Pillar 3

Security concerns

1. Citizens' concerns 2
2. The concrete experience of ICT security related problems 5
3. Attitudes and actions against protection 8
4. Businesses' concerns 10
5. Large European Enterprises' ICT security policy 10
6. ICT security incidents reported by enterprises 12
7. The specific case of SMEs, depending on eBusiness solutions adopted and by country 14
8. Sector analysis 18
9. Conclusion 19
10. Annex – methodological notes and references 20

This chapter analyses the 2010 results of two special surveys on the use of ICT by Europeans with reference to security risks on the internet. It explores three main dimensions: the level of concern; the damages effectively encountered; and the attitudes and initiatives undertaken to protect one self from the most common threats.

If the goal of "Every European Digital" is to become a reality, security concerns need to be addressed, as bad experiences may limit the internet experience. Lack of adequate skills relating to computer/data and identity protection online may endanger usage and participation, and as such represent important policy concerns.

The first part of this report analyses results of the survey proposed to citizens, aged 16-74, having used the internet during the last year. The second part will present some indicators concerning the experience of European enterprises, having 10 or more persons employed, in the main manufacturing and service sectors. The annex provides the key methodological notes and references.

1. CITIZENS' CONCERNS

The following table illustrate the reaction of European internet users to six of the more common threats and risks usually present when going online.

Table 1: Internet users level of concern with regard to security issues on the internet

How concerned are you about the following possible problems related to internet usage for private purposes? (% of internet users during last year, EU27)			
	strongly	mildly	not at all
a) catching a virus or other computer infection (e.g. worm or Trojan horse) resulting in loss of information or time	33%	45%	21%
b) unsolicited emails sent to me ('Spam')	29%	41%	29%
c) abuse of personal information sent on the Internet and/or other privacy violations (e.g. abuse of pictures, videos, personal data uploaded on community websites)	35%	36%	28%
d) financial loss as a result of receiving fraudulent messages ('phishing') or getting redirected to fake websites asking for personal information ('pharming')	32%	32%	36%
e) financial loss due to fraudulent payment (credit or debit) card use	35%	30%	35%
f) children accessing inappropriate web-sites or connecting with potentially dangerous persons from a computer within the household	34%	23%	42%

Source: Eurostat Community Survey on ICT Usage in Households and by Individuals

A majority of internet users shows some level of concern for each of the six security issues and around a third voice strong concerns. On the whole, more internet users show mild levels of concern than strong levels. Among those expressing mild concerns, a ranking emerges whereby users are mostly concerned with catching a virus or other computer infection.

However, this pattern is not the same across countries. Furthermore not all users have the same main concerns: for some it is the abuse of personal information, or spam and viruses, for others the possible financial losses, as well as the inappropriate content for children or dangerous contacts. Only 8% of internet users are not at all concerned about any of the six security issues.

Country level analysis reveals that in only three countries (Estonia, Lithuania and Ireland) are more than 20% of internet users not at all concerned. Although for most countries no strong ranking emerges across the six items, there are some exceptions:

- in some countries strong concerns about children accessing inappropriate content rank 20 percentage points (pp) more than unsolicited emails (spam) (BE, CZ, ES, PT, and a bit less in IT). This may reflect concern raised by recent child abuse scandals.

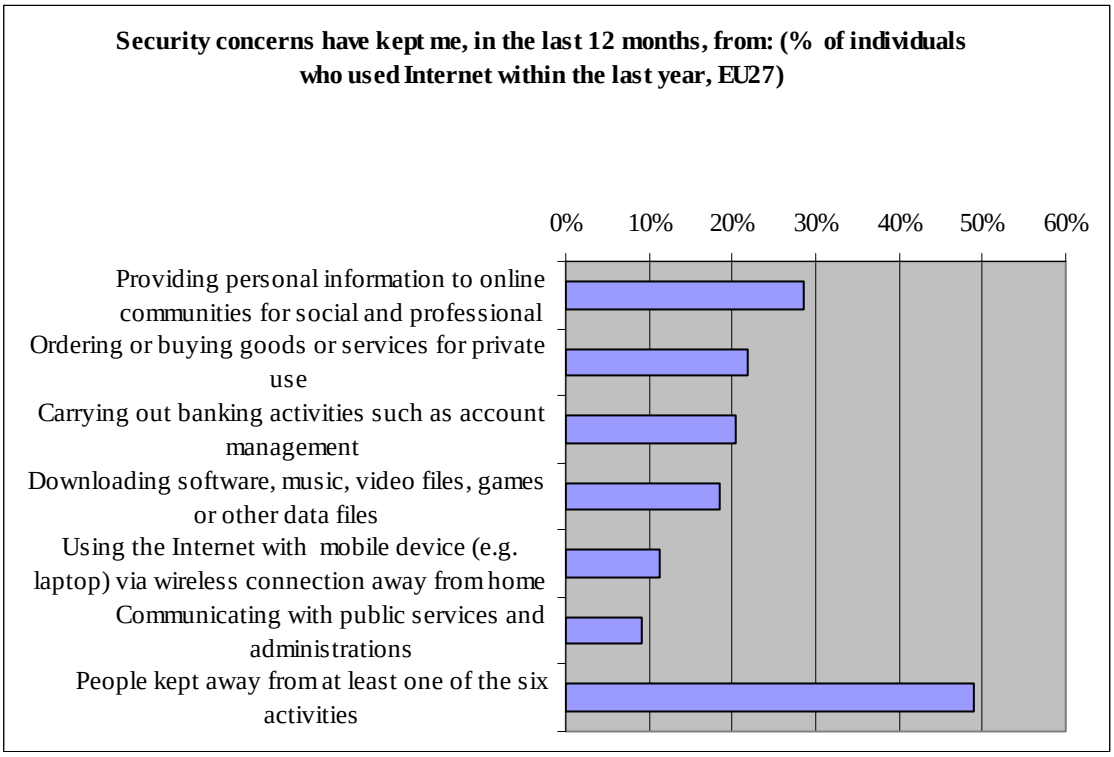
- in EL, FR, SK catching viruses or receiving spam is at the top of people's worries, well over financial losses and children accessing inappropriate content/dangerous contacts.

- financial loss during payments is of highest concern in UK, SI, LV and to a lesser degree also in SE and FI, the countries in which eCommerce is more widely diffused;

- in the NL, as well as in DE and AT, the main strong concern is about the abuse of personal information.

The less people are concerned with security issues, the less they are kept away from using the internet. Information security is critical to sustain trust in electronic transactions. Trust in the security of electronic means of communication is an important precondition for realising many potential benefits of internet use. In 2010, half of EU27 internet users have limited their use of the net because of security concerns. This proportion is quite homogeneous across social groups of the population. Youngsters/students are slightly more confident. Much more variation is observed between countries: higher percentages of people limiting their use of internet because of security concerns are observed in IT, BG, FI (65-75%), lower in IE, EE, MT, LT, RO, CZ (less than 25%). The general profile shows the following ranking:

Figure 1: **Limitations of internet use because of security concerns**



Source: Eurostat Community Survey on ICT Usage in Households and by Individuals, 2010

There is a clear and diffused reluctance to provide personal information to online communities. 55% of internet users have not posted messages on social networking sites, and 29% of internet users have made that choice, at least once, in the last 12 months prior to the survey because of security concerns. Moreover, more than a fifth of internet users did not engage in eCommerce in the last 12 months prior to the survey because of security concerns (half of those that did not buy online). Similar proportions can be observed for internet banking. Country analysis reveals that:

- for a majority of countries the more frequent decision by internet users is not to disclose personal information. This behaviour suggests significant presence of internet savy.

- the decision not to buy online is strongest in Italy (44% of internet users do not buy online for security concerns) and Greece, with significant values also in Spain, Bulgaria and France (more than 30%).

- the pattern in lack of use of online banking reflects that of eCommerce, with the notable exception of Finland, where trust in banking services is much higher than in online commerce.

- Finnish people also appear to be the most concerned with security issues to have been kept most frequently from downloading software, music, video files, games or other data files.[1]

- Italy and Germany are the countries with the lowest trust in communicating online with public administrations and services, with 20% and 13% of declared "opt-out" respectively.

2. THE CONCRETE EXPERIENCE OF ICT SECURITY RELATED PROBLEMS

One of the most common experiences is the receipt of unsolicited emails (known as "Spam"). Spam is reported by more than half of European internet users (56%) across most countries, with the notable exception for IE, AT, CY, RO and EL. Here incidents have been reported by less than one in three internet users. In any case spam is considered a strong concern only by one in two of those that reported such experience.

Spam represents an important part of all emails sent around the world. Botnets[2] are often used to diffuse such types of un-requested mails. The enduring character of the problem suggests that the issue cannot be solved by users alone. Important progress in this fight has been achieved since the adoption of the EU directive 2002/58 on privacy and electronic communications. The basic regulatory tools are there, and the Digital Agenda is focused around coordination activities and awareness raising initiatives to support the fight against spam.

Other, possibly more important problems encountered by users when surfing are (i) catching a virus, serious enough so as to result in loss of information or time; (ii) abuse of personal information; and (iii) financial losses due to phishing, pharming, or fraudulent payments associated with card use. About a third of internet users report having caught a serious virus over the previous 12 months; 4% have experienced an abuse of personal information and 3% financial losses. 34% of internet users have experienced at least one of these three. In particular (Figure 2):

- Loss of information or time due to virus infections is reported by around half of internet users in BG, MT and SK. By contrast it is less than 15% in RO, IE and AT.

- Reported financial losses are highest in LV, UK and MT (reported at between 5 and 8% of internet users). However, eCommerce is very differently diffused in these three countries: in the UK 67% of internet users report having ordered some goods or services during last year, in MT 38% and in LV only 17%. Therefore, in general, it cannot be concluded that there is a relation between eCommerce adoption and diffusion of such types of fraud. Indeed, the reverse is true for SE, DE and DK where

[1] An important national debate was open in Finland beginning of 2010 on the subject of legislative measures to reduce piracy.

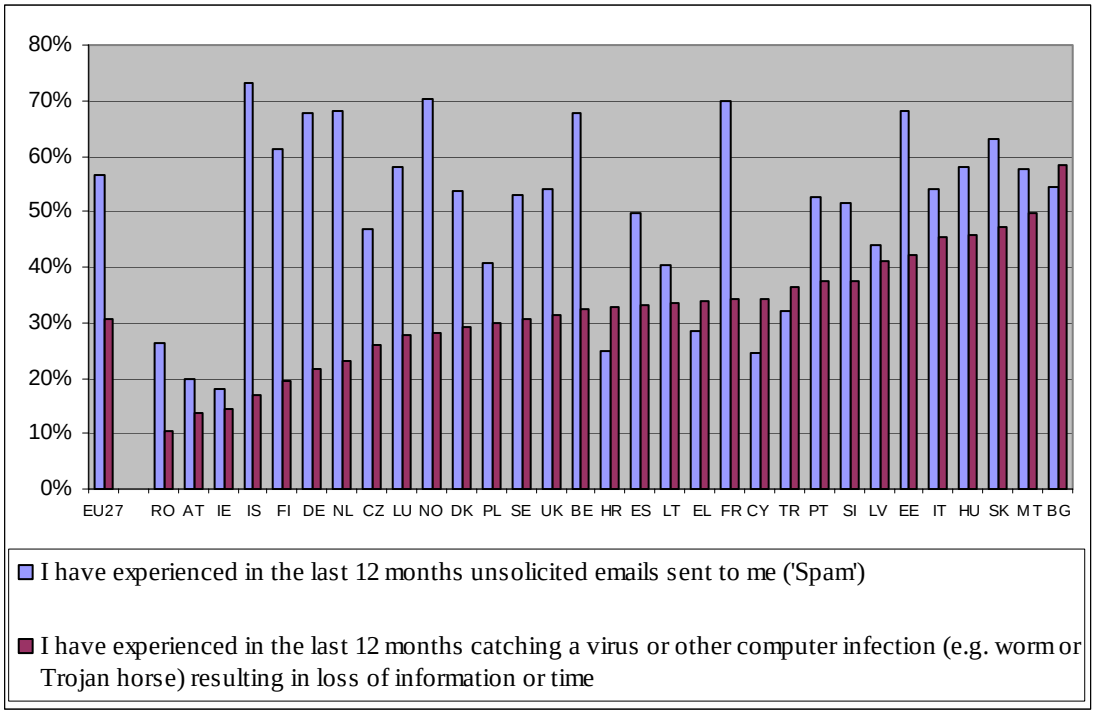
[2] A Botnet is a network of private computer infected by malicious software that allow for some kind of remote control of them.

eCommerce is high but the rate of reported losses is low compared to EU average.

– The abuse of personal information is relatively highly reported in BG, ES and IT, with frequencies between 6 and 7%, significantly above the EU27 average of 4%.

– Children accessing inappropriate content/dangerous persons is a case similarly highly reported by interviewed adults in IT, LV and BG.[3]

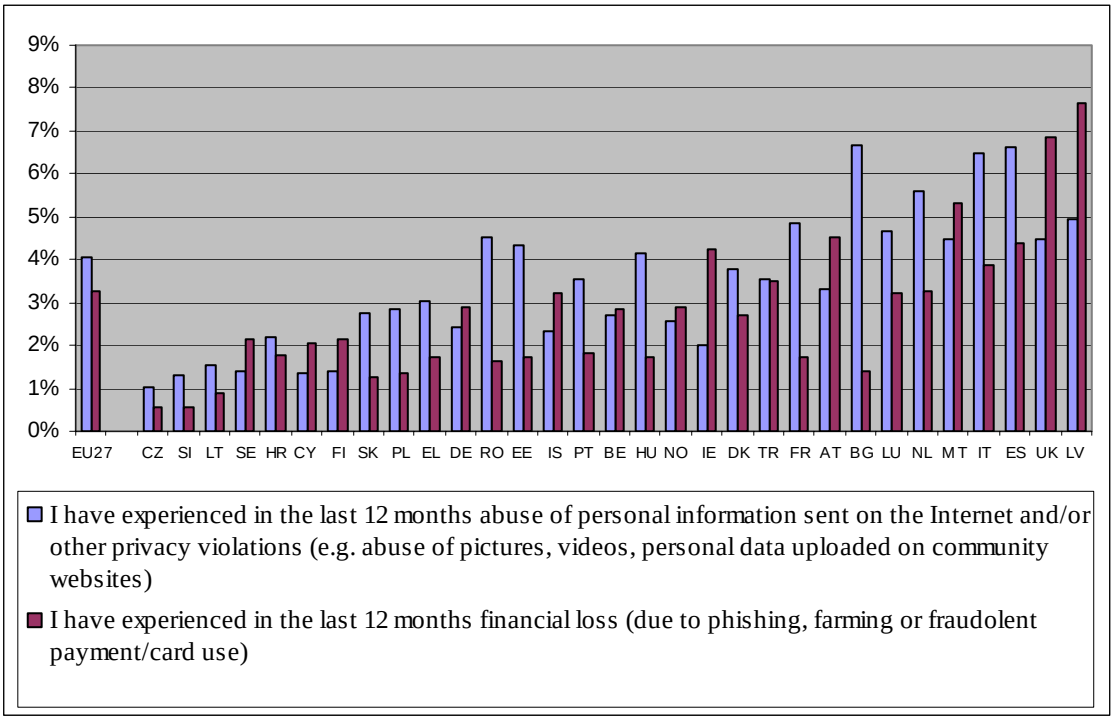
Figure 2: **Receiving Spam or catching a virus, in % of individuals who used Internet within the last year**



Source: Eurostat Community Survey on ICT Usage in Households and by Individuals, 2010

[3] See Eurostat press release of 7/02/2011 for the distribution of individuals who live in a household with dependant children and used the internet in the last 12 months and that reported incidence of children accessing inappropriate web-sites or connecting with potentially dangerous persons, available at : http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF

Figure 3: **Abuse of personal information and financial losses, in % of individuals who used Internet within the last year**



Source: Eurostat Community Survey on ICT Usage in Households and by Individuals, 2010

There is a relationship between the spread of experiencing a particular security problem and the concerns expressed**.** Half of the 31% of internet users having experienced virus infections during last year express strong concerns for that phenomenon. And the other way round, a bit less than half of the 33% expressing strong concerns about viruses have experienced it with losses of information and time. This quite extended overlap between "perceptions" and "experience" indicates that there is an important group of internet users, 15% at EU27 level, for which virus infection is a serious security problem. This reinforced conjunction of concern and experience is particularly strong in LV, PT, BE, CZ, UK and MT.

Spam is widely experienced (56% of internet users) but considered a concern by 30% of them only. The majority of users consider it a disturbing phenomenon although not too damaging. The main outlier is FR, where spam is diffused and represents a strong concern for a majority of internet users. The other problems of financial losses and abuse of personal information are more rare but perceived as more relevant and considered a strong concern, ten times more (32/35%) than they are actually experienced, illustrating the much more relevant damages and risks associated with them.

The large majority (two thirds) of those experiencing abuse of personal information have been using the internet for social networking and are people active in posting messages to chat sites, blogs, newsgroups or online discussion forum or instant messaging, and/or uploading self-created content (text, images, photos, videos, music, etc.), suggesting that the risk of abuse of personal information is slightly increased by the fact of being an active social net worker. Similarly, 67% of those having experienced one of the three more rare problems have

been ordering goods or services over the internet. As 57% of all internet users during last year have ordered goods or services, then buying online slightly increases the real risk of experiencing security threats.

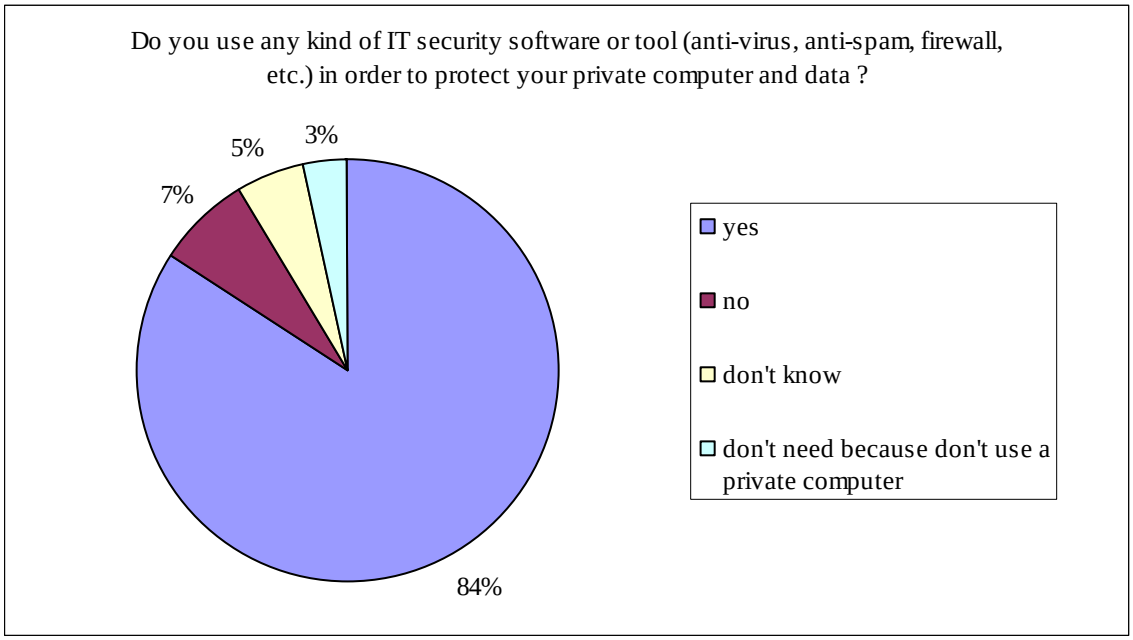
There are more victims of viruses (or users aware of having been victim of viruses), between students/16-24 than across other age groups, particularly if with high education (40% instead of 30%). Moreover, there are slightly more victims of abuse of personal information, as well as for financial losses, among highly educated people (5% instead of 4%, or 4.6% instead of 3%). On the contrary, children exposure is a bit more reported by adults with no or low education (4.4 instead of 3%).

These data should be interpreted carefully because they refer to facts that internet users are aware of and do not include events people have not had the opportunity or the ability to perceive. A second caveat comes from the absence of measures of the intensity of use. For example, it is likely that the risks of experiencing credit card related frauds increase with frequency of use. There are also qualitative aspects of individual behaviour online (e.g. the opening of files attached to e-mail received form unknown persons, etc) that could seriously change the exposure to major risks. Much more detailed research is needed on the subject.

3. ATTITUDES AND ACTIONS AGAINST PROTECTION

European citizens are trying to protect themselves from security risks. The two major tools they have at their disposal are running specific software and the practice of making regular backups of their data. A very large majority of internet users declares to use some sort of IT security software (84% on EU27 average). Only in LV, RO, EE, IT and CZ this percentage falls between 62 and 68%.

Figure 4: **Use of IT security software or tool, in % of individuals who used Internet within the last year**



Source: Eurostat Community Survey on ICT Usage in Households and by Individuals, 2010

5% of internet users do not know whether they are using some security software. This could be related to the fact that someone else in the household takes care of the issue. Moreover, software (IT tools) may be installed by default when computers are new. Some of the internet users have been unable to describe the security software running on their computer when surfing online. This is particularly true in CZ, EE, IT, CY, LV, BG and RO with frequencies between 24 and 12%.

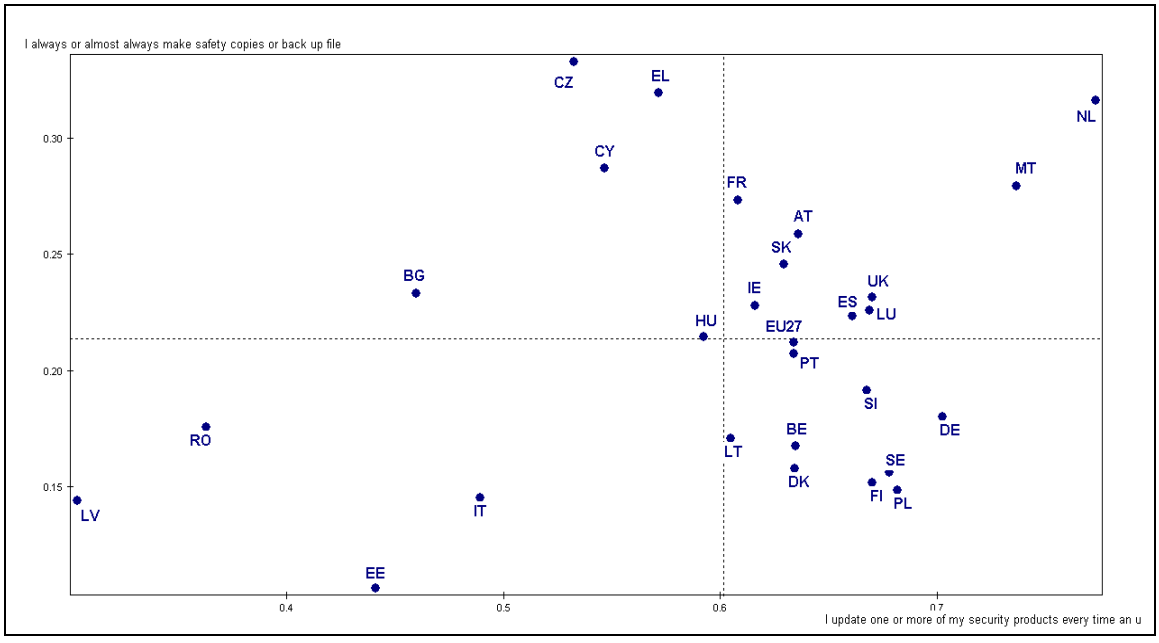
Lack of skills is also reflected by a small percentage of users of IT security software (13%) who are not aware of what the software does. Moreover, the effectiveness of this software very much depends on the frequency of its updates (because of the fast changing environment in terms of viruses, spam and other threats). Three out of four users do update the software, in particular when automatic updates are available, but a quarter risks to weaken its effect because they do not update it often enough or at all.

More than 40% of those who do not update their software do not do so because they don't know how to, and 8% because it's too expensive. This result reflects the importance of the lack of skills rather than the importance of affordability considerations.

A minority of internet users protects data through making safety copies or back up files. A third of internet users does so occasionally, and only 21% in a regular way. Results are correlated with the education level. As expected, the highest use of back-up and safety copies is done by ICT professionals (42%).

The use of IT security software (regularly updated) and regularly making safety copies or back up files are both correlated with skills and education and therefore between themselves (Figure 5).

Figure 5: **Use of "regularly updated security software" and of "back up files" by countries, in % of individuals who used Internet within the last year**



Source: Eurostat Community Survey on ICT Usage in Households and by Individuals, 2010

4. BUSINESSES' CONCERNS

ICT Security is a very relevant concern for enterprises because incidents may yield important damage with reference to destruction or corruption of data, disclosure of confidential data, unavailability of services. Security issues come hand-in-hand with increased ICT and eBusiness adoption by enterprises: the more ICT and eBusiness solutions are used, the more enterprises become dependent and potentially vulnerable to any type of malfunctioning or failure. The growing importance of collaboration and networking, together with the growing adoption of web-enabled applications and the diffusion of mobile solutions, is pushing companies to share data along extended value chains. There is an inevitable correlation between security investments and investments in collaborative data sharing technologies.

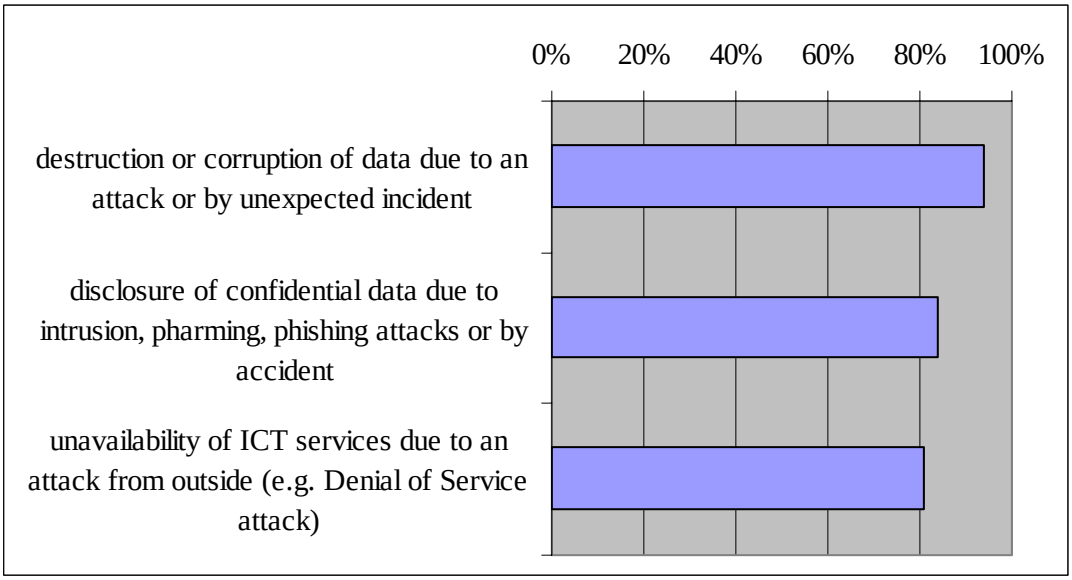
Large and small enterprises differ in their take-up of ICT and eBusiness: Large enterprises (those with 250 or more persons employed) take up ICT more intensively than SMEs and hence experience security issues in a different way. The following section reviews the security policy of large firms. A separate paragraph is afterwards dedicated to the characteristics of SMEs.

5. LARGE EUROPEAN ENTERPRISES' ICT SECURITY POLICY

Enterprises' concerns regarding security risks are addressed by the implementation of specific security policy with a plan for regular review. A majority of large European enterprises have such a policy (65% in 2010).[4] Almost all of them consider the risk of data destruction or corruption, due to an attack or any other unexpected incident. But two other important risks are very often also addressed: the disclosure of confidential data and the unavailability of ICT services due to an explicit attack from outside. Three quarters of ICT security plans address all three of these risks (Figure 6).

[4] Manufacturing and services, excluding the financial services.

Figure 6: **Risks addressed by ICT security policy or plans of large enterprises having ICT security policies, EU27, in % of large enterprises**



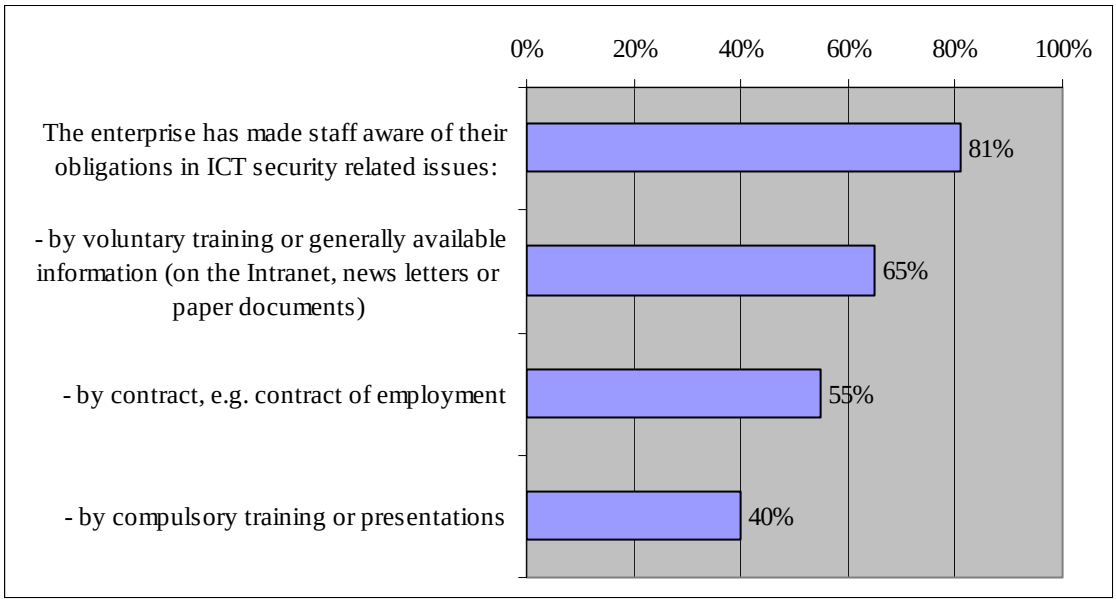
Source: Eurostat, Community Survey on ICT Usage and eCommerce in Enterprises

Nevertheless, 35% do not have a regularly reviewed security policy. They are particularly concentrated in PL, RO and BG (more than 60% of the large enterprises of these countries). But many of them are also in Germany where 19% of all large European enterprises are located. However, this does not mean that nothing is being done about security in these firms. Companies may have adopted security measures and initiatives that are not regularly reviewed, including technical measures and procedures involving employees (firewalls, new passwords, etc.).

With regard to technical measures, 61% of large enterprises **logged activities for analyses of security incidents** and 72% **stored data backups offsite**. The other very common and effective measure is to control and secure the access to the IT infrastructure. Coherently with the other indicators, 73% of large enterprises declare to use **strong password authentication** (i.e. min 8 characters, max 6 months, encrypted transmission and storage). 31% make use of **hardware tokens, e.g. smart cards**, for user identification and authentication. **Biometric methods** are still less diffused with around 10% of large enterprises using them at the beginning of 2010. Half of the companies that use strong authentication passwords or tokens/smart cards are also making use of **digital signatures** in some of the messages sent (39% of large enterprises). Finally, 21% of large enterprises use **secure protocols**, such as SSL or TLS, for reception of orders via internet.

For compliance with security measures and diffused vigilance, the involvement of employees has an important role to play in terms of the effective implementation of technological and procedural rules. This starts with making staff aware of their obligations regarding ICT security related issues. 81% of large enterprises are active on this front, to a large extent with relatively soft measures such as disseminating information on the Intranet or including security related norms in the contracts of employment. Compulsory training or presentations are relatively less common (40% of large enterprises). Often the approach adopted is a mix of these measures.

Figure 7: **Approaches adopted by enterprises to raise employees awareness, in % of large enterprises.**



EU27 without EE

Source: Eurostat Community Survey on ICT Usage and eCommerce in Enterprises

The lowest rates of awareness raising initiatives are observed in PL, LU, BG and HU, around 20 pp less than EU average.

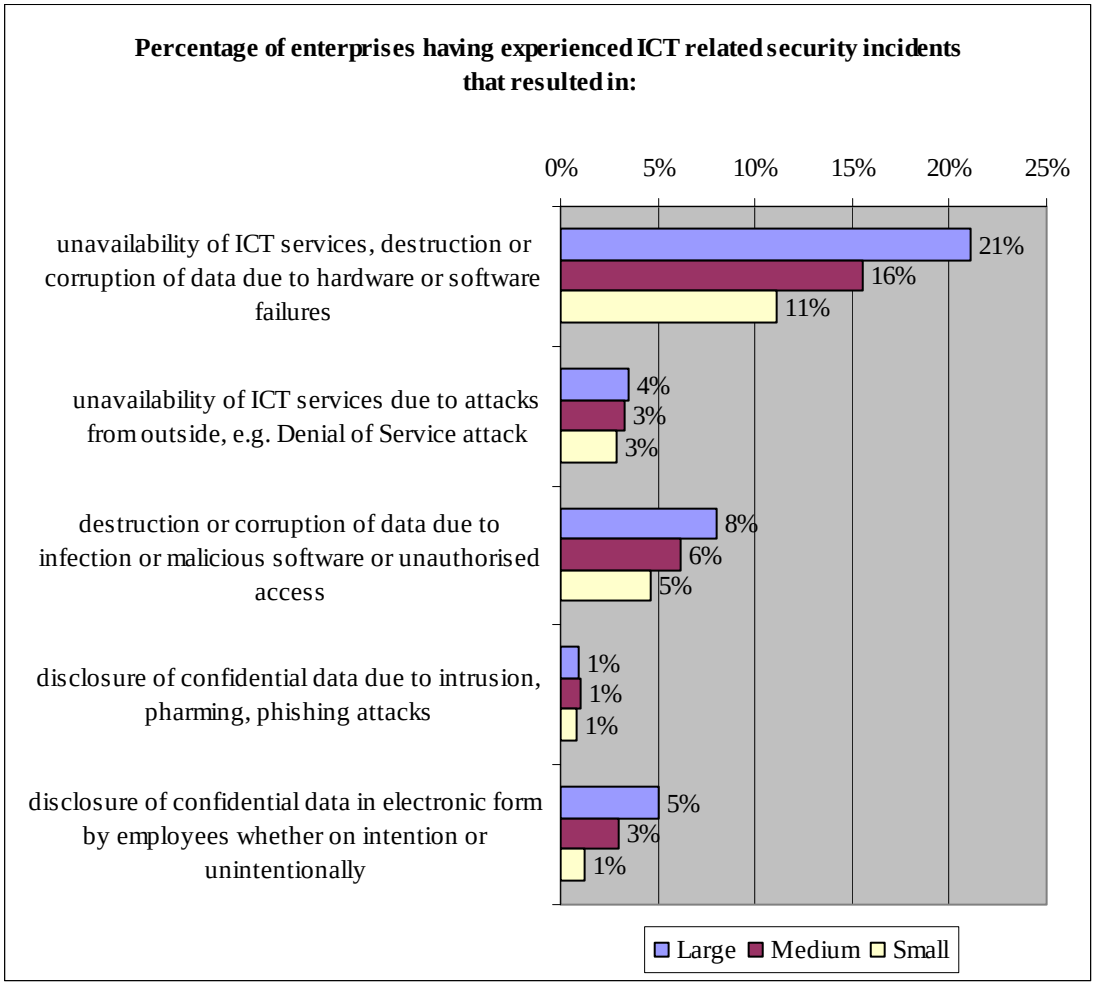
As such it can be concluded that large European enterprises are quite active in the security domain and a large majority of them are deploying the basic tools to protect the integrity, authenticity, availability and confidentiality of their data and IT systems. They are surely the main active consumers on the European network and security market, whose value has been estimated to reach between 10 and 15 billions of euros in 2010[5].

6. ICT SECURITY INCIDENTS REPORTED BY ENTERPRISES

It is very difficult to judge if the investment of European companies in IT security (hardware, software and services) is effective or sufficient. The most frequently reported breaches in 2009 concern the destruction or corruption of data, due to internal hardware/software failure or, to a lesser extent, due to malicious software or unauthorised access (Figure 8).

[5] IDC study

Figure 8: **Security breaches experienced during 2009, by size of enterprises**



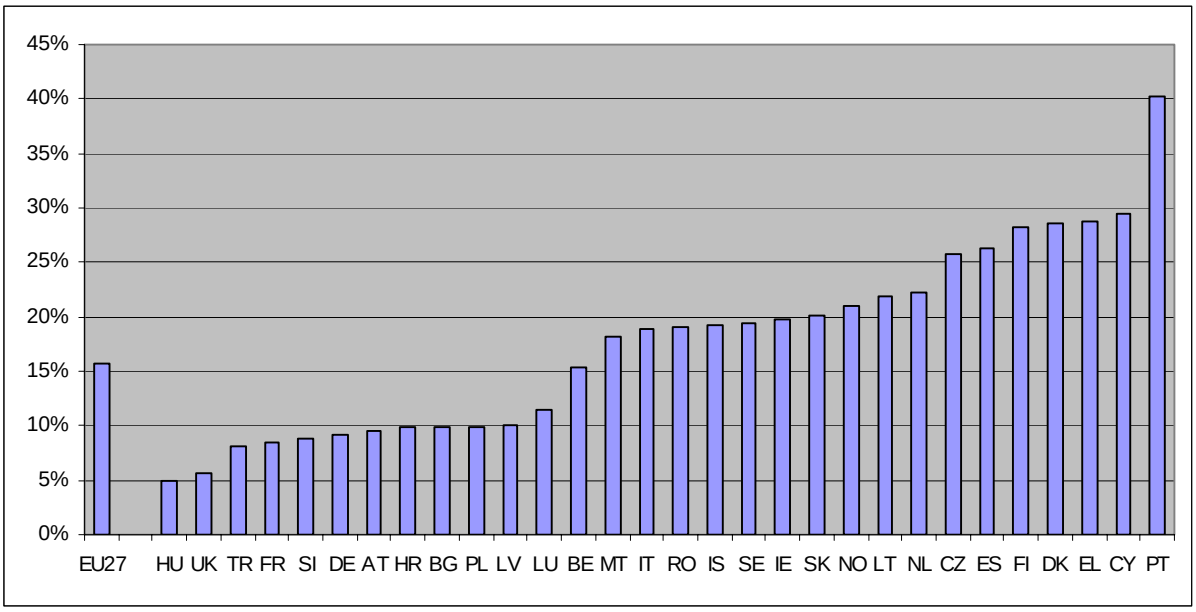
EU27 without EE

Source: Eurostat Community Survey on ICT Usage and eCommerce in Enterprises

Data in figure 8 should be interpreted with care. On the basis of observations by Internet Service Providers and network operators, security market experts consider that these types of incidents are reported much less frequently than they actually take place in reality. The higher incidence of breaches in large enterprises could be the result of the more rich and complex IT networks and services they manage relative to smaller enterprises, but also of their higher capacity to register and report about attacks and failures.

Country-level analysis confirms the existence of a mix of factors that make it so difficult to interpret victimisation indicators in this field (Figure 9). Countries with advanced levels of ICT use such as FI and DK show similar incidence rates to PT and EL, probably for reasons which go beyond this kind of analysis.

Figure 9: **Enterprises having experienced any security incident during 2009, by country (%)**



EU27 without EE

Source: Eurostat Community Survey on ICT Usage and eCommerce in Enterprises

7. THE SPECIFIC CASE OF SMES, DEPENDING ON EBUSINESS SOLUTIONS ADOPTED AND BY COUNTRY

This chapter formulates a hypothesis related to the expected correlation between security investments and investments in collaborative data sharing technologies. The latter can be used for sharing information within the enterprise, or to exchange it with business partners. Two indices derived from the survey questionnaire allow the identification of companies with these characteristics, and thus to assess the intensity of that relation:

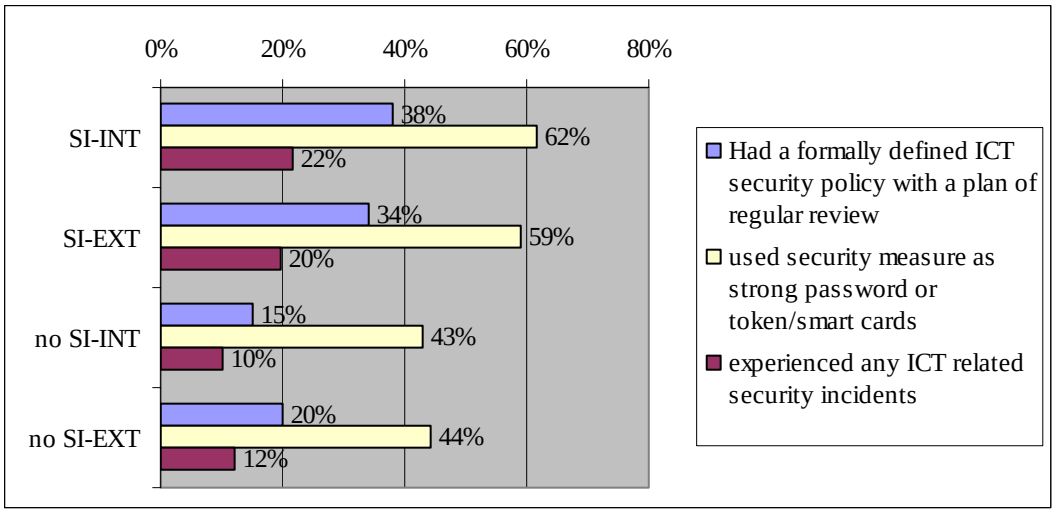
- SI-EXT is an index that identifies those enterprises that share electronically information suitable for automatic processing (as EDI, XML formats) with external business partners, suppliers or customers; 48% of all EU enterprises fall into this category;

- SI-INT is an index that identifies those enterprises that share electronically information within the enterprise, between different functions (through a common data warehouse or an ERP); 50% of all EU enterprises share this characteristic[6].

[6] The two indexes overlap, as 31% of all 10+ enterprises exploit eBusiness solutions that allow them to share information electronically both internally and externally with business partners. There are companies that use software only for automation and sharing internally (it is mostly the case of medium size enterprises), but also others using it only or mainly for the exchanges with external partners (often the case for small enterprises that doesn't require a sophisticated internal structure). There is a remaining group of 29% of all EU enterprises using none of these eBusiness tools, having computers and internet

The profiles presented in figure 10 relate to all 10+ enterprises, but due to the much higher number of small and medium enterprises compared to large ones in the sample, they can be interpreted as describing quite well the former patterns[7]. The comparison is carried out using three key indicators already presented in the previous paragraphs.

Figure 10: **Security issues compared to the adoption of eBusiness solutions (% of enterprises)**



Source: Eurostat Community Survey on ICT Usage and eCommerce in Enterprises

Formal ICT security policies/plans are adopted by more than a third of enterprises that have adopted structured eBusiness solutions. This represents half of the adoption rate of large enterprises, but twice the rate of those enterprises without intense sharing of information with internal functions or with business partners outside.

Security measures such as a strong password authentication (min 8 characters, max 6 months, encrypted transmission and storage) or via hardware tokens/smart cards are widely exploited also by enterprises without an eBusiness infrastructure (around 44%). These measures could be effectively justified to manage a simple website supporting eCommerce activities or also to protect little pieces of software for account or machinery control. These types of security measures were never the less more used by of large enterprises (77%).

Finally, as highlighted in the preceding paragraph, a much higher incidence of security breaches is observed in those enterprises that make higher use of ICT-based business solutions; twice as much as in the less equipped companies. Interesting to note is that in this case the gap with large enterprises is smaller (25% of them report security incidents, similar to the 20-22% of SME sharing information electronically).

connections, but for simpler usages as managing accounts, searching information on the web or managing a simple website.

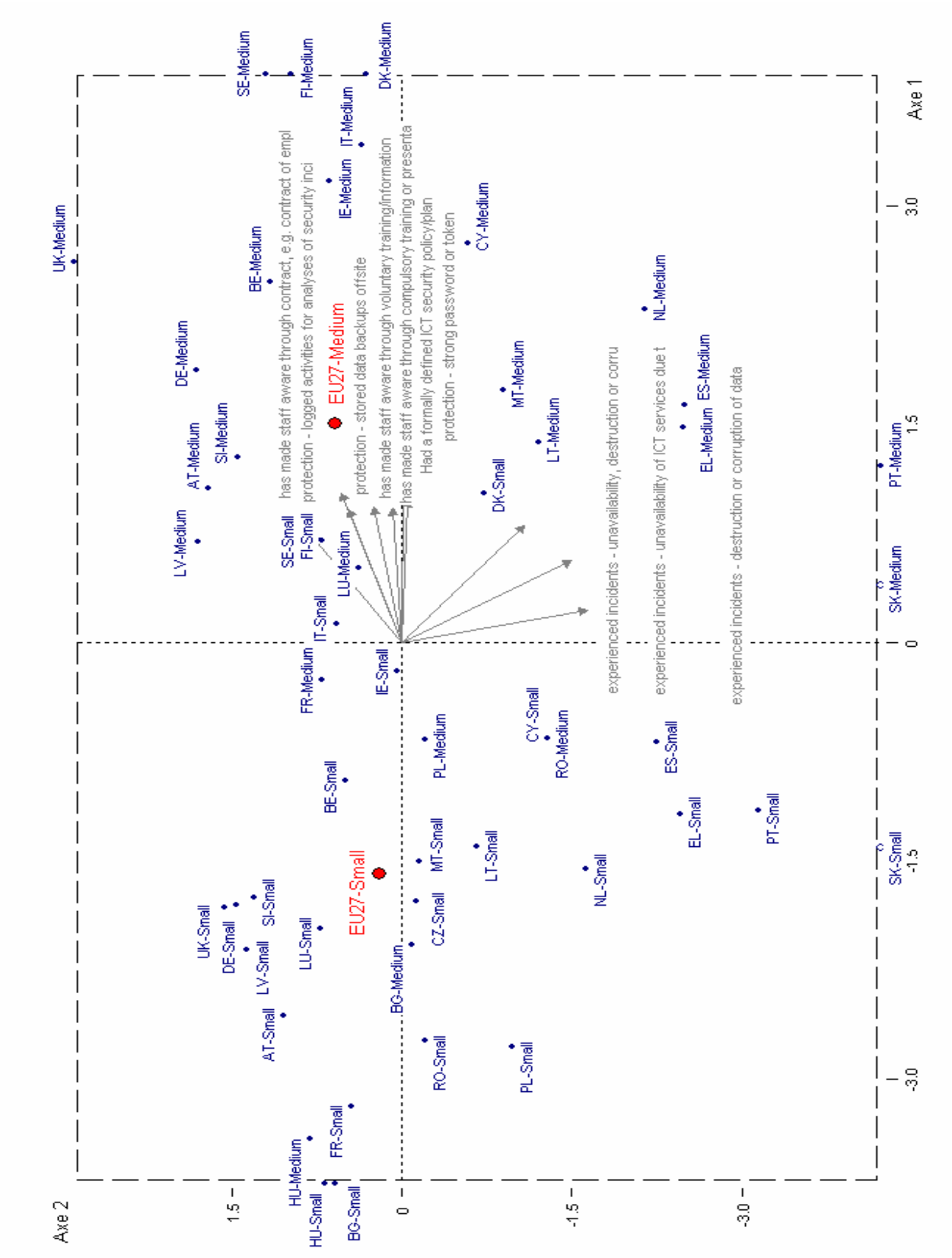
[7] The survey refers to a universe of around 1.5 million enterprises with 10 persons employed or more, without the financial sector. More than 80% are small enterprises with 10 to 49 employees, 14% are medium with 50-249 employed persons, and the remaining less than 4% are large enterprises. The latter category employs anyway 47% of the corresponding workforce (medium 24% and small enterprises 29%).

A synthetic profile has been constructed separately for the small and for the medium size enterprises of each country. The profile includes the key variables concerning protection: having a specific policy/plan, initiatives for awareness raising of staff, logging of incidents, offsite backups, strong passwords and tokens; and three indicators concerning breaches: destruction/corruption of data due to incidents, due to infections/intrusion and unavailability of ICT services due to attacks from outside. Figure 11 illustrates the main similarities and differences between those country specific profiles[8]. The horizontal axe (axe 1) summarises the degree of protection and the vertical one (axe 2) the security breaches' variables. In particular:

- the top right hand quadrant refers to companies implementing a higher than average degree of protection and declaring having experienced security breaches less frequently than average; these are mostly medium sized enterprises;

[8] It is the result of a principal component analysis of the correlation matrix between the mentioned 10 variables.

Figure 11: **Security issues compared to the adoption of eBusiness solutions (% of enterprises)**



Source: Eurostat Community Survey on ICT Usage and eCommerce in Enterprises

- the bottom left hand quadrant refers to companies implementing a lower than average degree of protection while declaring having experienced security breaches more frequently than average; these are mostly small size enterprises.

- the profiles of the medium sized enterprises of European countries are much more similar between them (they mostly lay on the right-hand side of the graph), than with the profiles of the small enterprises (left-hand side);

- The only exceptions are: medium companies in HU, BG, PL and RO are much more similar to EU average of small ones; and at the opposite, small enterprises from SE, FI and DK have a security profile similar to the one of medium enterprises;

- in the bottom left part are the medium size enterprises with the highest reported rate of incidents and attacks: SK, PT, EL, ES, NL. Also the small companies of these countries report high rate of breaches.

- country profiles in the top part of the graph present the lowest rates of reported victimisation: UK, DE, AT, LV, SI.

The analysis confirms also that strong correlations exist between the degree of adoption of security protection measures and the use of eBusiness solutions, mainly for the electronic/automated exchange of information within the enterprise (the index SI-INT has a correlation of 0.8 with the first horizontal axe).

8. SECTOR ANALYSIS

The economic sectors characterised by an important share of large enterprises are also those investing more in security plans, compulsory training of their staff and other protection measures[9]. Around 10% of large enterprises have introduced biometric methods for user identification (compared to an EU average of 3% of all enterprises). These efforts go together with the higher reporting of security incidents (almost the double than the average), both because these companies are best equipped to report about them and because they are more exposed to cyber crime and cyber attacks. This is the case for telecommunication, financial services, and other ICT sector enterprises.

Particularly concerned are also the enterprises within the content economic sector having publishing activities; motion picture, video & television programme production, sound recording & music publishing; programming & broadcasting. They are at the top for incidents involving the destruction-corruption of data by malicious software/intrusion, or the unavailability of ICT services due to attacks from outside, or for incidents due to hardware or software failures. But they are less frequently protecting themselves than the telecom or the financial services' enterprises.

[9] More detailed information about the characteristics of the main economic sectors is available in the Eurostat publication Statistics in Focus n 7/2011: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-11-007/EN/KS-SF-11-007-EN.PDF

Quite active on the security protection front are also the enterprises of the professional, scientific and technical activities sector, travel agencies and tour operators, which are also intensive ICT users despite generally being small size companies. Their tools are less sophisticated than those used by large enterprises: strong passwords and backup. Security breaches are just above average.

The opposite profile of scarce investment on security measures concerns sectors traditionally consuming less ICT solutions, such as Construction, or less exposed/concerned by security risks, as those manufacture sectors dominated by small enterprises.

9. CONCLUSION

Security concerns are confirmed to be an important and diffused concern among internet users that affect their trust in the internet. If the fact that a lot of citizens refrain from exchanging personal information could be interpreted as a signal of growing maturity in terms of a more critical approach to the internet, the defection from eCommerce, eBanking and eGovernment services indicates the need for a reinforced effort to promote security.

The results also suggest the relevance of the mismatch between risks/concerns/protection and the inadequacy of skills. The level of concerns and the efforts to protect, by enterprises and citizens, seem not always appropriate to the risks. For individual users a problem of skills is certainly present. Market products, but also public policies, have a role to play to make protection tools and secure behaviours on the net more understandable so as to really empower all internet users. In any case, security is a challenge for both, the more and the less advanced users and countries.

The analysis has not been able to assess if the security of internet users is better or worse than some years ago, but the indicators presented could be re-used in the following years to track any change and evolution and to monitor possible impacts of the policy initiatives that will be adopted by all the concerned stakeholders.

10. ANNEX – METHODOLOGICAL NOTES AND REFERENCES

Background characteristics of the individuals

- the population interviewed in 2010 is a sample of individuals aged 16-74 years resident in the Member States of European Union.
- 71 % have used internet during last year
- **69 %** have used internet during last 3 months (**Internet users**)
- 65 % are regular internet users = at least weekly
- 53 % use internet daily

The questions about security issues have been proposed only to those 71% of all individuals having used the internet during last year (i.e. the last 12 months prior to the survey, in general the second quarter of 2010). The majority of them, 91%, is composed of regular users (at least weekly). 6% of them used internet irregularly during last 3 months and a 3% used it more than 3 months ago. For some rare items it could be relevant to check if these answers come from this minority or from the large majority of regular users, but this cannot be controlled in the database and require an ad hoc analysis of microdata, to be requested to Eurostat if the case.

- Where do internet users have accessed internet (last 3 months) ?
  - 92% have done it at **home** (and 38,5% only at home)
    - and 78% of retired and inactive accessed internet only at home
  - 41% have done at **work**, other than home (and 3% only at work)
    - but this go up to 60% of employees and self employed (“only at work” remain a rare case valid for 4% of working people)
  - 12% at place of **education**
    - this go up to 71% for students (only at place of education remain a rare case, for only 2% of students)
  - 23% in other **people's houses** (2% only in other people's houses)
  - 14% in **other** places (1% only in other places)

- Which devices do internet users used (last 3 months) ?
  - 39% use a mobile device: a mobile phone, a handheld (PDA) or a portable computer; with or without also a fixed device. Inside this group it is possible to distinguish:

- 20% use a mobile phone (11% without a laptop)
    - 11% use a mobile phone with 3G, and 11% a mobile phone via GPRS
- 27% use a portable computer (away from home or work) (18% without mobile phone)
    - 9% use mobile phone and laptop
- 4 % use a handheld computer such as a PDA