	9
TR	22	15	10	9	8

Source: Eurostat (online data code : isoc_cisce_ra)

Column	ICT security incidents (Table 6)
(1)	Enterprises have experienced ICT related incidents that resulted in unavailability of ICT services, destruction or corruption of data due to hardware or software failures
(2)	Enterprises have experienced ICT related incidents that resulted in unavailability of ICT services due to attacks from outside e.g. denial of service attack
(3)	Enterprises have experienced ICT related incidents that resulted in destruction or corruption of data due to infection or malicious software or unauthorised access
(4)	Enterprises have experienced ICT related incidents that resulted in disclosure of confidential data due to intrusion, pharming, phishing attacks
(5)	Enterprises have experienced at least one of the above ICT incidents (1), (2), (3) or (4)

Table 6: ICT security incidents affecting the ICT systems of enterprises, by country, 2009 (% of enterprises)

	ICT security incidents				
Country	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
EU27	12	3	5	1	15
BE	12	3	5	1	15
BG	7	1	5	1	10
CZ	22	2	6	1	26
DK	24	6	6	0	29
DE	9	2	3	0	11
EE	:	:	:	:	:
IE	16	4	6	1	20
EL	23	5	10	:	29
ES	19	6	11	1	26
FR	6	2	4	1	9
IT	16	3	4	1	19
CY	26	5	3	1	29
LV	9	2	2	1	10
LT	19	4	7	2	22
LU	9	2	4	1	12
HU	4	0	2	0	5
MT	14	3	7	2	18
NL	19	7	7	4	22
AT	6	2	4	:	10
PL	8	:	:	:	10
PT	26	5	14	:	40
RO	15	2	7	1	19
SI	7	2	3	0	9
SK	20	11	16	4	20
FI	26	3	3	1	28
SE	16	4	2	1	19
UK	4	2	2	1	6
IS	16	3	4	0	19
NO	19	3	4	1	21
HR	7	1	5	0	10
TR	6	2	5	2	8

Source: Eurostat (online data code: isoc_cisce_ic); EU27 without EE

METHODOLOGICAL NOTES

Source: Data presented in this publication are based on the results of the 2010 Community survey on ‘ICT usage and eCommerce in enterprises’. Statistics were obtained from enterprise surveys conducted by National Statistical Authorities in 2010. The surveys' reference period was January 2010 or for some questions the year 2009.

Sample size: In 2010, 149 900 enterprises out of 1.6 million in the EU27 were surveyed.

Country codes: European Union (27 countries): Belgium (BE), Bulgaria (BG), the Czech Republic (CZ), Denmark (DK), Germany (DE), Estonia (EE), Ireland (IE), Greece (EL), Spain (ES), France (FR), Italy (IT), Cyprus (CY), Latvia (LV), Lithuania (LT), Luxembourg (LU), Hungary (HU), Malta (MT), the Netherlands (NL), Austria (AT), Poland (PL), Portugal (PT), Romania (RO), Slovenia (SI), Slovakia (SK), Finland (FI), Sweden (SE) and the United Kingdom (UK). Iceland (IS), Norway (NO).
Croatia (HR), Turkey (TR).

Symbols: Data in some tables are shown as ":" and refer to not available, unreliable or confidential. Unreliable data are included in the calculation of European aggregates.

Main concepts: The observation statistical unit is the **enterprise**, as defined in the Council Regulation (EEC) No 696/93 of 15 March 1993. The survey covered **enterprises** with at least 10 persons employed.
Economic activities correspond to the classification NACE Revision 2. The sectors covered are manufacturing, electricity, gas and steam, water supply, construction, wholesale and retail trades, repair of motor vehicles and motorcycles, transportation and storage, accommodation and food service activities, information and communication, real estate, professional, scientific and technical activities, administrative and support activities and repair of computers and communication equipment. Enterprises are broken down by size; small (10-49), medium (50-249) and large enterprises (250 or more persons employed).

ICT-related security incidents affect the ICT system of an enterprise and may cause different problems. The following security incidents were covered in the survey:

a) Unavailability of ICT services, destruction or corruption of data due to hardware or software failures refers to issues of data integrity caused by hardware or software failures, e.g. crashes of servers or hard disks due to hardware failures or crashes of servers due to software failures, e.g. erroneous updates.

b) Unavailability of ICT services due to attack from outside refers to attempts from outside to make an information system resource unavailable to its intended users. One aim of these attacks is to prevent an internet site or service from functioning efficiently, e.g. websites of banks, credit card payment gateways.

c) Destruction or corruption of data due to malicious software infection or unauthorised access.

d) Disclosure of confidential data due to intrusion, pharming, phishing attacks refers to an attempt to get confidential information on persons, staff or clients, intellectual property or other confidential information. Intrusion is an attempt to bypass security controls on an information system by viruses, worms, Trojan horses etc. Phishing is a criminally fraudulent attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Pharming is an attack which redirects the traffic of a website to another, bogus website in order to acquire sensitive information

User identification refers to the ability to identify and distinguish between individual users. **Authentication** means to assure the identity of a certain user. Authentication and identification of users are applied in the context of authorisation, to define access and usage rights related to specific information or services. Authentication can be done with the help of passwords, or with additional devices, such as smart cards, hardware tokens or identity cards. **Strong password authentication** means a minimum length of 8 mixed characters, a maximum duration of 6 months, encrypted transmission and storage. A **hardware token** is a physical device that authorises the access of the owner of the token to a computer or a network. Hardware tokens provide an extra level of assurance in addition to the personal identification number (PIN), which authorises users as the owner of that particular device; the device generates a number which uniquely identifies the user to the service, and allows logging in. Additionally, an enterprise’s ICT security information system may include the **logging of applications or user activities**. The logs can be used for analysis in case of security incidents in order to take appropriate action to prevent these kinds of incidents in future or to quantify any damage. Intrusion detection is a process with the purpose of detecting intrusions or attempts of intrusion into a computer or network to compromise confidentiality, integrity or availability by observation of system, application and user activity as well as network traffic.

Further information

Eurostat Website: http://ec.europa.eu/eurostat

Data on “Information society statistics”
http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/database

Further information about “Information society statistics”
http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/introduction

Journalists can contact the media support service:

Bech Building, Office A4/125, L-2920 Luxembourg
Tel.: (352) 4301 33408
Fax: (352) 4301 35349
E-mail: eurostat-mediasupport@ec.europa.eu

European Statistical Data Support:

With the members of the ‘European statistical system’, Eurostat has set up a network of support centres in nearly every Member State and in some EFTA countries.

Their role is to provide help and guidance to Internet users of European statistics.

Contact details for this support network can be found on the Eurostat website at: http://ec.europa.eu/eurostat/.

All Eurostat publications can be ordered via the ‘EU Bookshop’:
http://bookshop.europa.eu/.

Manuscript completed on: 23.02.2011
Data extracted on: 12.01.2011
ISSN 1977-0316
Catalogue number: KS-SF-11-007-EN-N