Worldwide Headquarters: 7600 Leesburg Pike, East Building, Suite 310, Falls Church, VA 22043, USA P.703.485.8300 F.703.485.8301
www.government-insights.com

SMART 2007/0005

Survey and Analysis of EU ICT Security Industry and Market for Products and Services

D.7.2 Final Study Report The Evidence Base - Demand Analysis

IDC Government Insights

April 2009

SMART 2007/0005

Survey and Analysis of EU ICT Security Industry and Market for Products and Services

D.7.2 Final Study Report
The Evidence Base – Demand Analysis

The opinions expressed in this Report are those of the authors and do not necessarily reflect the views of the European Commission.

Author(s)	IDC European Competitiveness and Innovation Expertise Centre – Government Insights
Deliverable	7.2 Draft Final Study Report: The Evidence Base – Demand Analysis
Date of delivery	30 April 2009
Version	1.0
Addressee officers	Gerard Galler European Commission Information Society & Media DG Unit A3: Internet; Network and Information Security Office BU33 05/087, 33 Avenue Beaulieu, B-1160 Bruxelles Tel: +32 2 299 93 55, e-mail: gerard.galler@ec.europa.eu
Contract ref.	Contract Nr 30-CE-0150192/00-00

TABLE OF CONTENTS

P

1 INTRODUCTION 1

This Report 1
The Main Drivers of Business Demand 2
Security Solutions and Business Market Segmentation 3

2. The EU NIS Market Clusters 6

Overview by Cluster 6
- Cluster 1, the Champions 7
- Cluster 2, the Pillars 8
- Cluster 3, the Runners-up 8
- Cluster 4, the Learners 8

Fears, Perceived Level of Protection, and Security Breaches 11
- Main Fears 11
- Perceived Protection against IT threats 13
- Significant IT Security Breaches 16

Main Trends of IT Security Spending and Future Plans of Adoption 17
Mobile Security Solutions Adoption 21
Relationship with Suppliers: Selection Criteria and Satisfaction 23
- Main Procurement Channels by Cluster 27

3 The NIS Business Users Profiles in the EU Market 31

Overview of the Business Users Profiles 31
- Low NIS Investment Business Users 34
- Average NIS Investment Business Users 34
- High NIS Investment Business Users 35

Fears and Perceived Protection by User Profile 36
- Security Breaches by Business User Profile 39

Main Trends of IT Security Spending and Future Plans of Adoption 39
Mobile Security Adoption by Profile 42
Relationship with Suppliers: Criteria of Selection and Satisfaction 44
- Main Procurement Channels by Profile 47

4 The EU NIS Market by Industry 49

Overview by Industry 49
- Manufacturing 49
- Services 50
- The Public Sector: Government, Healthcare, Education 52
- Finance 53

Fears, Perceived Protection and Security Breaches by Industry 54
Main Trends of IT Security Spending and Future Plans of Adoption by industry 58
Mobile Security Adoption by Industry 63
The relationship with Suppliers: Selection criteria and Satisfaction by industry 65
- Main Procurement Channels by Industry 68

5. The European Security Market by Company Size 70

Overview by Company Size 70

TABLE OF CONTENTS — Continued

P

Fears, Perceived Protection and Security Breaches by Company Size ... 72
Security Breaches by Company Size ... 75
Main Trends of IT Security Spending and Future Plans of Adoption ... 77
Mobile Security Solutions Adoption by Company Size ... 81
Relationship with Suppliers: Selection Criteria and Satisfaction by Company Size ... 83
Main Procurement Channels by Company Size ... 87
Towards "Security as a Service" for SMEs ... 89

6 The Survey of the EU NIS Business Users 92

Description of the Business Users Sample ... 92
The profile of Business Survey Respondents ... 94

7. The Analysis of Consumer Demand 97

Overview of NIS Consumer Users ... 97
Consumers' Perception and Experience of Security Threats ... 101
Awareness and Concern ... 101
Impacts of Security Concerns on Internet Usage ... 103
Security Breaches, Damages and Reactions ... 105
Current Adoption of IT Security and Perceived Protection ... 109
Mobile Security for Consumers: Main Fears and Solutions adopted ... 112
Main Trends of IT Security Spending and Plans of Adoption ... 114
Relationship with Suppliers: Criteria of Selection and Satisfaction ... 117
Main Procurement Channels ... 120

8. The EU ICT Security Consumer Market Survey 122

Overview ... 122
Description of the Consumers Sample: Socio-demographic Characteristics ... 123

LIST OF TABLES

		P
1	The EU NIS Business Market segmented in clusters	7
2	Low, Average, High NIS Investment Businesses: Distribution by Cluster (% of enterprises)	33
3	Low, Average, High NIS Investment Businesses: Distribution by Company Size (% of enterprises)	33
4	Low, Average, High NIS Investment Businesses: Distribution by Industry Sector (% of enterprises)	33
5	Business Survey: Number of Interviews by country, industry and company size	92
6	Business Survey: Weighted distribution of respondents by country and industry	93
7	Business Survey: Weighted distribution of respondents by company size and industry	94
8	Business Survey: Respondents' Job title by company size	95
9	Business Survey: Respondents' Job title by country	96
10	The EU NIS Consumer Market Clusters	123
11	Consumer Survey: Number of Interviews by Country and Age	123

LIST OF FIGURES

		P
1	EU Business Users, Current Adoption of Security Solutions (% of enterprises)	5
2	EU Business Users, Current Adoption of Security Solutions, by Cluster (% of enterprises)	10
3	EU Business Users, Fears related to IT Security, by Cluster (Mean rating)	12
4	EU Business Users, Perceived Protection related to IT Security, by Cluster (Mean rating)	15
5	EU Business Users, Companies that Experienced a Significant IT Security Breach in the Last Year, by Cluster (% of enterprises)	17
6	EU Business Users, Trends of IT Security Spending, by Cluster (% of enterprises)	18
7	EU Business Users, IT Security Products Future Adoption Plans, by Cluster (% of enterprises)	20
8	EU Business Users, IT Security Products for Mobile Users Current Adoption, by Cluster (% of enterprises)	22
9	EU Business Users, Protection of Personal Mobile Tools, by Cluster (% of enterprises)	23
10	EU Business Users, Criteria of Selection of Primary IT Security Provider, by Cluster (Mean rating)	26
11	EU Business Users, Satisfaction with Primary IT Security Provider's Performance, by Cluster (Mean rating)	27
12	EU Business Users, Procurement Channels of IT Security Products, by Cluster (%of enterprises)	30
13	EU Business Users, IT Security Products Current Adoption, by Profile (% of Enterprises)	32
14	European Union, Fears related to IT Security, by Profile (mean rating)	37
15	EU Business Users, Perceived Protection related to IT Security, by Profile (Mean rating)	38
16	EU Business Users that experienced a Significant IT Security Breach in the Last Year, by Profile (% of positive answers)	39
17	EU Business Users, Trends of IT Security Spending, by Profile (% of enterprises)	40
18	EU Business Users, IT Security Products Future Adoption Plans, by Profile (% of enterprises)	41
19	EU Business Users, Current Adoption of IT Security Products by Mobile Users, by Profile (% of enterprises)	43
20	EU Business Users, Protection of Personal Mobile Tools, by Profile (% of enterprises)	44
21	EU Business Users, Criteria of Selection of the Primary IT Security Provider, by Profile (Mean rating)	46
22	EU Business Users, Rating of Primary IT Security Provider's Performance, by Profile (mean rating)	47
23	EU Business Users, Main Procurement Channels of IT Security Products, by Profile (% of enterprises)	48
24	EU Business Users, Fears related to IT Security, by Industry, (mean rating)	56
25	European Union, Perceived Protection related to IT Security, by Industry (mean rating)	57
26	EU Business Users that Experienced a Significant IT Security Breach in the Last Year, by Industry (% of positive answers)	58
27	EU Business Users, Trends of IT Security Spending, by Industry (% of enterprises)	59
28	EU Business Users, IT Security Products Current Adoption, by Industry (% of enterprises)	61

LIST OF FIGURES — Continued

P

29 EU Business Users, IT Security Products Future Adoption Plans, by Industry (% of enterprises) 62
30 EU Business Users, IT Security Products for Mobile Users Current Adoption, by Industry (% of enterprises) 64
31 EU Business Users, Protection of Personal Mobile Tools, by Industry (% of enterprises) 65
32 EU Business Users, Criteria of Selection of Primary IT Security Provider, by Industry (Mean rating) 67
33 EU Business Users, Satisfaction of Primary IT Security Provider's Performance, by Industry (mean rating) 68
34 EU Business Users, Main Procurement Channels of IT Security Products, by Industry (% of enterprises) 69
35 EU Business Users, Current Adoption of Security Solutions, by Company Size (% of enterprises) 71
36 EU Business Users, Fears related to IT Security, by Company Size (mean rating) 74
37 EU Business Users, Perceived Protection related to IT Security, by Company Size (mean rating) 75
38 EU Business Users that Experienced a Significant IT Security Breach in the Last Year, by Company Size (% of positive answers) 76
39 EU Business Users, IT Security Breach Reporting, by Company Size (%of enterprises) 77
40 EU Business Users, Trends of IT Security Spending, by Company size (% of enterprises) 78
41 EU Business Users, IT Security Products Future Adoption Plans, by Company Size (% of enterprises) 80
42 EU Business Users, Current Adoption of IT Security Products for Mobile Users, by Company Size (% of enterprises) 82
43 EU Business Users, Protection of Personal Mobile Tools, by Company Size (% of enterprises) 83
44 EU Business Users, Criteria of selection of Primary IT Security Provider, by Company Size (Mean rating) 86
45 EU Business Users, Satisfaction of Primary IT Security Provider's Performance, by Company Size (mean rating) 87
46 EU Business Users, Main Procurement Channels of IT Security Products, by Company Size (% of enterprises) 89
47 European Union, Security-as-a-service, by Company Size (% of enterprises) 91
48 Consumer Survey: Broadband Adoption, by Age (% of answers by age group) 98
49 Consumer Survey: Internet Usage, by Age (% of answers by age group) 100
50 Consumers and IT Security: Threats Awareness, by Age (% of positive answers by age group) 102
51 Consumers' Security Concerns, by Age (Mean rating) 103
52 Consumer Survey: Security Concerns Impacts on Internet Usage, by Age (% of answers by age group) 104
53 Consumers and Security Breaches, by Age (% of consumers by age group) 106
54 Damages Experienced by Consumers, by Age (% of consumers by age group) 107
55 Consumers' Reaction To Damages, by Age (% of consumers by age group) 108

LIST OF FIGURES — Continued

P

56 Consumer Survey: Current Adoption of IT Security Products/Services, by Age (% of consumers by age group) 110

57 Consumers' Perceived Protection Related to IT Security, by Age (mean rating) 111

58 Consumer survey: Internet via Mobile access: Security concerns (Mean Rating) 113

59 Consumer Survey: Protection of Mobile Devices (% of consumers by age group) 114

60 Consumers' Security Spending Distributed by Solution, by Age (% of answers by age group) 116

61 Consumer Survey, Future Adoption Plans, by Age (% of consumers by age group) 117

62 Consumers' Criteria for Choosing Security Solutions, by Age (% of answers by age group) 119

63 Consumers' Level of Satisfaction for Security Solutions, by Age (Mean rating) 120

64 Consumer Survey: Main Procurement Channels of IT Security Solutions, by Age (% of answers by age group) 121

65 Consumer Survey Sample by Gender 124

66 Consumer Survey Sample by type of Occupation 125

67 Consumer Survey Sample by level of Education 125

1 INTRODUCTION

This Report

The focus of this study is the Network and Information Security Market in the EU27. This report is part of the Final Study Report (**Deliverable 7.2: The Evidence Base: Demand Analysis**) produced by IDC EMEA for the study "Survey and Analysis of the EU ICT Security Industry and Market for Products and Services" on behalf of the European Commission, DG Information Society and Media.

This report presents the detailed results of the Business and Consumer Demand Analysis, on the basis of the main field research activities (survey of business and consumer users), extrapolated to represent the universe of EU businesses and citizens. These data represent part of the evidence base used to reach the conclusions and recommendations of the study. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

The other components of the Draft Final Study Report are:

- **D.7.1 – The EU NIS Market: Scenario, Trends and Challenges**, which presents the overall NIS market scenario, the main conclusions and recommendations of the study, and the set of indicators proposed to monitor the market. This report is addressed to policy makers and main stakeholders.

- **D.7.2 – The Evidence Base: Demand Analysis**, which presents the detailed results of the business and consumer demand analysis. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

- **D.7.3 - The Evidence Base: Supply Analysis**, which presents the detailed results of the supply analysis. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

- **D.7.4**: **The Evidence Base: Critical Issues Analysis,** which presents the detailed results of the qualitative analysis of the main critical issues for the development of the NIS market, carried out on the basis of desk research and interviews with a selected sample of stakeholders. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

The authors of the study are a multidisciplinary group of experts from multiple units of IDC EMEA and MIP Politecnico. The project manager is Gabriella Cattaneo, Director of IDC EMEA Competitiveness and Innovation Expertise Centre, part of IDC Government Insights. Eric Domage, IDC Security Research Manager,

Giuliana Folco, VP of IDC EMEA Industry Solutions Expertise Centre, and IDC CEMA (Central and Eastern Europe, Middle East and Africa) participate in the study team.

This report is structured as follows.

After the 1st chapter of Introduction, the 2nd chapter analyzes business demand by Cluster, the 3rd chapter by User Profile, the 4th chapter by Industry, the 5th chapter by Company Size. The 6th chapter presents the sample of the business users survey and the profile of respondents.

The 7th chapter presents the results of the Consumer Demand analysis, segmented by age, and the 8th chapter describes the sample of the consumer users survey and the profile of respondents.

The Main Drivers of Business Demand

Network and Information security (NIS) is one of the most important IT application areas for business users, both in terms of current adoption and future investments. Indeed, a combination of recurring and new factors has been pushing security to the top of the IT investment agenda of most enterprises for several years now. Main demand drivers include:

- Globalization is increasing the need of enterprises to improve efficiency in their processes, to gain competitiveness, and to protect their own information and knowledge as key assets. This raises the priority for security protection for companies of all size classes;
- The growing importance of collaboration and networking is pushing companies to share data along extended value chains. There is a strong correlation among security investments and investments in collaborative/data sharing technologies;
- The widespread adoption of the Internet as a computing and communications platform, with its inherent weaknesses in terms of data and privacy protection;
- The growing adoption of Web-enabled applications and solutions;
- The emerging acceptance of mobile solutions and the propagation of remote workers;
- The progressing regulatory environment, which calls for compliance with disparate rules;
- The volume of threats and their sophistication, which keeps on increasing;
- The absence or lack of effectiveness of companies' internal security policies. Most employees do not always follow security policies: the human factor is extremely important when dealing with security.

The effect of these factors has driven business users to the widespread adoption of basic security tools and an increasing adoption of advanced security solutions.

Security Solutions and Business Market Segmentation

The scenario of business demand in the EU is highly complex. Present and future demand trends vary depending on industry sector, company size, and the socioeconomic context of the market where business users operate. For this reason, the study analyzed the differences of business users behavior, choices and opinions, according to four main segmentations:

- Four Clusters of EU Member States with similar IT market development, to analyze the impact of the market context;
- Three main typologies of business users (High NIS investment, Average NIS investment, Low NIS investment) based on their portfolio of security solutions;
- Four industry sectors (Manufacturing, Services, Public Sector and Finance);
- Four company size classes (1 to 9 employees, 10 to 99 employees, 100 to 249 employees, and over 250 employees). This allows a specific focus on small and medium enterprises (SMEs, under 250 employees, corresponding to the EU classification), which are segmented in 3 of the 4 classes.

The differences between business users have been examined for each main segment focusing on the following main issues:

- Level of fears on main security threats, perceived protection and security breaches experienced;
- Current adoption of security services and future investment plans;
- Mobile security adoption;
- Relationship with suppliers: criteria of selection, satisfaction with performance, main channels of procurement (sourcing).

The starting point of the study is the portfolio of the most important security solutions and their diffusion (*figure 1*), which is structured as follows:

- **Threat Mitigation Tools** (Anti-virus, Anti-Spam, Anti-Spyware, URL & Web Filtering, Firewall, VPN,) Basic IT security solutions of this kind are adopted by the almost all the EU business users (96%) across all industries and all company size classes.
- **Business continuity** (Backup and recovery, Availability and Downtime services) Business continuity solutions are the second

most adopted solution (74% of EU enterprises) Very small companies (1-9 employees) have a below average adoption (55%). Adoption is instead highly above average in cluster 1 (84%) and in the finance sector (91%).

- **Information and data protection tools**. Products in this application area, including encryption, port control, strong authentication, data leakage prevention solutions, are adopted by 66% of EU enterprises. The finance and public sectors show above average values (78 and 74% respectively).

- **Security hardware** (Unified Threat Management, Email Security) is used by 65% of EU businesses. The finance and public sector are again the stronger adopters.

- **Specific tools for mobile users**. This type of solution is quite widespread, being used by more than half of the interviewed companies (52%). Also in this area there is a clear correlation between company size and level of adoption. In particular cluster 1 and 2 have above average adoption rates (56 and 58% of adoption respectively).

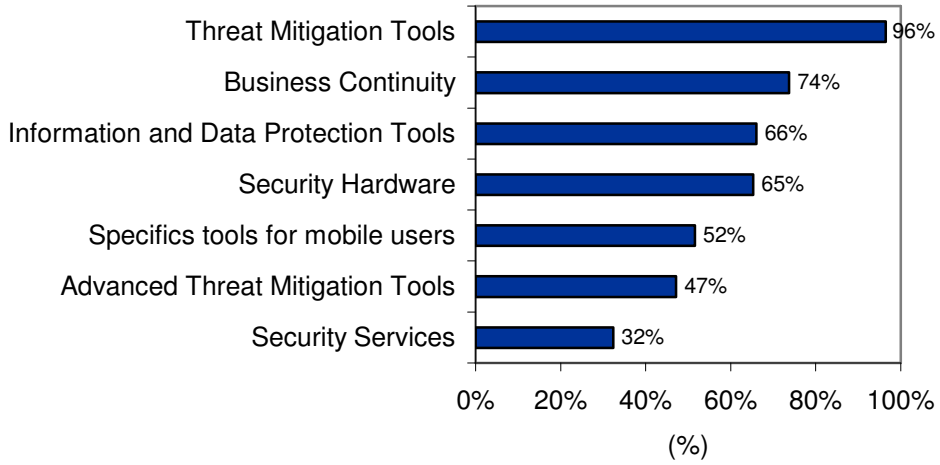
- **Advanced Threat Mitigation Tools**. (Anti-Phishing Web Reputational systems, Anti Intrusion Detection systems, Forensic collection, Internal Threat Management tools) These tools are presently adopted by 47% of users, but their diffusion is projected to grow fast (based on future plans).

- **Managed Security Services** are the least adopted solution, with a 32% of current use. They characterize the most advanced users and markets (see the analysis of Cluster 1).

FIGURE 1

EU Business Users, Current Adoption of Security Solutions (% of enterprises)

Q. Which of the following products has your organization implemented?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

The data presented in this report are extrapolated from the survey results, on the basis of a market model described in the methodology annex, and represent the universe of EU businesses and of EU citizens.

2. THE EU NIS MARKET CLUSTERS

Overview by Cluster

The EU NIS market is characterized by a wide variety of socio-economic conditions and IT dynamics, but the 27 Member States can be divided in four main groups (clusters) with broadly similar levels of IT spending, security market size and trends, and level of maturity. The clusters have been identified first of all on the basis of two significant parameters reflecting the development of their IT market, that is:

- Per capita IT expenditure;
- Percentage of IT spending on GDP.

The following chapter investigates the variations of business users' IT security strategies among the four main clusters of Member States, showing how the different socio-economic context and IT market conditions relate with their IT security choices. As explained in D.5.1 "The Key Messages" the clusters reflect also a different level of maturity of the NIS markets.

A key element for the differentiation of the MS Clusters was the identification of the three main typologies of business users (High NIS investment, Average NIS investment and Low NIS Investment users), on the basis of their portfolio of security solutions (see following chapter for more details). Advanced MS Clusters (Clusters 1 and 2) show a higher presence of High Investment users, while less advanced Clusters are characterized by more Low profile business users. The portfolio of security solutions analyzed by the study includes, in decreasing order by diffusion: Threat Mitigation Tools, Business Continuity solutions, Information and Data Protection Tools, Security Hardware, Specific tools for mobile users, Advanced Threat Mitigation Tools and Managed Security Services.

TABLE 1

The EU NIS Business Market segmented in clusters

CLUSTER 1 – THE CHAMPIONS	CLUSTER 2 – THE PILLARS	CLUSTER 3 – THE RUNNERS UP	CLUSTER 4 – THE LEARNERS
Denmark	Austria	Cyprus	Bulgaria
Finland	Belgium	Czech Republic	Estonia
Netherlands	Luxemburg	Hungary	Latvia
Sweden	France	Greece	Lithuania
UK	Germany	Italy	Malta
	Ireland	Portugal	Poland
		Slovenia	Romania
		Spain	Slovakia

Source: IDC Government Insights, 2008

Cluster 1, the Champions

Cluster 1 includes the Scandinavian countries, the Netherlands and the UK, well known as the most advanced IT and service-based economies. Confirming expectations, current adoption of advanced security products in this cluster is constantly above the EU average. In particular business continuity solutions, security hardware and security services are widely adopted (*see figure 1*). Cluster 1 is different from the others especially for the high level of adoption of security services: since this study defines the evolution towards security services as an indicator of maturity, this confirms again the more sophisticated profile of this group of Member States.

Within this cluster, the correlation between company size and level of adoption of IT solutions is very clear, with small enterprises (1-99 employees) consistently lagging behind the others. Mid-sized companies (100-249 employees) show a particularly high adoption of information and data protection tools and of security services. Future adoption plans are particularly bright concerning mobile security tools, while for more basic security products, which are already broadly adopted, future plans remain close to the EU average.

Despite being so advanced in terms of security products adoption, companies in this cluster do not show a high-perceived protection against potential security attacks. They are in general savvier about potential threats, and therefore also more realistic in assessing their protection level. Fears are mostly related to business interruption and to privacy breaches.

Cluster 2, the Pillars

France, Germany, Austria, Belgium/Luxembourg and Ireland compose cluster 2, which has a medium-high IT sophistication level. The level of adoption of security solutions is rather advanced, at the EU average or higher, with the exception of business continuity solutions, whose adoption is surprisingly lower (due to lower adoption in the mid-sized enterprises group). This cluster leads instead in the adoption of specific tools for mobile users and of advanced threat mitigation tools. Large companies with more than 250 employees drive this trend.

The level of perceived protection against main threats is highest in this cluster, with a majority of enterprises claiming to feel protected.

Cluster 3, the Runners-up

Cluster 3 is composed by Italy, Czech Republic, Spain, Slovenia, Portugal, Hungary, and Greece. These countries are characterized by IT sophistication and investment levels below the EU average and a high presence of SMEs.

From the point of view of IT security diffusion, this cluster shows a mixed panorama. Information and data protection tools are the most widespread. Also the adoption of security hardware and advanced threat mitigation tools is higher than the average. Instead the adoption of specific tools for mobile users and of security services remains below average levels.

Perceived protection is very low among companies in this cluster, who feel less protected than most of the enterprises in the other clusters. These business users show also a high fear score, particularly concerning the possible consequences of business interruption, such as revenue losses and negative impacts on the company reputation. This fear is high, even if many of these firms invest in business continuity solutions.

Still, the percentage of enterprises claiming security breaches remains well below the average in this cluster (only 5% against a EU average of 7%). The contrast between fears and low reported security breaches may depend on a lack of ability to monitor/recognize real attacks. Therefore these firms are probably aware that their IT security strategies are not advanced enough to insure tracking of risks and attacks, resulting in high fears and low perception of protection.

Cluster 4, the Learners

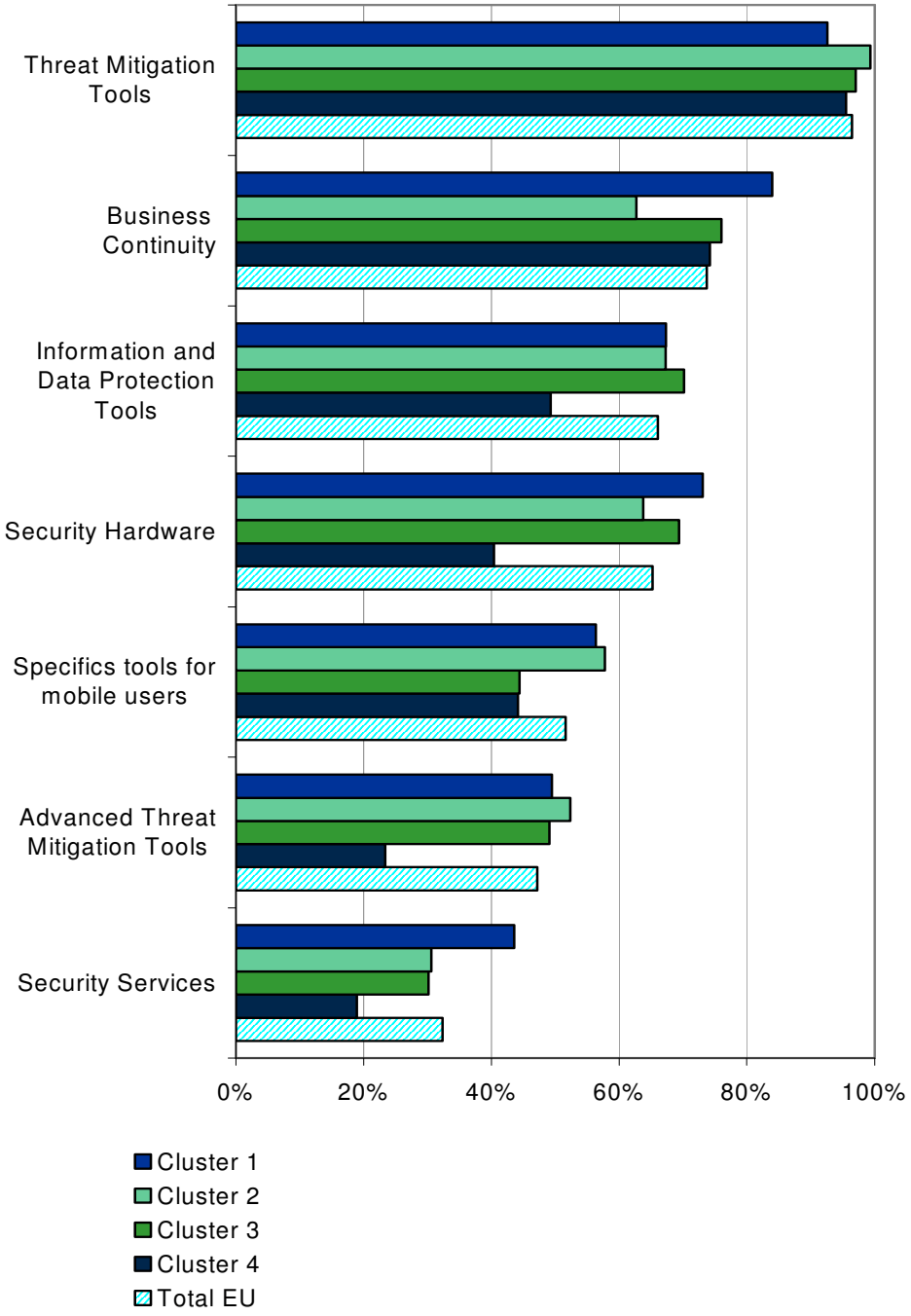
Cluster 4 is composed by Poland, Romania, Estonia, Slovakia, Latvia, Lithuania, and Bulgaria, countries starting from a low level of diffusion of IT. The security market in this cluster is clearly less developed than in the rest of Europe, and the business users profile is different from the other 3 clusters. The adoption of security solutions is high only for basic threat mitigation tools, and close to the average EU for business continuity solutions. Only a minority of enterprises use advanced threat mitigation tools and security services.

On the other hand, these countries are learning fast, with high rates of IT investment growth. In fact, 44% of the enterprises of this cluster are planning to increase their security spending in the next year (versus 35% EU average). More specifically, the percentage of enterprises planning to invest in information and data protection tools (15%), security hardware (13%) and advanced threat mitigation tools (17%) is roughly double the EU average.

FIGURE 2

EU Business Users, Current Adoption of Security Solutions, by Cluster (% of enterprises)

Q. Which of the following products has your organization implemented?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Fears, Perceived Level of Protection, and Security Breaches

Main Fears

The study measured business users fears and perceived protection on four main groups of IT security risks, namely:

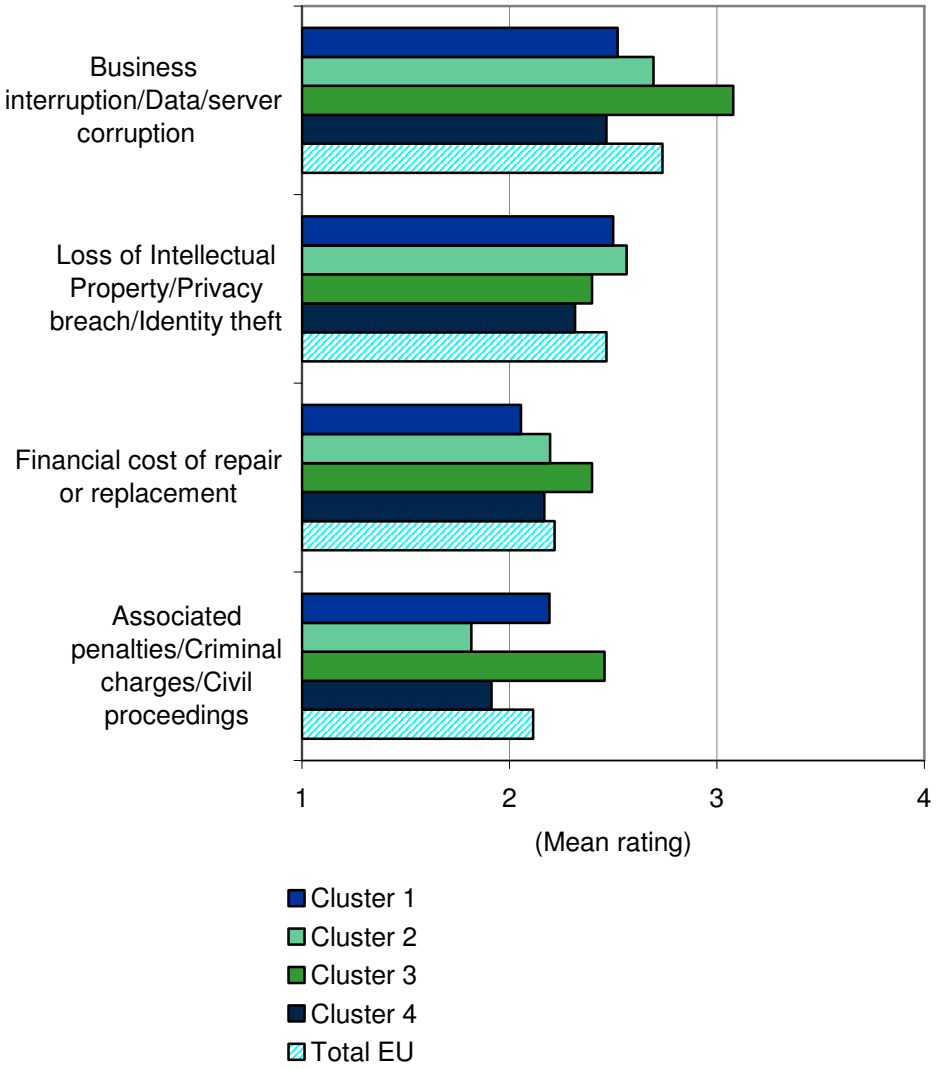
- Business interruption and/or data corruption and/or server corruption
- Loss of intellectual Property, Privacy breaches, or Identity Thefts
- Financial costs of repair or replacement (of missing or damaged data, or programs, for example)
- Associated penalties, criminal charges or civil proceedings

According to the survey results (*figure 3*), business users are only moderately worried about these risks, since their average level of concern is between "I am a little worried" (score 2) and "I am somehow worried" (score 3, in a scale of 1 to 4, with 4 being "I am strongly worried"). Concern is higher for Business interruption, followed by the other fears in descending order as shown in Figure 3.

FIGURE 3

EU Business Users, Fears related to IT Security, by Cluster (Mean rating)

Q. With respect to IT security, could you tell us what do you fear the most?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4= I am strongly worried

Source: IDC GI Survey of EU ICT Security Market, 2008

More in detail, analyzing results of fears related to IT Security ranking by cluster, we find the following:

- **Cluster 1 the Champions** Companies in this cluster are not extremely concerned about IT security as their fear levels score between 2.5 and 2.1 (where 2 means "I am a little worried" on a 1 to 4 scale). They fear in the same way business interruption and privacy breaches (2.5), while they fear relatively less issues related

to direct costs (cost of repair has been rated on average 2.1 while penalties 2.2).

- **Cluster 2 the Pillars** Companies in this cluster are slightly more concerned than those in cluster 1 for what regards business related problems scoring business interruption at 2.7 and privacy breaches at 2.6. For what is related to direct costs they are less concerned of suffering penalties (scored 1.8) than of having to pay the cost of repairs (scored 2.2). Still, fears of direct costs remain quite low.

- **Cluster 3 the Runners-up**. This cluster shows the highest levels of fears scoring the four areas between 3.1 and 2.4. In particular business interruption remains the main concern and is more emphasized by respondents in these countries, which give the highest score (3.1). The other three areas show a quite flat rating instead (between 2.4 and 2.5).

- **Cluster 4 the Learners** Countries pertaining to this cluster show quite low levels of concern. Firms in these countries do not know enough about IT security related problems, so their fear level is low as they do not understand potential threats.

Data show that there is no direct correlation between the cluster sophistication level and the fear related to IT security.

Perceived Protection against IT threats

The study measured the level of perceived protection against the same type of IT security risks selected to measure fears. They include business interruption, loss of intellectual property or privacy breach, financial cost of repair or replacement, or associated penalties, criminal charges, civil proceedings.

The perceived protection against IT security risks is moderate, according to survey results (*figure 4*). Most enterprises claim to feel "somewhat protected" (*corresponding to score 3 in a scale of 1 to 4*), without strong variations among the type of risks measured. A factor possibly influencing this evaluation is the role of the survey respondents, in majority IT managers, responsible for security investments. It is not so easy for these managers to allow that their security choices may not be sufficient to guarantee protection. On the other hand, they must underline the relevance of threats to justify security investments.

The variations by cluster are difficult to explain, as they are also strongly influenced by size and industry sector. However it is possible to present some considerations.

- **Cluster 1 the Champions**. Companies of cluster 1 declare to feel "somewhat protected" (score between 2.8 and 3.1). The highest score relates to business interruption. This score shows that sophisticated users with the more advanced monitoring tools do not perceive a high level of protection, but tend to be realistic about it. Cluster 1 shows for example the lowest level of perceived

protection against privacy breach risks (2.9 against an EU average of 3.1).

- **Cluster 2 the Pillars** Companies in this cluster declare a higher level of perceived protection than the average EU, even if they do not claim to feel highly protected (their scores range between 3.2 and 3.4). SMEs in this cluster declare a higher perceived protection, showing a mismatch between perception and reality (since this size class of enterprises suffer most breaches). Countries in this cluster have a strong presence of finance and manufacturing companies, whose perceived protection is higher than companies of the other industries: this may be a factor in the higher average score of this cluster.

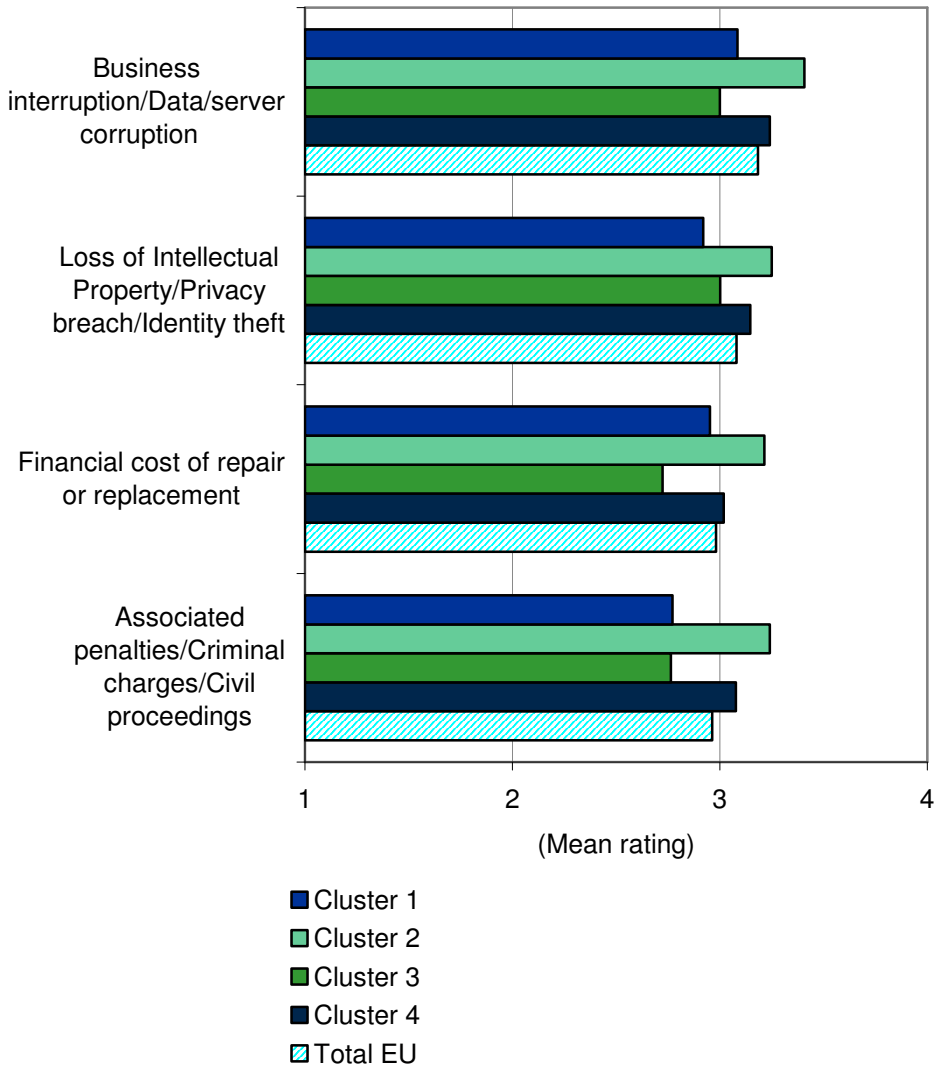
- **Cluster 3 the Runners-up**. The enterprises in this cluster of MS feel less protected than the other EU enterprises, rating their perceived protection at a consistently lower score than the other Clusters. The countries in this cluster (Southern European and dynamic Eastern European economies) have a strong presence of SMEs in all sectors, with a lower IT sophistication level and greater fears: this may be the reason for their lower confidence.

- **Cluster 4 the Learners**. Companies' perceived protection in this cluster is slightly above the EU average level, for all the risks measured. This corresponds to a relatively lower level of fears (*see figure 3 commented above*), but a high level of security breaches (*see figure 5 below*). Cluster 4 is characterized by less advanced IT maturity and many low profile business users; therefore the data may hide a lack of expertise in monitoring security risks and a misalignment between perception and reality.

FIGURE 4

EU Business Users, Perceived Protection related to IT Security, by Cluster (Mean rating)

Q. Could you provide us your feeling regarding your level of protection in each of the four areas? Do you feel protected/safe?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I do not feel protected and 4 = I feel highly protected

Source: IDC GI Survey of EU ICT Security Market, 2008

Significant IT Security Breaches

On average, approximately 7% of business users experienced a security breach in the last year (*see figure 5*). This percentage may appear low, when contrasted with the level of concern and widespread risk claimed by most IT security market experts. Market analysts, including IDC, believe in fact that the number of security breaches declared by enterprises is much lower than reality. The higher frequency of breaches is indicated by the observations of Internet Service Providers and network operators, as well as main vendors observatories (such as McAfee or Symantec and others). The low level of breaches declared depends on a combination of factors: on the one hand, many enterprises do not have the tools and experience to

monitor security breaches and are often unaware of their occurrence. On the other hand, only approximately 20% of EU enterprises have legal obligations to report security breaches, and even many of them do not bother to do so.

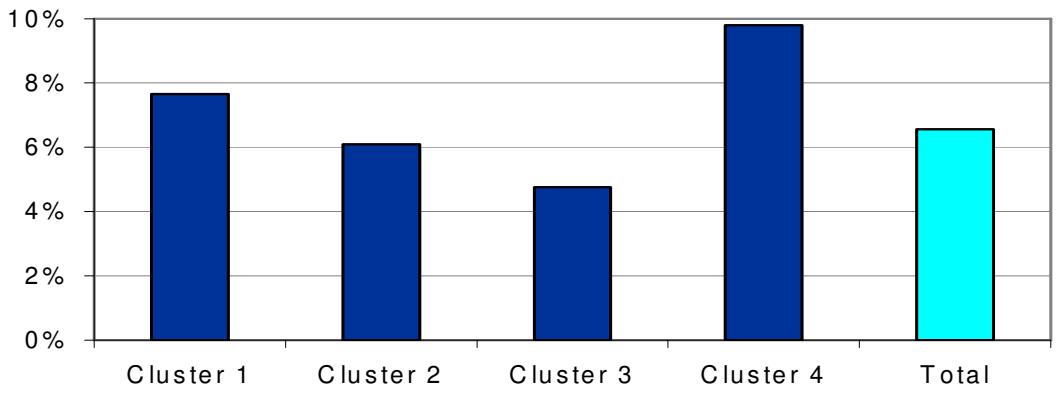
This said, there are significant variations by cluster of the number of enterprises declaring IT security breaches. The least advanced cluster (the Learners, cluster 4) shows a much higher presence of enterprises whose security was violated (almost 10%), contrasting with their higher than average perception of protection. Cluster 2 and particularly Cluster 3 instead show lower frequencies of security breaches.

The most advanced cluster (the Champions, cluster 1) also shows a percentage higher than the EU average of business users whose security was violated. This may be the result of a combination of factors. First, companies in these countries are usually more subject to attacks, as the intensity and scope of use of IT networks and services is more advanced. Second, their IT systems are more sophisticated and better able to trace security attacks. Enterprises with less sophisticated IT systems are more likely to experience attacks without knowing it.

FIGURE 5

EU Business Users, Companies that Experienced a Significant IT Security Breach in the Last Year, by Cluster (% of enterprises)

Q. Has your organisation experienced a significant IT security breach in the last year?



N = 1,180

Base = All sample

Source: Survey of EU ICT Security Market, 2008

Main Trends of IT Security Spending and Future Plans of Adoption

The business survey investigated the main trends of growth of IT security budgets in the near future as a whole (increase, decrease,

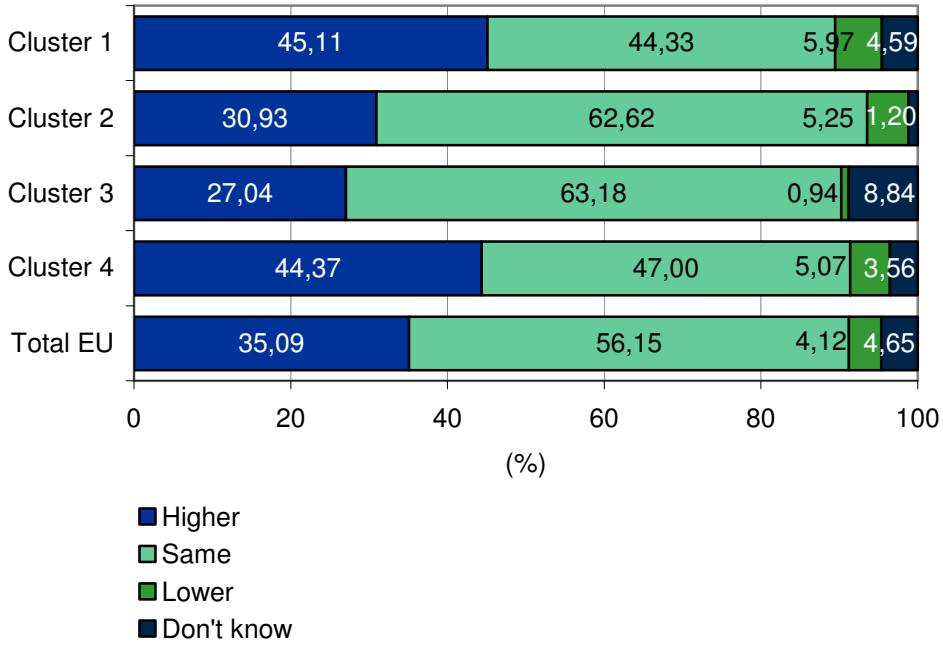
stability) and in terms of plan of adoption of security solutions. The percentage of EU enterprises planning a security budget increase (35%) is much higher than the percentage of those planning to decrease it (4%). Still, the majority of European companies plan to maintain a stable security budget (56%).

Interestingly enough, the most advanced (cluster 1) and the least advanced (cluster 4) show the highest percentages of businesses planning to increase their security spending. Still, the other two clusters show a higher number of users with stable spending, rather than decreased spending. The overall picture is quite positive in terms of demand growth (but the survey was made before the global financial crisis impacted the markets).

FIGURE 6

EU Business Users, Trends of IT Security Spending, by Cluster (% of enterprises)

Q. During 2008 how your IT security spending will change?



N = 1,138

Base = All sample

Source: Survey of EU ICT Security Market, 2008

In terms of plans of adoption in the next year, enterprises are focused on implementing advanced solutions (including Advanced Threat Mitigation Tools, Security Services and Mobile security tools) while very few business users plan to invest on business continuity or basic threat mitigation tools.

Investigating more closely the future plans of adoption by cluster leads to the following considerations:

- **Cluster 1**, **the Champions**. Enterprises planning to invest in advanced security solutions are more frequent in this cluster than EU average, particularly for specific tools for mobile users (12% of enterprises) and managed security services (10% of enterprises). This shows that the security market has not peaked yet, and there is room to grow even in the most advanced countries.

- **Cluster 2, the Pillars** In terms of current adoption, cluster 2 is very similar to cluster 1, but the percentage of firms planning new investments is relatively lower, showing less dynamism. On the other hand, almost 10% of enterprises in this cluster plan to invest in managed security services, which is higher than the EU average and an important signal of increasing sophistication in IT security adoption.

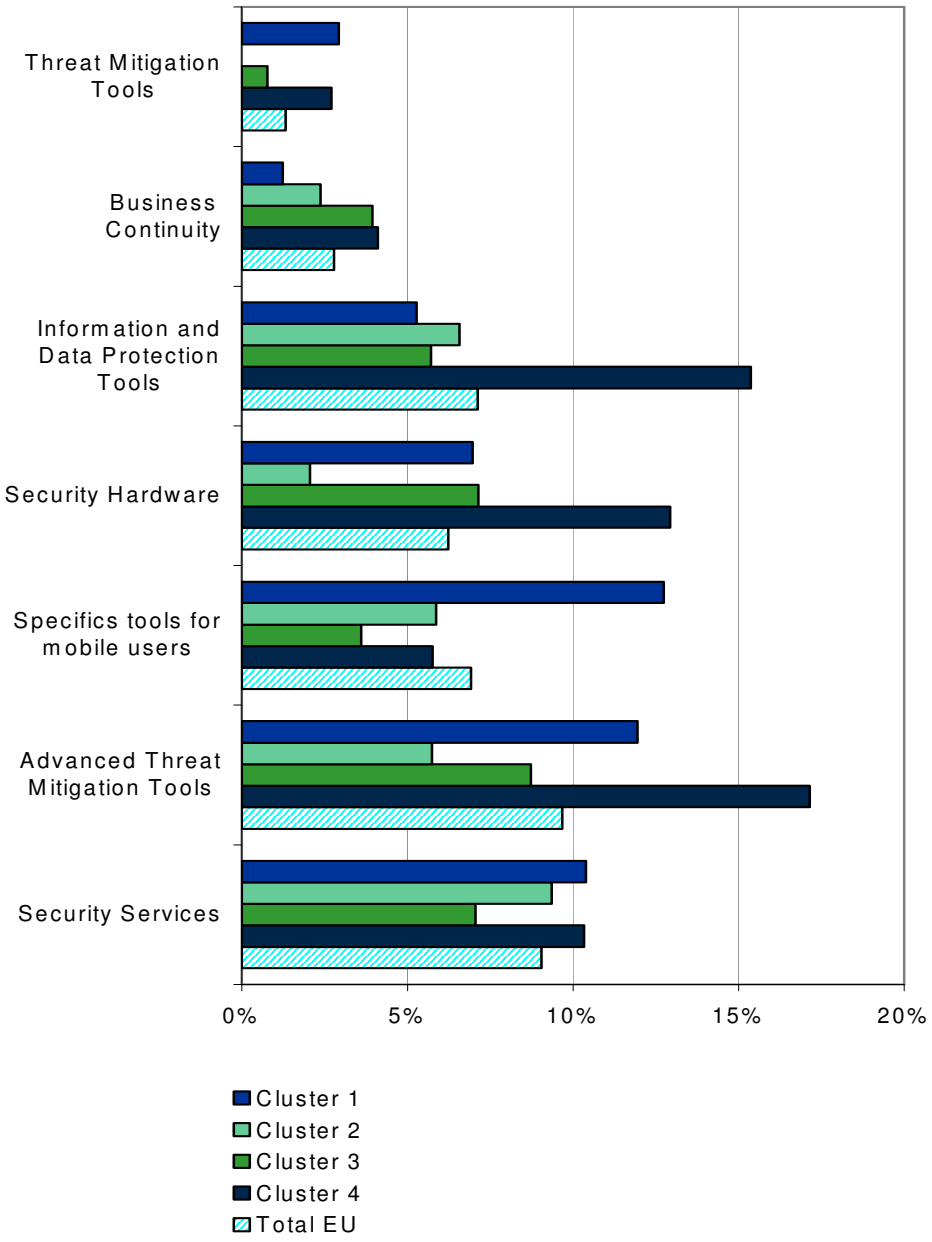
- **Cluster 3**, **the Runners Up** The percentage of enterprises of Cluster 3 planning new security investments is higher than the average EU level for business continuity solutions and security hardware. This may reflect the need to complete the IT security kit of the firm. For the other security solutions, future plans are near or lower than the EU average level.

- **Cluster 4**, **the Learners** Companies in these countries show a strong propensity to invest in information and data protection tools, security hardware and advanced threat mitigation tools. These companies show a propensity to invest well above the average EU and therefore a willingness to catch up with more advanced countries.

FIGURE 7

EU Business Users, IT Security Products Future Adoption Plans, by Cluster (% of enterprises)

Q. Of those products your company has not already implemented, which ones are you planning to implement in the next 12 months?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Mobile Security Solutions Adoption

The study shows that there is a relevant gap between the diffusion of mobile security solutions protecting employees' laptop computers,

which is rather advanced, and the more limited implementation of security for personal mobile tools, such as mobile phones and PDAs.

On this issue, there is a mismatch between supply and demand. Vendors tend to consider that mobile security should be operated in the network with "usual tools" (such as Firewalls, Threat mitigation, Identity Management). They do not provide advanced solutions for mobile tools, other than laptops. So existing security solutions for phones and PDAs are very limited, due to the lack of power in the mobile device, and also to the lack of willingness by users to pay more for security in this area. Security software is a high power consumption tool and must stay constantly connected for immediate patching. There is therefore a trade-off in energy use, on mobile devices, usually in favor of the user interface or communication functionality, over security.

Looking more closely at the market, data show that the majority of EU enterprises adopt security solutions for mobile computers in all clusters. The more advanced markets (clusters 1 and 2) show an extremely high rate of adoption of remote access security tools (92% and 94% of enterprises respectively). Interestingly, adoption of these solutions by mid-sized businesses (100-249 employees) is even higher than by large ones. End-point threat mitigation tools are widespread too, while specific backup & recovery solutions at the device level are relatively less diffused, but still adopted by more than 50% of users. Companies in cluster 2 show the highest adoption rate of backup & recovery solutions (61%), followed by companies in cluster 4 (60% of respondents).

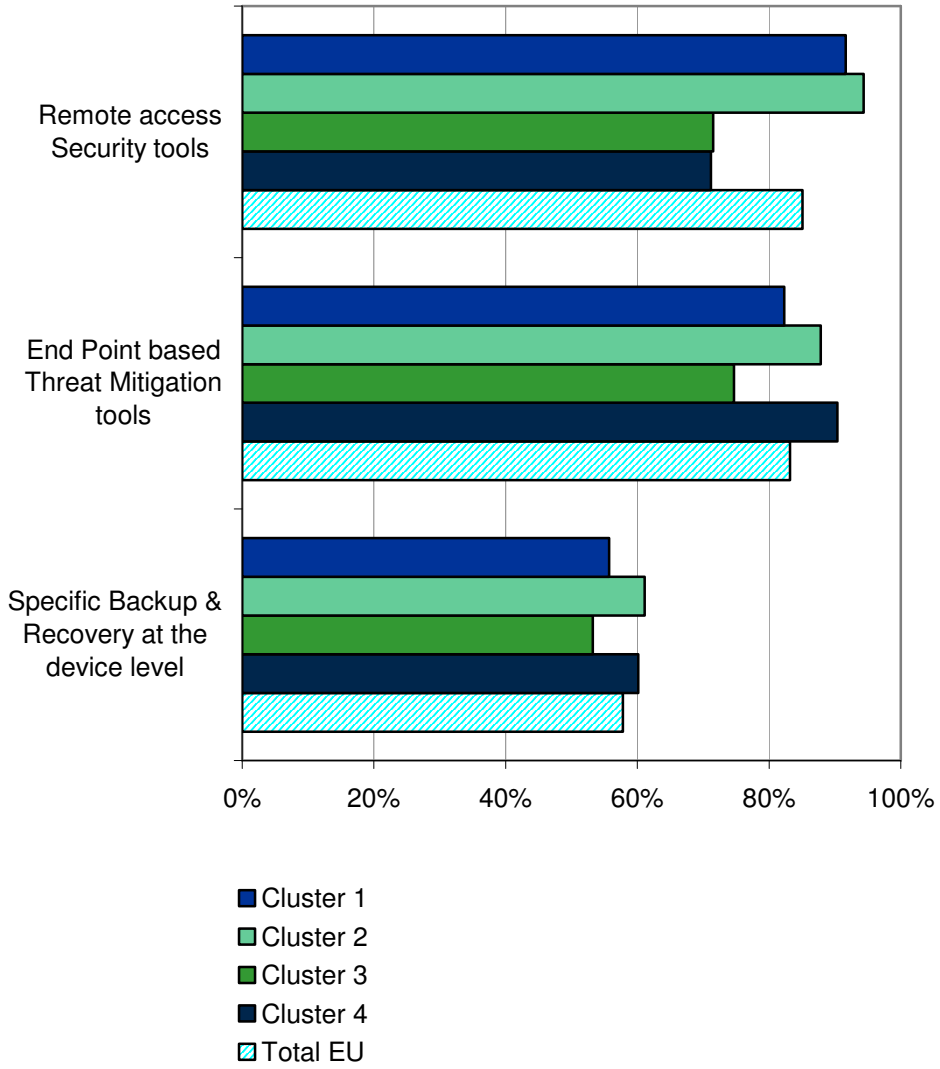
The protection of personal mobile devices is much more limited, as anticipated, with approximately half of enterprises (48%) admitting that they do not have any specific solution. This average hides a polarization between the advanced Clusters (1 and 2) where personal mobile security is more diffused, and the other Clusters (3 and 4) where respectively 70% and 50% of enterprises implement no solution.

The minority of enterprises active in this area deploys specific solutions or implement central management and monitoring of devices: they are more present in Clusters 1 and 2. However, it is clear that EU companies still need to invest and work in this area as mobile devices are increasingly becoming a potential critical point for security breaches.

FIGURE 8

EU Business Users, IT Security Products for Mobile Users
Current Adoption, by Cluster (% of enterprises)

Q. Which of the following specific tools for mobile users do you use?



N = 632

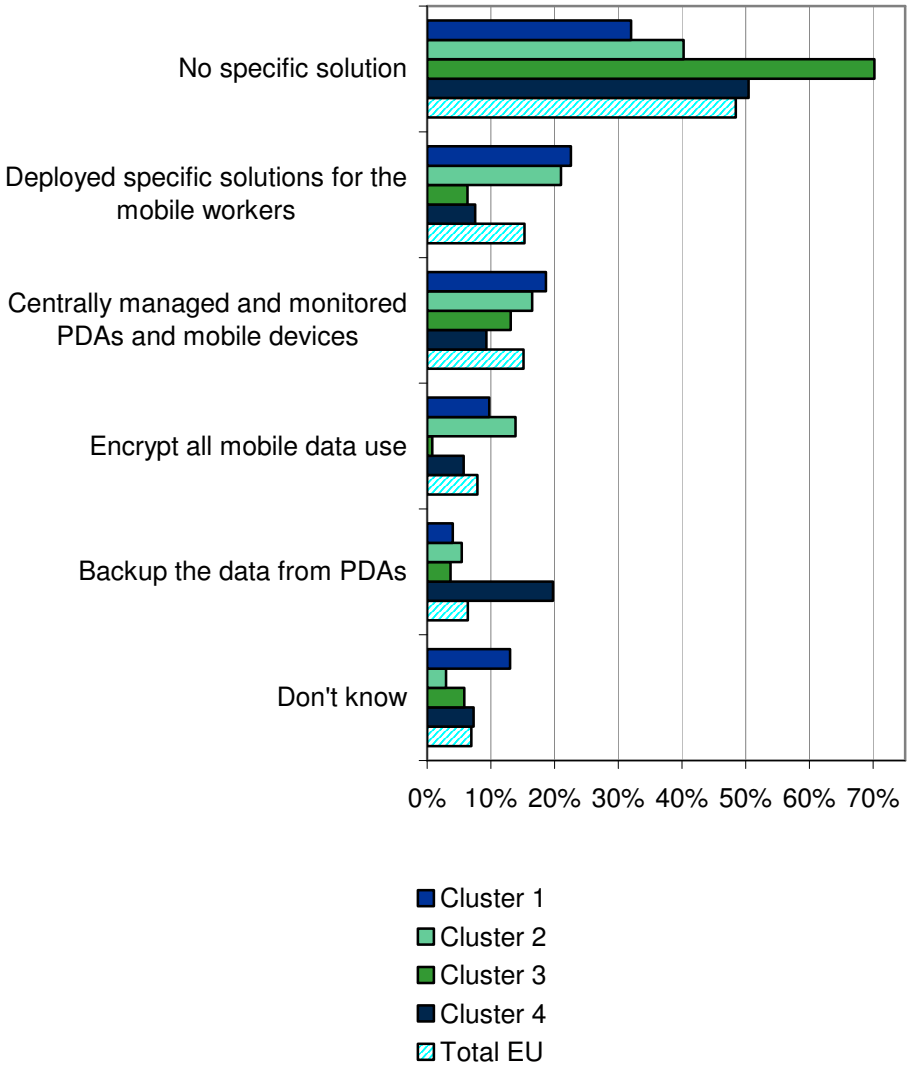
Base = Companies that deploy mobile solutions. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 9

EU Business Users, Protection of Personal Mobile Tools, by Cluster (% of enterprises)

Q. How do you protect the personal mobile tools provided by your organizations to employees?



N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

Relationship with Suppliers: Selection Criteria and Satisfaction

EU enterprises have no doubts about the most important factor influencing their choice of a security provider: customer service, which is ranked 3.5 on a 1 to 4 scale (where 3 stands for *important* and 4 for *highly important*). The level of technical superiority/innovation of the offering is also considered quite important, with an average score of 3.2. The survey included an additional question about the most important aspects of customer service for business users, from

quality to flexibility. The answers show that all aspects are considered extremely important. In particular, quality and reactivity are considered the most important aspects of customer services, followed closely by affordable costs. The vendors' country of origin, instead, is not a significantly important criterion of choice. This is also confirmed by the results of most important security providers: the top 3 are US companies, non European ones.

The survey investigated the level of business users' satisfaction with their suppliers, for the same factors measured by importance. Despite some differences, business users declare themselves mostly satisfied with the performance of their primary security suppliers, for all the aspects investigated (with a score between 3.0 and 3.2. in a scale of 1 to 4, where 3 means "satisfied" and 4 "very satisfied").

Ideally, if satisfaction levels are high on the most important aspects for the users, the match demand-supply should be adequate. The survey results instead show a gap between importance and satisfaction levels. For the three most important criteria, satisfaction remains below the importance level. In particular the gap between importance and satisfaction is widest for the most important selection criterion, customer service.

There appears to be a mismatch between the aspects of higher importance for the business users, and the performance of the vendors; the alignment between demand and supply does not appear sufficient. Companies are generally satisfied with the technical quality of the security products they buy. But technology is not enough. They clearly miss:

- A more effective support from their providers, covering both technical and business-related aspects. This can ultimately help companies building up security policies, able to protect the information lifecycle in companies' business processes.

- A lower cost of ownership, or cost associated to the time and resources needed to run, and maintain the solution. EU companies recognize that reducing indirect costs is key for their business success. With limited IT skills (especially at the low end of the market), a strong need to focus on core competencies, a compelling need to gain efficiencies and become more agile in the global world, the cost of ownership of IT solutions (and in particular of security solutions) is more of an issue than the costs of buying the solution itself.

The ranking of relevant factors and the gap with satisfaction levels are rather similar across the different Clusters, with a few variations reflecting (once again) their different level of IT sophistication. More specifically:

- **Cluster 1**, **the Champions** Enterprises in this cluster probably give for granted the technical performance of the offering and privilege Customer service as the key factor for a supplier's selection. In this cluster, companies are mostly satisfied with the

three most important parameters, which have been ranked between 2.9 and 3.1. Mid-sized companies are the most satisfied across all the criteria, which have been rated between 3.1 and 3.3.

- **Cluster 2**, **the Pillars** instead evaluate "low cost of ownership" above it as the most important critical factor. As we have seen this is the cluster attaching the highest importance to cost. At the same time it is also the cluster showing the highest satisfaction against this criterion (3.1). Despite of that, a small gap exists as satisfaction is lower than importance (3.1 against 3.2).

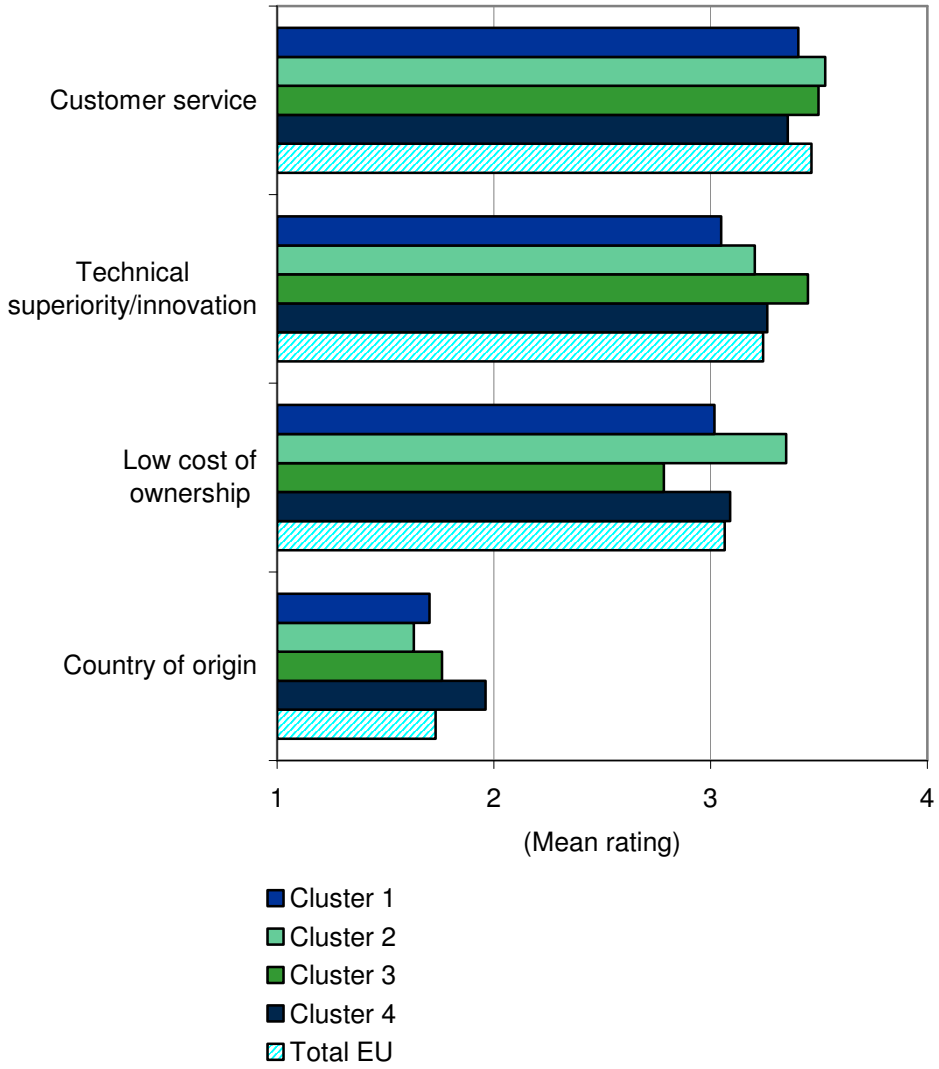
- **Cluster 3**, **the Runners-up** privileges the technical innovation of the offering, ranking costs at a lower level. But satisfaction levels are quite flat for the 4 investigated factors, which have been ranked between 3.0 and 3.2. The gap between importance and satisfaction is the widest for customer service, especially in the 100-249 employees size class (importance of 3.6 against a satisfaction of 3.0).

- **Cluster 4, the Learners.** Enterprises look at customer service and technical innovation as almost equally important, closely followed by cost of ownership In cluster 4 innovation performance gets the highest satisfaction score (3.2), followed closely by the other factors. The main relevance-satisfaction gap concerns customer service.

FIGURE 10

EU Business Users, Criteria of Selection of Primary IT Security Provider, by Cluster (Mean rating)

Q. Which criteria do you consider important for the choice of your primary IT Security Provider?



N = 1,180

Base = All sample

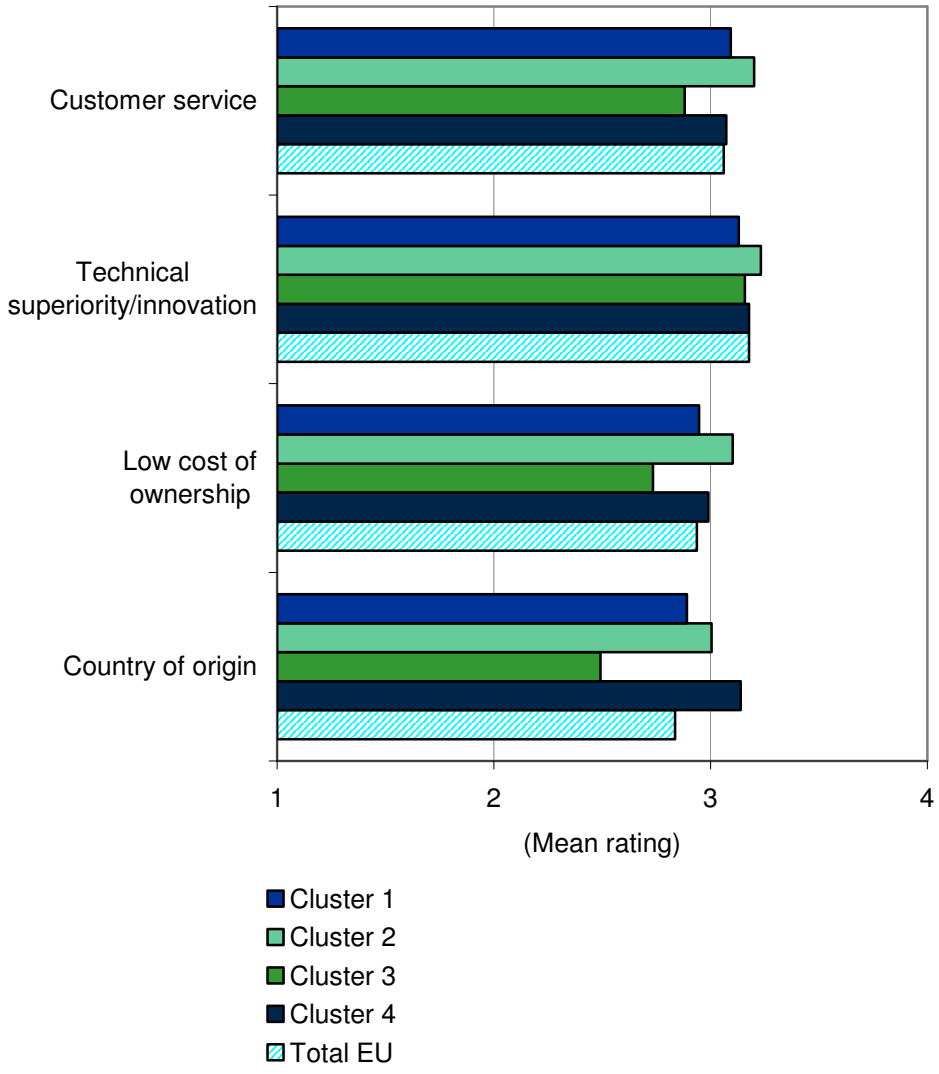
Note: Mean scores are based on a scale of 1–4, where 1 = Not at all important and 4 = Highly important

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 11

EU Business Users, Satisfaction with Primary IT Security Provider's Performance, by Cluster (Mean rating)

Q. Can you indicate your level of satisfaction, for each of the following areas, of your three most important security suppliers?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = Very unsatisfied and 4 = Very satisfied

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Procurement Channels by Cluster

The NIS security market shows a wide range of procurement channels and a complex web of relationships between business users and their suppliers. Many companies use more than one distribution channel (direct and indirect) at the same time for different solutions.

The most frequent procurement channel at the EU level is the direct one between the security provider and the business user (52% of EU enterprises), closely followed by VARs (Value Added Resellers, chosen by 47% of enterprises). Large corporations are more likely to use specialized security vendors and VARs, because of their complex security needs and quality requirements. Approximately 41% of EU business users buy their security embedded with their hardware purchases, more frequently small companies, but also many large and medium ones. This is by now normal practice, since basic antivirus and firewall tools are bundled with most PCs at the moment of sale.

Network or remote access security providers and retailers reach about a third of the business market, while managed services providers are used by 23% of business users, typically the most sophisticated ones.

The analysis of distribution channel by cluster (*see figure 12*) leads to the following considerations.

- **Cluster 1**, **the Champions:** The sophisticated business users of this cluster have articulated procurement strategies, using all the distribution channels more than the average EU level, with the exception of the hardware embedded procurement one (characteristic of low profile users), which is instead less used. They are twice more likely than the EU average to use Managed Service Providers. The absolute majority of enterprises in this cluster have direct relationships with vendors (62%) and with VARs (59%). Interestingly, in this cluster VARs are by far the first channel for mid-sized companies (100-249 employees) that show a high level of sophistication. These firms want suppliers able to offer solutions that are tailored to their needs and that embed support and services, providing high-quality solutions.

- **Cluster 2, the Pillars**. Similarly to cluster 1, the enterprises in this cluster are likely to buy directly from security vendors (50%), and/or from VARs (46%), and/or from Network service providers. But in these countries there are also many enterprises buying security solutions embedded in hardware, which tend to be basic solutions. This cluster includes the largest economies of the EU by far: these data show that the security markets are also large and comprehend both advanced and less advanced users, with a strong presence of very small firms who rely on the indirect channels.

- **Cluster 3**, **the Runners-up**. The high presence of SMEs in this cluster is shown once again by the predominance of the hardware embedded channel (which is more important in this cluster than in all the other ones) and of the retailer channel. At the same time security vendors and VARs are also important, as they cater to approximately half of the business users. These data reflect a medium-high level of development of the IT security market, where business users may rely on an articulated group of suppliers and distribution channels.

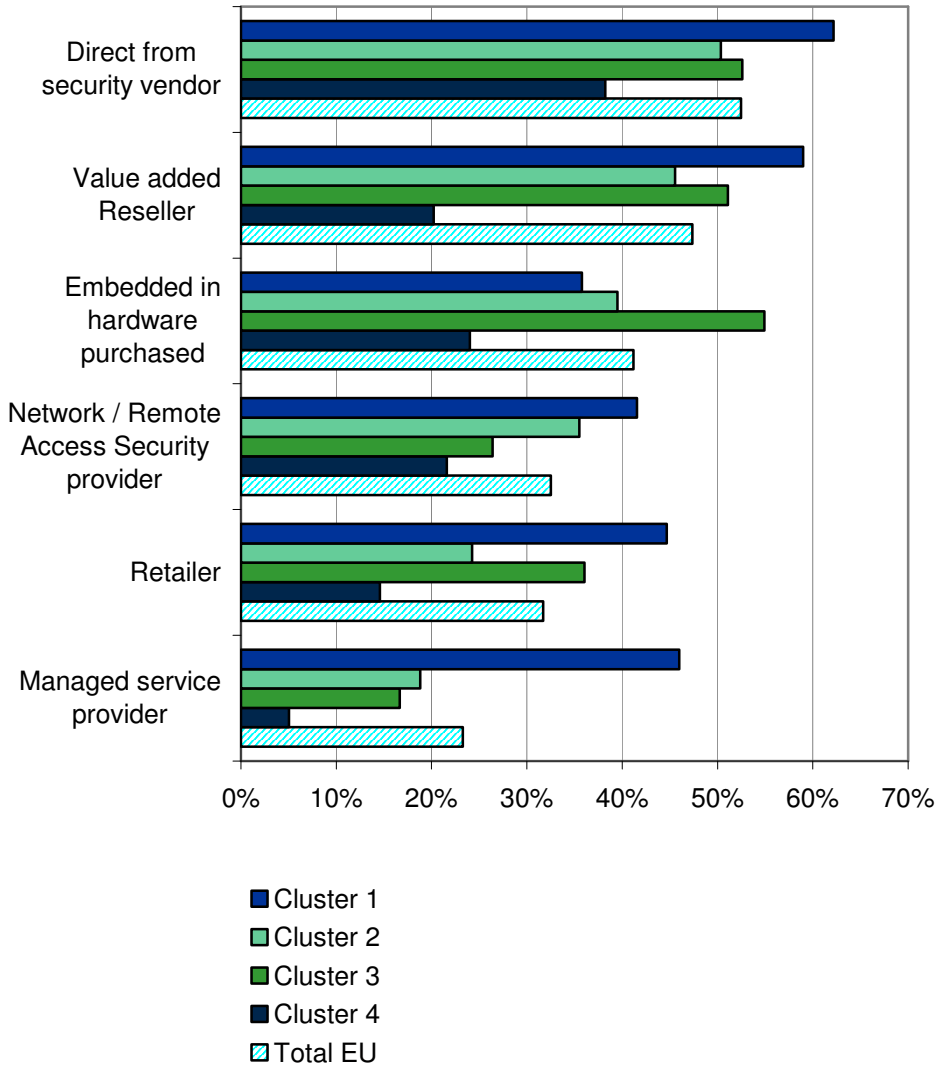
- **Cluster 4**, **the Learners** The enterprises of this cluster are less likely to rely on more than one distribution channel, reflecting less

complex procurement strategies. In these markets global, specialized security vendors are still very strong, so they appear as the most important distribution channel (38% of enterprises); but also the "mass market" distribution channel (that is, solutions bundled with hardware) is very frequent (24% of enterprises). The lower maturity of the market is shown by the lower importance of the service providers in the business users' procurement activities.

FIGURE 12

EU Business Users, Procurement Channels of IT Security Products, by Cluster (%of enterprises)

Q. Where would you normally source the security products you use or plan to use?



N = 1,169

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

3 THE NIS BUSINESS USERS PROFILES IN THE EU MARKET

Overview of the Business Users Profiles

A key element for the understanding of the NIS market is the analysis of the main typologies of business users, defined on the basis of their IT security choices. The mix of advanced and less advanced business users in each market is one of the most important factors differentiating the EU Clusters, providing the basis for the Market Maturity Indicator (presented in D.5.1).

The study identified 3 main typologies of business users (low, average and high NIS investment users, also abbreviated as low, average and high profile users), on the basis of the number of security solutions adopted, out of the 7 solutions listed in the study survey (*figure 13*). The business users profiles are the following ones:

- **High NIS investment users** are 22% of EU enterprises: they currently use at least five security solutions;
- **Average NIS investment user** are the absolute majority (54%) and adopt 3 or 4 security solutions indicated;
- **Low NIS Investment users** are 23%: they adopt only one or two security solutions (most often the basic Threat Mitigation Tools).

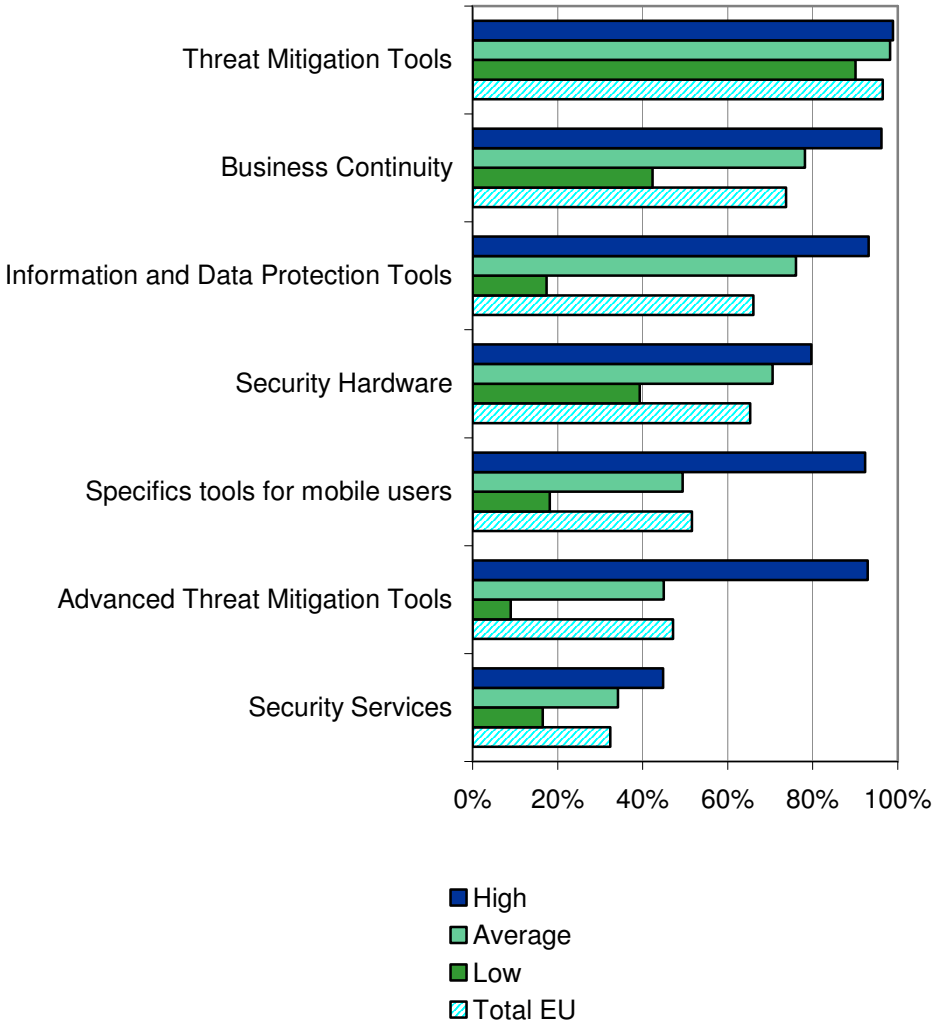
The study results highlight a strong correlation between the users' profile and the country where they are located, the sectors where they operate and their size by number of employees. High profile users are more present in the advanced clusters (especially cluster 1), in the finance or services sectors, and are more likely to be of large size. Symmetrically, low profile users are more present in the least advanced clusters, by sector in the manufacturing industry, and are more likely to be small or medium size enterprises. However, this does not exclude the presence of advanced users in all markets, sectors and size-classes.

The scenario is also dynamic, and these profiles are likely to change in time as the users' maturity increases. In fact, there is a correlation between the users' profiles and their future IT security adoption plans, as a higher percentage of average and low investment users plan to invest in security solutions in the near future (*see figure 18*).

FIGURE 13

EU Business Users, IT Security Products Current Adoption, by Profile (% of Enterprises)

Q. Which of the following products has your organization implemented?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

TABLE 2

Low, Average, High NIS Investment Businesses: Distribution by Cluster (% of enterprises)

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Total
Low	13%	23%	25%	43%	23%
Average	53%	54%	59%	48%	54%
High	34%	23%	17%	9%	22%

N = 1,180
Base = All sample

Source: Survey of EU ICT Security Market, 2008

TABLE 3

Low, Average, High NIS Investment Businesses: Distribution by Company Size (% of enterprises)

	1 to 9	10 to 99	100 to 249	250+	Total
Low	40%	30%	21%	13%	23%
Average	53%	55%	57%	54%	54%
High	7%	15%	21%	33%	22%

N = 1,180
Base = All sample

Source: Survey of EU ICT Security Market, 2008

TABLE 4

Low, Average, High NIS Investment Businesses: Distribution by Industry Sector (% of enterprises)

	Manufacturing	Finance	Government	Services	Total
Low	27%	9%	23%	23%	23%
Average	50%	62%	58%	54%	54%
High	23%	30%	19%	23%	22%

N = 1,180
Base = All sample

Source: Survey of EU ICT Security Market, 2008

More in detail, the main characteristics of the Business Users by profile are the following.

Low NIS Investment Business Users

Low profile users invest in threat mitigation tools (such as Anti-virus, Anti-Spam, Anti-Spyware, etc) and basic business continuity solutions (such as backup tools). These users' plans to invest in the next 12 months, though, are rather high. As today their adoption of

information and data protection tools is very low (17% against an average of 66%), it is coherent that they are willing to invest in this area. Similarly, advanced threat mitigation tools are currently adopted by only 9% of low investment businesses versus a EU average of 47%.

Perceived protection against potential security breaches is slightly lower than average values. Instead, these companies declare a high level of satisfaction when asked to rank the performance of their security suppliers. In particular, satisfaction is very high regarding security costs, which is rated at 3.2 (which means more than satisfied, on a 1 to 4 scale, where 4 stands for "very satisfied"). This is higher than the average EU satisfaction level, which stops at 2.9. This may be expected, because these enterprises use basic, that is cheap security solutions. But low profile users are also satisfied with the technical superiority/innovation of their security solutions, scored 3.2 (identical to the average EU score) and with the customer service, rated 3.1, (again EU average).

Therefore these companies spend less than the average EU, but are as satisfied as the average about technical aspects and customer services.

Average NIS Investment Business Users

Average investment users by definition show an intermediate profile between Low and High investment users, but at the same time, they are the least satisfied with their suppliers. Actually, these enterprises spend more than Low profile users, so they are not particularly satisfied with their security costs, but do not appear to enjoy the quality and performance achieved by the high profile users.

Indeed, companies in this group often face complex security needs and therefore are struggling to achieve a higher protection level. Their level of concern about security threats is close to the High profile users' one, showing a high level of awareness of their position as potential targets of attacks. At the same time, they are often medium or small-sized enterprises, and have greater difficulty to achieve economies of scale and scope in their IT procurement. These firms frequently cannot afford the most innovative and sophisticated security solutions. Therefore, their perceived protection level is lower than the High investment users level, coherently with the fact that they do not currently adopt the most advanced solutions.

In terms of future adoption plans, Average users are particularly keen in investing in advanced threat mitigation tools, managed security services, but especially in specific tools for mobile users. Mobile security appears as their most important investment area, more so than for High profile users. This shows that mobile security is moving towards the mass market, driven by the increasing number of mobile employees and the integration of mobile productivity tools in enterprises information systems. However, there remains a demand-supply gap in this area, as the offering does not appear to completely satisfy emerging needs also by SME users.

Concerning criteria for security suppliers' selection, Average NIS Investment users rank Customer services first, more often than the other users' groups. Because of their modernization process and IT usage evolution, these users need support and advice from their suppliers more than the other users' groups, and they do not seem to be getting it. In conclusion, since Average profile users are the majority of EU enterprises, their low level of satisfaction should be an alarm signal for the main IT security suppliers.

High NIS Investment Business Users

These enterprises are the most sophisticated in terms of adoption of security solutions. Coherently, they declare the highest level of perceived protection. Still, High profile users experienced the highest number of security breaches in the last 12 months (11% against an average of 7%). This might be due to the fact that companies in this group undergo a higher number of attacks but also to the fact that the level of perceived protection not always translates in an effective higher protection level. Frequently we find a lack of knowledge regarding the understanding of potential breaches and therefore companies do not make a correct valuation of their protection level. Also these companies have more efficient and sophisticated systems to track breaches and therefore are more likely to evidence a higher number of attacks.

As these enterprises are current adopters of highly sophisticated security solutions, future adoption plans remain constantly below the EU average levels. However, they have relatively higher investment plans than other users concerning managed security services, showing their evolution towards higher maturity. High profile users are more likely to deploy SaaS (security-as-a-service) solutions (16%) or to have plans to adopt it (8%).

These users are more than satisfied with the technical superiority/innovation of their solutions (with a score of 3.3, on a 1 to 4 scale where 3 means "satisfied"). They are also satisfied with the cost of their solutions (score 3). This score corresponds to the level of importance assigned to cost as a criterion to select a supplier. In other words, concerning cost no gap between importance and satisfaction appears for these users.

High profile users are also relatively satisfied for the customer service (score 3 again) but in this case, they assign a higher score in terms of importance (3.4), which signals a potential demand-supply gap.

In conclusion, all business users are less satisfied than they could be with the customer service performance of security suppliers.

Fears and Perceived Protection by User Profile

EU business users share similar fears about IT security (measured against 4 groups of potential threats, see fig.11) independently from their investment profile. There are however some variations as follows.

- **High NIS Investment Businesses**. They are the least worried about the financial cost of repairing security damages, while they are the most worried about business interruption. More advanced companies are more likely to have an insurance covering the direct cost of security breaches. Business interruption is the most relevant concern for all the three groups.

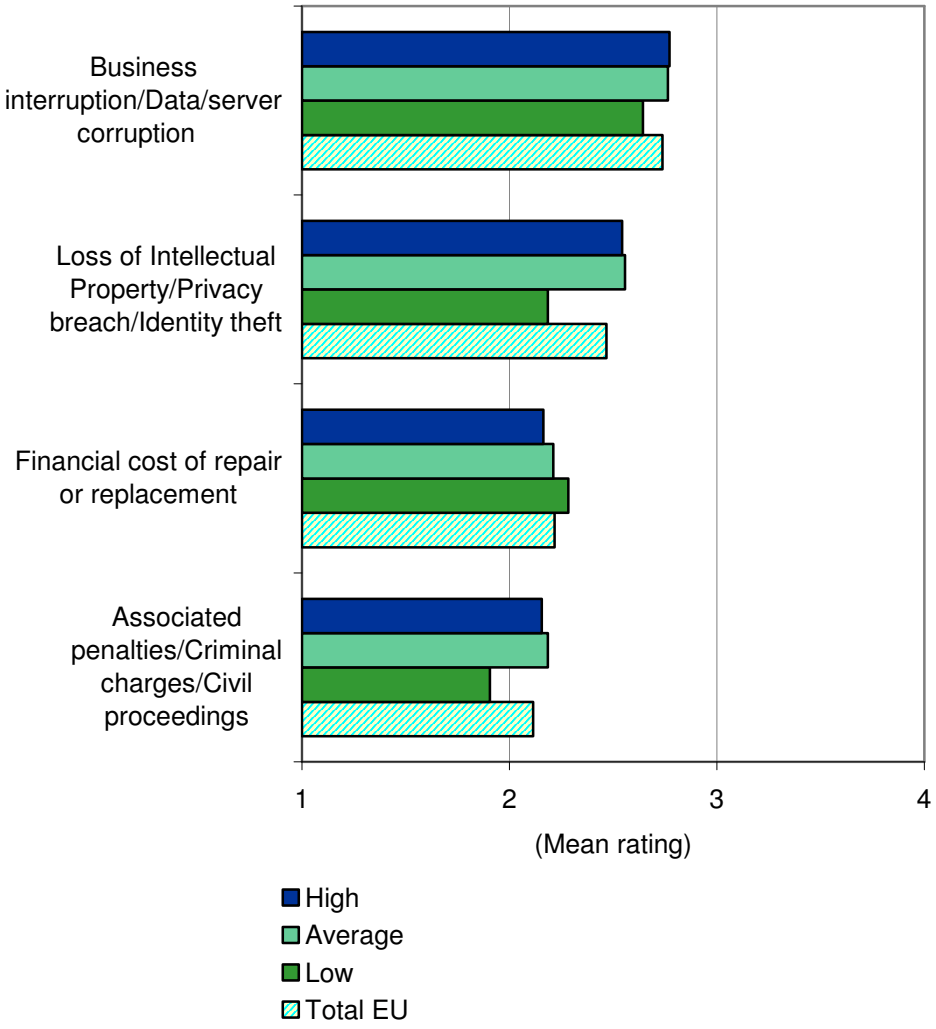
- **Average NIS Investment Businesses**. This group is the most worried about risks related with the loss of intellectual property facing charges. These companies are more worried than High profile users, probably because they do not employ high level solutions but face similar threats.

- **Low NIS Investment Businesses**. This group, generally speaking, appears less worried than the other clusters for all security threats, with the exception of financial costs. These enterprises are not likely to carry insurance against IT security damages, and at the same time they are often small size firms, whose small budgets may be strongly hurt by IT security braches creating damages.

FIGURE 14

European Union, Fears related to IT Security, by Profile (mean rating)

Q. With respect to IT security, could you tell us what do you fear the most?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4= I am strongly worried

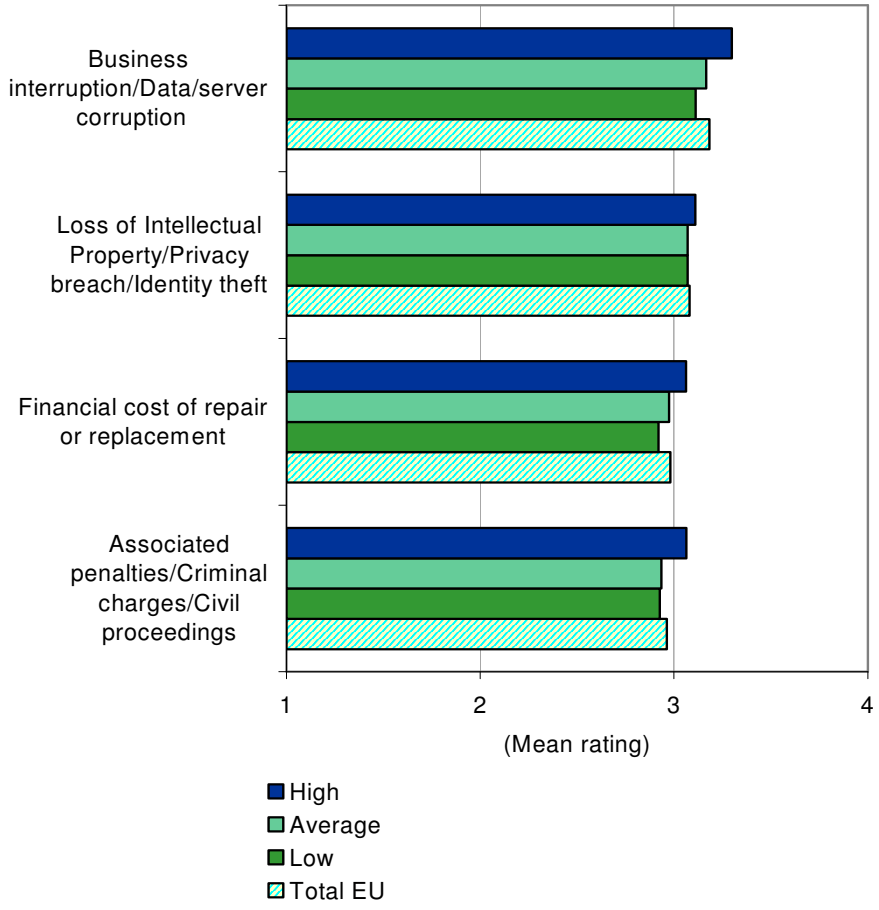
Source: IDC GI Survey of EU ICT Security Market, 2008

Perceived protection is rather high for all business users profiles, with a score around 3 (corresponding to "I feel protected"). High Investment businesses tend to score their perceived protection slightly higher than the other profiles, while. low and average investment companies score slightly lower for the financial cost of repair and risk of charge type of threats.

FIGURE 15

EU Business Users, Perceived Protection related to IT Security, by Profile (Mean rating)

Q. Could you provide us your feeling regarding your level of protection in each of the four areas? Do you feel protected/safe?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I do not feel protected and 4 = I feel highly protected

Source: IDC GI Survey of EU ICT Security Market, 2008

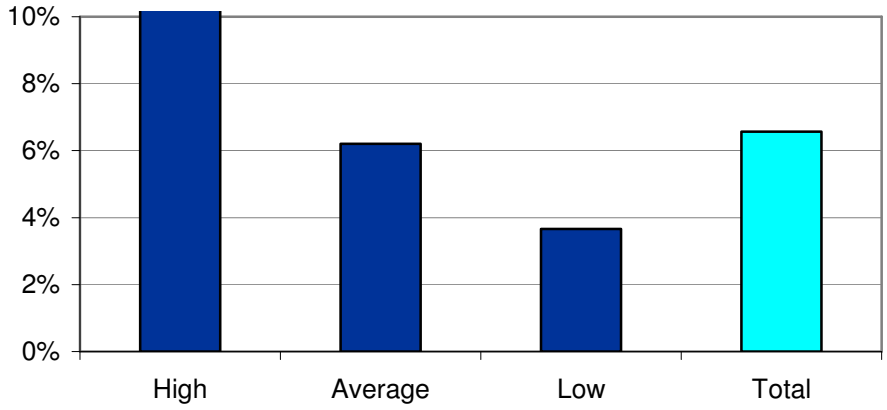
Security Breaches by Business User Profile

The incidence of security breaches across the three groups varies considerably with a direct correlation with the profile: High profile users are much more likely to report breaches occurred in the last year (10%), while Average users and especially Low users are less likely to do so (*figure 16*). This points to the greater intensity of IT information infrastructures use by advanced users, and also to their more sophisticated security tracking system. As indicated above, enterprises often are not aware of security violations. Therefore in practice a higher number of declared breaches may be seen as an indicator of the high sophistication of breaches tracking systems.

FIGURE 16

EU Business Users that experienced a Significant IT Security Breach in the Last Year, by Profile (% of positive answers)

Q. Has your organisation experienced a significant IT security breach in the last year?



N = 1,180

Base = All sample

Source: Survey of EU ICT Security Market, 2008

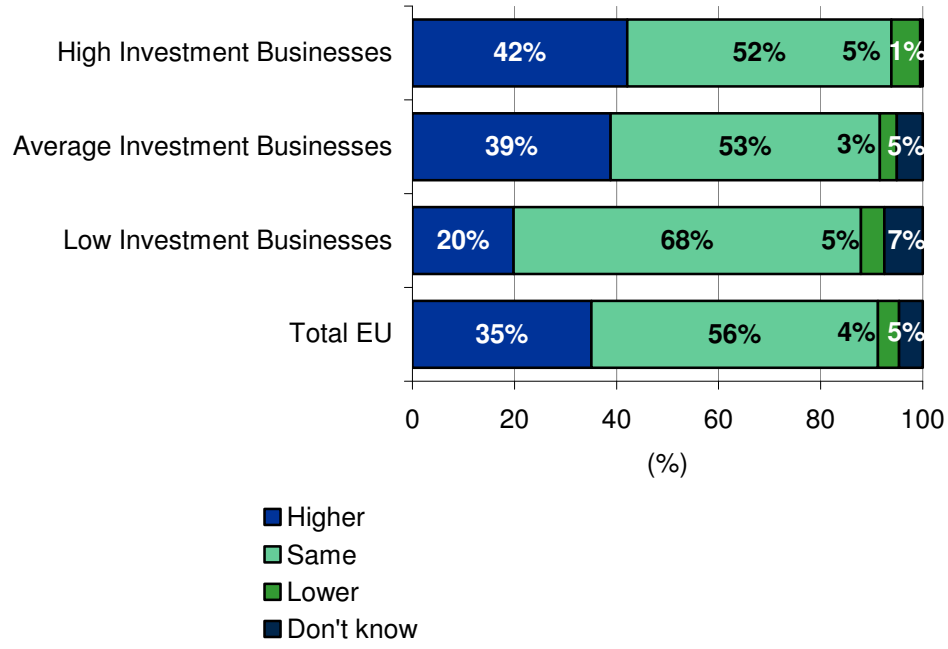
Main Trends of IT Security Spending and Future Plans of Adoption

There is a clear correlation between users' profiles and spending trends: High profile users are much more likely to plan to increase their security budget, closely followed by Average Investment users, while only a minority of Low profile users (20%) plan to do so. On the other hand, as discussed below, the Low profile users planning to invest are concentrated on advanced solutions and are clearly going to upgrade their profile.

FIGURE 17

EU Business Users, Trends of IT Security Spending, by Profile (% of enterprises)

Q. During 2008 how your IT security spending will change?



N = 1,138

Base = All sample

Source: Survey of EU ICT Security Market, 2008

There is an interesting contrast between actual IT security solutions adoption and future plans of investment, which is different by profile as follows.

- **High NIS Investment Businesses**. The security portfolio of these enterprises is already rich, so they are less likely to plan for increased investments.

- **Average NIS Investment Businesses**. The plans of these enterprises target particularly advanced threat mitigation tools and managed security services. They are engaged in catching up with High profile users and therefore, after the effort done to adopt advanced hardware and data protection tools, they aim at filling the gap especially in those areas where security needs are getting compelling, in order both to comply with regulations and to protect critical information.

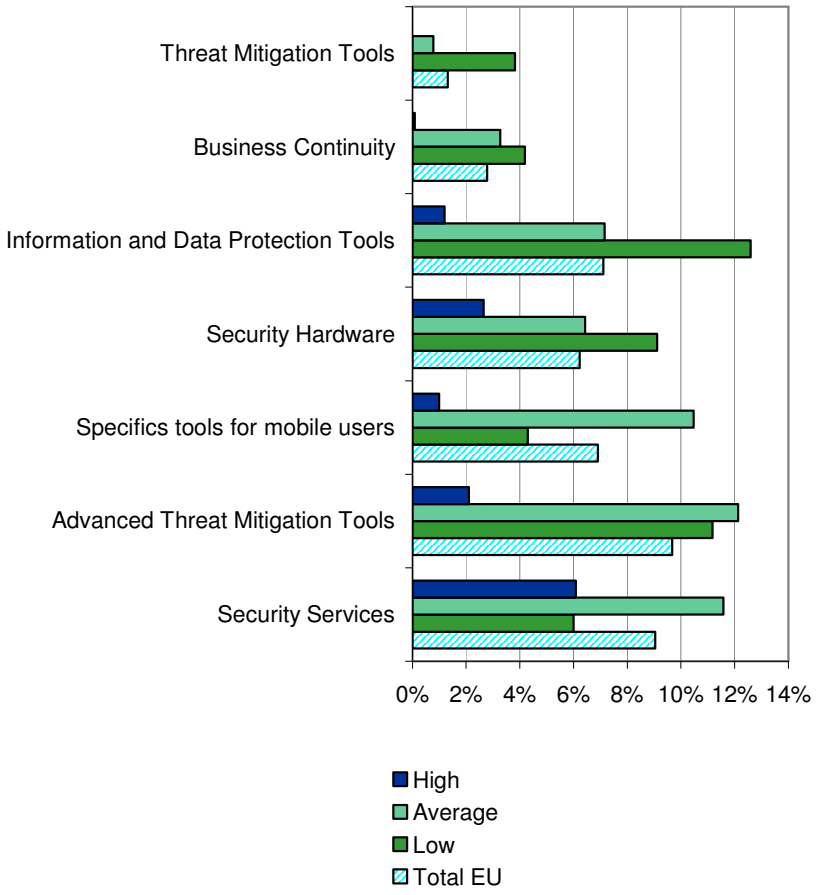
- **Low NIS Investment Businesses**. The minority of low users planning to invest is going to be particularly active in deploying information and data protection tools and security hardware. They are one step behind of average investment businesses; therefore many of them plan notable investments in data protection and

security hardware, which are expected to become commoditized solutions in the short term.

FIGURE 18

EU Business Users, IT Security Products Future Adoption Plans, by Profile (% of enterprises)

Q. Of those products your company has not already implemented, which ones are you planning to implement in the next 12 months?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Mobile Security Adoption by Profile

The adoption of security solutions to protect mobile users' laptops is one of the key aspects distinguishing advanced users from average and low profile ones. The implementation of mobile security solutions is clearly correlated with sophisticated information systems and procurement strategies.

This is also true for the protection of personal mobile devices and PDAs, even if the level of diffusion of mobile security in this field is still very low. The majority of enterprises doing nothing in this area

are low profile business users, while the minority doing something belongs to the high profile users group. More specifically:

- **High NIS Investment Businesses**. 26% of high-investment businesses deploy a specific solution for mobile workers, 21% encrypt mobile data and 20% have a central management and monitoring systems for personal devices. 26% of these companies do not have a solution in place.

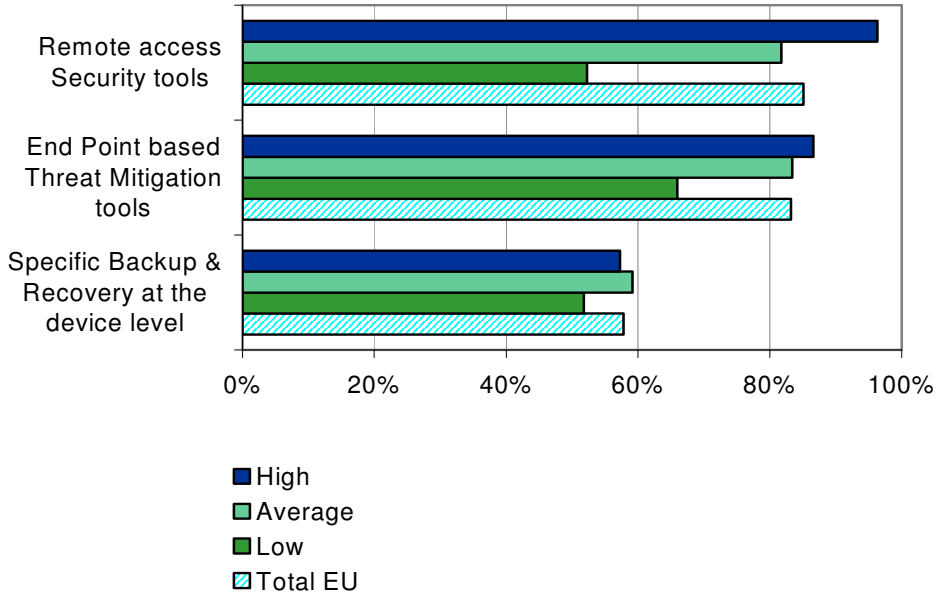
- **Average NIS Investment Businesses**. 16% of average-investment businesses deploy a specific solution for mobile workers, 17% have a central management and monitoring systems for personal devices while only 5% of respondents in this group encrypt mobile data. Almost half of companies (48%) do not have a solution.

- **Low Investment Businesses**. 71% of companies pertaining to this group do dot have a personal mobile security solution. Only 6% manage and monitor devices centrally and backup the data. 5% deploy a specific solution while 1% encrypt device data.

FIGURE 19

EU Business Users, Current Adoption of IT Security Products by Mobile Users, by Profile (% of enterprises)

Q. Which of the following specific tools for mobile users do you use?



N = 632

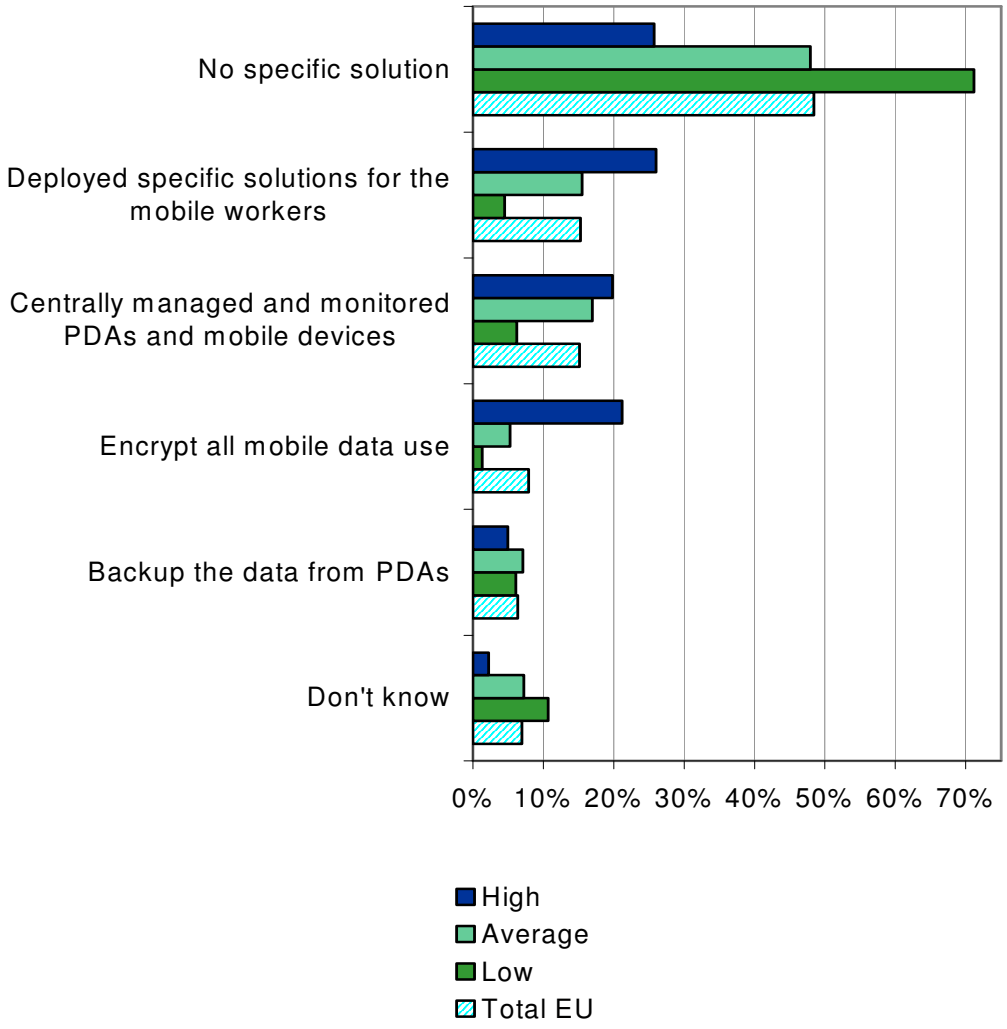
Base = Companies that deploy mobile solutions. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 20

EU Business Users, Protection of Personal Mobile Tools, by Profile (% of enterprises)

Q. How do you protect the personal mobile tools provided by your organizations to employees?



N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

Relationship with Suppliers: Criteria of Selection and Satisfaction

EU Business users rate Customer service, closely followed by Technical innovation, as the most important criterion to select a primary security provider (fig.18). Low cost of ownership is slightly less important and only a minority of users considers the country of origin. There are small differences by profile, but they do not change the overall ranking of criteria.

The survey investigated also the level of users satisfaction with their suppliers, for the same aspects already graded for importance in the selection of the vendors. Despite some differences, business users declare themselves mostly satisfied with the performance of their suppliers, for all the aspects investigated (with a score between 3.0 and 3.2. in a scale of 1 to 4, where 3 means "I am satisfied").

Nevertheless there are some interesting differences of satisfaction ratings, by profile, as follows.

- **High NIS Investment Businesses**. They are the most satisfied with technical superiority and innovation of their security suppliers. They adopt more sophisticated solutions and coherently they find them satisfactorily for what is related to technical aspects.

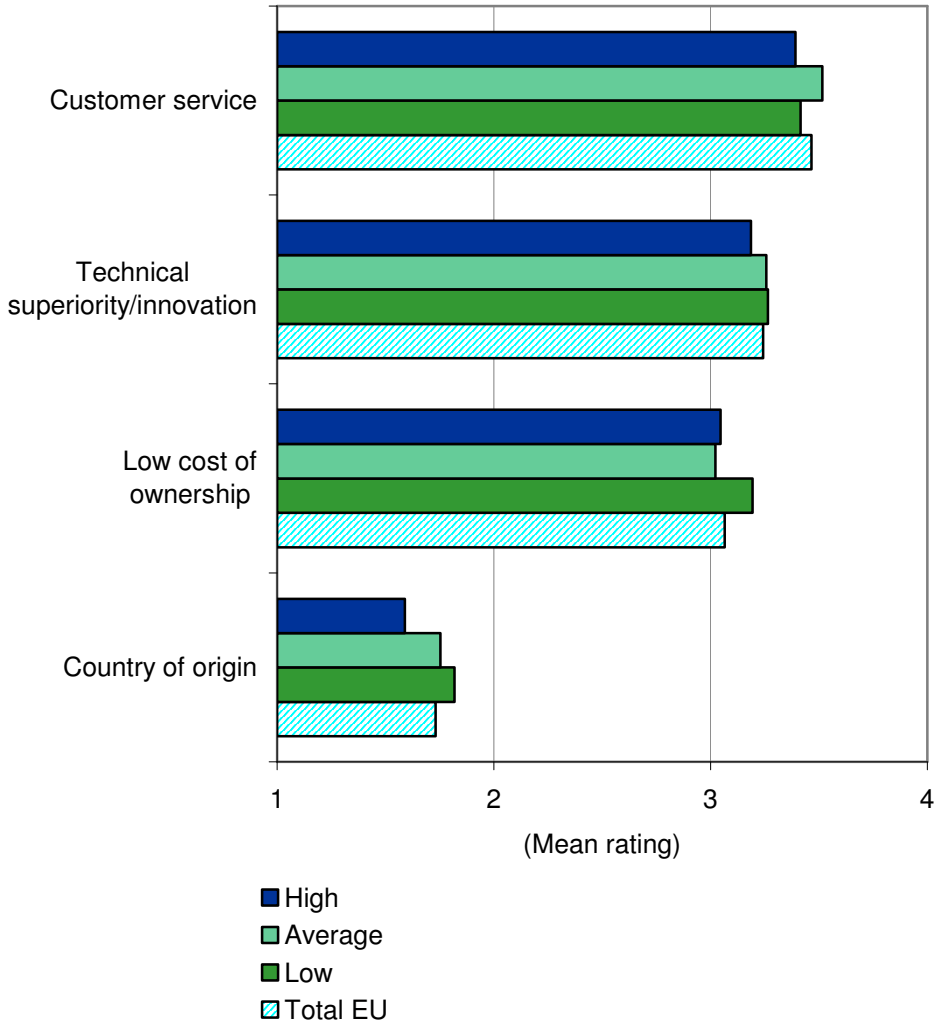
- **Average NIS Investment Businesses**. They are the least satisfied for the parameters under examination, particularly concerning costs. These enterprises face higher costs that low investment businesses, but are not able to achieve the level of protection that High profile users can afford. Therefore their satisfaction remains below the average level.

- **Low NIS Investment Businesses**. They are on average quite satisfied and in particular their satisfaction level is very high for what is related to the low cost of ownership. As we mentioned, basic solutions are also often cheap solutions, therefore this is not surprising. It is instead more surprising that Low profile users show also an average level of satisfaction for what regards the other two criteria. Indeed these enterprises, despite deploying only basic tools, do not show lower satisfaction levels for technical innovation and customer service aspects.

FIGURE 21

EU Business Users, Criteria of Selection of the Primary IT Security Provider, by Profile (Mean rating)

Q. Which criteria do you consider important for the choice of your primary IT Security Provider?



N = 1,180

Base = All sample

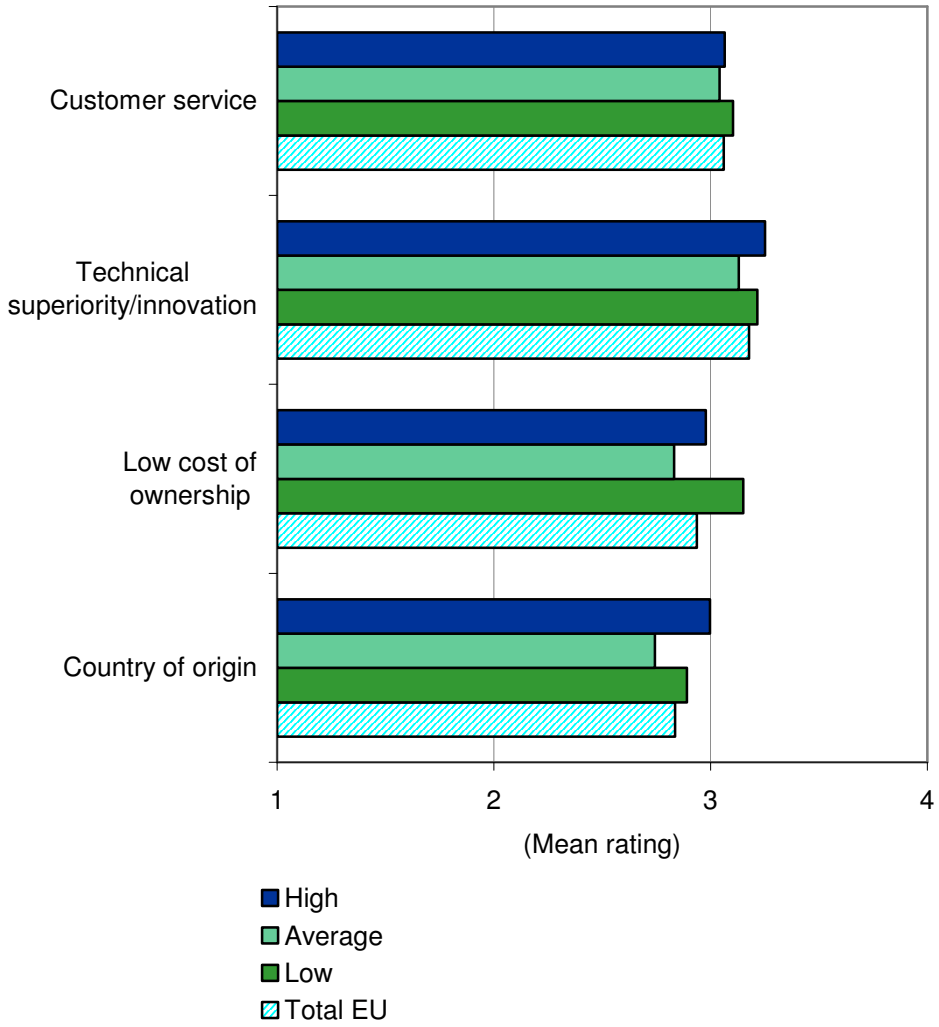
Note: Mean scores are based on a scale of 1–4, where 1 = Not at all important and 4 = Highly important

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 22

EU Business Users, Rating of Primary IT Security Provider's Performance, by Profile (mean rating)

Q. Can you indicate your level of satisfaction, for each of the following areas, of your three most important security suppliers?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = Very unsatisfied and 4 = Very satisfied

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Procurement Channels by Profile

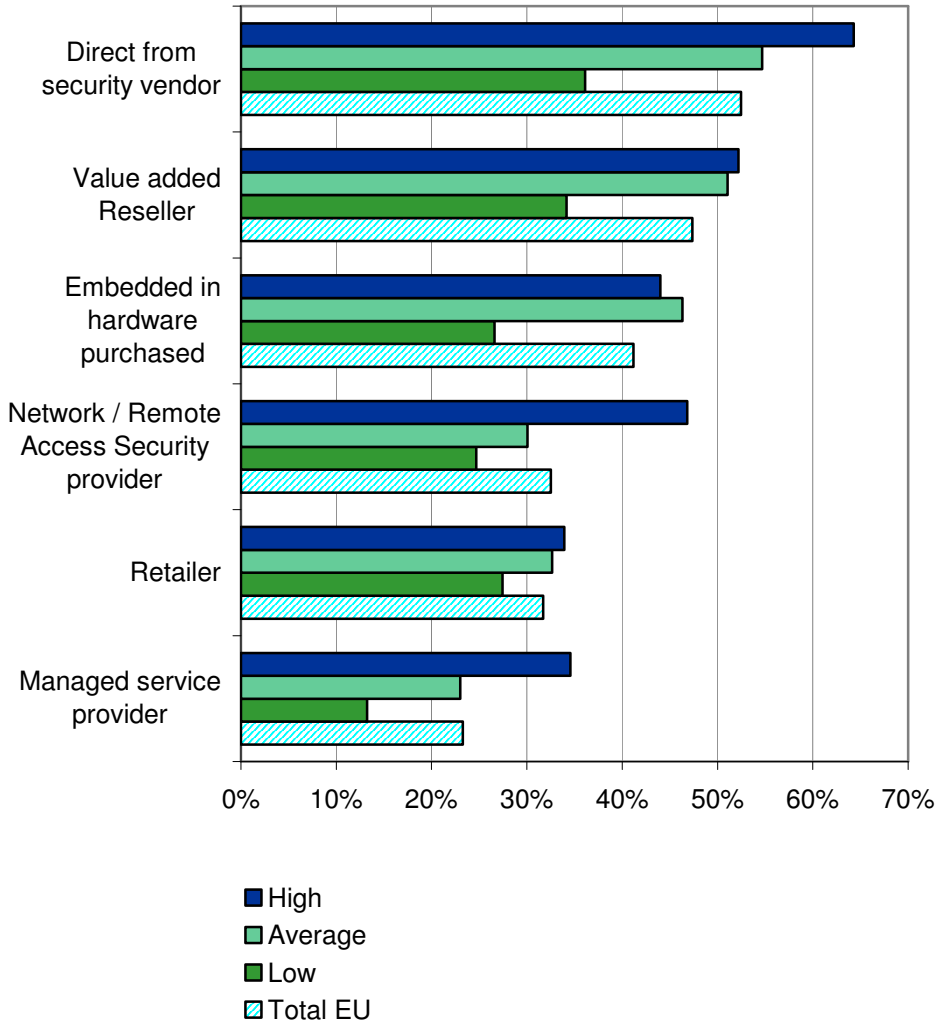
From the point of view of delivery channels, choices by Business Users profile lead to considerations similar to those presented for the Cluster segmentation. High profile users tend to implement a complex and articulated procurement strategy, using many channels, but particularly dealing directly with security vendors and with VARs. True mass-market channels (hardware embedded solutions and

retailers) are used by all types of users, with differences blurring among the three groups.

FIGURE 23

EU Business Users, Main Procurement Channels of IT Security Products, by Profile (% of enterprises)

Q. Where would you normally source the security products you use or plan to use?



N = 1,169

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

4 THE EU NIS MARKET BY INDUSTRY

Overview by Industry

The study analyzed the characteristics of EU Business Users by industry on the basis of four main sectors: Manufacturing and Agriculture (corresponding to 22% of overall security spending in 2007), Services (comprising utilities, telecommunications, transport, retail/wholesale, construction, business and professional services companies, accounting for 32% of EU security spending in 2007), Financial Services (21% of spending), and the Public Sector (government, healthcare and education) representing another 19% of spending. The Consumer market represents only a small share of the total market, around 6% (because many basic security solutions such as antivirus are distributed for free).

The following paragraphs present a brief overview of the EU security market by sector.

Manufacturing

The Manufacturing industry is not the most advanced sector in terms of security solutions' adoption, but demand is still growing, driven by main economic trends such as globalization, the evolution of international supply chains (with requirements such as zero latency and networking), the diffusion of e-procurement, and insuring business continuity. In addition, these enterprises must comply with new government regulations, and respond to higher requirements of transparency and information forecasting without increasing costs.

Therefore, IT security and the business value of data are becoming higher priorities. Manufacturers recognize that the security of their information assets is today much more of a strategic factor than previously perceived. The market is becoming increasingly competitive, and protecting intellectual property is a necessity to strengthen enterprises' competitive advantages.

In addition, the risk of unauthorized access to Web-based applications and resources is very important in this vertical market, as manufacturers share critical business information and applications with supply chain partners.

Also, manufacturers are increasingly protecting themselves against security breaches that could lead to loss of data, electronic snooping, hacker attacks, unauthorized access, stolen passwords, and sabotage. In this scenario, manufacturers are actually vulnerable to their product quality decreasing, resulting in a rise in costs. Also business continuity for manufacturing organizations means far more than simply ensuring backup and recovery capabilities. For manufacturers with global supply chains, business continuity means ensuring that vital components can be sourced and delivered regardless of political

situations, terrorism or the effects of weather-related conditions and other hazards.

Moreover, security needs vary considerably depending on the specific manufacturing industry: for example, the chemical, automotive and electronic industries show the highest level of sophistication in terms of security technology adoption.

Large manufacturers present higher levels of current security solutions adoption, while small and mid-sized enterprises are more likely to declare plans of future adoption, confirming their willingness to catch up with the advanced users, investing in more innovative and sophisticated solutions.

To face their competitive challenges, manufacturers look for security suppliers paying particular attention to customer service. Concerning distribution channels, the majority of manufacturing enterprises (51%) buy security products directly from security vendors, and/ or from VARs (48%), but they also buy security solutions embedded with hardware (45% of enterprises).

Services

The current adoption of security solutions in the services sector is above the EU average, particularly for large enterprises (with more that 250 employees), but is lower for small and midsized companies. This sector is very fragmented and composed by a high number of SMEs, especially in the retail/wholesale and business services subsectors. For this reason, SMEs choices are crucial for the evolution of the security market in this sector. These enterprises are more likely than those in other sectors to invest in managed security services (11% against a EU average of 9%).

The security market has not yet reached its maturity in this sector. For example, perceived protection by enterprises is below the EU average level in all of the four areas under exam. These enterprises are also more likely to buy security solutions through retailers, or embedded in hardware, that is through mass market channels, rather than relying on service providers and specialized suppliers as more advanced users do. Further considerations must take into account the different industries aggregated in this sector, as follows.

Telecommunications

The telecom industry is a very sophisticated and IT intensive sector, usually deploying high-end solutions. The telecom industry environment is increasingly complex, as fixed and mobile services are converging, but tariffs and pricing models remain distinct. Telecom service providers need to integrate and manage efficiently and seamlessly a broad portfolio of heterogeneous content-rich services, for both consumer and business customers.

The main needs driving investments in data-intensive applications and in securing information are: the enhancement of back-office operations,

to achieve efficiencies and improve profitability, also through the addition of industry-specific functionalities; the upgrade of outdated CRM (Customer Relationship Management) systems, and their integration with collaborative solutions, with advanced billing systems, and with analytics to improve customer insight will continue to drive.

Utilities

The European Utilities sector underwent a unique structural change following EU liberalization efforts to create a competitive single market. Higher competition has lead market players to prioritize the need to insure the security of their data and information systems, whilst also maintaining a continued focus on controlling IT costs.

Indeed, European utilities are today in the process of shifting from a production and technology-driven approach, towards being demand-driven, customer-oriented, compliant and secure enterprises.

Moreover, the increasing dependency of the European energy market on oil and gas imports is spurring utilities to diversify sources, which is further increasing the amount of data being analyzed, secured and exchanged with an enlarged number of partners. In this context, utilities companies need to be able to identify all risks that could potentially impact their value chain, and take the appropriate actions. A non-appropriate security protection level would mean potential financial losses, violation of stringent EU regulation and an increase in customer churn.

Transport

The transport sector has been touched by a liberalization and transformation process, which has led to increased competition while creating new business opportunities.

IDC believes that European transportation companies will undergo a period of broad modernization of ICT systems and operational processes, in order to enable the implementation of next generation Intelligent Transportation Systems. In this context, security represents a key area of investment, as transportation technology modernization is accompanied by a growth in complexity. For example, the deployment of contactless and wireless technologies pose additional security issues that transport companies need to take into strict consideration.

Also, transport companies in the past have been targets of hackers and therefore cannot underestimate the direct and indirect costs of security breaches.

Retail/wholesale

In the retail industry, data and unstructured information increasingly need to be shared throughout the integrated value chain with suppliers and with partners, to ensure end-to-end value chain visibility and real-time synchronization. Therefore retailers need to securely manage an ever-expanding set of data and information.

Also PCI DSS standards, as well as the growing importance and retention of customer data, require a continued focus on security.

Moreover, the increasing diffusion of e-commerce is further emphasizing the need for advanced security solutions that can empower safe e-commerce strategies.

Business and personal services

Security in general, and data security in particular, are hot issues across all vertical markets, but they are particularly critical for professional services companies as they deal with sensitive information. Document and content management solutions adopted not only to support regulatory compliance, but also to present information more effectively to customers, and to improve cooperation with business partners, will require more sophisticated security solutions also in order to maintain brand, image and reputation.

Indeed, business services companies such as law firms or human resources companies count trust and reputation as their cornerstone. They deal constantly with sensitive customers data, therefore security and privacy protection represent a vital part of their core business. The information they hold on their customers are their most valuable asset, to be managed with the appropriate care reflecting their relevance.

The Public Sector: Government, Healthcare, Education

This is a large and complex sector, with the common goal to maximize public value rather than increase revenues. IT security demand drivers are broadly similar, but not identical.

The Government sector is engaged in the development of customer-centric information systems, based on the interactive capabilities of electronic service delivery strengthening two-way communication between the citizens/enterprises and the government itself. Even so, the most important developments will be bound to the expanding needs for data integration and analysis as part of back-office improvement strategies, driven by government agencies' need for successful governance and simplification of administrative burdens. The main objectives are to achieve strong cost efficiencies, develop knowledge sharing and departmental interoperability. In this context, IT security acquires an increasingly notable importance. The government holds a huge amount of sensitive personal and company data; a main goal is not only to store information in a secure way, but also to enable a secure and rapid exchange of information with citizens/enterprises.

The public sector is the industry showing the highest adoption of not only basic threat mitigation tools, but also of advanced threat mitigation tools (including anti-phishing, web reputational systems, anti intrusion detection systems, forensic collection, internal threat management tools). In addition, it is the second industry (after financial services) by adoption of all the other solutions investigated by this study (business continuity, information and data protection,

security hardware, specific tools for mobile users and security services).

If we look instead to future investment plans, the public sector is the industry showing the highest propensity to invest in information and data protection, security hardware and advanced threat mitigation tools. Therefore, the current high adoption rate is going to increase even further in the near future.

Concerning procurement channels (fig.32), public sector organizations rely on security vendors (54%) and/or VARs (49%), while 36% of them buy solutions embedded in hardware. Interestingly, public agencies are more likely than all other industry businesses to use VARs. This underlines their need for personalized and specialized solutions and applications.

Finance

The financial services industry in Europe is very sophisticated and deploys a wide range of advanced security products and services. This is due to different reasons: starting from business issues, banks for the nature of their business hold very sensitive information on their customers. In addition, their business is based on trust and reputation. Therefore it is essential for them to keep very high security standards.

Also, strict regulations oblige financial organizations to implement solutions guaranteeing mandated security standards. Regulatory pressure is likely to increase, as a consequence of the global financial crisis, which will lead to greater information and transparency obligations, requiring updating of banks' IT systems and security solutions.

Therefore, security remains a primary concern for the financial industry, especially as organizations embrace mobility and Web 2.0 type of applications and networking. New security and fraud management tools are mandatory for data protection and to safeguard against identity theft, as well as to improve security, both internally and externally.

For these reasons, financial services companies are the most concerned about privacy breaches and the risk to undergo penalties. In particular, large financial institutions are much more concerned of penalties than smaller ones (2.7 against 1.7 mean rating, on a 1 to 4 scale where 3 means "I am worried"). In fact, regulations affecting large banks are stricter and more pervasive, thus strongly affecting complex financial institutions that need to coordinate multiple locations and business units.

The adoption of advanced security solutions reaches its highest levels in this industry, specifically for business continuity, information and data protection, security hardware, specific tools for mobile users and security services.

In addition, the financial industry shows the highest percentage by far of companies dealing directly with security vendors (71%) and with network security providers (40%), as well as with managed services providers. This confirms their profile as the most sophisticated security user industry.

Banks are constantly looking for ways to prevent new attacks, as they are conscious that security threats change very rapidly and that hackers continue to evolve. For this reason, financial institutions rated technical innovation as the most important criterion for the selection of their security suppliers. They also rate customer service as very important, while cost is relatively less important. Financial institutions want suppliers that are able to keep the pace of innovation and this is particularly true for large organizations. Smaller ones are more concerned with costs, but at the same time they evaluate more highly customer service and technical innovation. This confirms that smaller enterprises are the most demanding.

Fears, Perceived Protection and Security Breaches by Industry

The analysis by industry of fears related to IT security and the level of perceived protection shows similar reactions, with some variations due to the specific dynamics of each industry. More specifically:

- **Manufacturing**. Manufacturing companies show a level of concern between 2.7 and 2.1 (in a scale of 1 to 4, where 3 means "I am worried"). Large manufacturing corporations are more worried that SMEs, and correspondingly feel less protected than SMEs from security risks, even if the overall perceived protection in this sector is above the EU average.

- **Services**. Services companies show the lowest level of perceived protection, which ranges between 2.9 and 3.1 (where the score 3 means "I feel protected"). Still the difference with the EU average is not high. This is a very heterogeneous vertical including, among others, big telecom companies as well as a bunch of very small professional services businesses, with very diverse business and IT strategies.

- **Public**. Public organizations perceived protection scores between 3.0 and 3.2, confirming the general feeling of protection prevailing among business users. Smaller institutions, which are the most concerned about security, nevertheless declare a slightly higher perceived protection than large government agencies, particularly in the area of business interruption and privacy violations.

- **Finance**. Financial services organizations are the most concerned about privacy breaches and identity thefts. Even if companies in the financial industry deploy the most sophisticated solutions to protect against security breaches, they are also conscious of being a prime target of attacks. They also employ skilled staff as well as experienced consultants, who make them well aware of potential

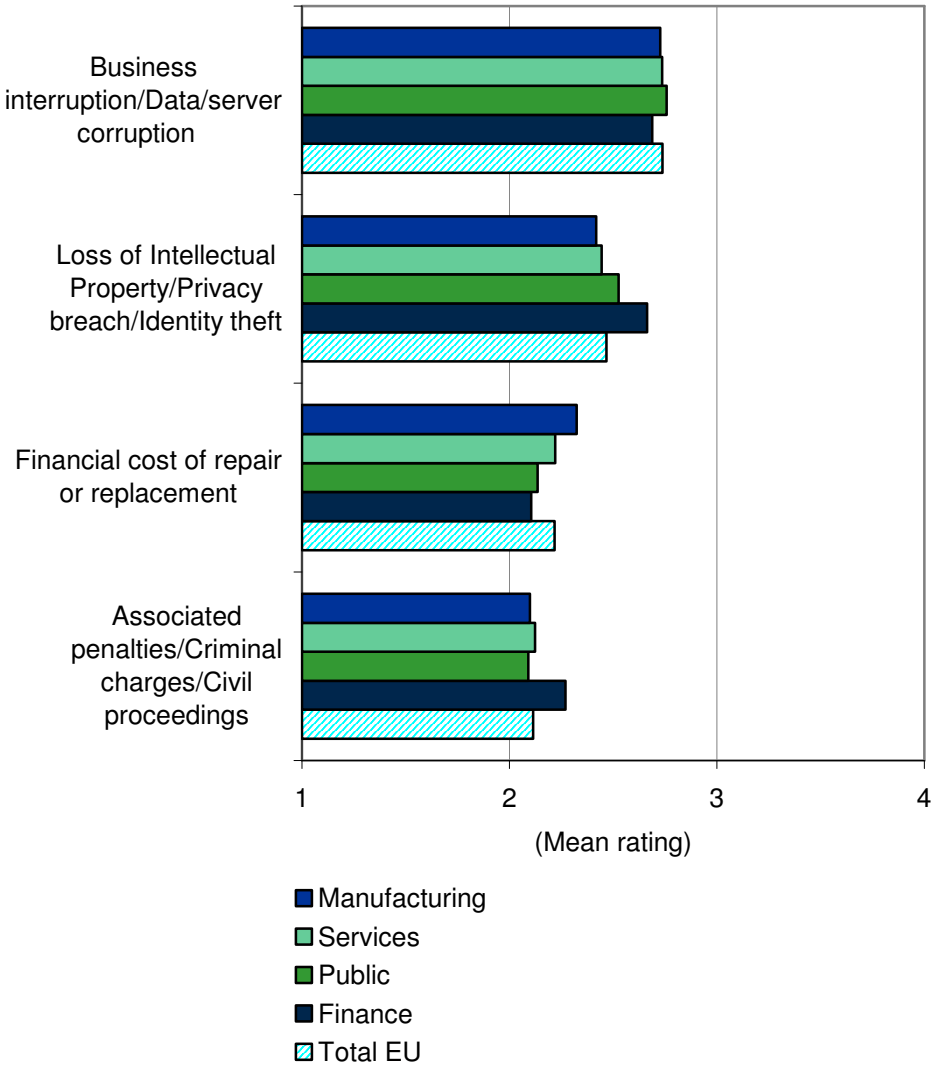
security issues. Also they have to respect stricter regulations. Thanks to their investment, these organizations declare a higher perceived protection than the other industries, for all the threats considered by the study.

Finally, the incidence of security breaches does not present significant variations by industry sector (*figure 24*). From this point of view, company size and geographical location (by cluster) are more relevant than the industry.

FIGURE 24

EU Business Users, Fears related to IT Security, by Industry, (mean rating)

Q. With respect to IT security, could you tell us what do you fear the most?



N = 1,180

Base = All sample

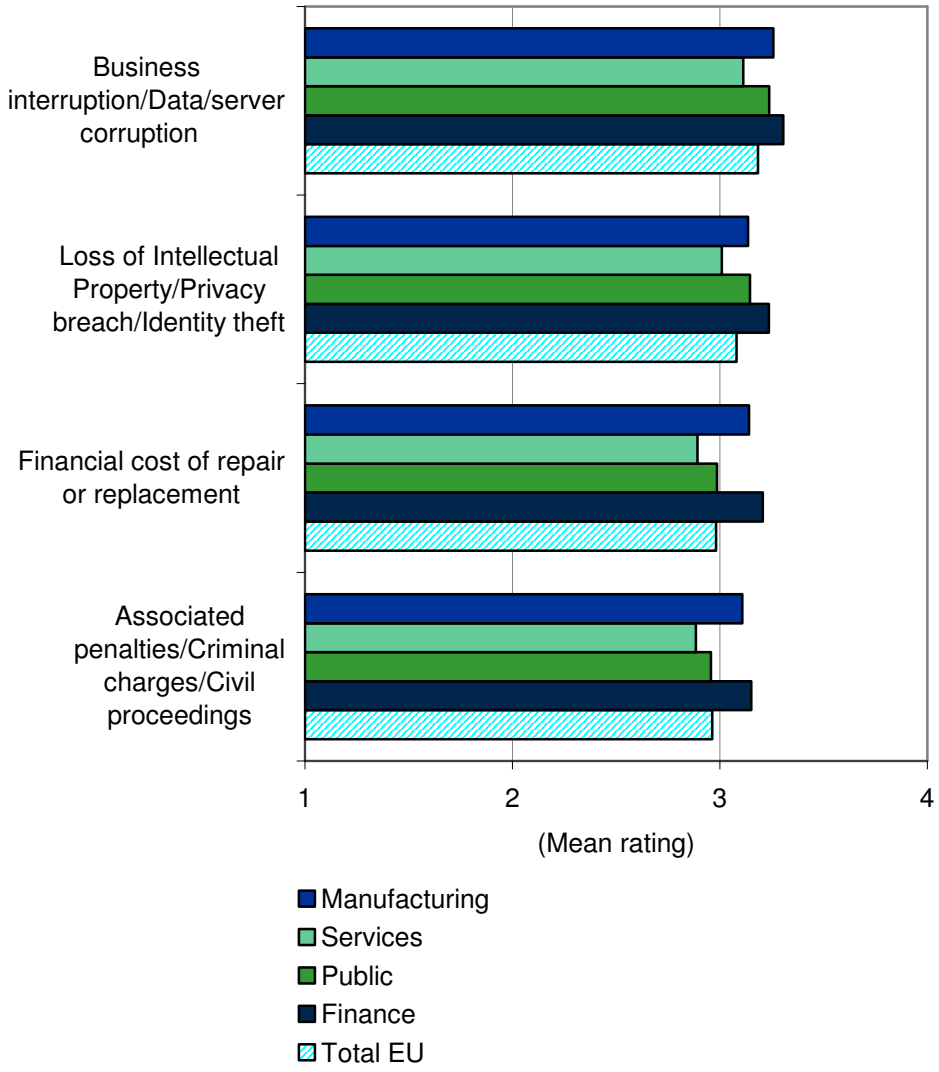
Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4= I am strongly worried

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 25

European Union, Perceived Protection related to IT Security, by Industry (mean rating)

Q. Could you provide us your feeling regarding your level of protection in each of the four areas? Do you feel protected/safe?



N = 1,180

Base = All sample

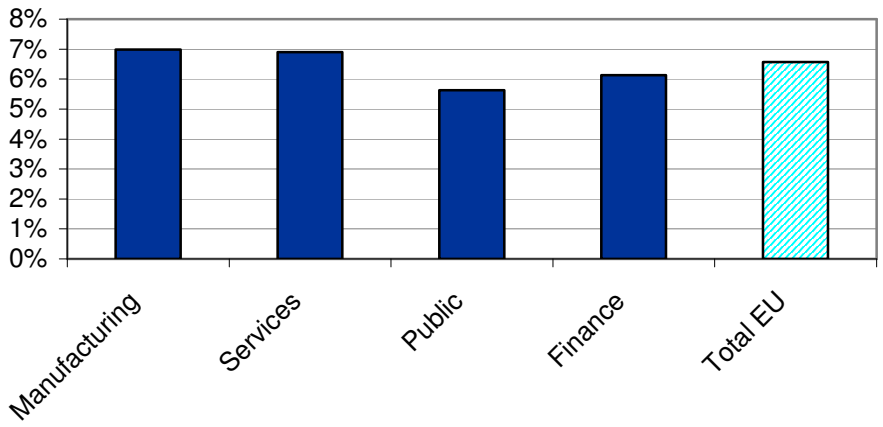
Note: Mean scores are based on a scale of 1–4, where 1 = I do not feel protected and 4 = I feel highly protected

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 26

EU Business Users that Experienced a Significant IT Security Breach in the Last Year, by Industry (% of positive answers)

Q. Has your organisation experienced a significant IT security breach in the last year?



N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Trends of IT Security Spending and Future Plans of Adoption by industry

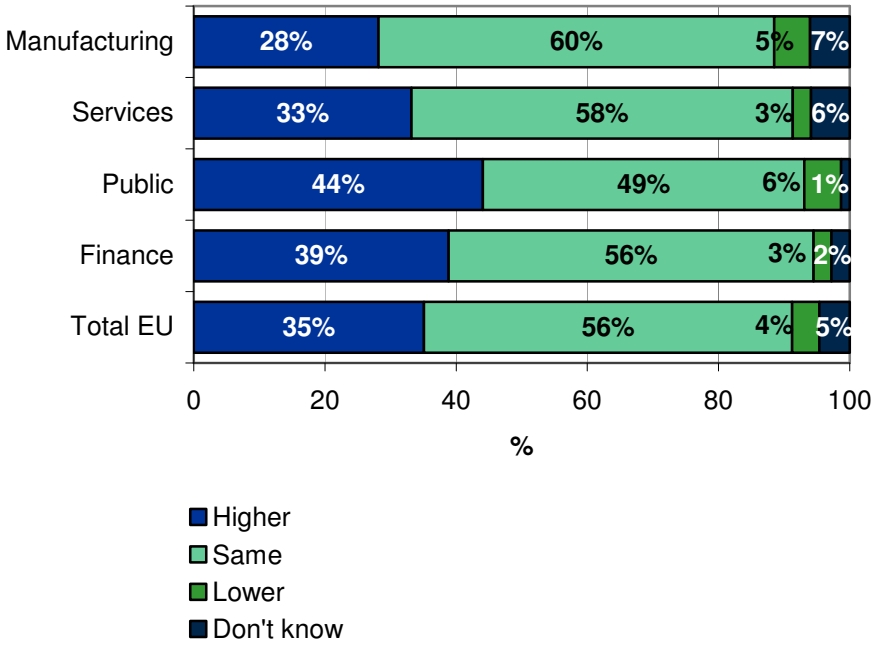
The majority of EU businesses plan to maintain stable their security budget in the near future, but about a third (35%) plan to spend more. Analyzing these trends by industry, it is clear from the following figure that more enterprises in the public sector and (less so) the finance industry plan to increase their budgets, than the EU average.

On the other hand, manufacturing and services industries count fewer enterprises than the EU average with plans to increase their security spending; these sectors' firms are more likely than the EU average to maintain stable budgets. Overall, only a tiny minority in all industries plans to decrease security spending (the highest percentage, 6%, is in the public sector).

FIGURE 27

EU Business Users, Trends of IT Security Spending, by Industry (% of enterprises)

Q. During 2008 how your IT security spending will change?



N = 1,138

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

Comparing future plans of adoption of security solutions by industry, we can draw the following considerations:

- **Manufacturing**. The level of adoption is quite aligned with the EU average, showing that also in this industry attention towards security is high. Still a wide gap exists between small and medium enterprises (under 250 employees) and large ones. Indeed, SMEs still lag behind in the adoption of advanced or sophisticated solutions. Apart from basic solutions, manufacturing companies future adoption plans are above EU level for information and data protection tools and specific tools for mobile users. This underlines the increasing importance for this industry to deal securely with information across the value chain, and the need to enable mobile employees to use laptops and smart-phones safely and efficiently.

- **Services**. This sector (highly differentiated) shows the lowest adoption rate of security hardware, security services and specific tools for mobile users. Also in this sector SMEs lag behind large corporations in terms of present adoption. Future adoption plans are very high (compared to the other sectors) for managed security services. For all other solutions, the number of enterprises planning adoptions remains close or below EU averages.

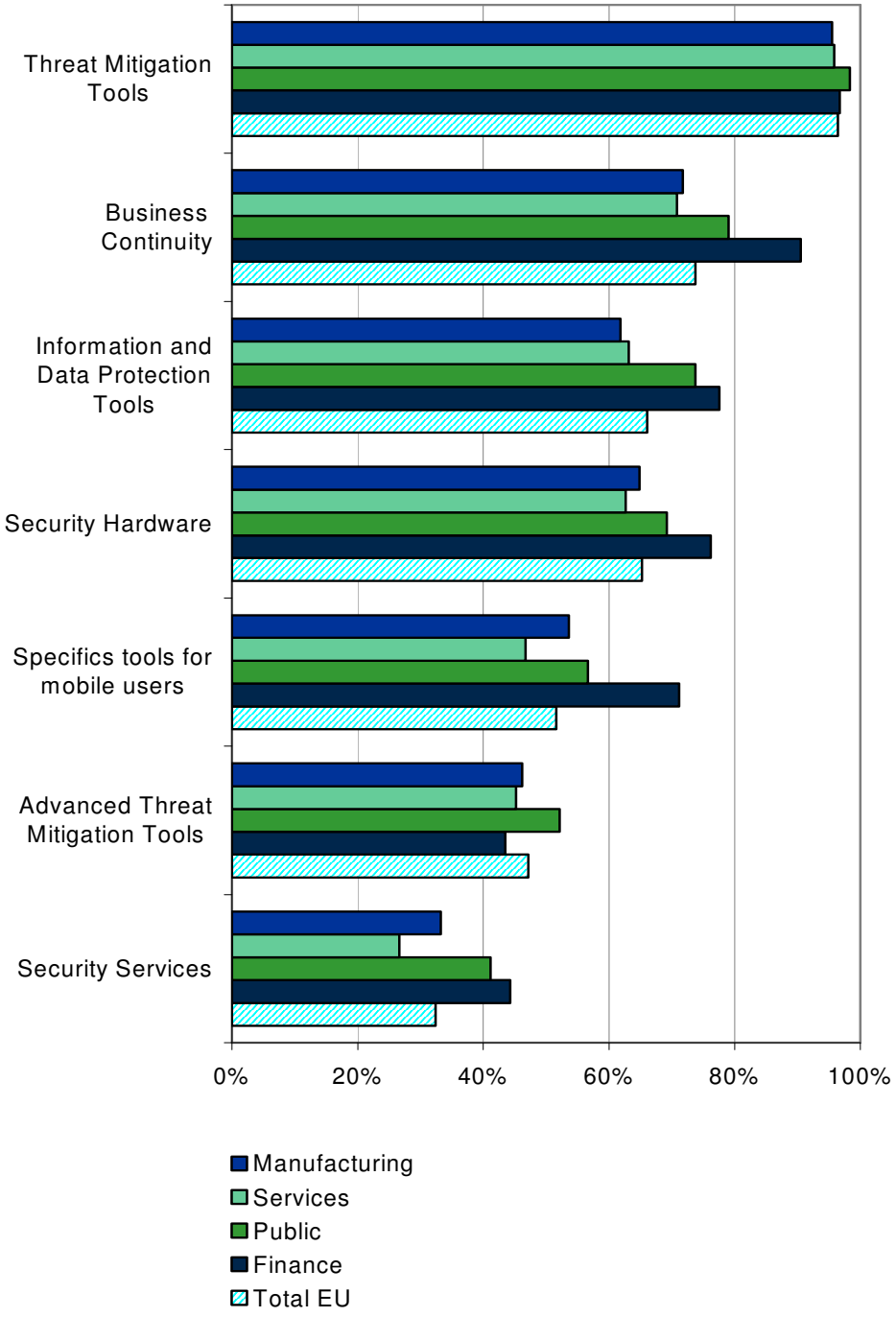
- **Public Sector**. Public agencies show security solutions adoption levels higher than the EU average; this sector shows the highest level of adoption of advanced threat mitigation tools, and also the highest level of future plans, indicating a continuing attention to sophisticated solutions. This sector shows strong demand trends, as plans of adoption are higher than average also for security hardware and information and data protection tools.

- **Finance**. This is the most sophisticated and advanced industry, as already mentioned, and has the highest adoption rate for many solutions, that are business continuity, information and data protection tools, security hardware, security services and specific tools for mobile users. The finance industry has been strongly negatively impacted by the global financial crisis and in addition companies in this industry already adopt very sophisticated solutions. Thus future plans of adoption are relatively low.

FIGURE 28

EU Business Users, IT Security Products Current Adoption, by Industry (% of enterprises)

Q. Which of the following products has your organization implemented?



N = 1,180

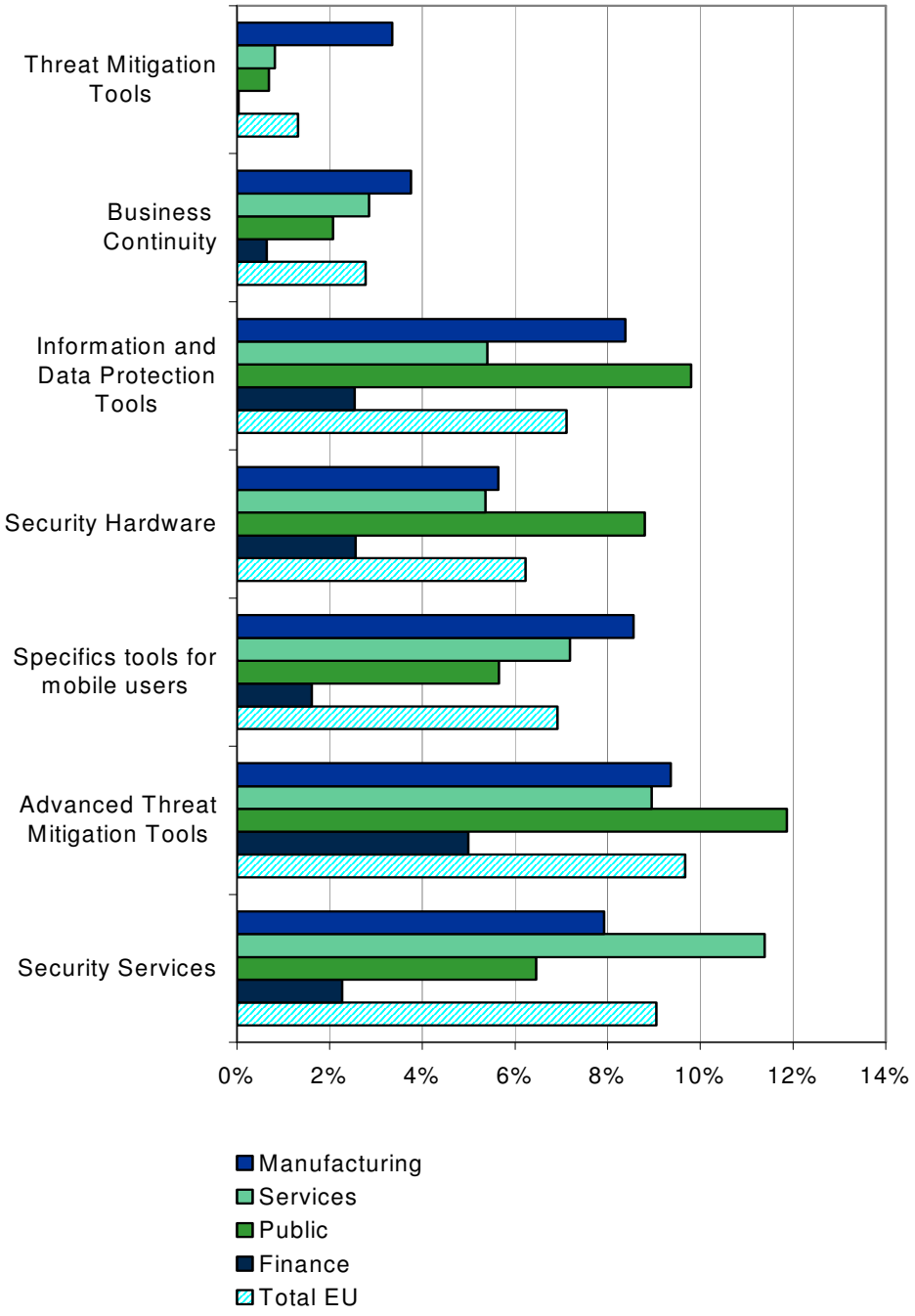
Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 29

EU Business Users, IT Security Products Future Adoption Plans, by Industry (% of enterprises)

Q. Of those products your company has not already implemented, which ones are you planning to implement in the next 12 months?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

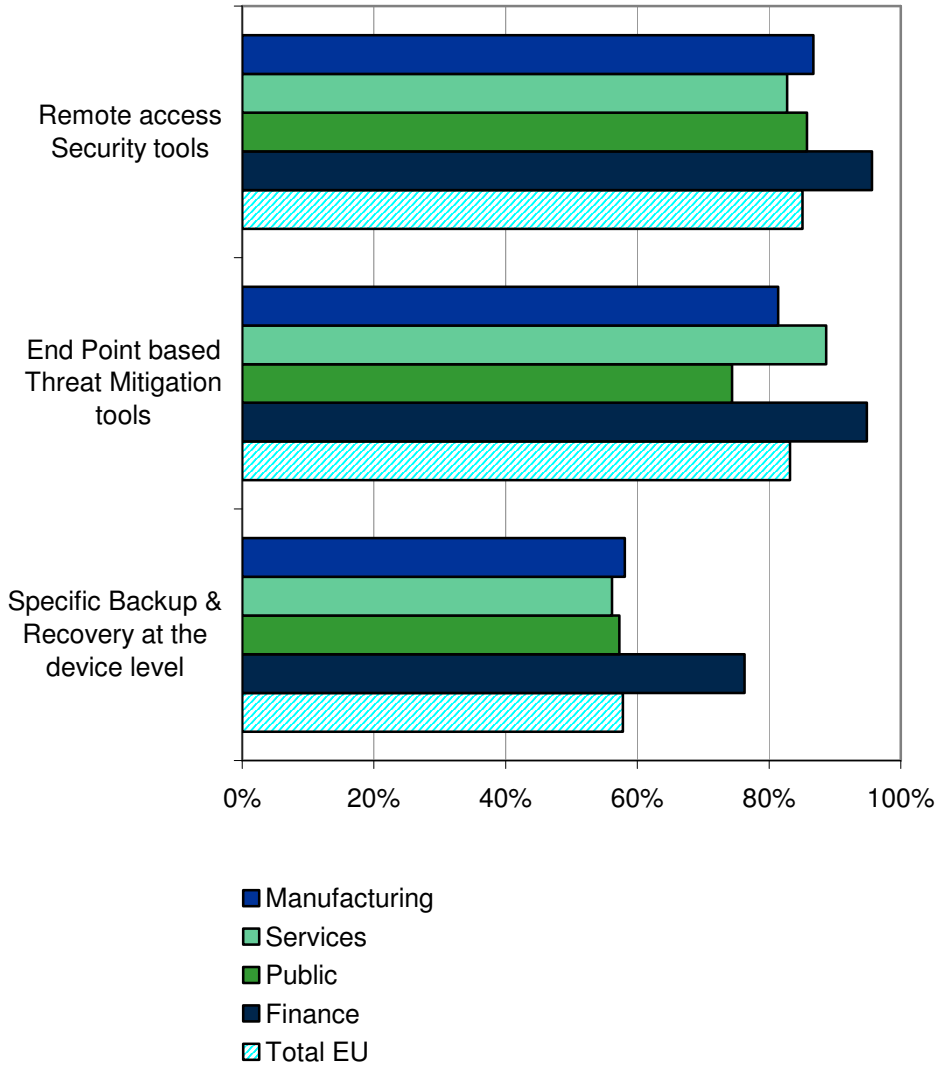
Mobile Security Adoption by Industry

The protection of mobile devices is increasingly important across all industries. Not surprisingly, financial organizations are the most advanced, with almost universal diffusion of remote access security tools and end point based threat mitigation tools (respectively by 96% and 95% of users). Also specific backup & recovery at the device level are quite common being used by more than 3 out of 4 enterprises in this industry. However, also in the other industries there is a high diffusion of mobile security tools for laptops, without strong differences by size. Concerning the protection of personal mobile tools, which is much less diffused, again the financial industry shows slightly higher rates, while manufacturing and services enterprises (particularly SMEs) show adoption levels lower than the EU average.

FIGURE 30

EU Business Users, IT Security Products for Mobile Users
Current Adoption, by Industry (% of enterprises)

Q. Which of the following specific tools for mobile users do you use?



N = 632

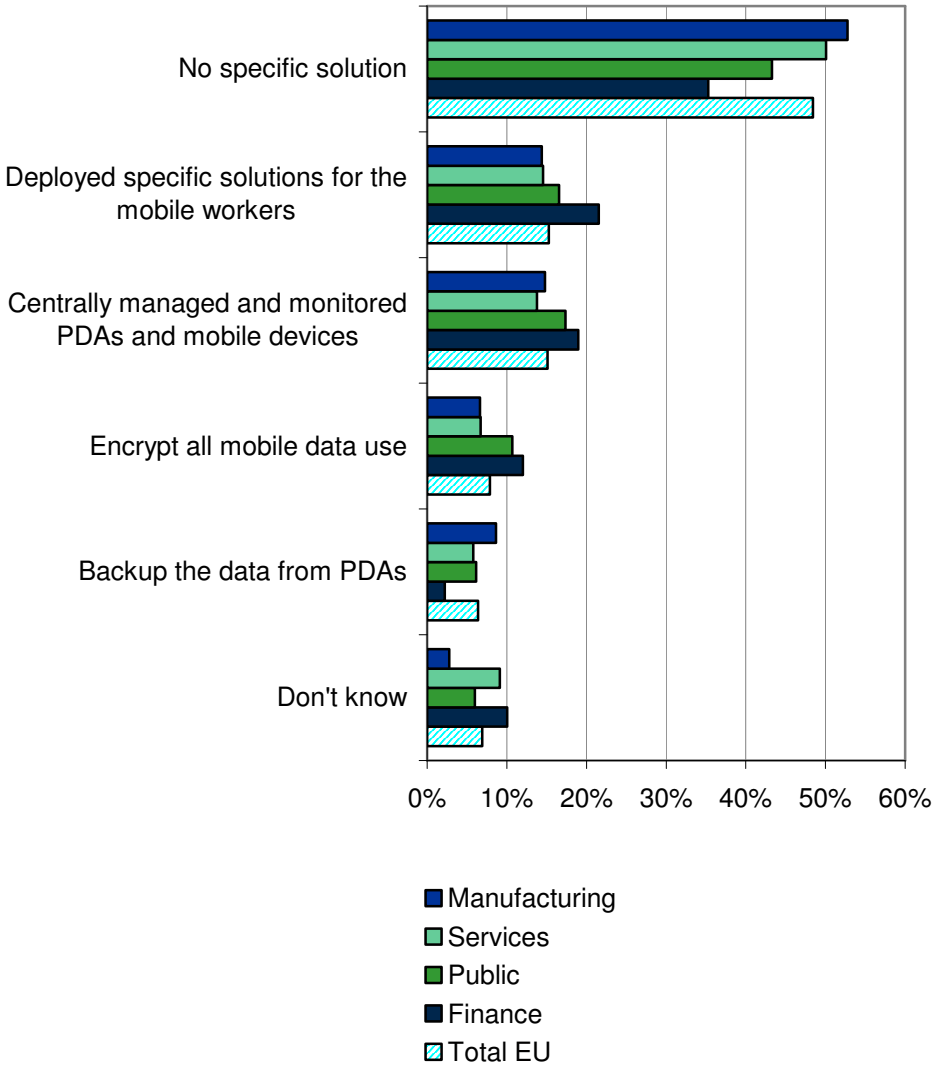
Base = Companies that deploy mobile solutions. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 31

EU Business Users, Protection of Personal Mobile Tools, by Industry (% of enterprises)

Q. How do you protect the personal mobile tools provided by your organizations to employees?



N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

The relationship with Suppliers: Selection criteria and Satisfaction by industry

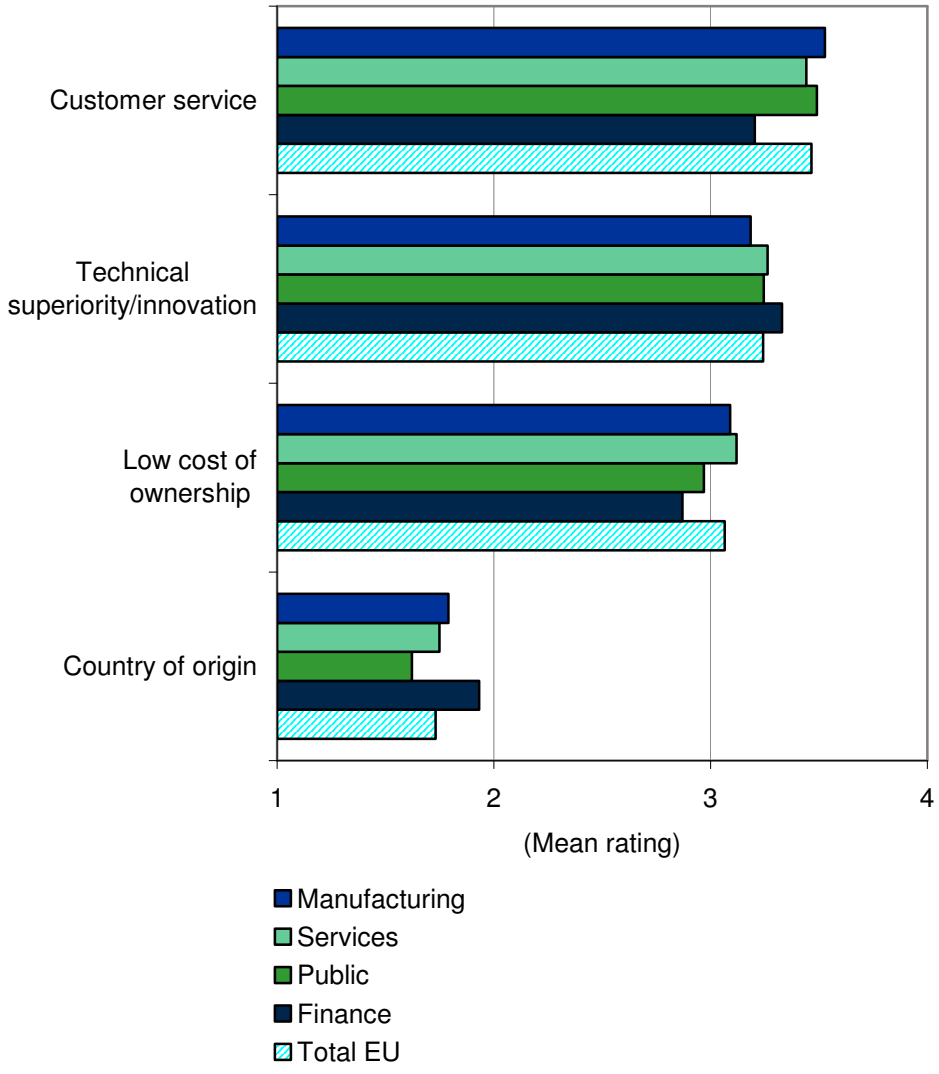
From the point of view of the relationship with suppliers, the Manufacturing, Services and Public sector organizations all rated customer service as the most important criterion for selecting a supplier, followed by technical innovation and total cost of ownership, with very similar scores. These same sectors rated their satisfaction levels for these items as slightly lower than importance, highlighting the existence of a gap, particularly in the case of customer service.

The financial services industry instead ranked innovation as the most important criterion (3.3, in a scale of 1 to 4 where 3 means "important"). Customer service follows closely (3.2), while cost is relatively less important (2.9). This depends on this industry's greater needs for sophisticated solutions keeping pace with new threats.

FIGURE 32

EU Business Users, Criteria of Selection of Primary IT Security Provider, by Industry (Mean rating)

Q. Which criteria do you consider important for the choice of your primary IT Security Provider?



N = 1,180

Base = All sample

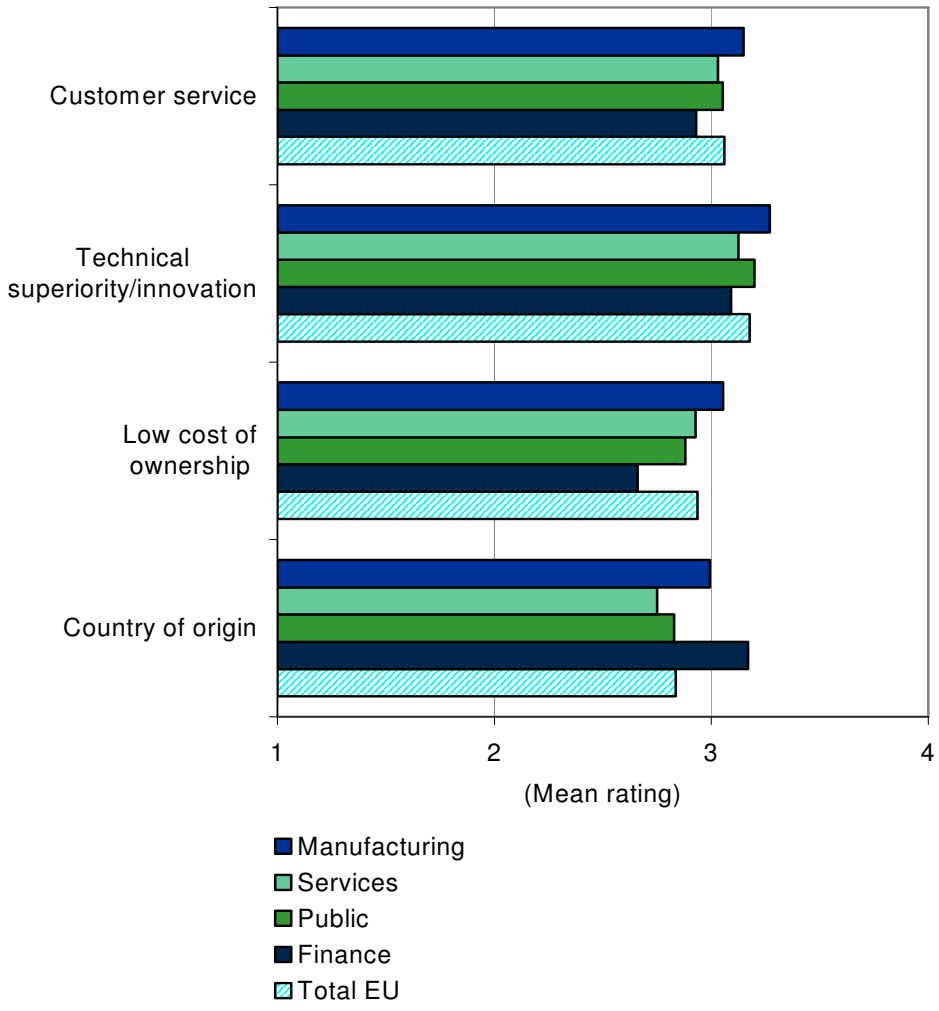
Note: Mean scores are based on a scale of 1–4, where 1 = Not at all important and 4 = Highly important

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 33

EU Business Users, Satisfaction of Primary IT Security Provider's Performance, by Industry (mean rating)

Q. Can you indicate your level of satisfaction, for each of the following areas, of your three most important security suppliers?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = Very unsatisfied and 4 = Very satisfied

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Procurement Channels by Industry

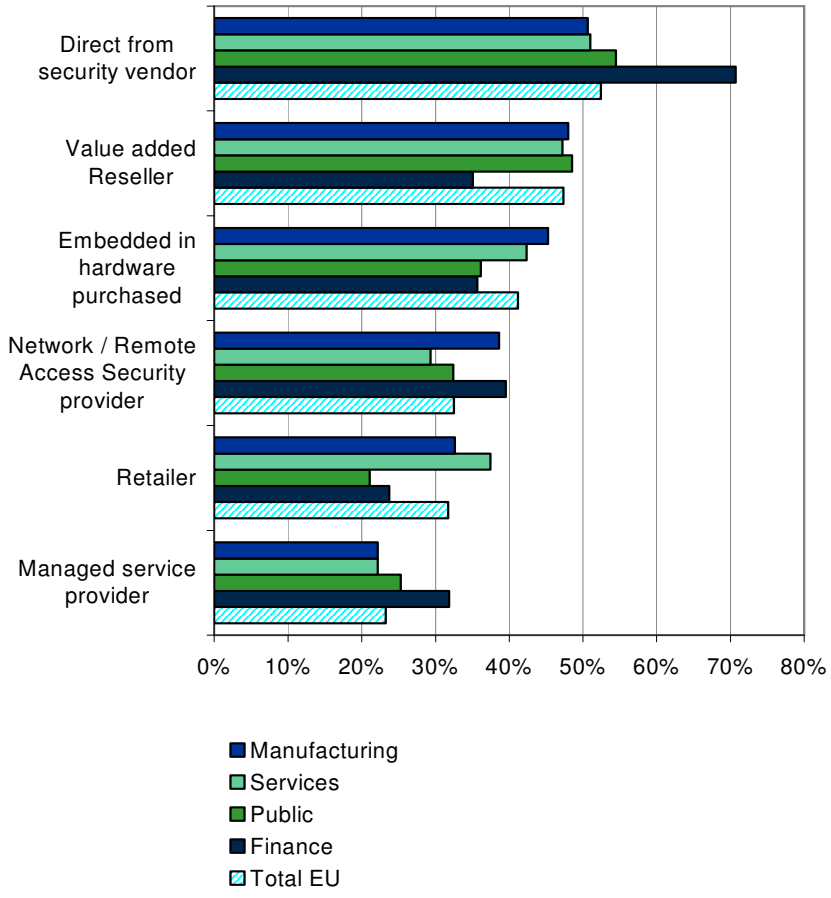
Concerning procurement channels, most business users use more than one source, most often on the one hand security vendors and on the other hand hardware embedded solutions (for the basic tools, normally). There is also an important role of VARs (which remains alongside with the direct relationship with vendors). Sourcing from

retailers is more frequent in the Manufacturing and Services industries particularly by SMEs of these sectors (more inclined to use mass market channels). The Public Sector instead shows the highest level of use of VARs. The financial industry again shows slightly different behavior from the other industries, with the higher incidence of direct relationship with security vendors, as well as with Network security providers and Managed Services Providers. This reflects their greater sophistication in the use of IT security and the broader range of their needs.

FIGURE 34

EU Business Users, Main Procurement Channels of IT Security Products, by Industry (% of enterprises)

Q. Where would you normally source the security products you use or plan to use?



N = 1,169

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

5. THE EUROPEAN SECURITY MARKET BY COMPANY SIZE

Overview by Company Size

Small, mid-sized and large enterprises behave differently in terms of security perception and related IT solutions adoption. The following paragraphs analyze the differences of EU enterprises security strategies, across four size classes:

- Small enterprises with 1 to 99 employees further segmented into:
    - Companies with 1 to 9 employees (micro-enterprises)
    - Companies with 10 to 99 employees
- Mid-sized companies with 100 to 249 employees
- Large companies with more than 250 employees.

Enterprises under 250 employees are defined Small and Medium Size Enterprises (SMEs).

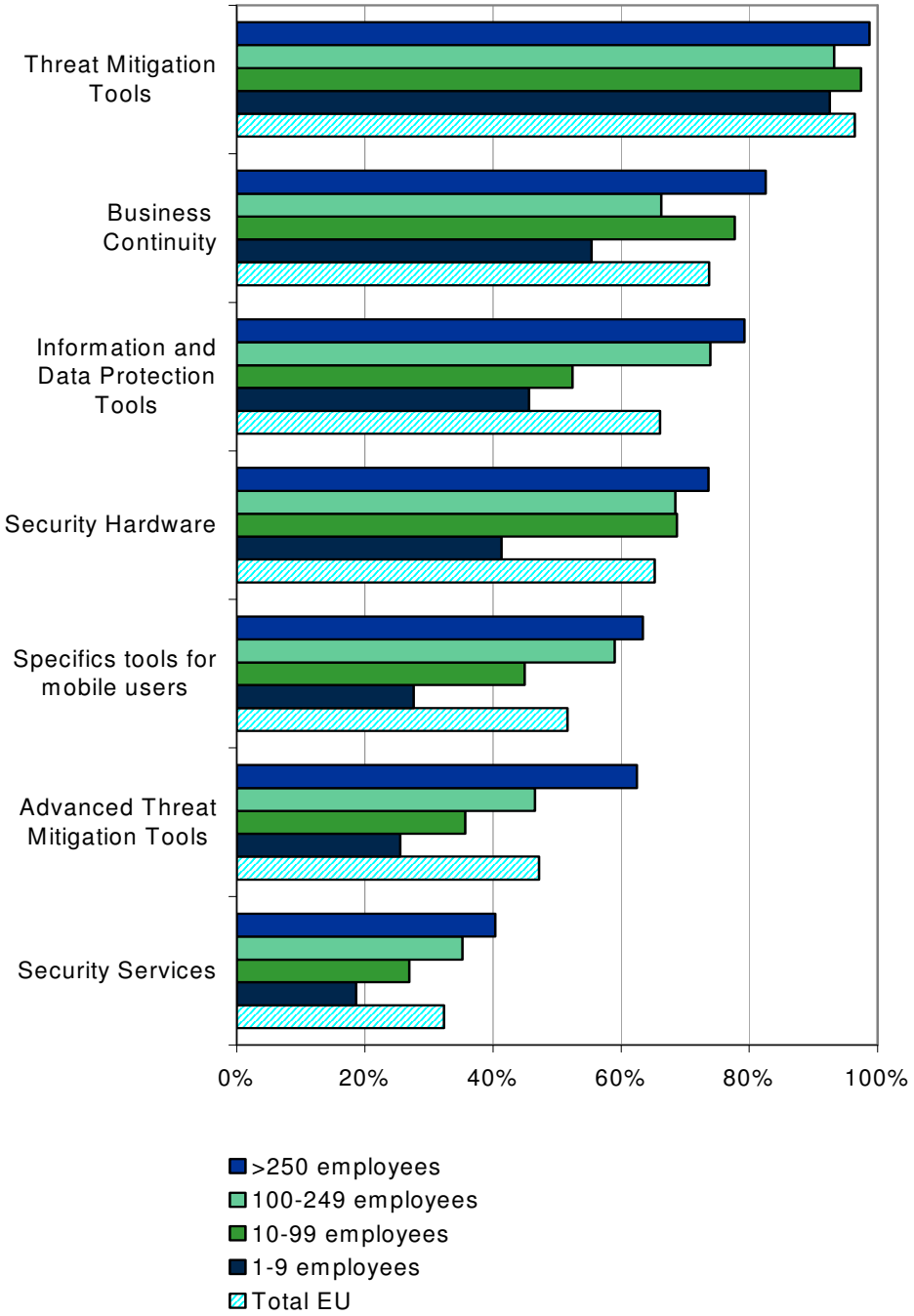
The range of security solutions adopted by business users is positively correlated with company size (*figure 35*). This was already anticipated in the description of the Business Users profiles (chapter 3), which shows how Low NIS Investment users are much more present in the small size-classes, while High NIS Investment Users are mainly enterprises with more than 100 employees. However, Average NIS Investment users are approximately half of all size classes; this means basically that small and micro-enterprises should not be undervalued, since many of them (around half) use more solutions than basic protection tools, particularly business continuity and information/data protection tools.

The solution areas where small enterprises lag behind medium and large ones concern the adoption of mobile security, advanced threat mitigation tools and, naturally, managed security services.

FIGURE 35

EU Business Users, Current Adoption of Security Solutions, by Company Size (% of enterprises)

Q. Which of the following products has your organization implemented?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Fears, Perceived Protection and Security Breaches by Company Size

Overall concern by EU enterprises about IT security varies between "I am a little worried" and "I am worried" (respectively measured as score 2 and 3 in a scale of 1 to 4), something which could be described as significant but not dramatic.

There is however a clear ranking of fears (without strong differences by size class), showing business interruption as the main concern, followed by loss of intellectual property and privacy violations. Companies understand that any forced interruption or loss of information may cause not only revenue losses, but also negative impacts on the corporate image and reputation. Recent cases of main government agencies and insurance companies mismanaging sensitive customer data generated wide press coverage, with very negative impacts on reputation. Therefore, European companies today are more concerned about avoiding similar accidents and more willing to invest in security. Indeed, business users evaluate the need to pay repair costs (because of security breaches) or penalties (because of violating security regulation) as less important than business interruption or loss of information. This indicates that European companies understand the high relevance of the indirect costs of a potential security breach, and attach to them a higher relevance than to direct costs for repairing systems or paying penalties.

The perceived protection against the same threats analyzed above is relatively high: the majority of EU enterprises declare to feel "somehow protected" (scores between 3 and 3.2 on a 1 to 4 scale, with few variations between the different threats). EU business users declare to feel more protected exactly for the two threats they fear most (business interruption and privacy breach). Analyzing results by company size, the ranking of fears does not change greatly for all the size classes, while perceived protection levels show some interesting variations as follows.

- **1-9 employees**. Companies in this size class present the highest level of concern about the financial cost of repair. Very small companies do not have enough economies of scale and usually more liquidity problems compared to large companies. For them, an unexpected repair activity can be more onerous than for larger companies. Not surprisingly, very small companies perceive the lowest level of protection. Their perceived protection is between 2.6 and 2.9 and is constantly the lowest if compared to the other size classes.

- **10-99 employees**. These companies have similar fears to the others, but surprisingly they show the highest level of perceived protection. These mid-sized enterprises probably underestimate their security risks, because in fact they tend to be the more likely targets of security attacks. Their perceived protection is measured between 3.1 and 3.4 (between I feel "somewhat protected" and "I feel very protected").

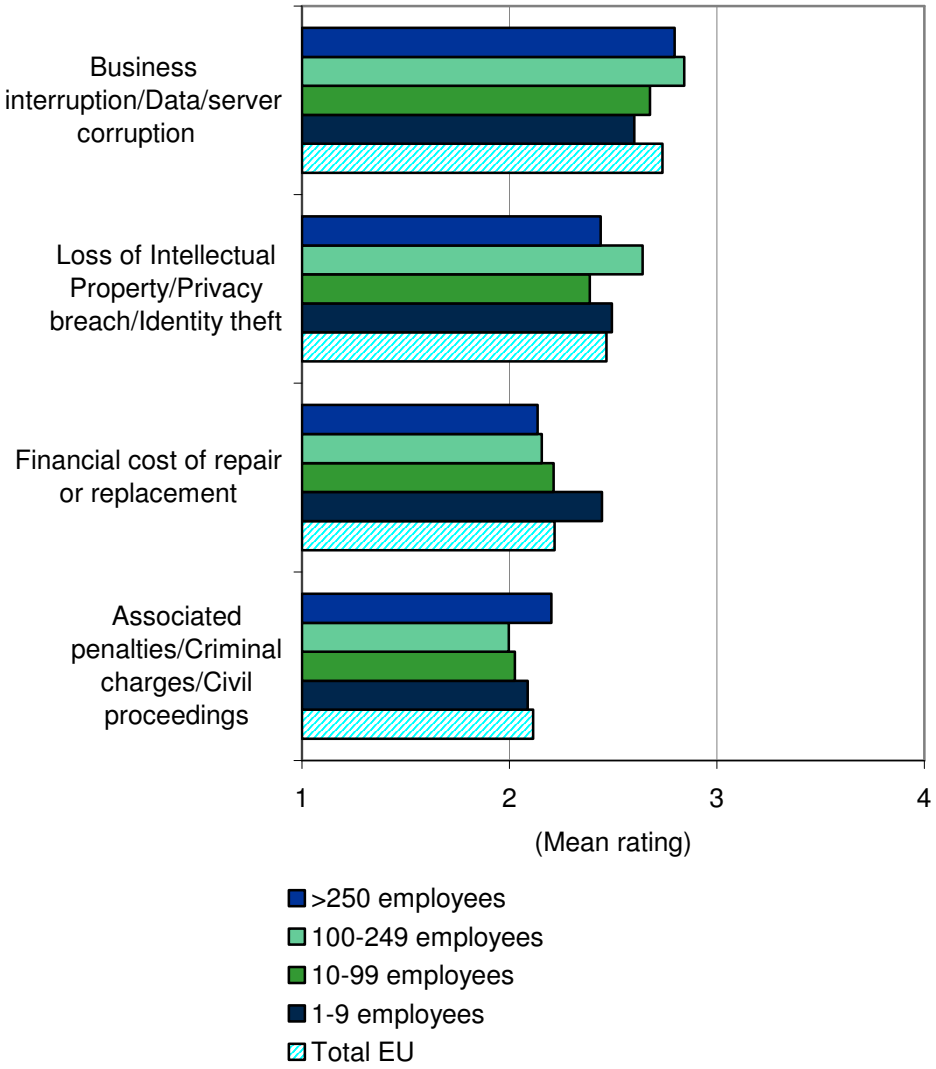
- **100-249 employees**. These enterprises show the highest fear score for business interruption and privacy breach issues (2.8 and 2.6 respectively). Also, for what is related to the cost of repair and to penalties, they have a score similar to those of large companies. This demonstrates that they are complex and IT savvy companies understanding the potential damages caused by security breaches. The management practices and needs of these enterprises are not so different from those of large ones, but must be maintained with lower budgets and fewer economies of scale (for specific investments and skills such as those required by IT security). This leads to their greater fears. At the same time, these enterprises appear to feel quite well protected (perhaps by their security investments).

- **>250 employees**. These enterprises have a keen awareness of potential threats and therefore a higher level of concern. They are particularly worried about the risk of penalties, since they are usually subject to strict regulations. At the same time, they are the least worried of the cost of repair. These companies are likely to have insurance or contracts with ICT suppliers, protecting them against the majority of accidents. Knowing the level and diffused presence of security threats, these large enterprises do not feel well protected (with perceived protection scores between 2.9 and 3.2).

FIGURE 36

EU Business Users, Fears related to IT Security, by Company Size (mean rating)

Q. With respect to IT security, could you tell us what do you fear the most?



N = 1,180

Base = All sample

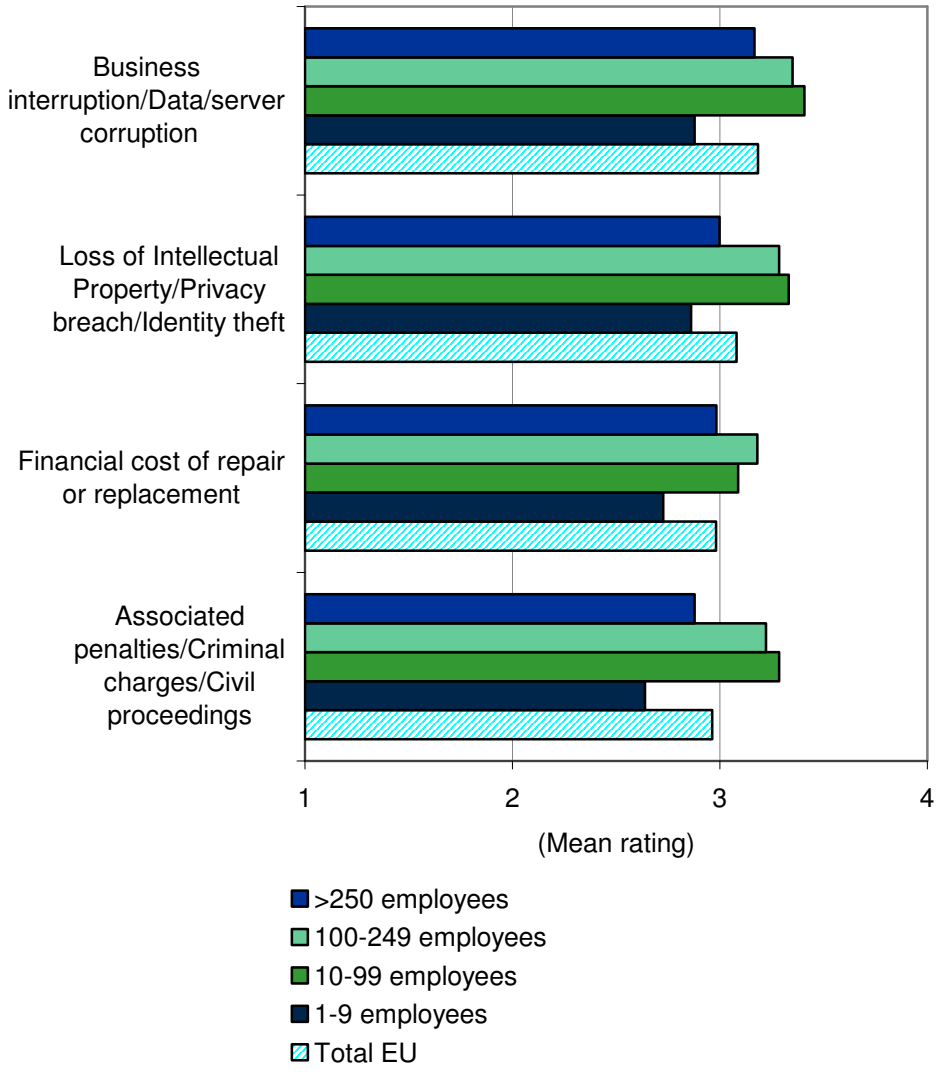
Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4= I am strongly worried

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 37

EU Business Users, Perceived Protection related to IT Security, by Company Size (mean rating)

Q. Could you provide us your feeling regarding your level of protection in each of the four areas? Do you feel protected/safe?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I do not feel protected and 4 = I feel highly protected

Source: IDC GI Survey of EU ICT Security Market, 2008

Security Breaches by Company Size

On average, 7% of interviewed companies experienced a security breach in the last year.

As anticipated above, firms in the 10-99 employees size class suffered the highest incidence of security problems, while they present the

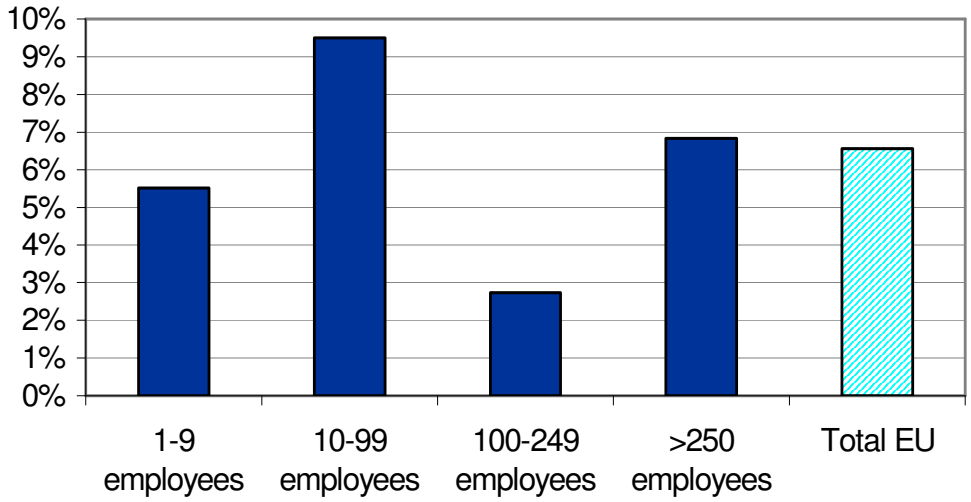
highest level of perceived protection. This mismatch is well known in the industry and is mentioned also in the stakeholder interviews. Very small companies (1-9 employees) are instead less advanced in terms of technology adoption and therefore are also less likely to be target of security attacks. However they have such a low level of sophistication, that they may have experienced an attack without even recognizing it.

An important factor is the visibility of security breaches, which is related with the frequency of reported problems. According to the study, only about 20% of interviewed companies have an obligation to report these accidents to a public body. This percentage does not vary substantially by size class, even if large firms (who are expected to have stricter security breaches reporting obligations) are more likely to do so. Clearly, monitoring security breaches is not a widespread obligation, and there is no guarantee that firms will respect it in absence of strong enforcement.

FIGURE 38

EU Business Users that Experienced a Significant IT Security Breach in the Last Year, by Company Size (% of positive answers)

Q. Has your organisation experienced a significant IT security breach in the last year?



N = 1,180

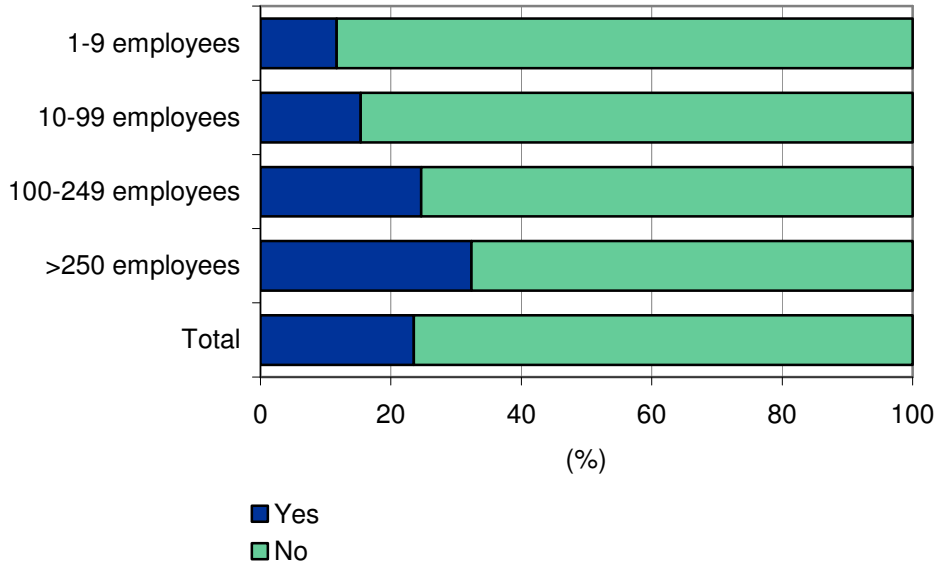
Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 39

EU Business Users, IT Security Breach Reporting, by Company Size (%of enterprises)

Q. In case of IT security breach, do you have to report it to a Public organization?



N = 1,180

Base = All sample

Source: Survey of EU ICT Security Market, 2008

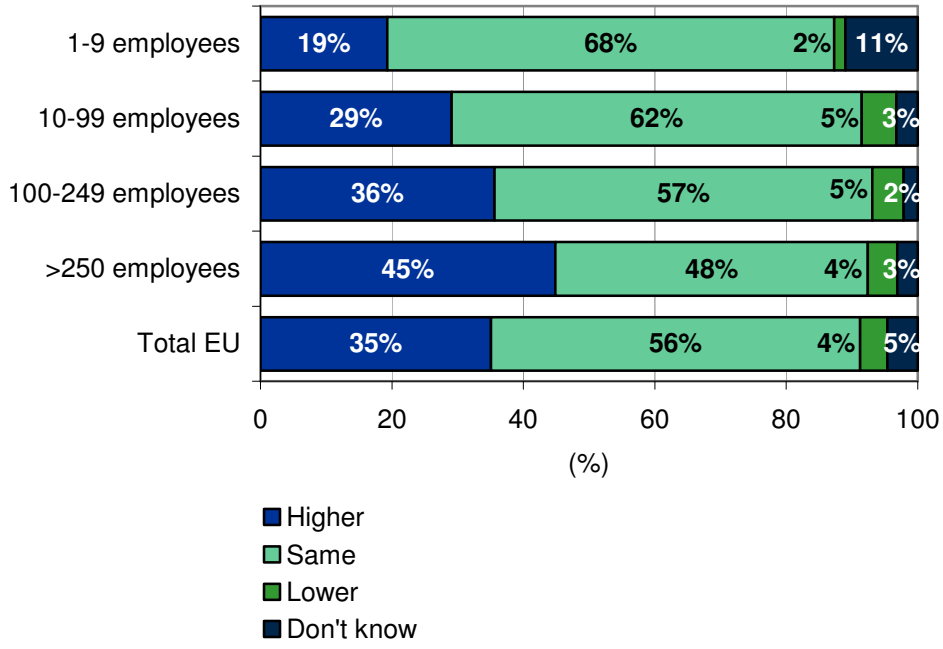
Main Trends of IT Security Spending and Future Plans of Adoption

The majority of European enterprises plan to maintain a stable security budget (56%), while very few plan to decrease their spending (*figure 40).* There is again a correlation between company size and future spending intentions: even if large enterprises already have the largest security budgets, still almost half of them (45%) plan to increase spending (adopting more advanced solutions, as indicated below). On the other hand, only 19% of micro enterprises think to spend more for security in the near future.

FIGURE 40

EU Business Users, Trends of IT Security Spending, by Company size (% of enterprises)

Q. During 2008 how your IT security spending will change?



N = 1,138

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

The next chart present the investment priorities indicated by EU enterprises for the solutions which they do not already implement. These results should not be read as growth areas in terms of market value, but as declarations of interest for new investments.

Given the very high current adoption of threat mitigation tools, only 1% of companies plan to invest in this area for the first time. This means that in 12 months from now, 97% of interviewed companies will have some basic security solution in place.

More interestingly, 10% of companies plan new investments in advanced threat mitigation tools (Anti-Phishing Web Reputational systems, Anti Intrusion Detection systems, Forensic collection, Internal Threat Management tools), and some 7% will invest in information and data protection (Encryption, Port Control, Strong authentication, Data Leakage Prevention).

This points to a move towards a more sophisticated and holistic approach to security. As companies keep on automating business processes, they will increasingly need identity and advanced threat management solutions. They will also need more services to build up

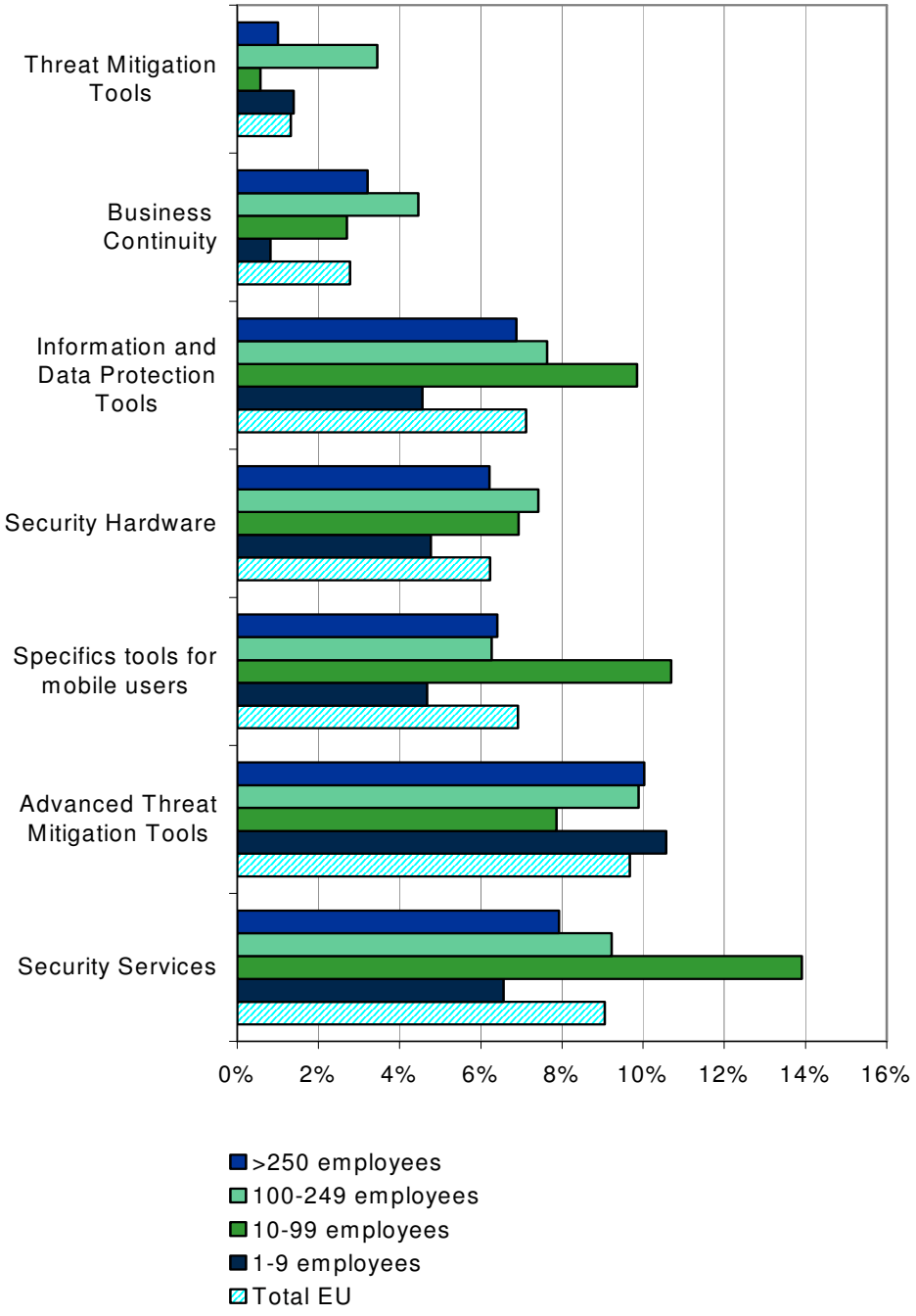
an effective company-wide security strategy: 9% of companies are planning investments also in security services.

The emerging adoption of new technologies, also by SMEs, including for example Voice over IP or Mobile solutions, will strengthen this need in the coming years. 7% of companies already plan new investments in specific tools for mobile users. These tools are analyzed in details in the following paragraphs.

FIGURE 41

EU Business Users, IT Security Products Future Adoption Plans, by Company Size (% of enterprises)

Q. Of those products your company has not already implemented, which ones are you planning to implement in the next 12 months?



N = 1,180

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Mobile Security Solutions Adoption by Company Size

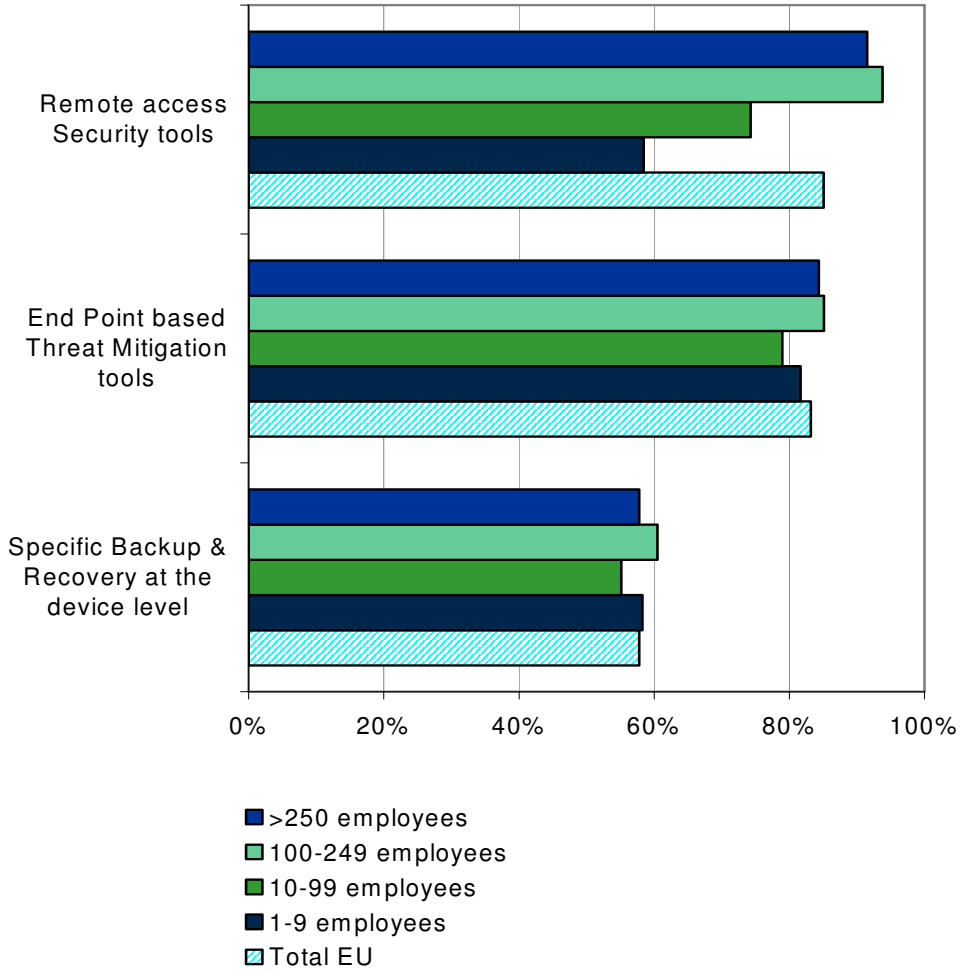
As the adoption of mobile solutions is increasing, some 52% of respondents already deploy some tools to protect mobile devices, and 7% plan new investments in this area in the next 12 months. The next figure shows a breakdown of IT security products used by mobile users. Both remote access security tools and end-point based threat mitigation tools are widespread: the adoption level is 85% and 83%, respectively. Instead, specific backup & recovery at the device level is deployed by 58% of the respondents that use mobile security products.

Companies with more than 100 employees are more advanced in the protection of their mobile devices. The survey investigated also the level of protection of personal mobile devices provided to employees, which is still far from widespread. Most companies do not have a specific solution in place: this hold true especially for small companies (with 1-9 employees).

FIGURE 42

EU Business Users, Current Adoption of IT Security Products for Mobile Users, by Company Size (% of enterprises)

Q. Which of the following specific tools for mobile users do you use?



N = 632

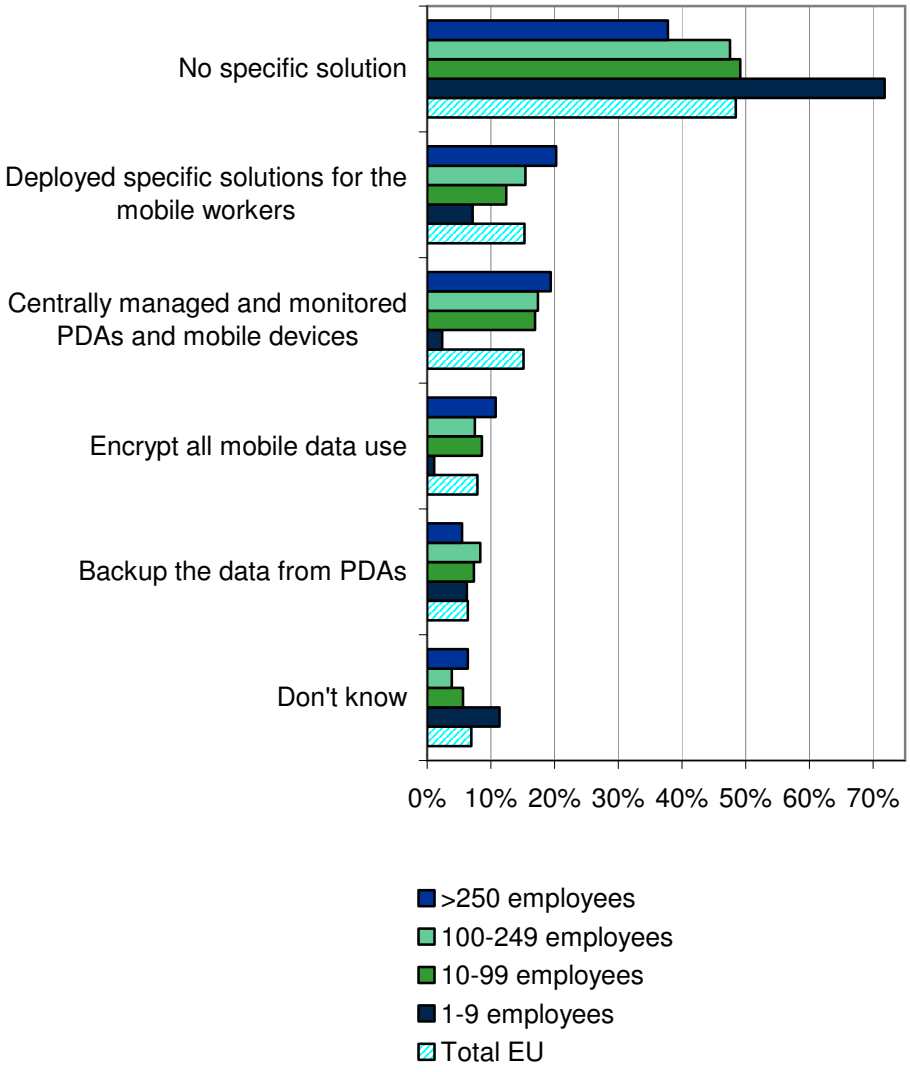
Base = Companies that deploy mobile solutions. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 43

EU Business Users, Protection of Personal Mobile Tools, by Company Size (% of enterprises)

Q. How do you protect the personal mobile tools provided by your organizations to employees?



N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

Relationship with Suppliers: Selection Criteria and Satisfaction by Company Size

EU enterprises have no doubt regarding the most important criterion of selection of a security provider: customer service, which is ranked 3.5 on a 1 to 4 scale (1 stands for *not at all important* and 4 for *highly important*) and is relevant for all size classes. The level of technical superiority/innovation of the offering is also considered quite important. The vendors' country of origin is not a significantly important criterion of choice.

The survey included an additional question about the most important aspects of customer service for business users, from quality to flexibility. The answers show that all aspects are considered extremely important. In particular, quality and reactivity are considered the most important aspects of customer service, followed closely by affordable costs.

The variations of business users' opinions by size class are rather interesting, as follows:

- **1-9 employees.** Very small companies assess technical superiority and low cost of ownership as more important for them than other enterprises. These companies ask to their suppliers to provide more with less, meaning that they are want to invest little, but still want innovation, despite their tighter budgets. In fact, they also rate customer service at the same level of importance.

- **10-99 employees.** Companies in this band attach a relatively lower importance than other enterprises to cost, while they privilege customer service.

- **100-249 employees.** These enterprises assess customer service at the highest level of importance, even if by a small margin compared to the other size bands.

- **>250 employees.** Larger corporations rate customer service over the other aspects by a small margin, while only the country of origin of the supplier is considered irrelevant.

The survey investigated the level of business users' satisfaction with their security suppliers, for the same criteria examined above. Despite some differences, business users declare themselves mostly satisfied with the performance of their suppliers, for all the aspects investigated (with a score between 2.8 and 3.2. in a scale of 1 to 4, where 3 means "I am somehow satisfied").

Ideally, if satisfaction levels are high on the most important aspects for the users, the match demand-supply should be adequate. The survey results instead show a gap between importance and satisfaction levels. For the three most important criteria, satisfaction remains below the importance level. In particular, the gap between importance and satisfaction is widest for the first selection criterion, customer service. The aspect earning the highest satisfaction score is the *technical superiority/innovation*, graded 3.2.

There appears to be a mismatch between the aspects of higher importance for the business users, and the performance of the vendors; the alignment between demand and supply does not appear sufficient.

Companies are generally satisfied with the technical quality of the security products they buy. But technology is not enough. They clearly miss:

- A more effective support from their providers, covering both technical and business-related aspects. This can ultimately help companies building up security policies, able to protect the information lifecycle in companies' business processes.

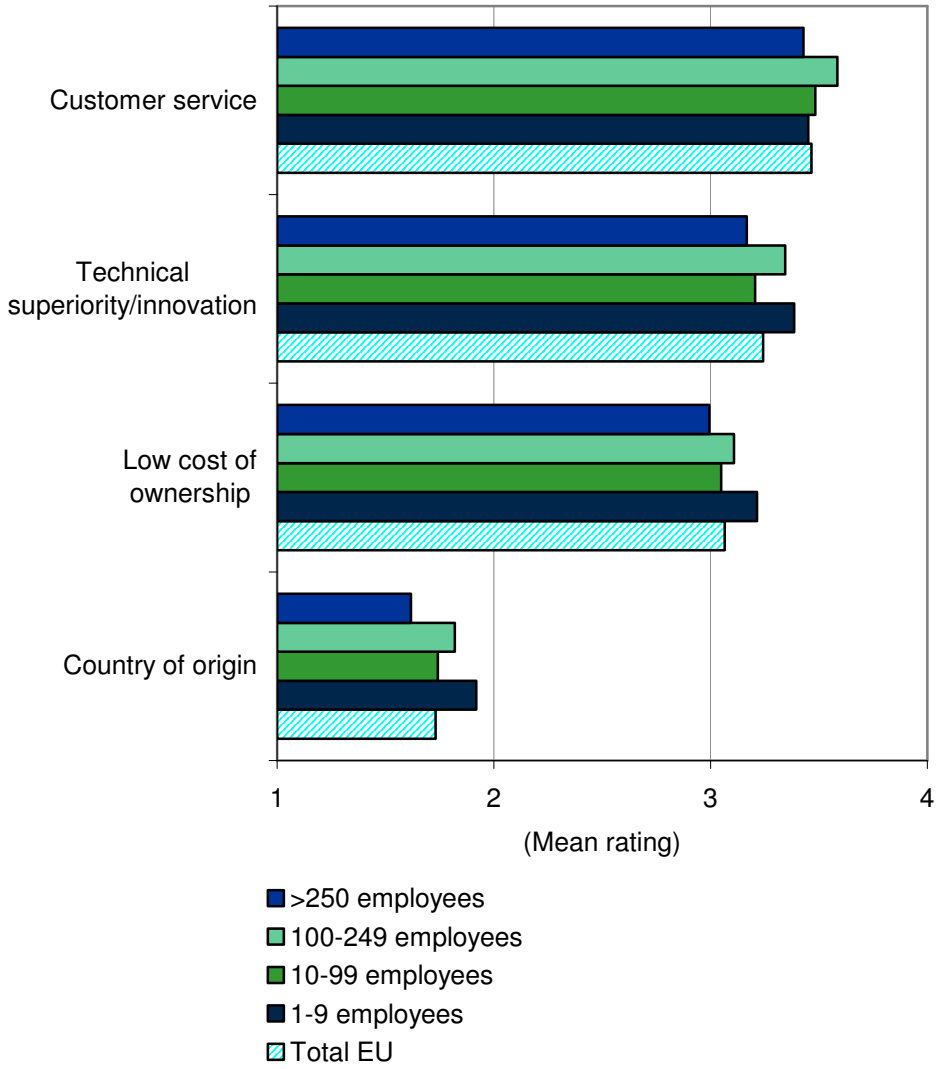
- A lower cost of ownership, or cost associated to the time and resources needed to run, and maintain the solution. Interviewed companies recognize that reducing indirect costs is key for their business success. With limited IT skills (especially at the low end of the market), a strong need to focus on core competencies, a compelling need to gain efficiencies and become more agile in the global world, the cost of ownership of IT solutions (and in particular of security solutions) is more of an issue than the costs of buying the solution itself.

Variations of satisfaction scores by company size appear limited, with the exception of small companies, that give a slightly higher satisfaction score to low cost of ownership. But small firms rate the total cost of ownership as relatively more important than other firms. Therefore a gap between importance and satisfaction exist also in this case.

FIGURE 44

EU Business Users, Criteria of selection of Primary IT Security Provider, by Company Size (Mean rating)

Q. Which criteria do you consider important for the choice of your primary IT Security Provider?



N = 1,180

Base = All sample

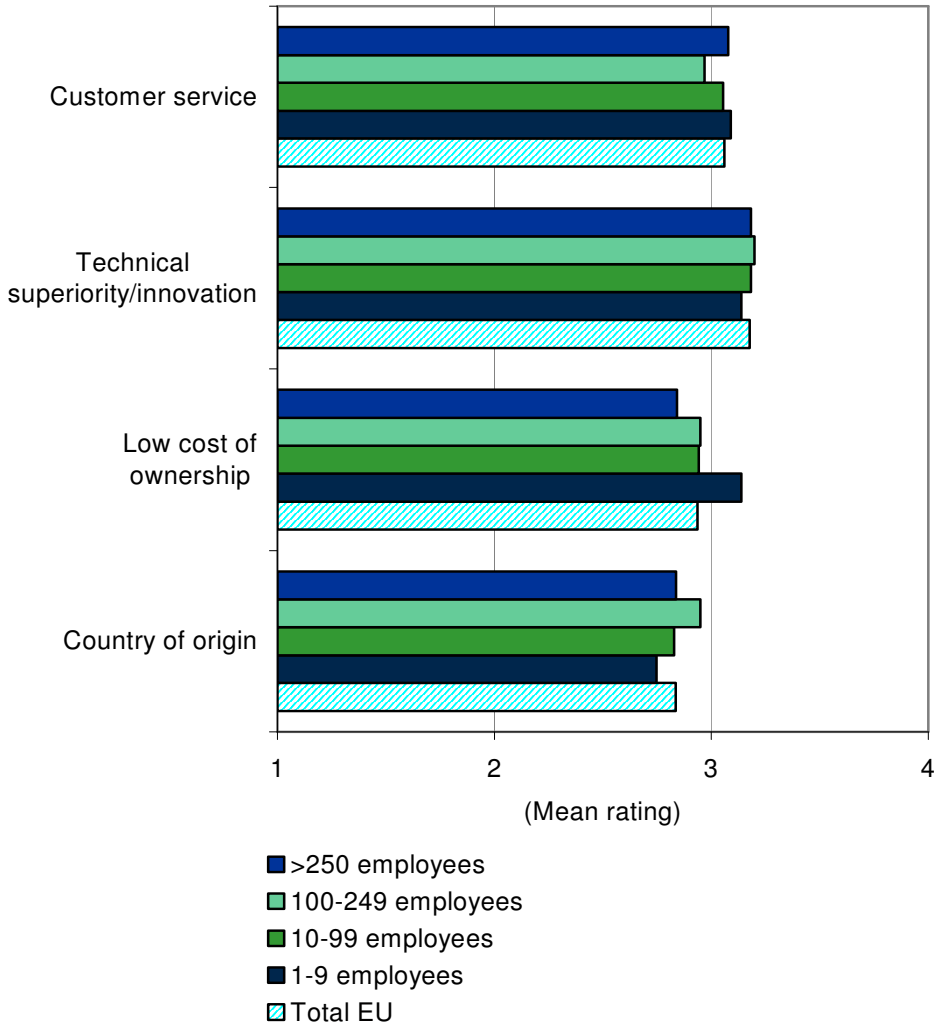
Note: Mean scores are based on a scale of 1–4, where 1 = Not at all important and 4 = Highly important

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 45

EU Business Users, Satisfaction of Primary IT Security Provider's Performance, by Company Size (mean rating)

Q. Can you indicate your level of satisfaction, for each of the following areas, of your three most important security suppliers?



N = 1,180

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = Very unsatisfied and 4 = Very satisfied

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Procurement Channels by Company Size

EU enterprises use a wide range of procurement channels for IT security products and services, as shown in the following figure. There are not exclusive relationships here, rather a web of relations, changing depending on needs and circumstances.

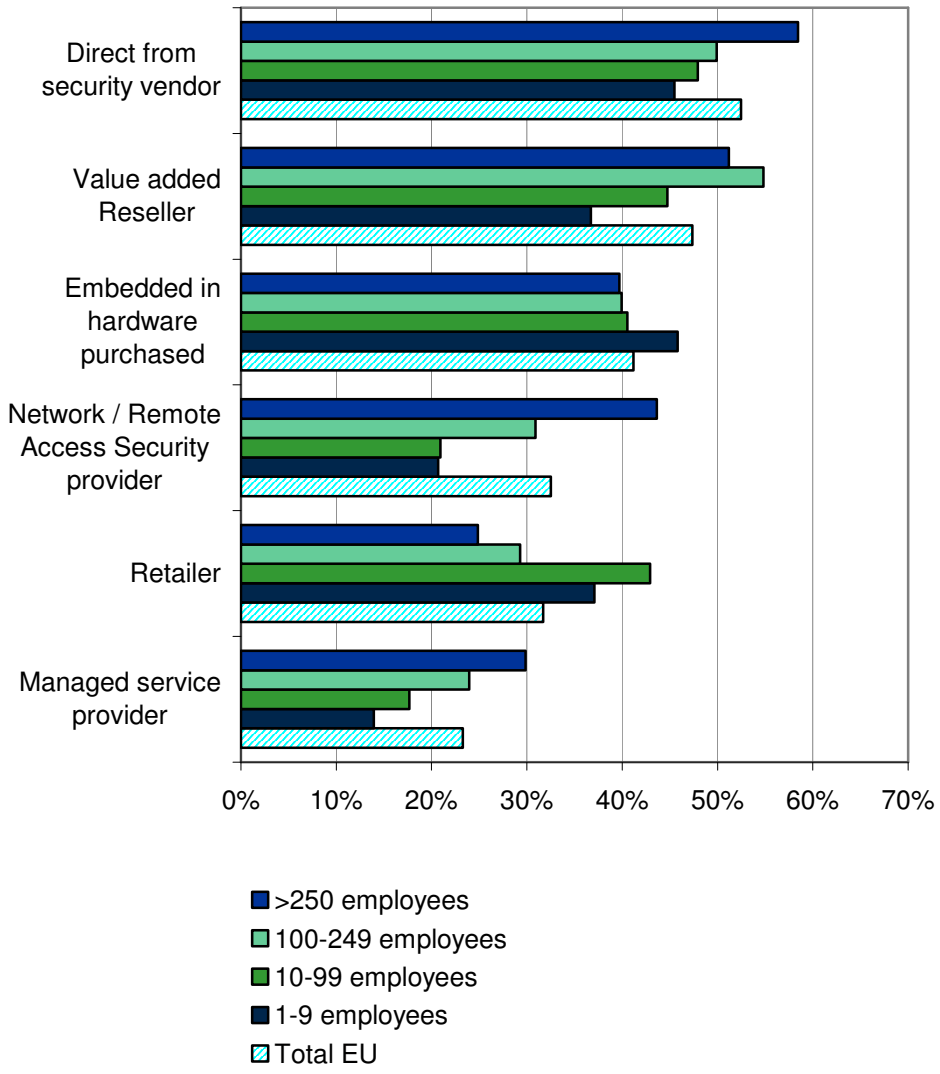
As anticipated in the analysis by profile, more sophisticated IT users (who tend to be large and medium-sized firms) tend to buy from

security vendors, VARs, and Network Service providers, as well as using (for the basic solutions) hardware embedded products. Small enterprises, instead, tend to rely more on mass-market channels that is hardware embedded products but also retailers. Still, they may very well buy from specialized suppliers or VARs. Micro enterprises are least likely to use Managed service providers.

FIGURE 46

EU Business Users, Main Procurement Channels of IT Security Products, by Company Size (% of enterprises)

Q. Where would you normally source the security products you use or plan to use?



N = 1,169

Base = All sample. Multiple responses

Source: IDC GI Survey of EU ICT Security Market, 2008

Towards "Security as a Service" for SMEs

Security-as-a-service (SaaS) is an emerging way to deliver security on-demand, with clear advantages for all enterprise size-classes. Nevertheless, so far only a minority of EU businesses has adopted it (about 12%, according to our survey data). Another 7% of companies have plans to adopt it in the next 2 years.

Overall, security as a service is particularly interesting for SMEs, because it represents a way to deploy innovative solutions without incurring in huge investments. For larger enterprises, it can provide greater flexibility and scalability advantages.

Other factors are driving this emerging demand:

- Increasing broadband availability, enabling delivery;
- Vendors entering the market;
- Lower cost to implement and maintain security solutions;
- The ability to transfer implementation and infrastructure risks, which is seen as increasingly important;
- The possibility to serve multiple remote offices, a key requirement stressed by globalization trends.

There is a strong ongoing discussion on the attractiveness of software-as-a-service for the SMEs market. The on-demand delivery mode can certainly bring many advantages to SMEs, including:

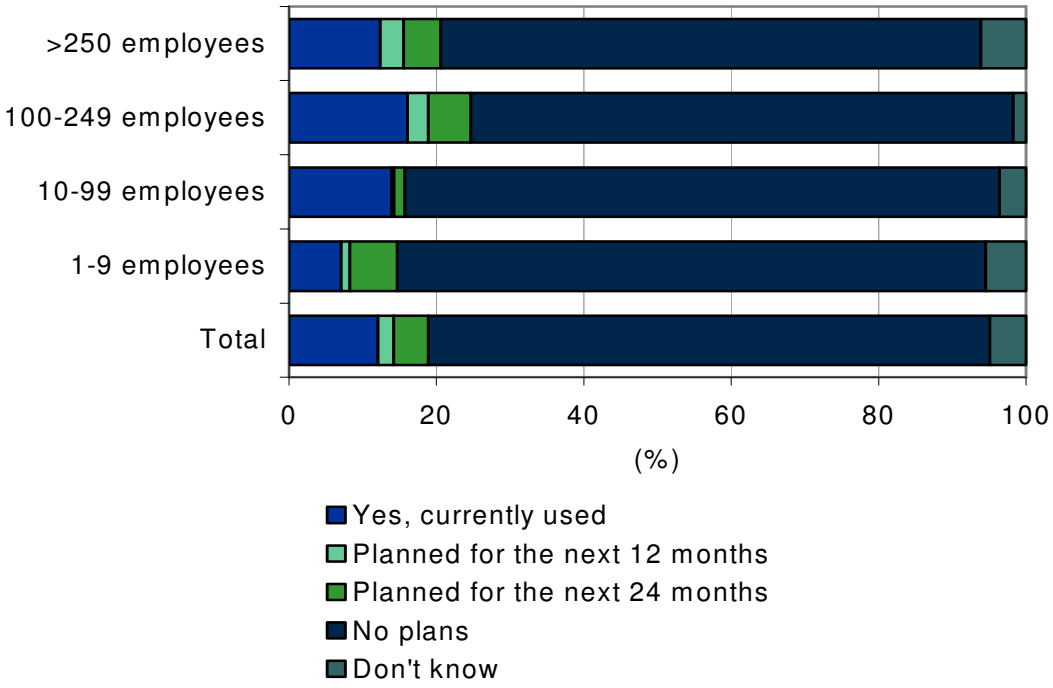
- Overcoming the hassles and costs of traditional packaged software;
- Purchasing the functionality they need without needing to purchase an entire solution;
- Achieving faster time to market;
- Eliminating the complexity of software updates;
- Keeping maintenance costs predictable;
- Allowing companies to focus on their core capabilities.

However, SMEs adoption of security-as-a-service has been so far quite limited and plans of adoption are more frequent among companies with more than 100 employees. Key barriers to wider adoption by SMEs include the lack of understanding of the subscription based pricing model, the fear to lose control, as well as the fear of adding complexity instead of reducing it.

FIGURE 47

European Union, Security-as-a-service, by Company Size (% of enterprises)

Q. For your security needs, do you use or plan to use Software on demand (called also Security-as-a-service or Security in the cloud)?



N = 1,180

Base = All sample

Source: Survey of EU ICT Security Market, 2008

6 THE SURVEY OF THE EU NIS BUSINESS USERS

Description of the Business Users Sample

The data presented in this report are based on a CATI (Computer Aided Telephone Interviews) survey of 1180 business users in a selected sample of 8 EU Member States, segmented by size and by industry sector. The number of interviews is substantially higher than the 1040 targeted and corresponds well to the balance of sectors and size class initially planned. According to the study methodology, IDC developed a market model dividing the Member States in four clusters (see chapter 2), on the basis of the level of development of their IT security market and their IT spending. The survey was carried out in two countries for each of the clusters. The results were extrapolated to the other Member States of each cluster, using appropriate indicators to estimate the cluster totals. The data were cross-checked and weighted to represent the business users universe. Therefore the data are representative of the NIS business market in the EU. (*For more details see Annex I – Methodology*).

TABLE 5

Business Survey: Number of Interviews by country, industry and company size

	N.
Country	
Sweden	138
UK	168
France	135
Germany	139
Italy	163
Czech Republic	171
Poland	134
Romania	132
Total	1180
Company size	
1 to 9 employees	230
10 to 99 employees	220
100 to 249 employees	249
250+ employees	481
Total	1180
Vertical market	
Manufacturing	338
Finance	198
Government	316
Services	328
Total	1180

Source: IDC GI Survey of EU ICT Security Market, 2008

The segmentation by vertical market was defined according to the European NACE coding systems and grouped into 4 major industry segments: Manufacturing, Public sector (including government,

healthcare and education), Finance (including banking, insurance, other finance) and Services (including retail, wholesale, transport, utilities, telecommunication, business and personal services).

The segmentation by company size was structured in four classes, three of which segmenting SMEs (small and medium enterprises) under 250 employees. The definition of SME included independently owned entities (therefore excluding local subsidiaries of large multinationals). An employment-weighting scheme was then applied to reflect the real demographic distribution of the EU economy by company size and vertical market. The distribution of the weighted sample is shown in tables 6 and 7.

TABLE 6

Business Survey: Weighted distribution of respondents by country and industry (% of respondents)

	Sweden	UK	France	Germany	Italy	Czech Republic	Poland	Romania	Total
Manufacturing	19.7%	14.0%	18.3%	29.4%	28.5%	29.7%	21.7%	32.5%	24.2%
Finance	2.4%	4.7%	3.4%	2.1%	3.5%	4.4%	2.7%	1.7%	3.2%
Government	37.2%	27.0%	29.3%	21.6%	19.2%	20.1%	33.7%	24.9%	26.3%
Services	40.8%	54.2%	49.0%	46.8%	48.8%	45.8%	41.9%	40.9%	46.3%
Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

TABLE 7

Business Survey: Weighted distribution of respondents by company size and industry (% of respondents)

	1 to 9 employees	10 to 99 employees	100 to 249 employees	250+ employees	Total
Manufacturing	15.1%	28.9%	34.9%	23.1%	24.2%
Finance	1.6%	2.5%	2.9%	4.4%	3.2%
Government	6.3%	17.6%	24.9%	39.9%	26.3%
Services	77.0%	51.0%	37.3%	32.6%	46.3%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

The profile of Business Survey Respondents

The survey was addressed to enterprises using PCs, targeting their managers responsible for ICT procurement, management and maintenance (the IT decision makers). The high profile of respondents is an additional validation of the quality of the survey data. In addition, the analysis of their job titles provides an interesting overview of the management structure of enterprises for ICT (tables 8 and 9).

Overall, approximately 67% of respondents head or work in the IT department, as IT managers/directors (34%) or as CIOs (chief Information Officer), CTOs (Chief Technology Officer) or IS VPs (Information System Vice President) (a share of 25.5%) .

Of course there are strong differences by company size. They are connected to the presence or lack of dedicated IT departments and to the different role of business functions, as follows:

- Nearly 80% of respondents from large enterprises (250+ employees) have IT-related job titles. Large European companies usually have internal IT departments, sometimes very articulated, particularly in the case of the banking or telecommunication sectors. So it is not surprising that companies' ICT decision makers (the target of our survey) belong to IT departments in this size class firms.

- Only one third of respondents in very small companies (1-9 employees) work within an IT department. Up to 53% of respondents in this size class are presidents or companies' owners. Very small companies usually lack dedicated IT departments; IT functions are generally outsourced, and key decisions are taken directly by companies' presidents and/or owners.

- It is also interesting to note the role of administration/finance functions, in the 1-9 and 10-99 employees size classes. In the firms of this size finance/administration departments often take responsibility for IT tasks and related decisions.

TABLE 8

Business Survey: Respondents' Job title by company size (% of respondents)

	1 to 9 employees	10 to 99 employees	100 to 249 employees	250+ employees	Total
President, Owner, MD, CEO	53.0%	12.8%	4.9%	4.8%	16.6%
CIO, CTO, VP of IS	13.5%	27.3%	24.9%	30.5%	25.5%
IT Manager & director, planner	8.8%	27.3%	46.0%	44.8%	33.9%
Business operation manager	4.5%	2.2%	0.8%	1.1%	2.0%
Administration & finance manager	11.1%	13.3%	5.3%	3.9%	7.4%
Other IT	7.0%	13.0%	14.6%	12.2%	11.6%
Other non-IT	2.2%	4.1%	3.6%	2.6%	3.0%

N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

The analysis of the respondents' job titles by country provides an interesting confirmation of the level of IT sophistication of business users. The presence of dedicated IT departments is strongly correlated with the level of development of the IT market. In practice, surveyed Member States characterized by high IT sophistication show a higher number of respondents with IT departments' job titles. For example, Swedish respondents with IT-related job titles are some 87.5%. This compares with 40.2% and 47.8% in Romania and Czech Republic respectively.

TABLE 9

Business Survey: Respondents' Job title by country (% of respondents)

	Sweden	UK	France	Germany	Italy	Czech Republic	Poland	Romania
President, Owner, MD, CEO	6.9%	10.4%	10.4%	7.8%	15.8%	21.5%	27.6%	32.3%
CIO, CTO, VP of IS	63.4%	4.7%	4.1%	10.4%	53.3%	21.0%	43.2%	3.6%
IT Manager & director, planner	17.7%	61.6%	64.8%	56.0%	15.3%	25.9%	9.8%	20.4%
Business operation manager	2.1%	1.6%		2.5%		4.8%	3.3%	1.5%
Administration & finance manager	6.5%	11.8%	9.5%	10.6%	5.0%	0.9%	0.7%	16.2%
Other IT	2.8%	9.9%	6.4%	12.4%	10.4%	22.4%	12.6%	13.4%
Other non-IT	0.6%		4.8%	0.3%	0.1%	3.5%	2.8%	12.6%

N = 1,180

Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

7. THE ANALYSIS OF CONSUMER DEMAND

Overview of NIS Consumer Users

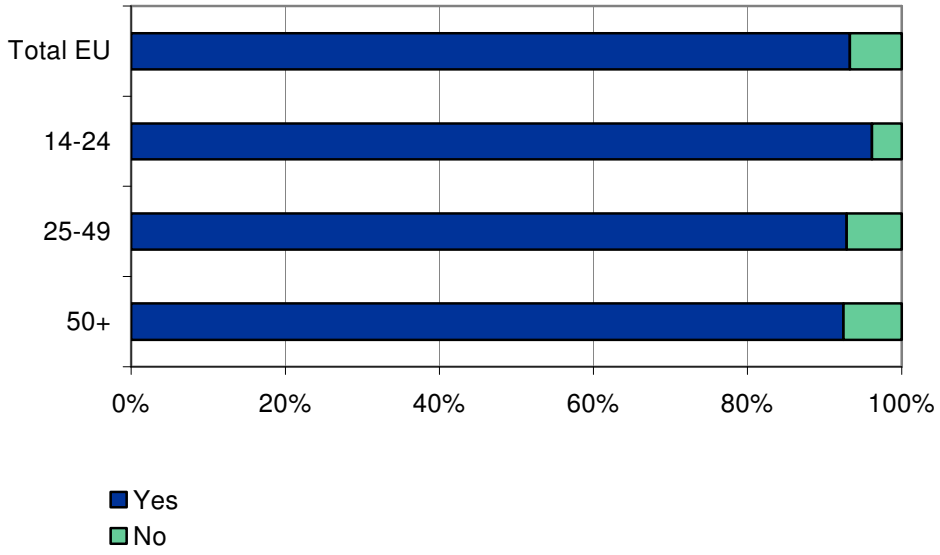
This chapter analyses the behavior and opinions of advanced European Internet users of Network and Information Security, focusing on their level of adoption, their awareness and concern about IT security threats, their relationship with suppliers. The study investigates the main differences of consumers' behavior by age, dividing Internet users in three main groups: young (14 to 24 years old), adults (25-49 years old), and mature/old users (over 50 years old). Age is in fact one of the most important factors differentiating Internet usage patterns, possibly the most important together with the level of education.

The data comes from the survey of a sample of advanced EU Internet users, representative of the EU population by age, gender and main socioeconomic characteristics (see chapter 8 for a description of the sample). They use the Internet every day (95%), most of them have broadband access, and the majority has a higher education level. About 45% occasionally access the Internet with laptops or mobile devices, such as mobile phones or PDAs. These are all characteristics identifying advanced Internet users.

FIGURE 48

Consumer Survey: Broadband Adoption, by Age (% of answers by age group)

Q. Do you have a High-Speed / Broadband / ADSL internet Connection at home?



N = 808

Base = All sample

Source: IDC GI Survey of EU ICT consumer security market, 2008

Advanced Internet users are comfortable with a wide range of Internet-based services. As it could be expected, practically all consumers in the sample use email and search engines (99% of respondents). But many other services are used by a majority of EU consumers, including ecommerce and Internet banking (practiced by over 80% of them) and online chatting (70%).

Internet banking is the only widespread service less used by the young than by the average population (the leading users are in the 25-49 age bracket). For all the other services (with the exception of eGovernment), the young show higher percentages of usage than the average population. The age correlation is most relevant with social networking, representing the most recent wave of innovation in the Internet world, which is practiced by 79% of the young, 52% of the adults and "only" 25% of the mature users.

The age correlation is strong for all the Internet services based on active interaction and networking, such as chatting online, playing online, using the Internet to make telephone calls, using peer to peer applications, having a website or blog and/or contributing to collaborative websites. This points to the lack of maturity of the Internet market, which is still evolving rapidly, as the young of today become the adults of tomorrow, increasing the diffusion of services and the time spent on the Web. Not surprisingly, many researchers are starting to call the young "digital natives" (because they were born and grew up with the Net, so they move effortlessly in the virtual environment).

Adults and mature users appear more motivated by the practical (rather than social) aspects of the Web, driving the diffusion of applications such as eCommerce and eGovernment.

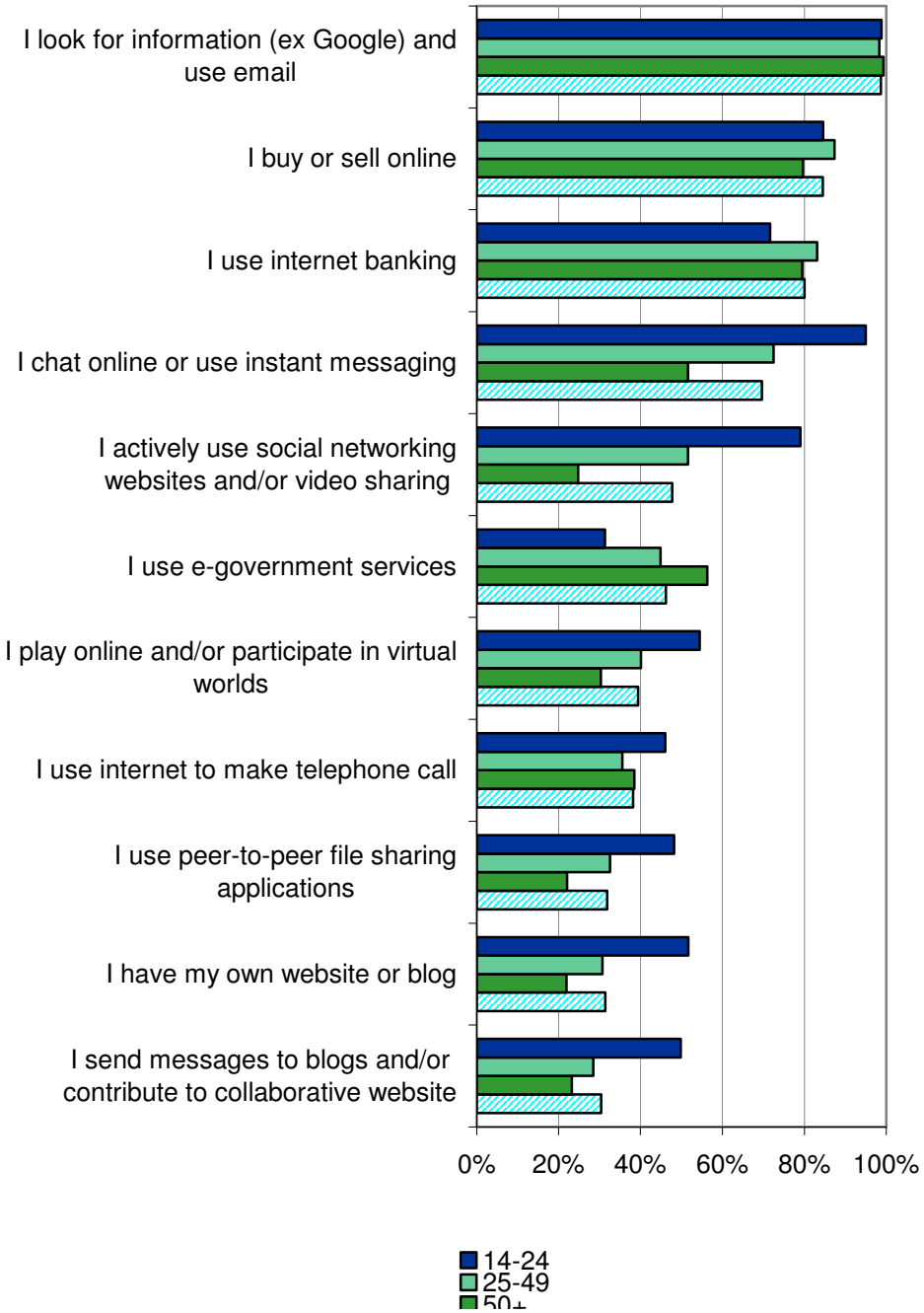
The only service for which the age correlation works backward (greater usage by older users) is eGovernment, used by 56% of mature users and 31% of the young. This level of diffusion is comparable to the Eurostat Information Society Statistics data(2008), which indicated a 47% of European Internet users accessing public websites to obtain information and 31% downloading official forms.

But mature users are also interested in making phone calls on the Internet (perhaps to keep in touch with their young relatives), the only service for which the users over 50 are more numerous than the adults.

FIGURE 49

Consumer Survey: Internet Usage, by Age (% of answers by age group)

Q. For which activities do you use internet from home?



N = 808

Base = All sample

Source: IDC GI Survey of EU ICT consumer security market, 2008

Consumers' Perception and Experience of Security Threats

Awareness and Concern

A very high level of awareness of potential security threats characterizes EU advanced Internet users (*figure 50*). Almost all of them know about viruses and spam mails (97%). The third best-known threat is the misuse of the Internet by children (92% of respondents). But also the other threats mentioned (misuse of credit cards, phishing, abuse of personal information sent online) are known by more than 90% of the respondents. This confirms that the level of awareness about security threats is very high among advanced users, and is positively correlated with the education level. At this level of awareness, differences by age are minor.

The ranking of threats changes, when moving from general awareness to personal concerns about accessing the Internet from home (figure 51) The respondents were asked to score their concern on a scale from 1 to 4, where 1 stands for "not worried" and 4 for "strongly worried". All the main security concerns are scored above 2 ("I am a little worried"), which means that the level of worry is moderate, never reaching the "I am strongly worried" level but never absent, either.

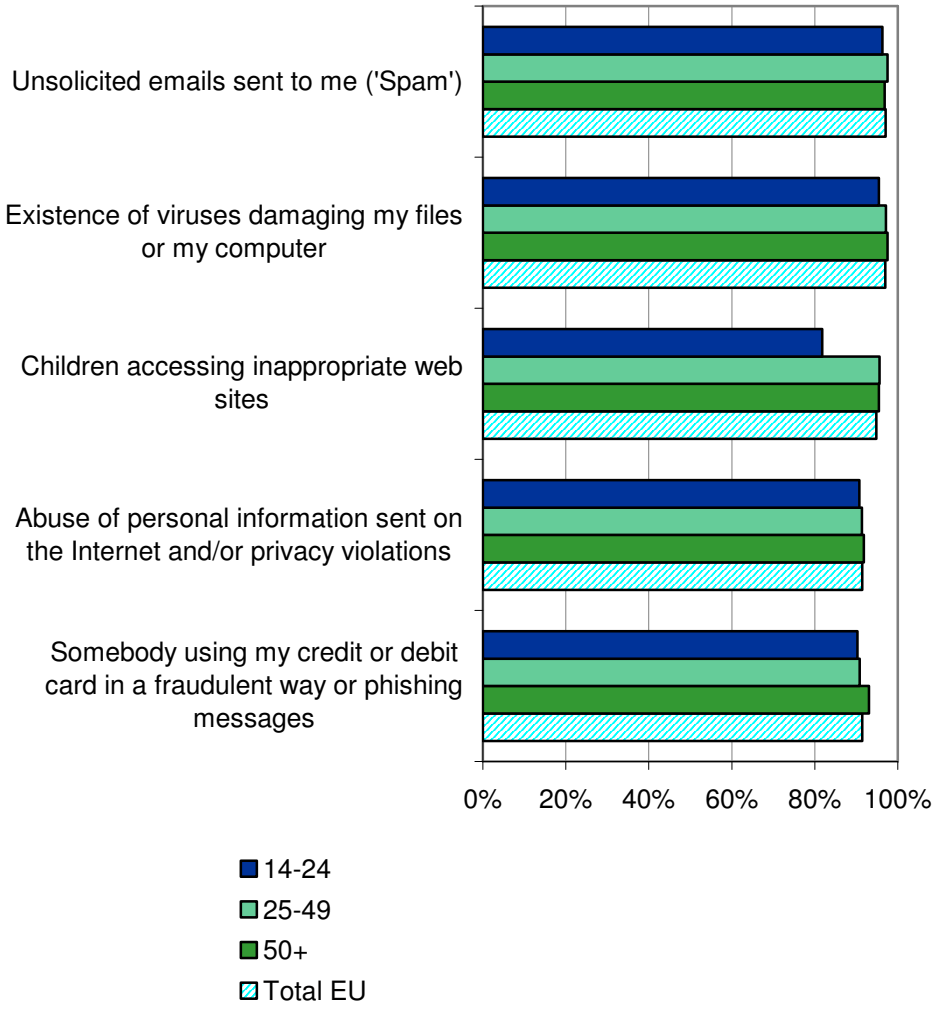
The number one concern is the abuse by third parties of personal information sent over the Internet, and/or the violation of one's privacy (rated at 2.8, very close to the "I am worried" score). But also the inappropriate access of websites by children receives a similarly high score (it was measured only for respondents with under-age children, directly interested). Credit cards frauds and catching viruses also receive high concern scores. Spamming (receiving unsolicited emails) is considered as the least important problem.

There is a small, but noticeable increase of the level of concern correlated with age, with the younger generation less worried, particularly about unsolicited emails.

FIGURE 50

Consumers and IT Security: Threats Awareness, by Age (% of positive answers by age group)

Q. Are you aware of the following security problems related to internet usage?



N = 808 (Only respondents with children aged less than 18 have been considered for the item "Children accessing inappropriate web sites" where N=252)

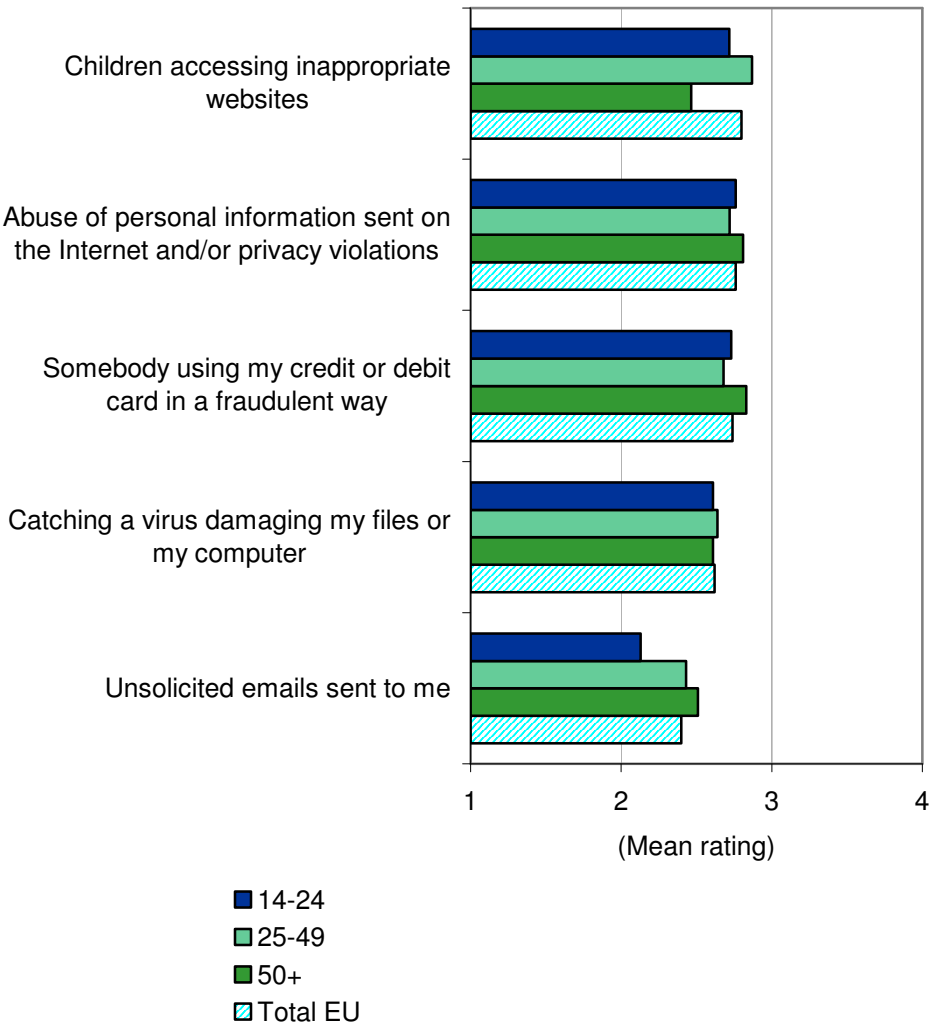
Base = All sample

Source: IDC GI Survey of EU ICT consumer security market, 2008

FIGURE 51

Consumers' Security Concerns, by Age (Mean rating)

Q. When you use internet from home what are your security concerns?



Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4 = I am strongly worried.

N = 808 (Only respondents with children aged less than 18 have been considered for the item "Children accessing inappropriate web sites" where N=252)

Base = All sample

Source: IDC GI Survey of EU ICT consumer security market, 2008

Impacts of Security Concerns on Internet Usage

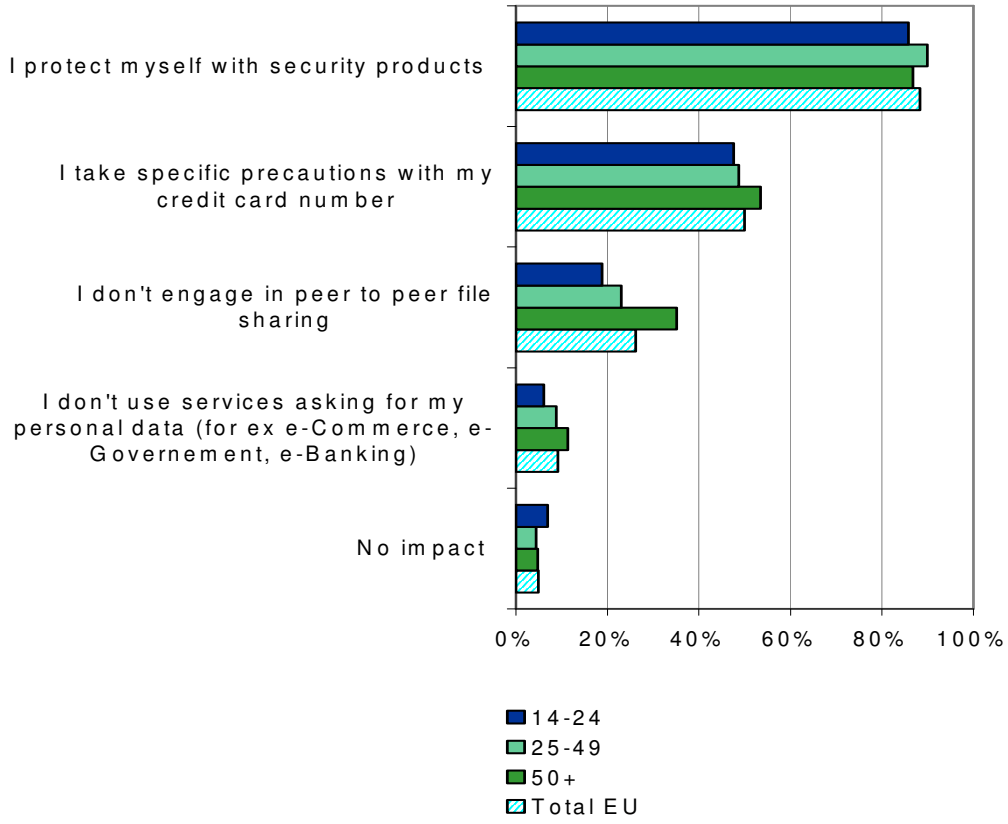
The study investigated the actions taken by respondents to protect themselves against security threats (*figure 52*). The vast majority of EU users react to security concerns using IT security products (88%), without great differences by age. The other most common response is to take precautions in the use of personal credit cards' information (50%, slightly higher for mature users). The goal of this question was also to analyze whether security concerns prevent users from engaging in some activities. This seems to affect only a minority of users (but

we must remember that the sample is composed by advanced users). About a fourth of respondents avoid using peer-to-peer file sharing applications, and about 10% don't use services asking for personal data, such as eCommerce or online banking. Even if this is a minority, it still seems a relevant impact of security concerns. For both activities, however, there is a strong correlation with age, with mature users over 50 years old twice as likely to refrain from these activities because of security fears than the young. Finally, there is also a tiny group of users (5%) who do not take any action against security threats.

FIGURE 52

Consumer Survey: Security Concerns Impacts on Internet Usage, by Age (% of answers by age group)

Q. What is the impact of security concerns on your use of the internet?



N = 808

Base = All sample

Source: IDC GI Survey of EU ICT consumer security market, 2008

Security Breaches, Damages and Reactions

Despite the diffusion of security products, 85% of EU Internet users received unsolicited emails in the past year, and another 42% were infected by a virus (*figure 53*). The other security threats investigated, which are arguably more serious (abuse of personal information and privacy violation, credit cards fraud, children accessing inappropriate

web sites) were experienced by small percentages of the population, under 10%. The young users were more likely to catch a virus, while they were less exposed to the other security breaches.

Coherently with these data, the damages declared by consumers suffering security breaches appear relatively light (*figure 54*). All of them (100%) complained about time lost (for example to reset a pc). Beyond this, 27% lost some personal data, but only 16% mentioned economic damages and 13% complained about suffering embarrassment and/or humiliation. Again, the young users differ from the average users, as they were more likely to declare damages due to personal data loss (39% of them) and economic damages (27% of them), but less likely to complain about personal embarrassment and humiliation (10% vs. an average of 13%). These data design the profile of young users more inclined to intensive and frequent Internet usage, therefore more exposed to damages.

The study investigated also the remedial actions taken after suffering a security breach (*see figure 55*). The most common reaction, logically, is to improve security protection (77% of Internet users who suffered a security breach), buying more products and services. Greater attention to the use of credit card information on the Internet is also a fairly common reaction (45%) by consumers. Since only about 10% of them actually suffered from a misuse of credit card information, it seems that any security breach (even a relatively minor one) may motivate users to change their behavior from this point of view.

A quarter of the users (28%) decided to stop engaging in peer to peer file sharing while 17% gave up using services asking for personal information. Considering that this is a sample of advanced users, this impact of security breaches is not at all minor and must be considered with attention as a potential market constraint.

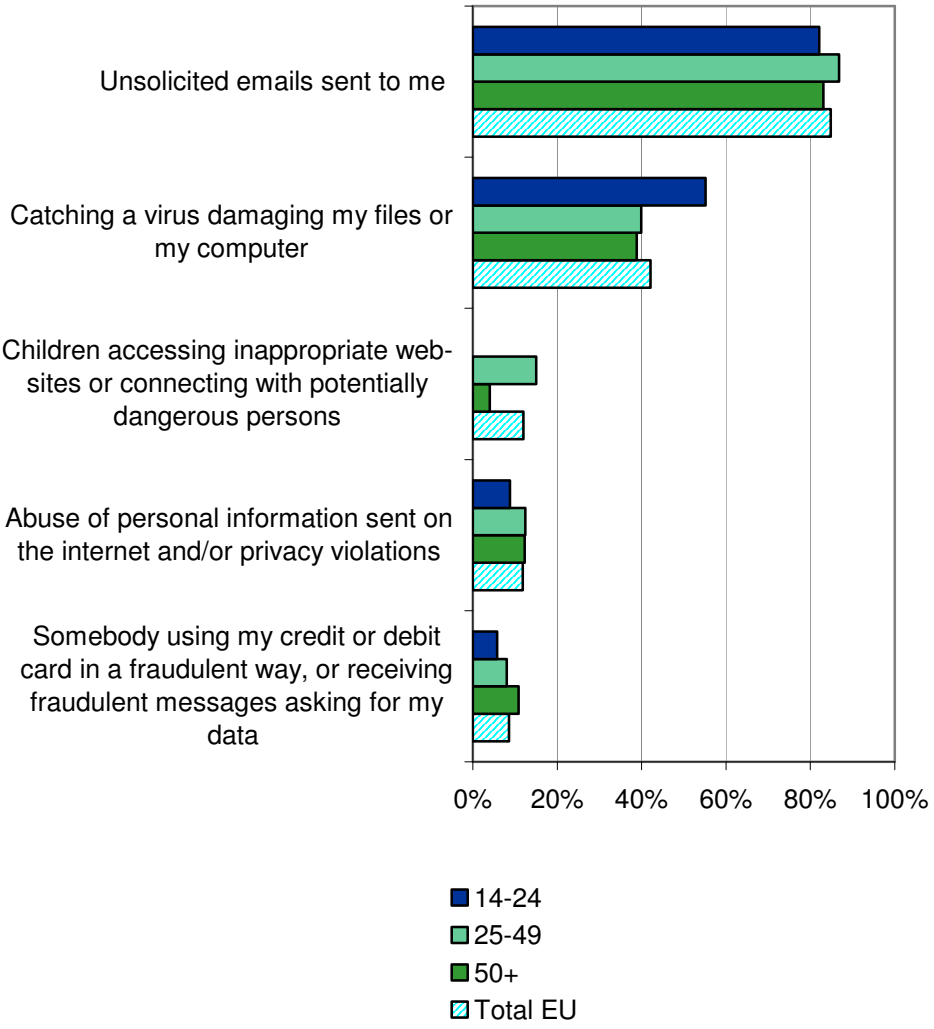
Finally, 35% of respondents continued as before. This may be because they already had as much security as they considered reasonable, or because the security breach was relatively minor.

Variations of behavior by age are relatively minor, with the mature consumers more likely to take active precautions than the young ones.

FIGURE 53

Consumers and Security Breaches, by Age (% of consumers by age group)

Q. Did you have any of the following security problems using the Internet in the past year?



Base = All sample

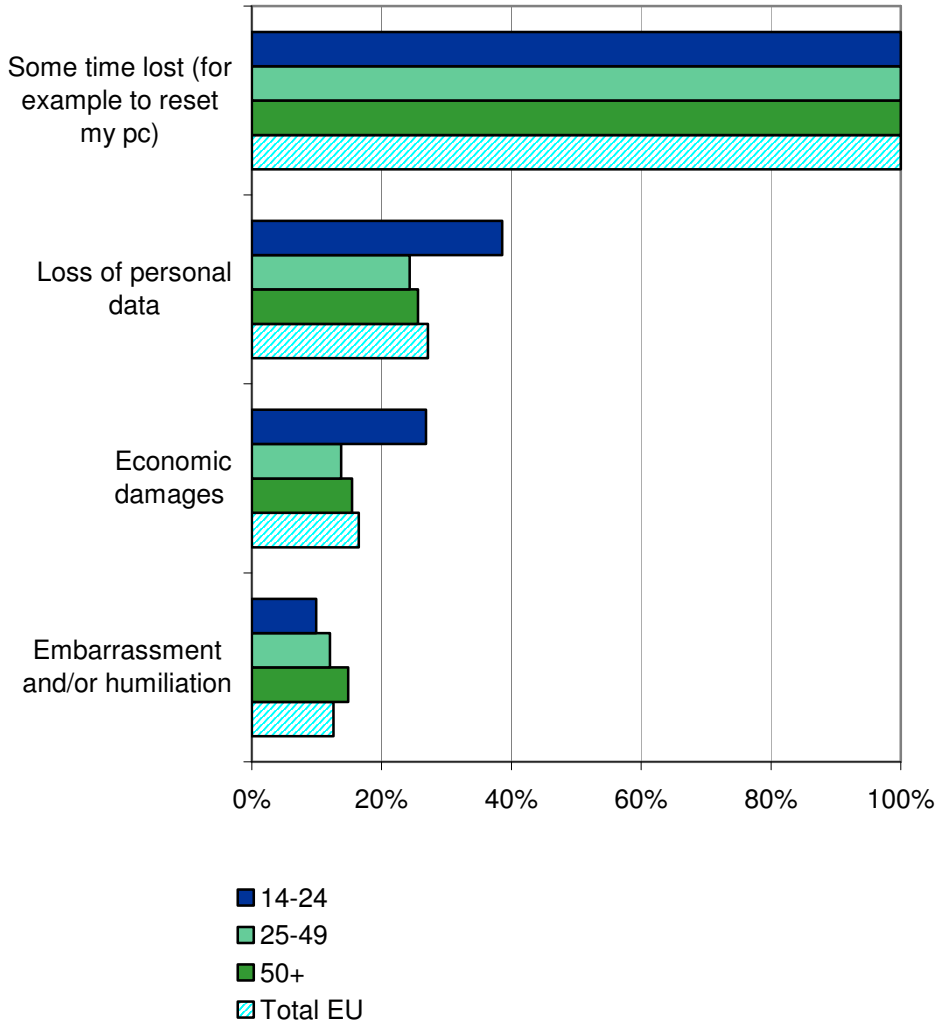
N = 808 (Only respondents with children aged less than 18 have been considered for the item "Children accessing inappropriate web sites" where N=252)

Source: IDC GI Survey of EU ICT consumer security market, 2008

FIGURE 54

Damages Experienced by Consumers, by Age (% of consumers by age group)

Q. Which damages did you experience?



N = 727

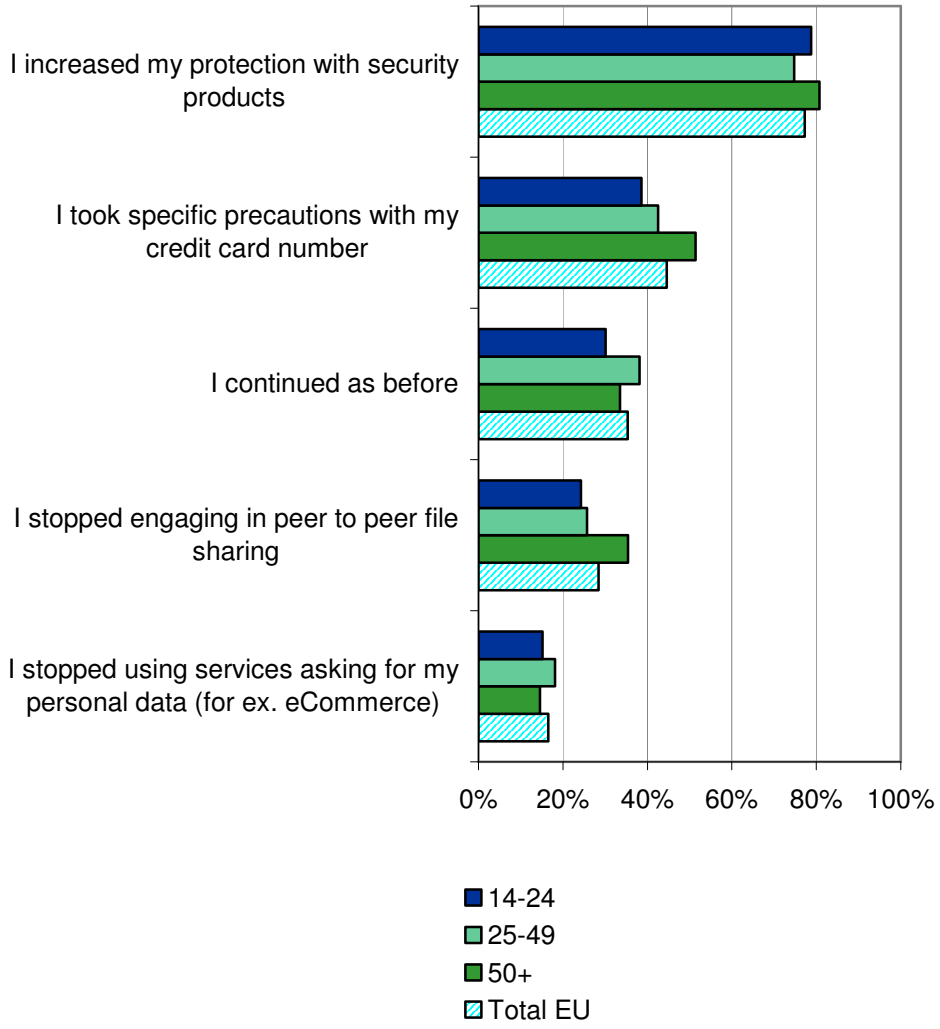
Base = Respondents who experienced security problems

Source: IDC GI Survey of EU ICT consumer security market, 2008

FIGURE 55

Consumers' Reaction To Damages, by Age (% of consumers by age group)

Q. What did you do after your security problem occurred?



N = 727

Base = Respondents who experienced security problems

Source: IDC GI Survey of EU ICT consumer security market, 2008

Current Adoption of IT Security and Perceived Protection

The diffusion of basic security solutions among EU Internet users is rather high (fig 54). The majority (81%) use simple stand-alone solutions, and/or packaged IT security suites "all inside" (67% of users).

All the other security products and solutions do not reach diffusion rates above 40% of the users. The young are more likely than the other age groups to use simple stand-alone solutions.

The adoption of these security products does not seem to lead to a feeling of safety. EU Internet users on average declare to feel somewhat less than protected for the five security threats examined in the survey. As shown in the following figure 57, the users score their perceived protection between 2.0 and 2.7 (on a scale from 1 to 4, where 2 means "I feel a little protected" and 3 means "I feel protected"). This shows a gap between the fear level and the perceived protection level for all of these threats, with the exclusion of catching viruses, as follows.

- **Abuse of personal information**. This is the security threat most feared by EU Internet users, with a mean rating of 2.8 (close to score 3 which means "I am worried", *figure 51*). Instead, the perceived protection mean rating is only 2.4, showing a statistically significant gap between fear and protection.

- **Children accessing inappropriate websites**. The concern of consumers with under age children is rated at 2.8, while the perceived protection level is 2.4, so also for this threat there is a gap between fear and protection.

- **Somebody using my credit or debit card in a fraudulent way**. For this threat the gap is more limited, but still the fear rating (2.7) is higher than the perceived protection rating (2.6).

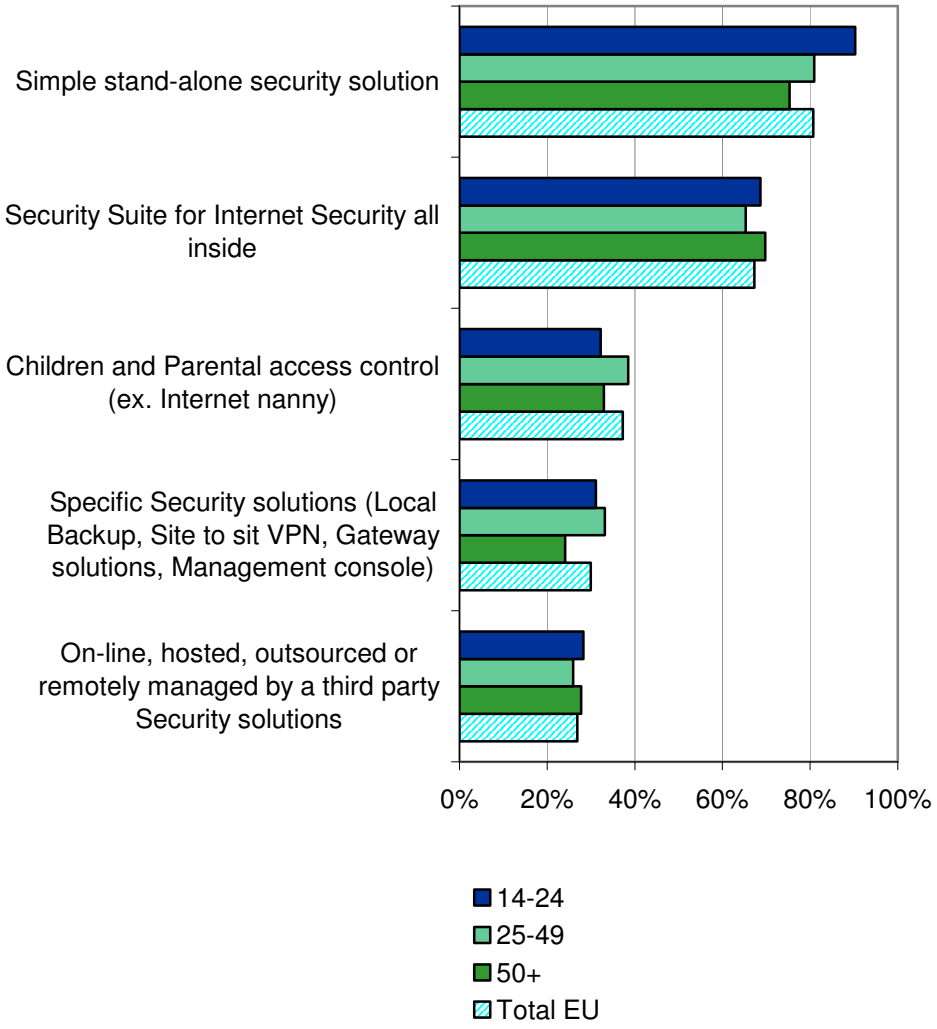
- **Catching a virus**. In this area there is no gap between fear and perceived protection. On the contrary, perceived protection is slightly higher than the concern rating.

- **Unsolicited emails (spam)**. Internet users declare to be only a little worried about this threat (score 2.4, the lowest one among the threats measured); but the perceived protection is also quite low (the mean rating is 2.0), showing a gap between protection and concern which is a clear potential demand for better defense against spamming.

FIGURE 56

Consumer Survey: Current Adoption of IT Security Products/Services, by Age (% of consumers by age group)

Q. Which kind of security products do you use?



N = 792 (Only respondents with children aged less than 18 have been considered for the item "Children and Parental access control" where N=244)

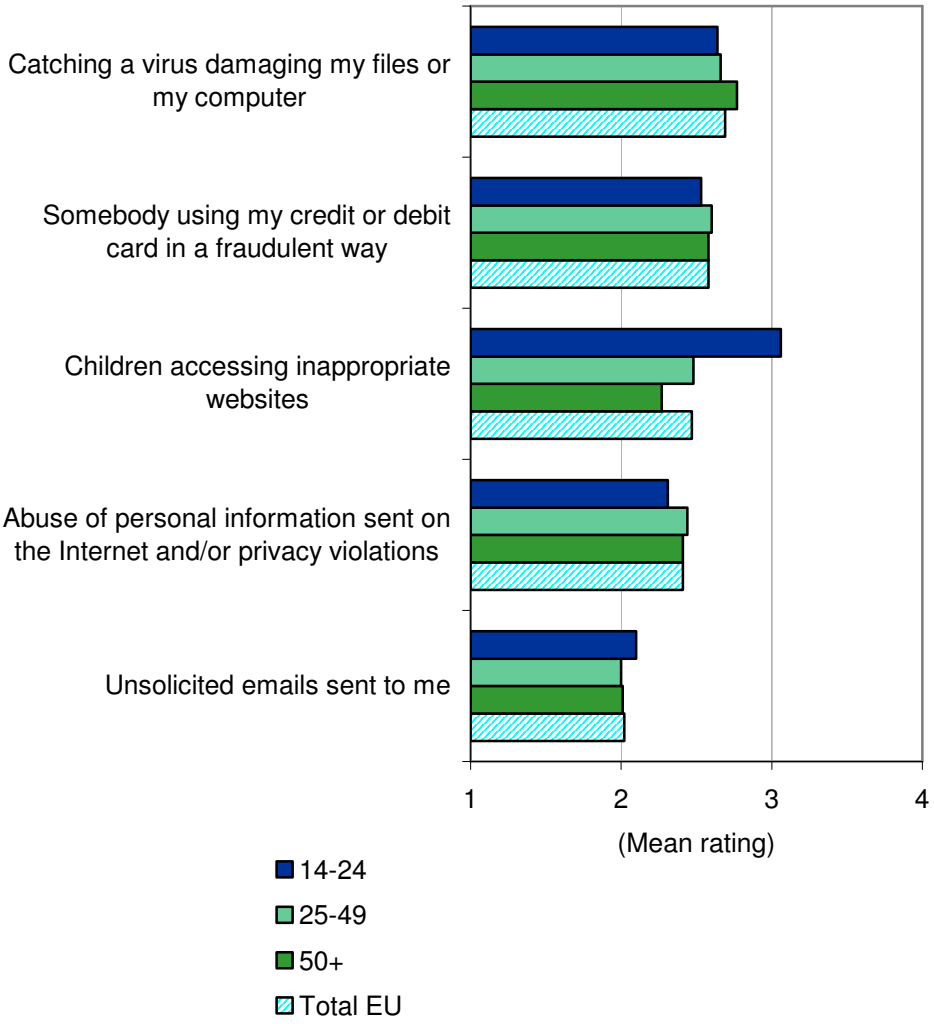
Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 57

Consumers' Perceived Protection Related to IT Security, by Age (mean rating)

Q. Do you feel protected or safe when you use Internet?



N = 808 (Only respondents with children aged less than 18 have been considered for the item "Children accessing inappropriate web sites" where N=252)

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = I do not feel protected and 4 = I feel highly protected

Source: IDC GI Survey of EU ICT consumer security market, 2008

Mobile Security for Consumers: Main Fears and Solutions adopted

Almost half of EU Internet users occasionally connect to the Internet using a laptop pc, a mobile phone or a mobile device such as a PDA. The study investigated their main security concerns about mobile security, for the same threats investigated for average users (*figure 58*).

The overall level of concern by mobile users is lower than that indicated by the average EU users, with a mean rating around 2.4 (on a scale from 1 to 4, where 2 means "I am a little worried"). The respondents give very similar scores for all the measured threats.

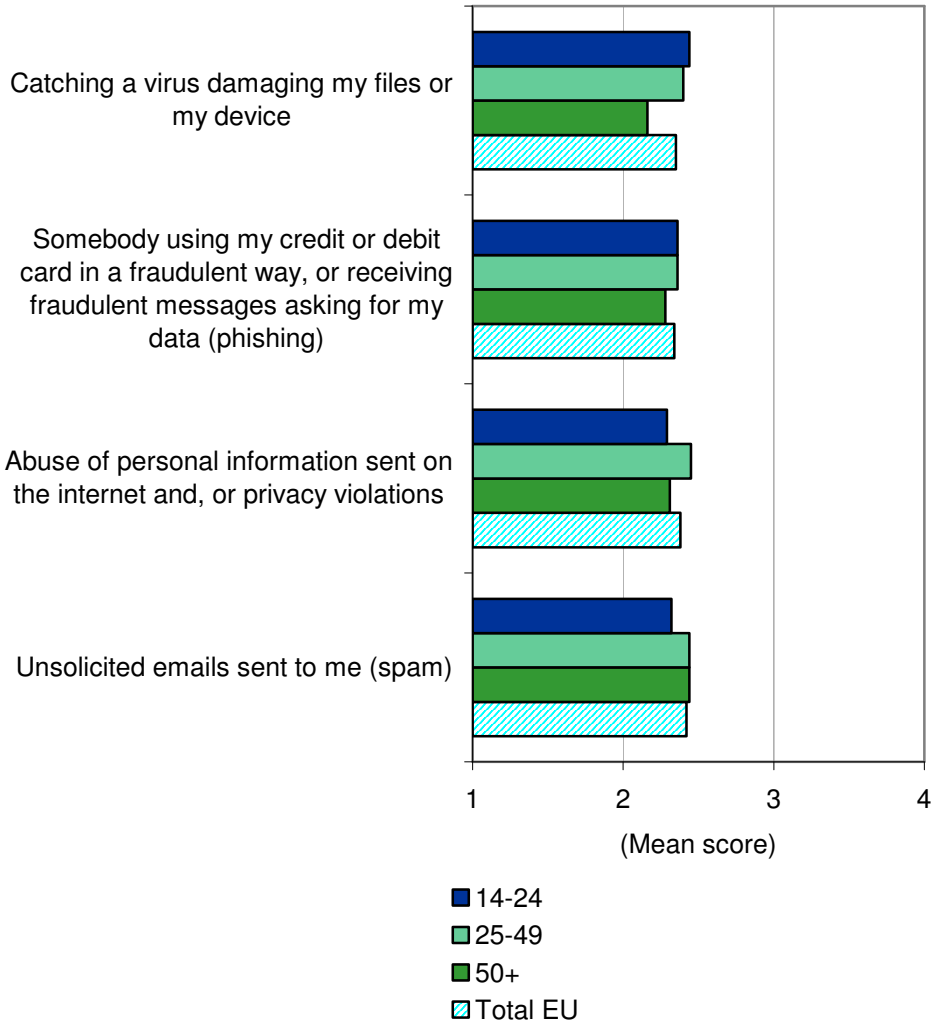
More specifically, the fears of abuse of information and credit card information frauds are lower for mobile users than for the average EU user. On the other hand, mobile users appear more concerned about spamming than the average user.

Specific protection by mobile users also appears relatively low. Approximately 37% of mobile users adopt specific security solutions, and 39% simply back-up their data (*figure 59*), many of them belong to the young age group. At least one out of five mobile users does not implement any specific solution. This corresponds to the observation that mobile security for personal devices is lagging behind mobile security for business users.

FIGURE 58

Consumer survey: Internet via Mobile access: Security concerns (Mean Rating)

Q. When you access the Internet with a mobile access what are your security concerns?



N = 361

Base = Respondents using a mobile Internet access

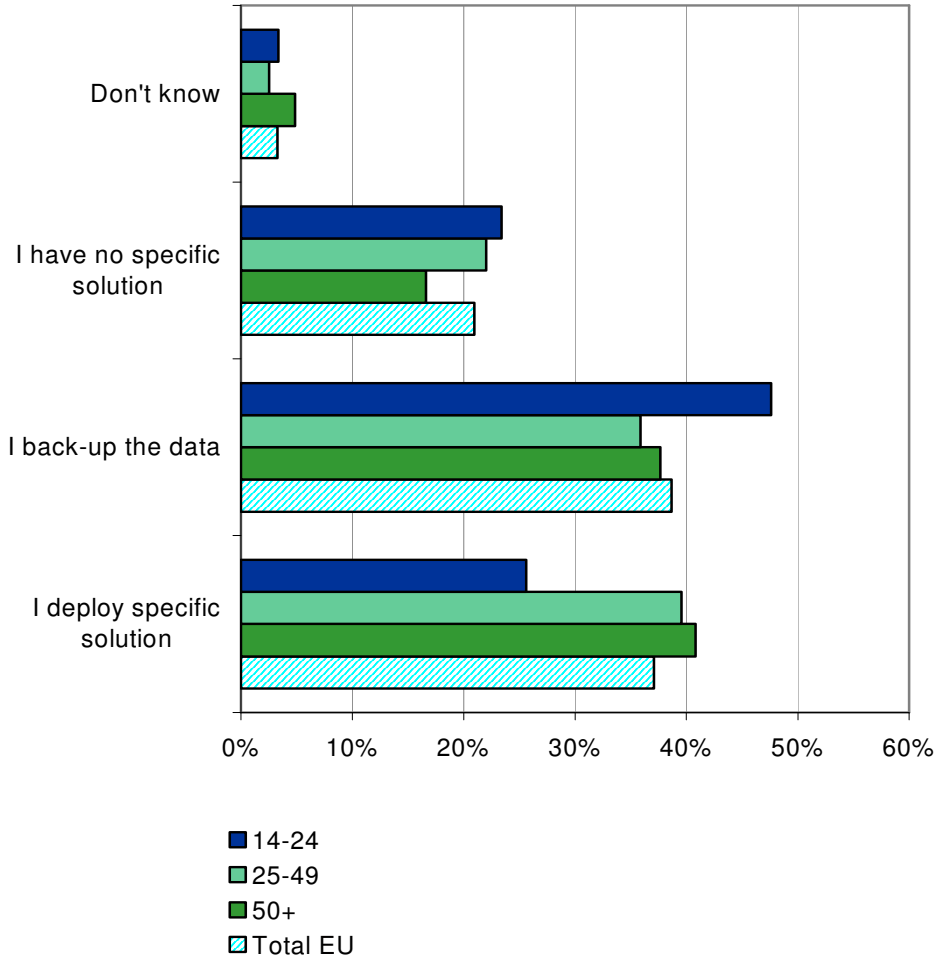
Note: Mean scores are based on a scale of 1–4, where 1 = I am not worried and 4= I am strongly worried

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 59

Consumer Survey: Protection of Mobile Devices (% of consumers by age group)

Q. How do you protect your device?



N = 361

Base = Respondents using a mobile Internet access

Source: IDC GI Survey of EU ICT Security Market, 2008

Main Trends of IT Security Spending and Plans of Adoption

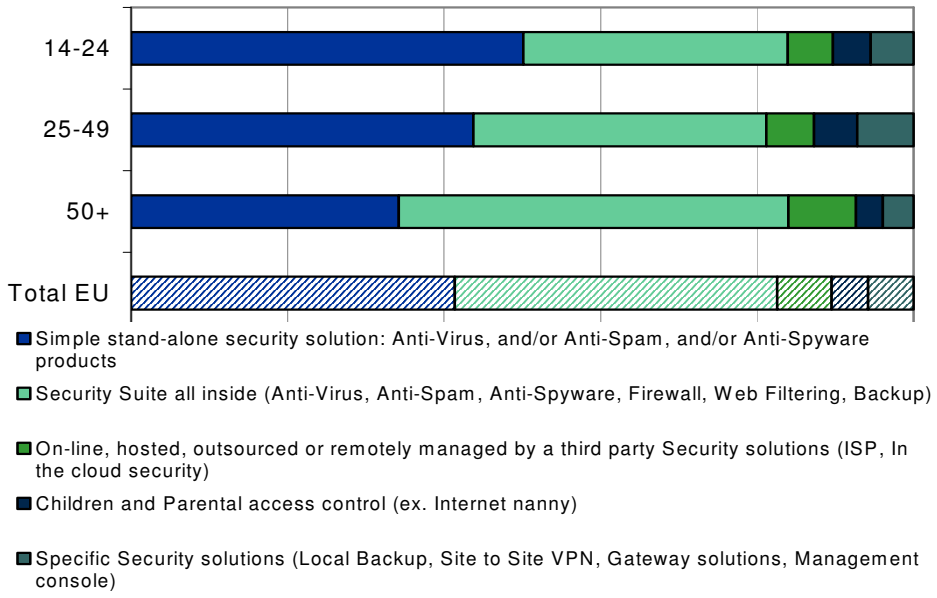
The Consumers budget for security is mostly employed to buy the basic security solutions (40.5% of users) and security suites (40.3%), with the young more likely to spend for the first type of solutions than the second. Adult users (25-49 years old) are more likely to invest into specific solutions, even if these solutions account on average for only 5.7% of the average EU consumer budget. From this starting point, the security budget of EU consumers (*figure 60*) is likely to remain stable in the near future (58% of users) or grow (21% of users), while only 5% of users declare that it will decrease. These trends are similar to those found in the business market, even if the share of users planning

to increase their spending in the consumer market (21%) is lower than the business users' one (35%). These data confirm that the security market is likely to keep growing in the foreseeable future: this is reinforced by the observation that the young users are slightly more likely to increase their spending (22%). Future plans of adoption (*figure 61*) provide additional evidence about the growth perspectives of the security market. According to our study, 36% of EU consumers plan to buy basic security solutions or security suites, while 19% think to buy solutions for children protection, 13% specific security solutions and 12% online solutions. There is a definite correlation between plans of adoption and age, with the young more likely to buy in the near future, followed by the adults, while the mature users are least likely to do so. It is interesting that most of the future plans are focused on the basic and self-contained solutions, showing that the mass market of commodity security products has the highest potential of development.

FIGURE 60

Consumers' Security Spending Distributed by Solution, by Age (% of answers by age group)

Q. Can you tell us how your security spending was distributed among the following solutions?



N = 792

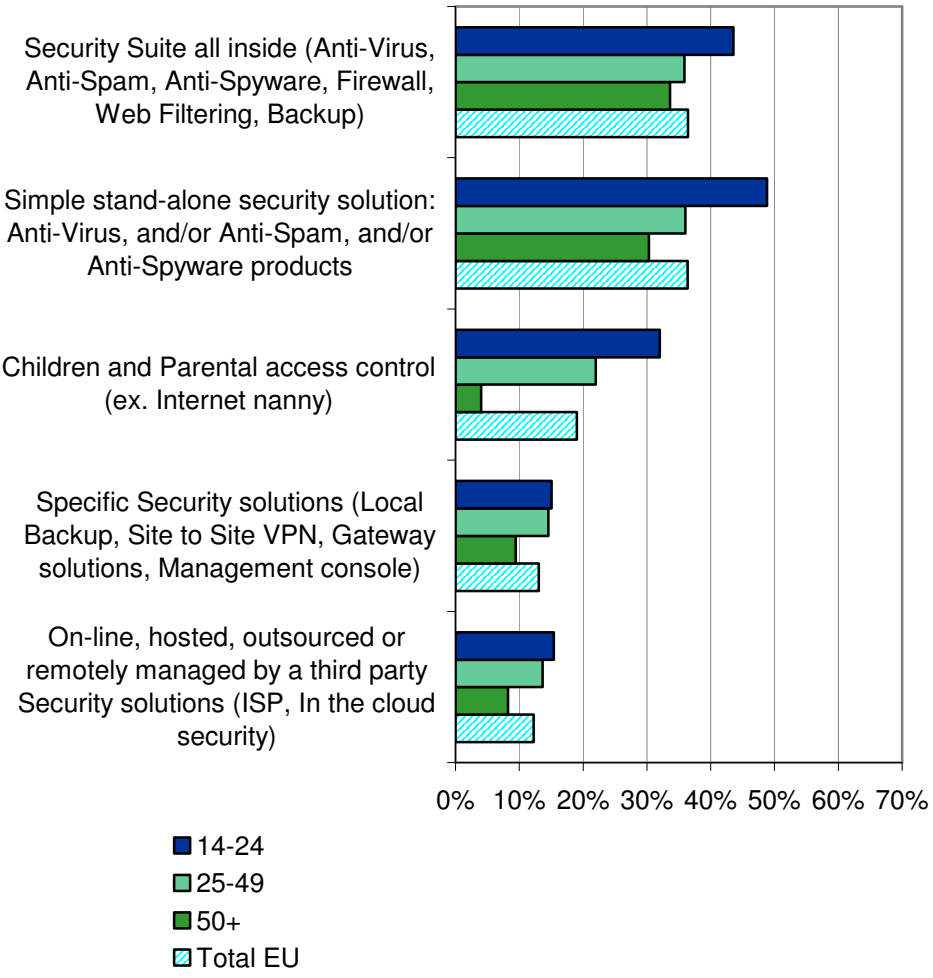
Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 61

Consumer Survey, Future Adoption Plans, by Age (% of consumers by age group)

Are you planning to buy or upgrade or source any of the following products in the next 12 months?



N = 808 (Only respondents with children aged less than 18 have been considered for the item "Children and Parental access control" where N=252)

Base = All sample. Multiple response

Source: IDC GI Survey of EU ICT consumer security market, 2008

Relationship with Suppliers: Criteria of Selection and Satisfaction

Which criteria do consumers use to select an IT security solution? Consumers were asked to score the relevance of a series of selection criteria, on a scale of 1 to 4 (where 1 is "not at all important", and 4 "highly important").

The factor with the highest average score (3.7, very close to highly important) is reliability and completeness of protection: this means that the quality of the proposed solution ranks first in the eyes of the customers. This is followed by price (3.4) and then ease of use (again 3.4). But all selection criteria seem to be relevant, since all the scores vary from 3.2 to 3.7. Actually, the apparently lower relevance of price should not be overestimated: experience shows that price may not be the first factor considered, but is likely to be the condition making or breaking the deal. The ranking by relevance does not change by age group, even if the Mature users rank higher than the other groups aspects such as ease of use and adaptability.

More interesting is the analysis of consumers' satisfaction for their security solutions, on the basis of the same criteria, (on a 1 to 4 scale, where 1 corresponds to "not at all satisfied" and 4 to "delighted"). The average level of satisfaction corresponds to slightly more than 3 (which means "acceptable") for all the characteristics of the IT solution, varying between 3.0 and 3.3.

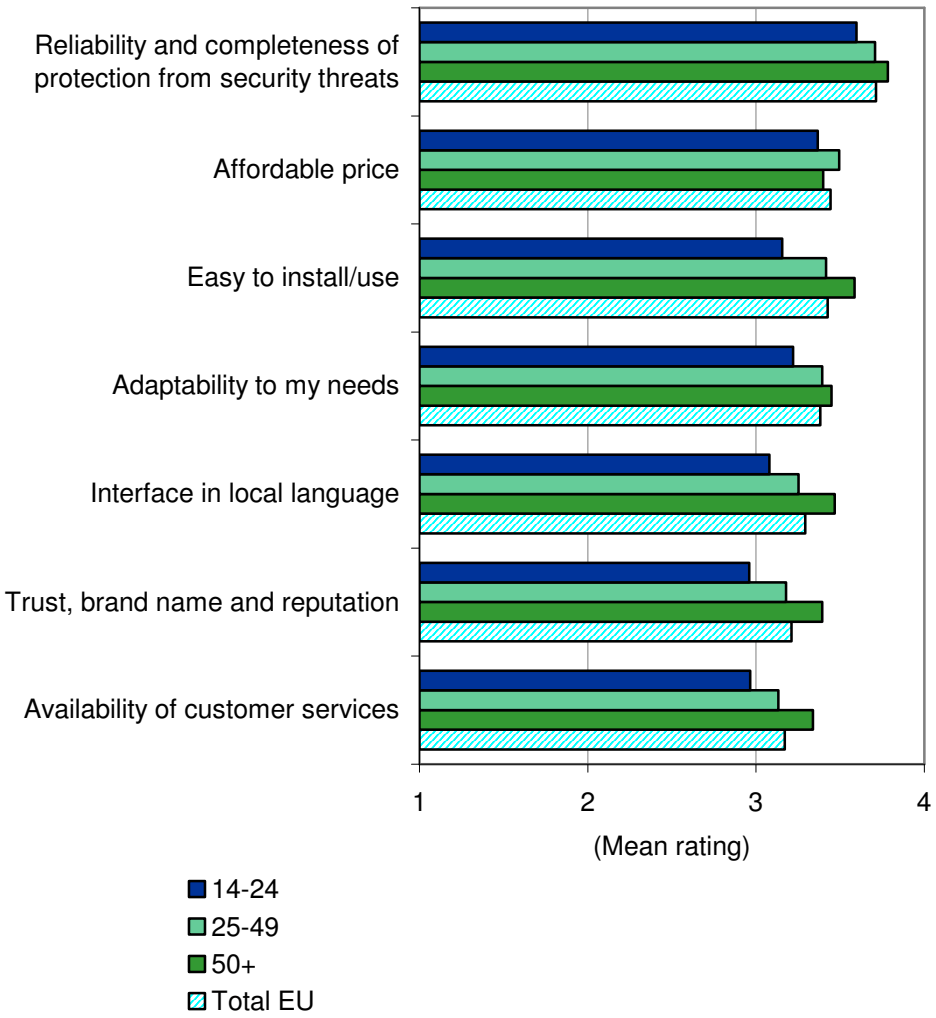
Matching importance scores with satisfaction scores shows a negative gap (low satisfaction corresponding to high relevance) for the most important selection criteria, that is reliability and completeness of protection. The gap exists, but is narrower for four other criteria: price, adaptability to the users' needs, availability of services and easy to install/use. Only for brand name/reputation and for the presence of interface in national language satisfaction is higher than relevance. (see also Del.5.1 Key Messages for the indicator of the match demand-supply, based on these data).

These results suggest a mismatch between supply and demand, even if the average score levels indicate an acceptable level of satisfaction.

FIGURE 62

Consumers' Criteria for Choosing Security Solutions, by Age
(% of answers by age group)

Q. Which criteria do you consider important for the choice of your Security Solution?



N = 808

Base = All sample

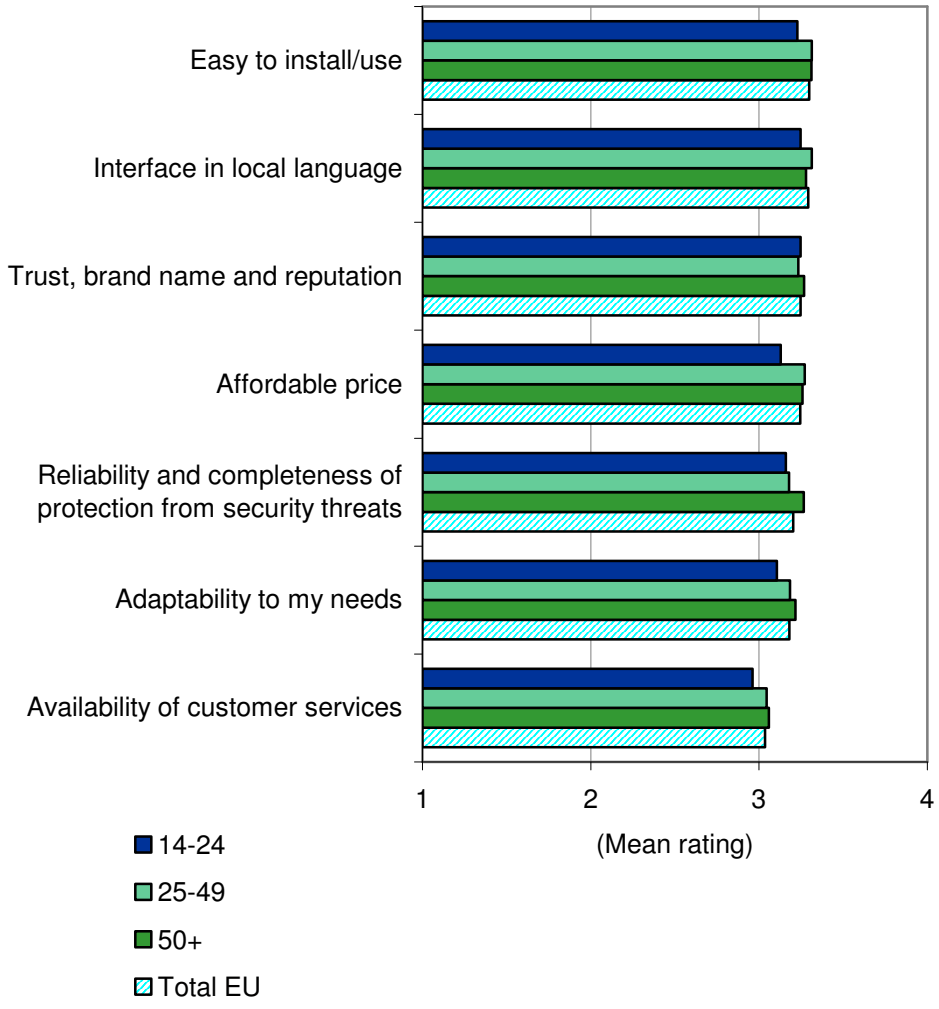
Note: Mean scores are based on a scale of 1–4, where 1 = not at all important and 4 = extremely important.

Source: IDC GI Survey of EU ICT consumer security market, 2008

FIGURE 63

Consumers' Level of Satisfaction for Security Solutions, by Age (Mean rating)

Q. Can you indicate your level of satisfaction, for each of the following areas, of your security solution/s?



N = 808

Base = All sample

Note: Mean scores are based on a scale of 1–4, where 1 = Very unsatisfied and 4 = Delighted.

Source: IDC GI Survey of EU ICT consumer security market, 2008

Main Procurement Channels

As is the case for the business market, consumers use several procurement channels of security solutions, sometimes at the same time. As shown by the following figure, the most popular ways to procure a security solution are to get it from the security vendor website (66% of EU consumers) and/or to download it for free directly from the web (64%). But many users also receive their security when

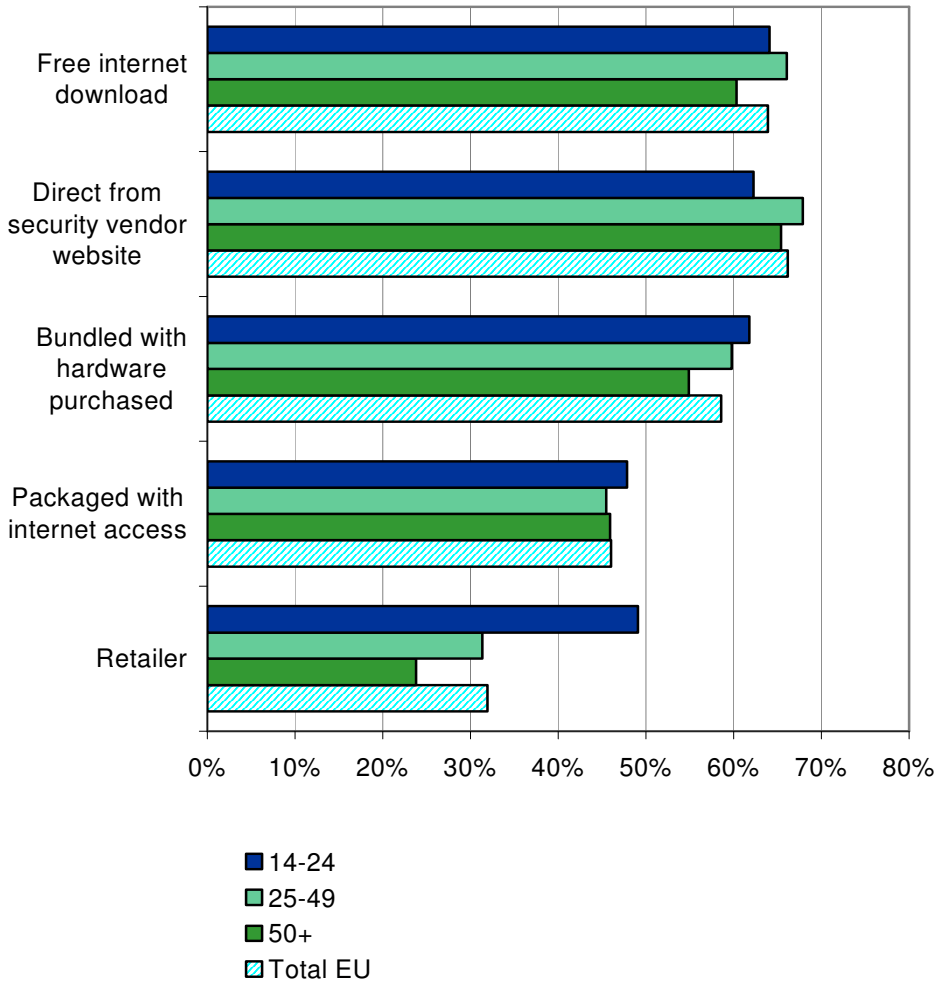
they buy a pc (59%) or packaged with their Internet access subscription (46%). Only a third of users buy from a retailer.

There are some small differences by age group, with the young users more likely to download for free their security solution or to procure it from a retailer (49% of the young do so).

FIGURE 64

Consumer Survey: Main Procurement Channels of IT Security Solutions, by Age (% of answers by age group)

Q. Where did you buy or source your security solution?



N = 792

Base = Respondents that use IT security solutions. Multiple response

Source: IDC GI Survey of EU ICT Security Market, 2008

8. THE EU ICT SECURITY CONSUMER MARKET SURVEY

Overview

The Consumer data presented above is based on a CAWI (Computer-aided Web Interviews) survey of 808 individual Internet users in a selected group of 7 EU Member States: Denmark, UK, France, Germany, Estonia, Italy and Poland.

These Member States were selected in order to represent the population of all of the EU, with a focus on more advanced Internet consumer markets. To do so, all the Member States were grouped in four clusters, based on two main parameters measured by Eurostat: the adoption of Internet broadband by households and the frequency of households declaring problems with virus or spamming over the Internet (*see the Methodology Annex for more details*). Two of the clusters can be defined "advanced" in terms of broadband adoption and use of the Internet (Cluster A and Cluster B, above the average EU level): Cluster C includes several countries right below the EU27 average and Cluster D the laggards (only 4 of the New Member States suffering from a gap in consumer broadband diffusion).

The study team decided to carry out the survey in 5 countries from advanced Clusters A and B and only 2 countries from laggards Clusters C and D, in order to focus on the analysis of the more advanced consumers. The data from the surveyed countries was extrapolated to all of the EU, weighted to reflect the age distribution of the population in each country.

These Clusters, because of the parameters selected, are different from the Clusters used for the Business demand analysis, and were used only for the extrapolation of the data.

TABLE 10

The EU NIS Consumer Market Clusters

Clusters	Member States
Cluster A	Survey: Denmark Other countries: Finland, Netherlands, Sweden
Cluster B	Survey: Estonia, France, Germany, UK Other countries: Belgium, Luxemburg
Cluster C	Survey: Italy Other Countries: Austria, Cyprus, Czech Republic, Hungary, Greece Ireland, Latvia, Lithuania, Malta, Portugal, Slovenia, Spain
Cluster D	Survey: Poland Other Countries: Bulgaria, Romania, Slovakia

Source: IDC GI Survey of EU ICT Security Market, 2008

Description of the Consumers Sample: Socio-demographic Characteristics

The Consumers sample is balanced by gender (51.8% female) and age in each country, as shown in the following table. The survey had a target of 157 interviews for the age-band over 65, but this proved impossible to achieve: only 20 interviewees were found of that age. As a consequence, their interviews were included into the age band of over 50 years old. However, the sample data is weighted on the basis of the age distribution in each country, so the older users are well included in the survey.

TABLE 11

Consumer Survey: Number of Interviews by Country and Age

	Between 14 and 24 years	Between 25 and 49 years	More than 50 years	Total
Denmark	16	61	36	113
United Kingdom	19	62	36	117
France	22	73	45	140
Germany	17	61	36	114
Italy	20	58	37	115
Estonia	17	49	27	93
Poland	18	61	37	116
Total	129	425	254	808

Source: Survey of EU ICT Security Market, 2008

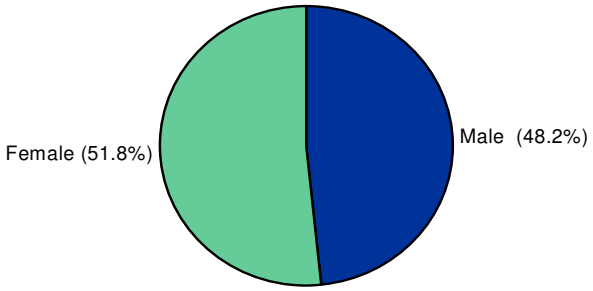
The other socio-demographic characteristics represent well the world of Internet users. In terms of occupation (*see following figure*), the relative majority of the Internet users of the sample are employees, but there is also a 13% of retired citizens, a 12.8% of students, and minor groups of unemployed, entrepreneurs and house workers. This confirms that Internet is a mass medium now, used by all social groups, but with a stronger presence in groups with higher levels of education.

The chart on the level of education shows that 46.7% of the sample consumers have a higher level of education, which is higher than in the general population. The sample includes 57% of Internet users with children, of which 20% with children under 12 and 14% between 12 and 18 years old, investigated to analyze fears and security application in the specific case of child protection.

FIGURE 65

Consumer Survey Sample by Gender (% of respondents)

Q. What is your gender?



N = 808

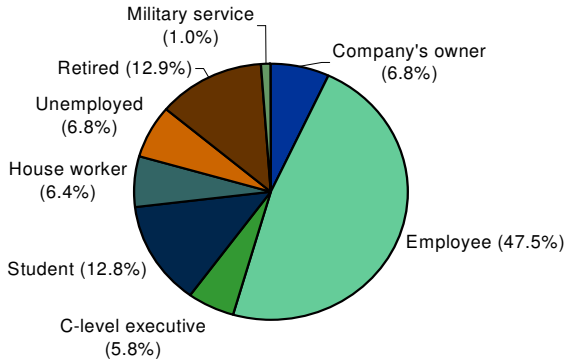
Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 66

Consumer Survey Sample by type of Occupation (% of respondents)

Q. What is your occupation?



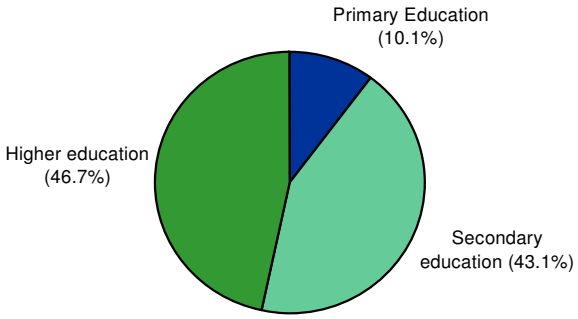
N = 808 - Base = All sample

Source: IDC GI Survey of EU ICT Security Market, 2008

FIGURE 67

Consumer Survey Sample by level of Education (% of respondents)

Q. What is the highest level of education you have acquired?



N = 808 - Base = All sample

Source: Survey of EU ICT Security Market, 2008