

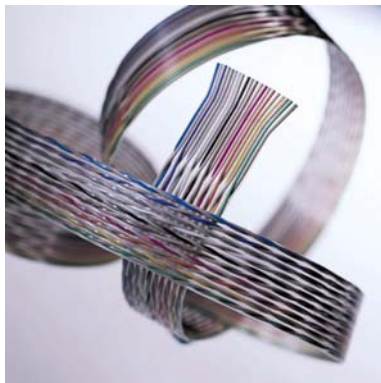
**Kommunikations- und
Technologieforschung**



empirica Schriftenreihe

Report 05/2006

Serie: e-Business



ICT Security, e-Invoicing and e-Payment Activities in European Enterprises

Simon Robinson, Hannes Selhofer,
Alexander Mentrup

September 2005



empirica Gesellschaft für Kommunikations-
und Technologieforschung mbH

Oxfordstr. 2

D-53111 Bonn

Tel. (+49) (228) 98530-0

Fax (+49) (228) 98530-12

www.empirica.com

empirica GmbH

empirica ist ein privates, international tätiges Forschungs- und Beratungsunternehmen mit diesen thematischen Schwerpunkten:

- Telearbeit / Zukunft der Arbeit
- Elektronischer Geschäftsverkehr / eBusiness
- Telematik für ältere und behinderte Menschen
- Telemedizin / Gesundheitstelematik
- Informations- und Wissensgesellschaft

empirica verfügt über langjährige Erfahrung mit quantitativen und qualitativen Forschungsmethoden. Unsere Kunden und Auftraggeber sind private Unternehmen und öffentliche Einrichtungen: große und mittelständische Unternehmen aus der Versicherungs-, Pharma- und Automobilbranche sowie Software- und Hardwarehersteller, des weiteren Telekommunikations-Dienstleister und -Netzbetreiber, soziale Dienstleister und medizinischen Einrichtungen, Bundes- und Landesministerien sowie die Europäische Kommission.

Unsere interdisziplinären Projektteams befassen sich u.a. mit Markt- und Begleitforschung, Politik- und Strategieberatung sowie Technikfolgenabschätzung. Wir beraten Kunden bei der Produktentwicklung und – einföhrung, der Konzeption und Umsetzung von Pilotprojekten und der Durchführung von Wirtschaftlichkeitsanalysen und Benchmarkingstudien.

Haftungsausschluss

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

Impressum

empirica Schriftenreihe

Report 5/2006

Januar 2006

empirica Gesellschaft für Kommunikations- und Technologieforschung mbH

Oxfordstr. 2

D-53111 Bonn

Tel. (+49) (228) 98530-0

Fax (+49) (228) 98530-12

E-Mail: info@empirica.com

Internet: <http://www.empirica.com>

Redaktion: Werner B. Korte

ISSN 1613-2726

Die Wiedergabe von Informationen aus diesem Bericht ist mit entsprechender Quellenangabe vorbehaltlich anderslautender Bestimmungen gestattet.

© empirica GmbH, Bonn, 2004.

Table of Contents

Introduction to the <i>e-Business W@tch</i>	4
Executive Summary.....	7
1 Introduction	10
1.1 Objectives and scope of the study	10
1.2 ICT security - important issues in information society policy	11
1.2.1 <i>The growing importance of ICT security</i>	11
1.2.2 <i>ICT security terms and concepts</i>	13
1.3 Electronic invoicing: saving money by replacing paper-based processes	16
1.3.1 <i>Electronic invoicing: terms & concepts</i>	16
1.3.2 <i>EU legal initiatives on e-procurement and e-invoicing</i>	17
1.3.3 <i>The public sector as role model in e-invoicing</i>	19
1.3.4 <i>The role of intermediaries in e-invoicing</i>	22
The e-Business Survey 2005	24
Part A: Information and network security in European enterprises.....	25
2 Information and network security in European enterprises	25
2.1 Incidence of security breaches and security-related costs	25
2.2 Deployment of ICT security controls	37
2.3 Summary	47
Part B: Electronic payments and e-invoicing activities in European enterprises.....	48
3 Electronic payments and e-invoicing activities in European enterprises.....	48
3.1 Adoption of e-invoicing and e-payment activity by EU enterprises	49
3.1.1 <i>Readiness for e-invoicing and e-payment processing</i>	53
3.1.2 <i>E-invoicing and e-payment activity</i>	58
3.2 E-payment consumer behaviour and the risk of fraud	64
3.2.1 <i>Consumer behaviour in making e-payments in 2004</i>	65
3.2.2 <i>e-Payment sector profiles</i>	67
3.2.3 <i>The risk of fraud and non-payment in online credit-card transactions</i>	70
4 Policy conclusions.....	73
4.1 Information and network security	73
4.1.1 <i>Policy objectives and measures</i>	73
4.1.2 <i>Policy deficits and requirements</i>	73
4.1.3 <i>Possible actions</i>	74
4.2 Promoting the diffusion of electronic billing, invoicing and payments	78
References.....	80
Annex I: The e-Business Survey 2005 – Methodology Report.....	82

Introduction to the *e-Business W@tch*

e-Business W@tch – observatory and intermediary since late 2001

The European Commission's *e-Business W@tch* monitors the adoption, development and impact of electronic business practices in different sectors of the economy in the enlarged European Union. The background of this initiative was the eEurope 2002 Action Plan, which provided the basis for targeted actions to stimulate the use of the Internet for accelerating e-commerce, acknowledging that "*electronic commerce is already developing dynamically in inter-business trading*" and that "*it is important for SMEs not to be left behind in this process.*" The eEurope 2005 Action Plan confirmed and built further upon these objectives with Action 3.1.2 "A dynamic e-business environment", which defined the goal "*to promote take-up of e-business with the aim of increasing the competitiveness of European enterprises and raising productivity and growth through investment in information and communication technologies, human resources (notably e-skills) and new business models*".

It is against this background that the European Commission, Enterprise & Industry Directorate General, launched the *e-Business W@tch* in late 2001. The objective of this initiative is to provide sectoral analysis based on empirical research, including representative enterprise surveys in countries of the European Union, the EEA and Accession States, with special emphasis on the implications for small and medium-sized enterprises (SMEs).

Since its launch, the *e-Business W@tch* has published more than 50 e-Business Sector Studies on 17 different sectors of the European economy, three comprehensive synthesis reports about the status of electronic business in the European Union, two statistical pocketbooks and various other resources (newsletters, special issue reports, etc). These are all available on the website at www.ebusiness-watch.org.

The quantitative analysis about the diffusion of ICT and e-business is based to a large extent on regular representative surveys among decision-makers in European enterprises. The 2005 survey covers more than 5000 enterprises from 10 different sectors across 7 EU member states. In addition, more than 70 case studies on e-business activity in enterprises from all EU, EEA and Accession countries are carried out, to complement the statistical picture by a more detailed analysis of current e-business practices.

Survey results of the previous years have confirmed the initial assumption and rationale of the *e-Business W@tch* that the sector in which a firm operates and the size of a company, rather than its location, are the main determinants of its e-business activity. The large demand for the various publications and statistics provided by the *e-Business W@tch*, and their exploitation by other research institutions (for example, in the EITO Yearbook 2003 and in the OECD Information Technology Outlook 2004), document the demand for sectoral e-business analysis. Facilitated by positive responses and the growing interest in its analysis, the *e-Business W@tch* is increasingly developing from an observatory into a think-tank and intermediary, stimulating the debate about the economic and policy implications of e-business among stakeholders at an international level.

The wide-angle perspective: *e-Business W@tch* provides the "big picture" as a basis for further research

The mission of the *e-Business W@tch* is to present a "wide-angle" perspective on e-business developments and practices in the sectors covered. This has important implications regarding the level of detail in which various issues can be explored, both in terms of the quantitative picture (survey) and in terms of the qualitative assessment and background research.

Over the past 10 years, "*electronic business*" has increased from a very specific to a very broad topic to be studied. The OECD proposes a definition of e-business as "*automated business processes (both intra-and inter-firm) over computer mediated networks*". This definition is useful as it makes clear that e-business is more than e-commerce (which focuses on commercial transactions between companies

and their customers, be it consumers or other companies) and that e-business includes internal processes within the company as well as processes between companies. Furthermore, the OECD definition implicitly indicates that the focus and main objective of electronic business is to be found in business process automation and integration, and the impacts thereof.

This implies that the potential scope for e-business analyses has also broadened. The measurement of e-commerce transactions (the volume of goods and services traded online) can and should be complemented by studies analysing the degree to which business processes, including intra-firm processes, are electronically linked to each other and have become digitally integrated. Hence, it becomes practically impossible to cover in depth all areas and facets of e-business in one study. Thus, study scope needs to be carefully defined.

The *e-Business W@tch* Sector Studies apply a wide-angle perspective and zoom into selected aspects of electronic business only. In general, studies with a wide-angle approach allow for a wider range of issues to be covered and investigated at the same time. This, however, necessarily limits the level of detail in which each single issue is explored. This must be considered when using the Sector Studies prepared by the *e-Business W@tch*.

The role of economic analysis in the Sector Reports

In addition to the analysis of e-business developments, the *e-Business W@tch* Sector Studies also provide some background information on respective sector. Following the configuration of the sector (on the basis of NACE Rev. 1.1 classification) at the introduction of each study, this overview includes some basic industry statistics, as well as information about the latest trends and challenges concerning the specific sector. Readers should not mistake this background information, however, as the main topic of analysis. An *e-Business W@tch* "sector report" is not a piece of economic research on the sector itself, but **a study focusing on the use of ICT and e-business** in that particular sector. The introduction to the sector is neither intended to be, nor could it be a substitute for more detailed and specific industrial analysis.

The data presented in each sector's overview are mainly derived from official statistics prepared by Eurostat, but are processed and refined by DIW Berlin. The purpose is to close the many gaps that occur in the official statistics, with missing data being imputed on the basis of extrapolations and own calculations.

The **mission** of the *e-Business W@tch* is to monitor, analyse and compare the development of e-business in different sectors of the European economy – not the sectors themselves.

Its **objective** is to provide reliable results, based on commonly accepted methodologies, which are not readily available from other sources and would trigger the interest of policy-makers, researchers, and other e-business stakeholders for more in depth analyses (or statistical surveys).

The *e-Business W@tch* has adopted a "wide-angle" perspective in its **approach** and the necessary trade-offs are transparently depicted in all its deliverables.

The definition of sectors and the adequate level of aggregation

Economic sectors constitute the main level of analysis for *e-Business W@tch*. In 2005, the sample consists of ten sectors. Their configuration and definition are based on the NACE Rev. 1.1 classification of business activities.

The rather broad aggregation of different business activities into sectors in 2002-2004 made it possible to cover a broad spectrum of the economy, but also caused some challenges for the analysis of e-business developments. For instance, it was hardly possible to focus on individual sub-sectors in much detail within a single sector report. The selection and definition of sectors proposed for 2005 reflect these concerns. Six out of the ten sectors proposed are sub-sectors that were part of

(aggregated) sectors analysed in 2002-2004. The rationale for "zooming in" on former sub-sectors is that the broad picture for the whole sector is now available from previous sector studies, and that this seems to be the right time within the prospective life-cycle of the *e-Business W@tch* to focus the analysis on more specific business activities.

The 10 sectors covered in 2005 were selected on the basis of the following considerations:

- The current dynamics of electronic business in the sector and the impact of ICT and electronic business, as derived from earlier *e-Business W@tch* sector studies.
- Interest articulated by the industry in previous years on studies of this type.
- Policy relevance of the sector from the perspective of DG Enterprise & Industry.
- Roll-out strategy of 2003: New sectors (not covered in 2002/03 and/or 2003/04) have been added, as well as specific industries which have only been covered as part of a larger sector in the past

In 2005, the *e-Business W@tch* will also deliver four cross-sector studies. These Special Reports will focus on a particular e-business topic of interest across different sectors rather than on a single sector.

The 10 sectors analysed in 2005

The 10 sectors which are being monitored and studied in 2004/05 include seven manufacturing, construction and two service sectors. Four of these sectors have been covered in the previous years of implementation, while the other six were covered as well, but as part of (aggregated) sectors analysed in 2002-2004.

Exhibit: Sectors and topics covered by e-Business W@tch in 2005

	Sector Studies	NACE Rev. 1	Publication date(s) *	
1	Food and beverages	15	July 2005	Sep. 2005
2	Textile industry	17, 18	July 2005	---
3	Publishing and printing	22	July 2005	Sep. 2005
4	Pharmaceutical industry	24.4	July 2005	Sep. 2005
5	Machinery and equipment	29	July 2005	Sep. 2005
6	Automotive industry	34	July 2005	---
7	Aerospace	35.3	---	Sep. 2005
8	Construction	45	July 2005	Sep. 2005
9	Tourism	55, 62.1+3, 92.3+5	---	Sep. 2005
10	IT services	72	July 2005	Sep. 2005
	Special Topic Reports			
A	A User's Guide to ICT Indicators: Definitions, sources, data collection		July 2005	---
B	International Outlook on E-Business Developments		July 2005	---
C	E-Business Standards and Interoperability Issues		---	Sep. 2005
D	ICT Security and Electronic Payments		---	Sep. 2005

* There will be 1 report (in 2005) on 4 of the 10 sectors, and 2 reports on the other six.

Executive Summary

Objectives of this study

This report is one of four special studies published by *e-Business W@tch* in 2005, in addition to its sector studies. While sector studies present e-business developments from a specific industry's perspective, special studies focus on a particular ICT related topic, across sectors. This study has two objectives:

- to investigate the incidence and pattern of damage from ICT security breaches and the extent of controls and other measures introduced by European enterprise to counter these threats;
- to summarise evidence on the uptake of e-invoicing and e-payment activity among firms from the 10 sectors covered by the *e-Business W@tch* in 2005.

Since security mechanisms, and concerns of trust, are important aspects in e-invoicing, and because the analysis of both issues is largely based on results of the e-Business Survey 2005, the presentation of results on these areas has been integrated in one report. However, the topic of ICT security is broad and also covers areas that are not directly related to invoicing and payment processes. Therefore, the analysis is presented in two distinct parts that can be read and used independently from each other.

Security incidents experienced by EU enterprises

Results from the survey show that the mean time between security-related incidents with significant impact on an enterprise is well under 2 years in the most vulnerable sectors in Europe, such as tourism and IT services. Malicious software and unsolicited e-mail currently have the greatest impact, followed by failures of hardware or software and problems faced by providers of services to the enterprise, such as leased lines or Internet access. Though not by any means negligible in scale, the impact of employee misconduct or unauthorised access to systems is reported to be at much lower levels than damage from spam or component failure. Despite the evidently increasing burden of compliance with legislation and regulation, this aspect of economic impact is reported to be least frequent, although the overall cost is likely to be very high, and is concentrated in a minority of sectors.

Incidence of damage from breaches of security and other security-related costs vary with size of enterprise, but the trends of incidence with size are mixed in direction. It is clear that in many cases the level of *threat* increases with size, e.g. with the number of staff employed or premises operated. At the same time, small enterprises are much less likely than large corporations to implement *controls* and other measures to reduce the impact of security threats. The opposing trends of threats and controls lead to the mixed picture in European enterprise overall, a picture which can hide real disadvantages faced by small organisations. For example, although the likelihood of employee negligence causing significant damage in any year is reported to be considerably lower in micro enterprises compared to larger organisations, the level of threat to micro organisations is very much smaller. It is estimated that damage could be reduced up to twenty-fold in cases such as these if means could be found to enable small organisations to counter the associated threats as effectively as larger organisations.

From a sector perspective, enterprises in the IT services sector report the greatest number of incidents causing significant damage, nearly three times as many as in the construction or food & beverages sectors. Whereas the rate of incidence in tourism is nearly as high as in IT services, other sectors are in mid field. The automotive industry is an interesting case, exhibiting very low levels of incidence of both hardware and software malfunction. It is probable that large manufacturers in the sector are being particularly effective at setting standards for hardware and software and ensuring that quality hardware/software solutions are introduced into and used throughout their supply chain. This would have the effect of improving the resilience of smaller enterprises in the sector to this kind of security threat, and it may well be that other sectors could learn lessons from the automotive industry. At the

same time the sector was found to have a particularly high incidence of damage from spamming, and it appears that no sector can lay claim to universal best practice in avoiding damage from security-related threats.

ICT security measures used by EU enterprises

The analysis of security controls and other measures applied by European enterprises to counter security threats shows that basic components such as firewalls and secure servers – for those enterprises requiring these – already exhibit high levels of penetration. Major deficits in security controls in European enterprise are evident in the low levels of reported application of data encryption, which is generally regarded as essential in distributed and mobile computing environments. The yet lower levels of deployment of public key infrastructure could represent an obstacle in the evolution of interoperable solutions for many e-business processes, particularly those with strong contractual content such as the transfer and agreement of large liabilities.

Given the importance of the human factor in breaches of security, the low proportion of enterprises reporting that they train their staff in security awareness, carry out risk assessment or, in particular, have put a security management system in place, should be a cause for concern among policy makers. Though the proportion of larger enterprises which have drafted disaster recovery plans and developed a security policy is over 70% (in each case), the picture is much bleaker among smaller businesses. Only 21% or 33% respectively of micro- and small enterprises report having an ICT security policy in place, despite strong consensus among security consultants and standards-setting bodies that such planning is essential in building a proper response to security threats.

The lower levels of control deployment found in smaller enterprises have a clear economic foundation. The ability to profitably deploy resources in combating security threats tends to be a function of the size of a business, particularly where in larger enterprises key ICT functions are centralised. These economies of scale can be clearly seen in the behaviour of enterprises in respect of the security controls included in the survey.

To simplify sectoral analysis, the underlying covariance structure was investigated and security controls and measures grouped along three principal factors: 'management and policy', 'secure components', and 'PKI (Public Key Infrastructure) and encryption'. The resulting picture by sector shows the clear dominance of enterprises in the IT services sector in the introduction of security controls in the areas of 'secure components' and 'management and policy'. Yet despite this leading position the incidence of damage is high for these enterprises, showing that the sector clearly faces some of the highest levels of threat. Fortunately, perhaps, enterprises in this sector can draw the know-how to select, implement and maintain secure systems from core business units, in contrast to other sectors.

The strongest contrast with the behaviour of enterprises in the IT services sector is given by companies in food and beverages, textile industries, tourism and construction. These latter sectors score lowest on all three factors. At the same time, these sectors are among those with the smallest average size, from which follows that they have a particularly large proportion of small and micro enterprises, whose behaviour dominates the statistics.

Adoption of e-invoicing

In total, about 5% of all firms from the 10 sectors and 7 countries surveyed in 2005 reported using ICT systems for electronically invoicing their customers. Similarly, about 5% reported using systems for billing invoices from suppliers electronically. Diffusion of e-invoicing activity may gain further momentum in the near future, as its benefits for firms of all sizes and from practically all sectors become more apparent, the main ones being cost savings and improved customer relationships.

In B2C markets, the highest initial potential is seen for firms that issue regular and similarly-structured invoices to a large number of customers. Such enterprises include telecommunications service providers, other utilities, insurance companies and publishers of newspapers and periodicals. Here, EBPP (Electronic Bill Presentation and Payment), i.e. the web based presentation of invoices and accounts to customers, will be the main platform. In B2B, electronic invoicing is tightly linked and

integrated with ERP (Enterprise Resource Planning) systems and has a high potential particularly in sectors with deep supply chain integration and long-standing supplier-customer relationships. This applies, for example, to the automotive, the aerospace and parts of the chemical industry.

Demand-side (consumer) trends in e-payment activity

Regarding demand-side (consumer) trends, the credit card has become by far the most important payment method in B2C electronic commerce. Pago eTransaction Services, for example, reports that about 80% of electronic payments made via its platform were made by credit card. However, there are considerable variations in e-payment methods by sector, by country and depending on the amount to be paid. Analysis of chargeback rates in e-payments shows an interesting and alarming trend. About 37 out of every thousand transactions of over 500€ result in chargebacks, possibly due to fraud.

Policy conclusions

Some aspects of the structural variation in security threats and response to these exposed in this study calls for appropriate public policy measures. A key objective is to improve the cost-benefit equation for SMEs, perhaps by reducing the cost of controls through standardisation, encouraging market offerings or promoting inter-enterprise cooperation and the sharing of resources.

Current policy on ICT security in Europe continues to be somewhat fragmented, providing opportunities to improve security through coordination and exchange of best practice, including adopting best practice into EU policy instruments where appropriate. The recently founded European Network and Information Security Agency (ENISA) can be expected to contribute to security policy coordination in this respect. As sector developments have been shown to be quite divergent, benchmarking exercises or other models of exchange of best practice could also be profitably used to accelerate exchange between sectors, in parallel with exchange at national level.

The exchange of best practice is also recommended as an instrument to promote successful national and regional programmes in the area of e-invoicing. In many EU countries and regions, the public sector has launched initiatives in order to exploit the cost saving potential of e-invoicing. This calls for International monitoring and impact assessments of different policy approaches. Within the EU, the European Commission could instigate such measures; globally the role might be taken on by the UN or the OECD.

E-invoicing is considered to lead to a 'win-win' situation for both parties involved, i.e. the paying and the receiving entity. Public authorities could act as role model by introducing e-invoicing themselves, or they can promote and facilitate the adoption of related activities among enterprises by other means, e.g. through facilitating access by enterprises to information on best practice or increasing the transparency of the market by supporting system and service comparison.

1 Introduction

1.1 Objectives and scope of the study

This is one of the four special studies published by *e-Business W@tch* in 2005, in addition to its sector studies. While sector studies present e-business developments from a specific industry's perspective, special studies focus on a particular ICT related topic, across sectors.¹

This special study has two objectives:

- to investigate the incidence and pattern of damage from ICT security breaches and the extent of controls and other measures introduced by European enterprise to counter these threats;
- to summarise evidence on the uptake of e-invoicing and e-payment activity among firms from the 10 sectors covered by the *e-Business W@tch* in 2005.

Results are predominantly based on the e-Business Survey 2005. In January and February 2005, *e-Business W@tch* interviewed more than 5200 companies from ten sectors and seven EU countries (EU-7²) about their use of ICT and e-business. This report features the main results in the area of ICT security, and on the use of ICT for making electronic payments and for e-invoicing.

Since security mechanisms, and concerns of trust, are important aspects in e-invoicing, and because the analysis of both issues is largely based on data from the same survey (except for chapter 3.2 on consumer behaviour in e-payments), the presentation of respective results has been integrated in one report. However, the topic of ICT security is broad and also covers areas that are not directly related to invoicing and payment processes. Therefore, the analysis is presented in two distinct parts that can be read and used independently from each other. However, the main focus of this report is on the analysis of ICT security (Part A), as related data are not featured in the specific sector reports.

Results are discussed against the background of current policy initiatives in these areas. Conclusions on possible implications for policy are drawn from the empirical evidence available. The report is complementary to another special study prepared by *e-Business W@tch* on 2005 on the use of electronic standards and interoperability³.

¹ The other three special studies of 2005 are: "A User's Guide to ICT Indicators: Definitions, sources, data collection"; "International Outlook on E-Business Developments"; and "e-Business Standards and Interoperability Issues"

² The e-Business Survey 2005 included companies from Czech Republic, France, Germany, Italy, Spain, Poland and the UK ("EU-7"). These seven countries account for roughly 75% of the EU-25 population and GDP.

³ e-Business Special Study on Interoperability and Standards, September 2005, [Hwww.ebusiness-watch.org](http://www.ebusiness-watch.org)H ('resources').

1.2 ICT security - important issues in information society policy

1.2.1 The growing importance of ICT security

Importance of ICT security

The use of ICT systems has grown enormously in recent years across all sectors of business activity and public services but also in leisure and family activities. The economic well-being of enterprises in Europe has come to depend increasingly on instant access by all enterprises and their customers to an unlimited flow of information based on interoperable public networks and information technology systems. Considering the growing dependency of enterprises and society in general on communications and information technology systems (ICT), weaknesses and vulnerabilities in these networks and systems are posing an increasingly serious threat to the proper functioning of key value chains in Europe. The magnitude of this threat continues to grow along with the number of networks users and the value of the transactions they carry out.

Fact-box

Increasing use of hacking for espionage and blackmail?

Viruses, Trojan horses and other malicious software developed by hackers have been commonly associated with mass attacks on large numbers of users targeted largely at random. The perpetrators appeared not to be intent on enriching themselves but apparently enjoyed having some kind of mildly destructive or just irritating impact on thousands of computer systems and their users. The situation has been changing recently, however.

In May 2005 the Israeli police charged a number of people who had built and used a Trojan horse to spy on competitors with industrial espionage. The Trojan was delivered via harmless-sounding e-mails and an advertising CD-ROM addressed to managers. Once installed, the Trojan laid a user's PC completely open to remote control by the virus originators, by which means confidential information could be stolen. Though the companies attacked had effective firewalls in place, the Trojan passed undetected. Because of its very focussed and limited use, anti-virus specialists had not been alerted, had not identified the new virus' signature and not provided their clients with the ability to defend themselves against it.

Another Trojan, Pgpocoder, gained notoriety in the same month. Unlike the Israeli spy software, after entering a user's system as malicious code attached to e-mails, Pgpocoder proceeded not to spy on but to blackmail its victim. It encrypted files - documents, photos or spreadsheets - and made them inaccessible to the legitimate user, who was prompted on trying to access the files to purchase a 'decoder'. Fortunately, the encoding algorithm used was not particularly sophisticated, and others soon built a decoder provided free to victims. There is of course no guarantee that a virus writer will not deploy military-grade encryption next time.

These examples, together with the recent explosion of password spying - phishing - to obtain access to bank accounts, show how hacking is no longer simply a mildly destructive hobby of isolated computer freaks, but is increasingly being deployed by organised gangs with criminal objectives. Today, designers of malicious software are increasingly likely to be professional criminals and belong to established organised criminality.

Sources: Various online articles, including Informationweek, computerweek, ynetnews. See references for the full list.

Reliance on ICT is also growing as a result of changes in the structure of business enabled by ICT. Business processes are increasingly reliant on ICT networks and applications to link activities in multiple organisations. ICT, and the e-business applications built on it, integrates the different elements of the supply chain and enables extension of chains to new participants, including outsourcing operations to cheaper labour markets. This change in structure is further increasing the vulnerability of businesses to a range of security threats to the ICT infrastructure.

Features of the regulatory environment - national legislation and sector-specific regulation with global and cross-sector reach

European enterprises increasingly must deploy security measures ('controls') not just to avoid damage to their own operations but to meet new legislative and regulatory requirements, such as data protection, designed in the main to protect the interests of others, their customers, suppliers, staff or partners.

Some legislation impinging on European enterprise has its origins in EU directives, which take effect through national legislation. According to the provisions of the Treaty of Rome, regulation initiated by the European Parliament through the medium of directives is reflected into national legislation through a process of transposition. The national legislation resulting from transposition is not simply a copy of the directive, but is nevertheless binding for European enterprises operating in the member state concerned.

In some cases, conformance of national legislation to the minimum conditions of a directive is called into question. The Commission has recently questioned⁴ whether the UK 1998 Data Protection Act properly transposes provisions of EU Data Protection directives⁵. In other cases, national legislation goes beyond the provisions of the EU directive it transposes. For instance, in transposing the 1999 Electronic Signature Directive⁶ into the *Signaturgesetz*⁷ the German government imposed more stringent requirements on actors in the Public Key Infrastructure. These requirements are nevertheless legally binding on enterprises operating the Germany.

In addition to legislation at EU or national level, regulation relating to ICT security is being imposed by other parties endowed with specific powers, such as a stock exchange, and by regulatory organisations recognised internationally for a particular sector. In an increasingly networked global economy, regulation in one country or in one sector has knock-on effects across sectors and regions.

⁴ In July 2004 the European Commission called upon the UK Government to justify its approach to data protection law because it fears that it does not comply with the European Data Protection Directive. Jonathan Todd, European Commission Spokesman on the Internal Market, cited by OUT-LAW News (OUT-LAW News, 15/07/2004), stated that the Commission has sent a letter of formal notice to the UK Government about the conformity of several aspects of the 1998 Data Protection Law with the EU data protection Directive of 1995 (95/46/EC). These relate to insufficient controls on international transfers of data and to the definition of personal data, which in the 1995 Directive applies to that recorded personal information which directly or indirectly relates to an individual. In the light of the UK's reply, the Commission will decide whether or not it considers the UK law is in conformity or not, and whether or not to request the UK Government to amend its legislation.

⁵ There are several EU Directives relevant to data protection. The EU Directive on Privacy and Electronic Communications 2002/58/EC updated the Telecoms Data Protection Directive (97/66/EC) which itself supplemented EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁶ EU Directive 1999/93 of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures.

⁷ Stammfassung BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.); 1. Novelle: BGBl. I Nr. 137/2000 (NR: GP XXI IA 313/A AB 372 S. 44. BR: AB 6277 S. 670.) [CELEX-Nr.: 399L0093]; 2. Novelle: BGBl. I Nr. 32/2001 (NR: GP XXI IA 370/A AB 507 S. 57. BR: 6315 AB 6322 S. 673.); 3. Novelle: BGBl. I Nr. 152/2001 (NR: GP XXI RV 817 AB 853 S. 83. BR: AB 6499 S. 682.) cited from <http://www.signatur.rtr.at/de/legal/sigg.html>

One example of sectoral regulation with wider impact on ICT security in enterprises is the introduction of new regulation addressed primarily at the banking sector, known as Basel II. Basel II represents an upgrade of the international capital rules for bank safety, drafted following large-scale bank failures such as the Bank of Credit and Commerce International. The world's major banks aim to introduce measures to meet the Basel II by the beginning of 2007.

As a result of this sectoral regulation, financial stakeholders – banks and other financial institutions - are beginning to put pressure on their customer enterprises in all sectors, not just to provide better collateral for loans, but also to meet improved network and information security standards. This pressure is designed to enable the financial services providers themselves to meet their regulatory commitments. The 'operations' pillar of the three pillars of Basel II requires banks properly to manage their operational risks, including those associated with the use of ICT by themselves and their suppliers and customers.

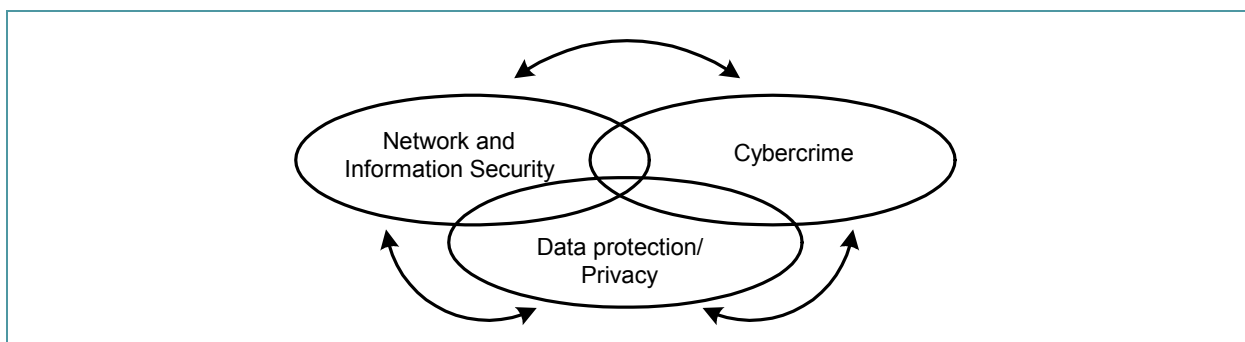
Thus sectoral requirements in banking are already having an impact on ICT security measures introduced by organisations beyond the financial sector. The Sarbanes-Oxley legislation, introduced in the United States after massive accounting fraud in large enterprises, is an example of national legislation with global impact. Its provisions are in some way similar to those of Basel II, but the act further expands auditing requirements applicable to trading partners of the US. The act specifies for instance that the auditor of an enterprise must report on the suitability and appropriateness of internal control systems, including on any ICT security controls in place, in the context of an objective risk analysis.

Clearly this increasing regulatory load cannot be complied with by the enterprises affected without incurring possibly significant expense, and forces enterprises which might otherwise have been lax about ICT security to provide evidence of appropriate action and implemented controls. Against this background, the impact of costs from regulation has been included specifically in this study of European enterprise.

1.2.2 ICT security terms and concepts

To understand the impacts on enterprise and policy implications of ICT security we distinguish three distinct but related areas: Network and information Security, cybercrime and data protection, illustrated below.

Exhibit 1-1: ICT security domains⁸



Network and information security

Network and information security can be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that

⁸ Adapted from: Network and Information Security: Proposal for a European Policy Approach, 2001. European Commission, p.15

compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks or systems.⁹

In this respect 'availability' refers to whether data is accessible and services are operational, despite possible disruptive events. 'Authenticity' can be achieved by authentication, which is the confirmation of an asserted identity of entities or users, whereas 'integrity' is the confirmation that data which have been sent, received, or stored are complete and unchanged in comparison to those originally sent. Finally, 'confidentiality' can be seen as the protection of communications or stored data against interception and reading by unauthorised persons.

Cybercrime

The terms 'computer crime', 'computer-related crime', 'high-tech crime' and 'cybercrime' are often used synonymously and usually in the broad sense of *"any crime that in some way or other involves the use of information technology"*.¹⁰ A distinction can usefully be made, within the concept of cybercrime, between 'computer-specific' crime and traditional crimes performed with the aid of ICT technology¹¹ Smuggling and counterfeit are examples of traditional crimes which can be supported by ICT, whereas computer viruses and hacking can be seen as computer- specific crimes.

Data protection/Privacy

Data protection means the protection of fundamental rights and freedoms, especially the protection of privacy concerning the processing of personal data. Directive 2002/58/EC on privacy and electronic communications¹² harmonises the provisions of Member States required to ensure:

- an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and
- the free movement of such data and of electronic communication equipment services in the Community.

"Personal data" as defined by Directive 95/46/EC¹³ means *"any information relating to an identified or identifiable natural person"*. The same directive defines *"Processing of personal data"* to mean *"any operation or set of operations which is performed upon personal data whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, blocking, erasure or destruction."*

Moreover privacy does not only mean 'data protection' in the sense of, for instance, avoiding interception of communications or unauthorised access to personal data, but can also be interpreted in a broader sense including for example the reception of unsolicited emails (spamming)¹⁴ – meaning the right for what is sometimes referred to as 'informational self-determination'.

⁹ Network and Information Security: Proposal for a European Policy Approach. European Commission, 2001 (p.5)

¹⁰ See: European Commission, Justice and Home Affairs: "Anti cybercrime legislative proposals on Council table", [Hhttp://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm](http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm)H (accessed in August 2005)

¹¹ Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. European Commission, 2001

¹² Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002. The European Parliament and the Council.

¹³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

¹⁴ Impact and Priorities - A communication to the Spring European Council in Stockholm, 23-24 March 2001 - Communication to the European Parliament and the Council. European Commission, 2001

Security threats and control measures

Threats in today's ICT world are manifold. When it comes to network and information security, not only malicious actions but also accidental events have to be taken into account, since their impact on the network or data can result in similar damage. For instance, the intended destruction of a certain set of data by a hacker or its unintended deletion by an employee may well have effectively the same impact on business. Exhibit 1-2 features an overview of a range of ICT-related threats faced by the modern enterprise. The table also provides an indication of relevant control measures discussed by policy¹⁵, without implying that these solutions are the most effective for a given threat.

Exhibit 1-2: ICT security threats and control measures

Threat	Description	Control measure
Interception of communications	Often called 'sniffing'; physical access to network lines (e.g. wiretapping, monitoring radio transmissions)	Encryption of data, network security enhancement by operators
Unauthorised access into computers / networks	Technically called intrusion (e.g. hacking)	From password protection and firewalls to biometrics, intrusion detection and application level controls
Network or server failure, software failure	Breakdown through switch or link failure, failure of application or infrastructure software, hardware failure	Quality control and regular maintenance planning, filtering, access control, secure Domain Name Services (DNS), back-up procedures, recovery plans
Malicious software (e.g. viruses) and unsolicited communications (spam)	Software used to disable a computer, to delete or modify data or to spy and steal information and identity, attacks on name servers and general flooding with e-mail or other messages to achieve denial of service.	Specialist software (virus scanners for files, mail etc.), alert systems and virus analysis
Malicious misrepresentation	Theft of identity and use for malicious purposes, often by 'insiders'	Higher levels of authentication (e-signatures)
Natural and environmental events	Unforeseen and accidental events (e.g. natural disasters)	Investment in traditional security, maintenance of public networks in catastrophic events
Human error	Negligence, lack of competence	Awareness raising, improved training, information campaigns, simulation

¹⁵ Network and Information Security: Proposal for a European Policy Approach. European Commission, 2001 (p. 5-12)

1.3 Electronic invoicing: saving money by replacing paper-based processes

1.3.1 Electronic invoicing: terms & concepts

Electronic invoicing is a computer-mediated transaction between a seller/biller (invoicing entity) and a buyer/payer (receiving entity), which replaces traditional paper-based invoicing processes. In e-invoicing, the invoice is electronically generated and sent by the biller and electronically received, processed and archived by the payer. In practice, e-invoicing typically goes hand in hand with making payments electronically.

Electronic invoicing activities can be grouped in different ways. Two dimensions are particularly important for differentiation when discussing technicalities and business implications of e-invoicing:

- The **target group**: E-invoicing services can be designed for business-to-business (B2B) or for business-to-consumer (B2C) transactions. The main difference is that B2B e-invoicing systems are usually designed as a two-way process, i.e. both sides can issue and/or receive invoices, while B2C systems are predominantly designed in a way that consumers can receive (and pay) invoices in a web-based environment. Transactions between businesses and the public sector are structurally similar to B2B processes, enabling similar systems to be used in principle.
- The **technical platform**: E-invoicing can either be accomplished in a web-based environment, or processes can be integrated with the ERP system of a company. ERP-based systems (which are used in B2B e-invoicing) promise the highest cost-saving potential for companies, but have certain requirements on B2B connectivity that can cause difficulties.

In B2B exchanges and in transactions with the public sector, from an accountant's perspective, the business processes concerned are a combination of activities undertaken by two disparate organisations, commonly known as Accounts Receivable (A/R) and Accounts Payable (A/P). The A/R business process includes the steps necessary to create and deliver the invoice, and to reconcile entries once payment is received; the A/P process includes the corresponding steps for receiving, reviewing, (possibly) disputing and paying an invoice.¹⁶

For web-based e-invoicing and payment, some technical terms have been established for the respective processes and related ICT solutions. The acronym EBPP (or EIPP) means Electronic Bill / Invoice Presentment and Payment. EBPP software solutions are provided by the large software companies that offer the broad spectrum of business solutions as well as by companies and consortia that have specialised on providing electronic billing and payment solutions (see Exhibit 1-3).

ERP-based and web-based systems can be integrated; it is quite likely that this will be the way forward for many medium-sized and large companies in an increasingly web-based economy. Large vendors of ERP systems, such as SAP or People Soft, offer their customers interfaces from their ERP solutions to existing (web based) EBPP systems.¹⁷

¹⁶ For a more detailed and systematic presentation of the processes involved, see "Electronic Invoice Presentment and Payment (EIPP): A Win-Win Proposition". White Paper by CheckFree iSolutions (2003).

¹⁷ Cf. "ERP auf Electronic Payment gefasst", Computerwoche, 24 February 2003, [Hwww.computerwoche.de/H](http://www.computerwoche.de/H) (July 2005)

Exhibit 1-3: Technical terms related to ICT supported invoicing and payment processes

EBPP / EIPP	<u>Electronic Bill / Invoice Presentment and Payment</u> Invoices which are presented and can be paid on the internet (based on TCP/IP). End user equipment that can be used for receiving and paying an invoice include computers, mobile phones (e.g. through WAP), PDAs. Invoicing data are typically converted from the biller's system into XML format. When used for B2C transactions, 'bills' are usually regular, standardised payments to be made by consumers, e.g. monthly payments to mobile network providers, to utility providers or insurance premiums.
ESP	<u>Electronic Statement Presentment</u> Presentation of (payment-related) documents on the internet (e.g. current account, reports, analyses).
BSP	<u>Biller Service Provider</u> Third party service provider who handles payment processes on behalf of the billing entity.
CSP	<u>Customer Service Provider</u> Companies presenting electronic invoices on a graphical user interface for the receiver of invoices, and offering EBPP functionalities.
Consolidator	A consolidator collects and bundles invoicing data from different companies. Thus it is an additional intermediary between biller and receiver.

Source: ERP auf Electronic Payment gefasst, Computerwoche, 24 Feb. 2003, www.computerwoche.de

Private sector companies which are considering using e-invoicing have to take several strategic decisions. They have to decide on the e-invoicing model, for example whether to use a consolidator or whether to go for direct billing. Moreover, they have to consider whether the main objective should be to reduce processing costs, or whether e-invoicing is seen as a long-term investment for deepening customer relationships. Particularly in B2B, the latter is an important question with implications on the implementation strategy. Customer or supplier acceptance is a critical issue in any case.

1.3.2 EU legal initiatives on e-procurement and e-invoicing

It has long been recognised that electronic procurement offers significant potential opportunities for the public sector. In April 2004, the European Parliament and the Council adopted two **Directives on e-procurement**.¹⁸ The Directives are supposed to provide for the first time a coherent EU framework for the transparent and non-discriminatory use of electronic means in public procurement. They aim to computerise traditional procedures for the award of contracts and to introduce new purchase techniques and instruments enabled by advances in technology and the internet. Member States are required to implement the new legal framework by 31 January 2006.

In order to support the implementation process, the European Commission has issued a Communication that proposes an **Action Plan** for the implementation of the new legal framework.¹⁹ The aim is to assist Member States in writing the rules into national law and contracting authorities in implementing them. Ultimately, the objective is "to enable any business with a PC and an internet connection to bid for public contracts electronically anywhere in the EU."²⁰

¹⁸ Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (30.04.2004); Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (30.04.2004).

¹⁹ Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Action plan for the implementation of the legal framework for electronic public procurement. 13 December 2004.

²⁰ "Public procurement – Commission sets out Action Plan to move public purchasing in Europe online", Press Release by the EC, IP/05/66, 19 Jan. 2005

The need for such a European e-procurement Action Plan was confirmed by a consultation which the Commission had carried out as part of an impact assessment.²¹ In addition to the Action Plan, the Commission has published an explanatory document that explains and interprets the rules on electronic public procurement.²²

The Commission argues that, if online procurement is generalised, it can save governments "up to 5% on expenditure and up to 50-80% on transaction costs for both buyers and suppliers".²³ In order to exploit this cost-saving potential, the Commission's Action Plan proposes **measures along three axes**:

- Ensure a well functioning Internal Market when public procurement is conducted electronically;
- Achieve greater efficiency in procurement and improve governance;
- Work towards an international framework for electronic public procurement.

The Commission points out that "early adoption of the new e-procurement provisions is essential to avoid barriers to and distortion of competition", and that "Member States should deploy all efforts to comply with the Directives' deadline".²⁴ However, the Commission is aware that "slippages cannot be excluded". In fact, the implementation of e-procurement schemes on a systematic basis involves substantial technical and organisational challenges. Experience from earlier efforts to promote and facilitate the adoption of digital technology in public procurement has shown some of the difficulties involved, not only for the public sector, but also for business. The use of digital signature may serve as example. Freek Posthumus, project manager for NORMAPME (www.normapme.com), an EU body established to represent the interests of small businesses, points at possible breaches of EU legislation in this context: "In 2001, an EU directive was issued requiring the source of electronic invoices to be authenticated either through EDI links or through digital signatures. The deadline to implement that legislation was January 2004, meaning that for nearly a year now many companies will have been operating in breach of EU taxation law by emailing invoices without a digital signature."²⁵

The framework and action plan include specific measures to make it easier for suppliers to comply with the new requirements. In particular, there are measures to cut 'red tape', for example by agreeing on electronic certificates that every public purchaser usually requires and on standards for electronic catalogues.

Within the broader framework of e-procurement, the **processing of related invoices and payments** has also attracted attention among policy. Procurement related activities do not end with the tendering process and the selection of a supplier, but also include the processing of invoices and payments. While the primary objective for electronic tendering and ordering is to reduce direct procurement costs, additional opportunities for saving costs arise from processing supplier invoices electronically. Here, the public sector could have a role model.

²¹ See: Commission Staff Working Document: Impact Assessment of the Commission on an Action Plan on electronic public procurement. 13 December 2004

²² "Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC." The document is available on the web at the following address: [Hhttp://europa.eu.int/comm/internal_market/publicprocurement/e-procurement_en.htm](http://europa.eu.int/comm/internal_market/publicprocurement/e-procurement_en.htm)H. The publication of this document was one of the actions envisaged by the e-procurement Action Plan.

²³ European Commission (2004a). Action plan for the implementation of the legal framework for electronic public procurement, p. 3

²⁴ *ibid*

²⁵ Quoted from: "Taking the paper out of financial paperwork", interview with Freek Posthumus, published in "Small and Medium Enterprise Use", Issue 09, Dec. 2004, by Oracle.

Activities by European standardisation organisations

European standardisation organisations are addressing the issue of e-invoicing. CEN/ISSS²⁶ has launched a new Workshop on "Interoperability of Electronic Invoices in the European Community" on 21 April 2005, in connection with an EU/EFTA standardization mandate concerning standardization in support of Directive 2001/115 of the Council and Parliament on this topic.²⁷ The Workshop is rooted in the former e-Invoicing Focus Group.²⁸

1.3.3 The public sector as role model in e-invoicing

The main driver to implement e-invoicing and e-payment processes is the opportunity to save process costs. The saving potential obviously depends on the number of invoices that have to be processed. For companies, organisations and public authorities that have to process a very large number of invoices as part of their day-to-day work, e-invoicing promises substantial benefits.

In theory, and ideally, e-invoicing leads to a win-win situation for both parties involved, i.e. the invoicing entity and the receiving entity. This is why e-invoicing is such a highly attractive proposition for the public sector: By adopting e-invoicing, thus acting as a role model and promoting adoption in the private sector, the public sector may hope to achieve two important objectives at the same time: save costs in public administration, while improving the competitiveness of the local / regional economy. What sounds like a policy maker's dream could turn into reality, provided that the right measures are taken.

Many EU countries and regions have already launched e-invoicing initiatives in order to benefit from these opportunities. The most radical approach has been adopted by **Denmark**. Since February 2005, Danish public authorities only accept digital invoices from their suppliers (see fact-box: 'The Danish e-invoicing initiative'). Other countries and regions have taken a different, less radical path.

In **Austria**, for example, the Ministry of Economic Affairs and Labour, in cooperation with the Chamber of Commerce, has launched an initiative for standardizing a common e-billing interface ('eblInterface'). The objective is that major vendors of financial accounting software and ERP systems integrate this interface in the systems which they sell to Austrian companies. Cooperation has been established with about 10 software companies (including BMD, datev, IGEL, Mesonic und Microsoft Austria) and first results appear encouraging.²⁹

In **Finland**, which together with other Nordic countries is a forerunner in the adoption of e-invoicing (particularly in B2C, where e-invoicing enjoys high user acceptance), the region of South Karelia has launched an initiative to promote e-invoicing adoption among SMEs. The general objective is to reach a critical mass of SMEs that adopt various e-solutions. In a first step, the focus is on e-invoicing, as a possible 'killer application' for follow-up adoptions. E-invoicing is estimated to reduce aggregate processing costs for invoices in B2B transactions (i.e. costs of the biller and payer) by about 50%. Distribution channels for e-invoices include consolidators, such as internet banks, and ASP operators specialised in finance and accounts.³⁰

²⁶ CEN/ISSS was created in mid-1997 by CEN (European Committee for Standardization) as the focus for its ICT (Information and Communications Technologies) activities.

²⁷ See <http://www.cenorm.be/cenorm/businessdomains/businessdomains/iss/activity/wseinvoice.asp>, accessed in Aug. 2005

²⁸ The full Report and Recommendations of CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing relating to VAT Directive 2001/115/EC is available at <http://www.cenorm.be/cenorm/businessdomains/businessdomains/iss/activity/finalreportefig.zip>

²⁹ Presentation by Robert Kromer, Consultant, IT Consulting & Coaching GesmbH & Department of Enterprise and Technology, Ministry of Economic Affairs and Labour, Austria, at the eBSN workshop on "eProcurement and eInvoicing: European experiences and trends", 18th Bled eConference, 7 June 2005.

³⁰ Presentation by Antti Eskola, Ministry of Trade and Industry, Finland: "ICT, eBusiness and SMEs – The Policy Environment. Case Finland", at WSIS Thematic Meeting, 17-19 Jan. 2005, Antigua / Guatemala.

The significant opportunities arising from e-invoicing not only for the public sector, but also for business, have triggered activities by international organisations. UNECE, the **United Nations** Economic Commission for Europe, argues that the main reason why the vast majority (about 95%) of invoices are still processes on paper is the lack of a common international standard for the layout and the data elements, the legal requirements and the XML message. Against this background, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) has set up a new Trade Facilitation project to revise its existing recommendations on invoices for international trade.³¹

UNECE says that experience shows it is not sufficient to have a high-level legal framework. *"The continuing differences in national regulatory requirements, even within the European Union, or the various interpretations of the legislation, including technology requirements, still are a hurdle for business to move towards electronic invoicing. Therefore, an initiative at United Nations level is very important to remove the remaining barriers to expedite adoption."*

At national level, however, strict legal frameworks, if accompanied by appropriate supporting measures, may be the most effective instrument to bring the fast adoption of e-invoicing, as the Danish initiative shows (see Fact Box).

³¹ "UN/CEFACT puts its weight behind e-invoicing", press release by UNECE, United Nations Economic Commission for Europe, Geneva, 25 January 2005.

Fact-box:

The Danish e-invoicing initiative

Since February 2005, Danish public authorities only accept digital invoices from their suppliers. According to the government, this move, which is mandated by legislation, affects about 440.000 companies. The number of invoices to be exchanged is estimated at about 18 million per year. About 75% of those are sent to municipalities.

The business case

This rather radical approach makes the Danish public sector a world leader in the field of e-invoicing. The goal is to save between 700 and 900 million Danish Kroner (94 to 120 million euros) per year. This 'business case' is based on the expectation that processing invoices electronically will reduce the average processing time per invoice by 10 minutes. This should, in turn, translate into staff reductions in the public sector.

The government further estimates that, if ordering could also be done electronically, 17 minutes would be saved in the handling process of each invoice. Potential savings would then increase to about 160 million euros per year. This could be a logical next step.

Scanning agencies convert printed invoices to e-invoices

As not all enterprises that provide services to the public sector, in particular small firms, have the technical facilities for e-invoicing, they can send their invoice in the traditional way to a 'national scanning agency' (NSA). All certified companies may act as a scanning agency. The NSAs scan a printed invoices and forward an electronic invoice (with the scan attached to it) to the respective public body.

OASIS Universal Business Language has been selected as the technical standard for the e-invoices. OASIS maintains close alignment with existing EDI systems.

Lessons learned

The Danish approach is currently much debated in Europe. Many people regard this initiative as a prime example of how the public sector can become a role model in electronic business. Critics, on the other hand, point at problems for companies and expect that substantial parts of the expected savings could be consumed by extra costs and work, such as the extra fees charged by a number of businesses for sending digital invoices.

First results, however, are encouraging. The vast majority of public authorities and private companies have reacted positively, as it is widely recognized that electronic procurement is the way forward. The government admits that the overall legislation, standardization and implementation schedule was extremely tight, which led to some technical difficulties in the beginning. But these have mostly been eliminated.

There are already some lessons to be learned. The Governments recommends that the adoption of old EDI technology is not necessarily the best solution, while basing the technical infrastructure on internet technologies should be considered.

Sources:

- Presentation of the initiative by Peter Larsen Borresen, Danish Ministry of Science, Technology and Innovation, at the e-Business W@tch Workshop on e-Invoicing, Athens, 31 May 2005. Available at www.ebusiness-watch.org ('events')
- IDABC of the European Commission, "Danish e-invoicing savings plans frustrated by extra costs and work", 25 April 2005.
<http://europa.eu.int/idabc/en/document/4215/194> (July 2005)

The diversity of national approaches to introducing e-invoicing in the public sector and to promoting its uptake among firms has to do with differences in the legal frameworks, for example with regard to electronic signature and the acceptance of electronic documents as valid invoices.³² For example, the fast development of e-invoicing in the Nordic countries is clearly facilitated by comparatively light regulation, particularly in terms of the legal and technical requirements to be met for invoices to be accepted by internal revenue and tax authorities in these countries. In contrast, the rather strict regulation on the use of electronic signature in Germany, which may have its advantages in other areas, is not a favourable environment for the broad adoption of e-invoicing, in particular among SMEs.

The legal framework is only one aspect, however. How fast and to what extent e-invoicing will be adopted in the public and private sector in different areas of Europe will also depend on many other parameters, such as technical preconditions, industry structure, and cultural aspects. Policy is well advised to monitor the developments in different countries and to identify successful practices, as well as the required framework conditions for implementing them. The e-Business Support Network (www.e-bsn.org) of the European Commission, DG Enterprise & Industry, has indeed recognised the importance of e-invoicing and started relevant activities in this domain.

1.3.4 The role of intermediaries in e-invoicing

In the private sector, e-invoicing is not only an attractive opportunity for those who use the respective services, but also for intermediaries who provide these services to businesses and consumers. This includes a broad range of companies from different service sectors that are currently trying to get a share in this emerging business.

Intermediaries for e-invoicing can be grouped in two categories:

- technical system and service providers who develop the required software and implement it in their clients' companies;
- banks and other financial services firms who wish to continue to play a role in conducting payments on behalf of their business clients and customers and for whom the development is of utmost importance.

The trend toward e-invoicing and e-payment could have major implications for banks, similar to the deployment of online banking a few years ago. However, the border line between technical and financial service providers is difficult to draw. There are new intermediaries specialising in providing e-invoicing / EIPP services, 'consolidators' (see Exhibit 1-3) and 'acquirers' (such as Pago eTransaction Services, see chapter 3.2). Since developments are rather recent, players are still trying to position themselves in the game, and the winning business models are not yet clear. It is possible that the model will vary from country to country.

In any case, while banks already conduct the vast majority of payments in B2B transactions electronically, most invoices are still printed out and delivered by mail. Against this background, banks have started to extend their financial services from processing payments to also processing invoices electronically. As in this case of payments, they act as intermediary between the billing and the paying company. The Nordic banks currently have a leading role in providing such services (see fact-box: Nordea e-invoice).

One of the problems that might arise in this context is that banks are still rather regional or national institutions in the EU. Consequently, they tend to develop regional solutions, with little international coordination. Observers warn that a lack of coordination and agreements on common standards could hamper international (cross-border) e-invoicing. Freek Posthumus, project manager for

³² Cf. in particular Directive 1999/93/EC of the European Parliament and the Council of the European Union (Electronic Signature Directive).

NORMAPME³³, maintains that "the European banking sector is not ripe to cooperate much beyond the SWIFT system." He expects to see local solutions developing. "Then the pressure will come on banks to find an international solution that works."³⁴

Fact-box:

Nordea e-invoice

Nordea, a leading financial services group in the Nordic and Baltic Sea region, offers e-invoicing as part of its services for business customers. Nordea e-invoice is designed to enable B2B electronic invoicing, primarily in the Nordic countries. Nordea claims that the service can be used by companies of all sizes, does not require an ERP system and allows cross-border invoicing electronically. A company that makes use of Nordea's e-invoice service can choose from different options for processing invoices:

First, the firm can send and receive invoicing material in file transfer format, which requires an ERP or financial administration system. In this case, the company creates outgoing invoices in its ERP system and transmits it to Nordea. The bank will then send it to the firm's customers in the format suitable for them. That includes forwarding the invoice by mail, if a customer is not yet able to receive e-invoices. Vice versa, incoming invoices are retrieved from Nordea to be checked and posted to the company's ERP system. This allows companies to integrate payments with their financial administration systems.

Second, companies can send and receive invoices in a web-based environment via Nordea's Netbank. This does not require an ERP system, thus enabling a company to adopt electronic invoicing without costly IT investments. E-invoices sent to the company can also be checked, posted and paid in Netbank.

Finally, it is still possible to print the invoice and send it by mail if the recipient cannot receive electronic invoices.

Nordea points out that the ICT systems used by a company or by business partners are no obstacles to e-invoicing. The bank argues that its e-invoicing service has several important advantages for firms: It leads to substantial savings in costs, offers access to the entire Nordic market, and strengthens customer relationships. As the service does not involve major investments in ICT, benefits can be gained within a short time frame, which, in addition to costs, is an important aspect for SMEs.

Sources: Nordea Bank (www.nordea.fi); "Elektronische Rechnung spart Milliarden", Computerwoche, 14 Dec. 2004;

³³ NORMAPME (www.normapme.com) is an EU body established to represent the interests of small businesses.

³⁴ See: Oracle, Small and Medium Enterprise Use, Issue 09, Dec. 2004: "Taking the paper out of financial paperwork", interview with Freek Posthumus, project manager for NORMAPME (www.normapme.com).

The e-Business Survey 2005

e-Business W@tch collects data on the use of ICT and e-business in European enterprises by means of representative surveys. The e-Business Survey 2005, which was the third survey after those of 2002 and 2003, had a scope of 5,218 telephone interviews with decision-makers in enterprises from seven EU countries (the **EU-7**, i.e. Czech Republic, France, Germany, Italy, Poland, Spain and the UK), which account for roughly 75% of the EU-25 population and GDP.

The survey was carried out as an enterprise survey: data collection and reporting focus on the enterprise, defined as a business organisation (legal unit) with one or more establishments. Interviews were carried out in January and February 2005. Except for the aeronautics industry, where only 163 company interviews could be realised due to the small universe of firms in this sector in the EU-7, about **560 interviews per sector** were conducted.³⁵

In contrast to the surveys of 2002 and 2003, the survey of 2005 considered only **companies that used computers**. Thus, the highest level of the population ("base") was the set of all computer-using enterprises that were active within the national territory of one of the respective countries, and that had their primary business activity in one of the sectors specified by NACE Rev. 1.1 categories. Therefore it makes a difference if a figure represents a percentage of "*all companies*" (as in 2003) or a percentage of "*companies using computers*" (as in 2005). Differences are much less pronounced, though, when figures have been weighted by employment.³⁶ The second important difference between the 2003 and 2005 surveys concerns the configuration of sectors. Three very large sectors (retail, health, business services) that had a major impact on aggregate results in 2003 were not continued in 2005. Instead, another huge sector (construction) was introduced. For these reasons, direct comparisons of aggregate results should be cautiously made and only with explicit reference to these differences.

More detailed information about the survey methodology, including information about sampling and the business directories used, the number of interviews conducted in each country and sector, and data on non-response rates, are available in **Annex I** and on the website of the *e-Business W@tch*.³⁷

³⁵ The survey was conducted using computer-aided telephone interview (CATI) technology. Field-work was coordinated by the German branch of Ipsos GmbH ([Hwww.ipsos.de](http://www.ipsos.de)) and conducted in co-operation with local partner organisations.

³⁶ Employment-weighted figures should be read as "*enterprises comprising x% of employees*" in the respective sector (or country). Employment weighting is useful because, due to the significantly greater number of micro- than non-micro-enterprises, un-weighted figures would effectively represent mainly the smallest sizes of firms.

³⁷ See [Hwww.ebusiness-watch.org/about/methodology.htm](http://www.ebusiness-watch.org/about/methodology.htm)

Part A: Information and network security in European enterprises

2 Information and network security in European enterprises

Introduction

Part A of the study investigates the incidence and pattern of damage from ICT security breaches (chapter 2.1) and the extent of controls and other measures introduced by European enterprise to counter these threats (chapter 2.2). The analysis is predominantly based on results the e-Business Survey 2005 (see chapter 1.3), which included for the first time a module on ICT security.³⁸

Structure of chapter 2: ICT adoption and e-payment acceptance

	Chapter 2.1: Incidence of security breaches and security-related costs	Chapter 2.2: Deployment of ICT security controls
Focus	<ul style="list-style-type: none"> Evidence of ICT security breaches that have caused damage in companies Comparative analysis across sectors, countries and size-bands 	<ul style="list-style-type: none"> Measures to counteract ICT security breaches used by companies Comparative analysis across sectors, countries and size-bands
Main data source	<i>e-Business W@tch</i> : Representative enterprise survey (e-Business Survey 2005)	
Method	<ul style="list-style-type: none"> Descriptive analysis of survey results 	<ul style="list-style-type: none"> Descriptive analysis PCA (Principal component analysis)
Reference year for data	2004/05	

2.1 Incidence of security breaches and security-related costs

2.1.1 Introduction: data tables and questionnaire reference

This chapter features the results of survey question D11:

"During the past 12 months, which of the following incidents have had an impact on your business, for example by causing economic damage or endangering customer relationships? Has ... [item(a)-(j)] had a significant impact, little impact or was there no incident in this period?"

- (a) hardware failure
- (b) software failure or malfunction
- (c) employee lack of security awareness or negligence
- (d) viruses, Trojan horses, or Internet worms
- (e) spam
- (f) unauthorised access to your systems
- (g) inadequate confidentiality of information, for instance on customers
- (h) failure of the internet or other IT services provided by third parties
- (i) new legislation relating to information security
- (j) other security-related incident

³⁸ These questions were not included in the surveys of 2002 and 2003.

An overview of the results by sector, firm size and country is presented in Exhibits 2-1 to 2-3. Results are then analysed and discussed in detail.

Exhibit 2-1: Companies having experienced ICT security incidents with a significant impact on the business (I)

	Hardware failure		Software malfunction		Employee negligence		Viruses, Trojan horses, worms		Spam	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Weighting:										
Total (10 sectors, EU-7)	6	7	5	7	2	2	8	9	11	9
1-9 empl.		7		7		1		9		8
10-49 empl.		6		6		2		9		12
50-249 empl.		5		5		3		8		12
250+ empl.		5		5		3		8		11
By sector (EU-7)										
Food & beverages	5	6	5	3	3	1	7	6	9	6
Textile	5	6	4	4	2	2	7	10	7	10
Publishing & printing	5	10	5	5	2	1	5	7	17	11
Pharmaceutical	7	7	5	5	7	1	5	11	7	11
Machinery, equipment	7	7	6	5	5	3	10	10	12	8
Automotive	4	5	1	3	0	2	8	9	8	13
Aeronautics	--*	6	--*	5	--*	0	--*	10	--*	13
Construction	4	4	5	5	1	1	9	8	6	5
Tourism	9	12	8	10	3	3	11	13	15	10
IT services	6	7	4	6	1	2	6	9	17	21
By country (10 sectors)										
Germany	6	8	4	4	2	1	5	6	9	10
Spain	4	4	7	9	3	3	10	7	11	6
France	4	5	4	4	3	1	7	5	7	3
Italy	7	9	7	9	1	0	14	17	11	11
United Kingdom	5	6	5	5	1	2	8	9	16	18
Czech Republic	3	3	2	1	1	0	2	2	4	3
Poland	15	15	10	10	6	3	14	13	11	7
Base (100%)	all		all		all		all		all	
"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country. "% of firms" = % of firms as legal units, irrespective of their size --* Confidence interval for employment-weighted percentages would be disproportionately high, due to small number of observations (N = 163 for Aeronautics sector)										

Source: e-Business W@tch (e-Business Survey 2005)

Exhibit 2-2: Companies having experienced ICT security incidents with a significant impact on the business (II)

	Unauthorised access to systems		Inadequate confidentiality of information		Failure of services provided by third parties		New legislation on ICT security		Other	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Weighting:										
Total (10 sectors, EU-7)	1	1	1	0	7	6	2	1	1	1
1-9 empl.		0		0		6		1		1
10-49 empl.		2		1		5		2		0
50-249 empl.		1		1		7		2		1
250+ empl.		1		1		8		3		0
By sector (EU-7)										
Food & beverages	2	1	1	0	6	3	3	1	1	1
Textile	1	1	1	0	8	12	1	0	1	1
Publishing & printing	0	1	0	0	7	8	3	1	1	1
Pharmaceutical	0	1	0	0	5	7	3	2	0	0
Machinery, equipment	2	1	1	2	8	10	1	1	1	1
Automotive	0	1	0	0	14	7	7	1	1	1
Aeronautics	--*	1	--*	0	--*	11	--*	0	--*	1
Construction	2	1	0	0	4	3	1	0	1	1
Tourism	0	0	1	0	6	8	2	3	1	1
IT services	1	0	1	0	11	16	4	3	1	2
By country (10 sectors)										
Germany	1	1	1	1	6	5	3	2	0	0
Spain	1	1	0	0	7	5	3	3	1	2
France	0	0	0	0	4	2	1	0	0	0
Italy	1	0	0	0	10	9	2	1	0	0
United Kingdom	1	1	0	0	6	9	2	2	1	3
Czech Republic	0	0	0	0	3	3	0	0	0	0
Poland	4	3	4	0	10	11	3	3	4	1
Base (100%)	all		all		all		all			
<p>"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country. "% of firms" = % of firms as legal units, irrespective of their size.</p> <p>--* Confidence interval for employment-weighted percentages would be disproportionately high, due to small number of observations (N = 163 for Aeronautics sector)</p>										

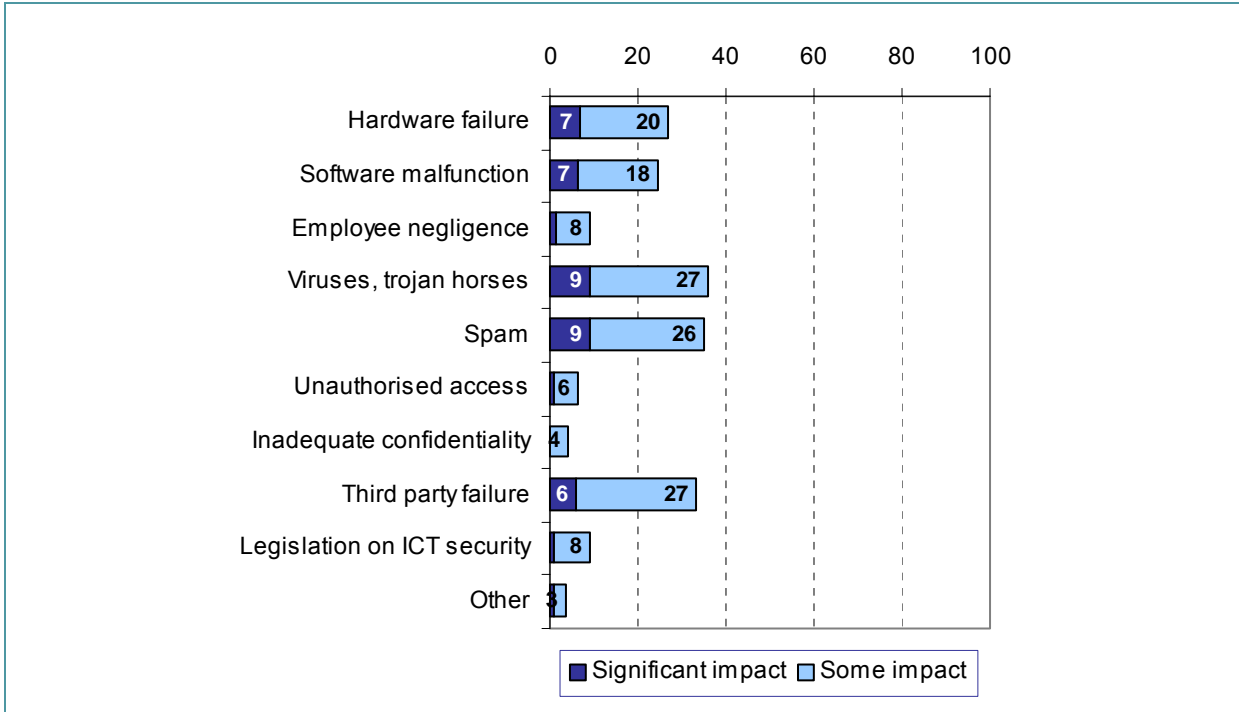
Source: e-Business W@tch (e-Business Survey 2005)

From the above tables, security breaches appear not to be common: levels of reported incident rarely exceed 10% of a category. However, this should not be taken to imply that no action should be taken.

There is clearly a motivation to underreport security breaches. Unlike the use of advanced e-business solutions by an enterprise, which is generally seen positively by other market participants and where reporting use lends an innovative glow to the image of the enterprise, the opposite is true of security breaches. Enterprise management typically wishes to minimise the number of people who learn of breaches to security, and particularly to prevent clients and lenders gaining insight into security failures. Information about the incidents is not published widely, and the fact they have occurred may even be lost to corporate memory as a whole. The resulting motivation to "sweep under the carpet", erase from record and underreport may be a reason for the small number of incidents reported, however, the category included in the above table also required that an incident had a *significant* impact on the business, i.e. caused real damage. This makes the answers particularly interesting. Whereas it would not be surprising to find a large number of enterprises which use external email complaining about the amount of spam their employees have to deal with, it is interesting, and

perhaps surprising, to find that as many as 10% of enterprises have within the space of a single year suffered damage, which they themselves rate as significant, just from spam and denial of service attacks based on spam.

Exhibit 2-3: ICT security incidents that had an impact on the business (% of firms having experienced such an incident)



Source: *e-Business W@tch* (e-Business Survey 2005)

The above figure provides an overview of gross frequency of incidents per category including both those with 'some impact' as well as those with 'significant impact', bringing the level of incidence up to near 40% in some categories, but diluting the relevance of the statistic to some degree. The figure shows that the most frequent reports of damage and significant damage are from security breaches related to e-mail, both unsolicited – 'spam' – and malicious – e-mail containing viruses or trojan horses. Over a quarter of enterprises report damage within the past year for each of these two types of incident, and in nearly 10% of cases the damage reported is rated 'significant'. Failure of systems and networks is the next most important area of security breach.

The proportions of European enterprises reporting damage within a year from malfunction of their software, failure of hardware such as workstations or servers, and failure of third parties to provide network services such as Internet are 18%, 20% and 27% respectively. Reports of significant damage run at about one third of this level. From the survey results it appears that incidence of security breaches relating to an organisation's own personnel, e.g. damage caused by negligence, or unauthorised access – which may also be from outsiders - is quite considerably lower, with, for instance, roughly one incident of this type for every three occurrences of damage through hardware failure. The domain of security legislation and data protection is – in terms of reported economic impact – least important: negative economic impact on business from requirements to comply with ICT legislation is reported by a similar proportion of enterprises as report employee negligence, but breaches of confidentiality are the most infrequently reported type of incident among all categories investigated.

The following sections discuss the variation in incidence of significant damage from the various security threats across enterprises of different sizes, from different countries, and operating in different sectors.

2.1.2 Variation by size of organisation

The low percentage values in Exhibit 2-1 mask quite considerable variation in rates of incidence by size of organisation. This variation is strongest in categories such as 'employee negligence', where the incidence of damage is some three times higher in larger companies compared to the smallest, and weakest in categories such as 'software failure', where incidence is much less strongly dependent on size.

Employee negligence

To understand the impact of employee negligence we consider the simple reference model of a constant propensity to be negligent across the working population. In this model, the larger the enterprise the more frequent damage through negligence would be. If negligent acts were the only factor affecting the level of impact, typically 60 times as many enterprises in the largest size category would report an incident compared to enterprises in the smallest category³⁹. This very strong rise in incidence with size is not reflected in the data. The likelihood of employee negligence causing significant damage is some three times higher in larger organisations companies compared to the micro enterprise.

It is clear that employee propensity to be negligent is not the only factor affecting impact from such action, and the very likely explanation is that larger enterprises are able to counter their higher levels of threat more effectively than smaller enterprises. In general, the larger the company, the more sophisticated the measures which can be taken to reduce the impact of negligence: the cost per employee for most controls decreases. As is well known, there are no complete defences against human error or negligence, and it is often the case that elaborate defences tend to hinder work execution and impact negatively on productivity. Nevertheless, the difference in impact is huge. The best estimate which can be made on this data is that micro-enterprises suffer some 20 times more damage from employee negligence than would be the case were they able to introduce the controls larger enterprises can afford.

Component malfunction

Though many kinds of damaging security incident occur in larger enterprises more frequently than in small or very small organisations, because the level of threat increases with size, the opposite is true of some types of incident, most clearly hardware and software malfunction. In this case damaging incidents are proportionately more prevalent in the smallest organisations. Though the differences are not large, there is evidence of economies of scale in terms of maintaining hardware and software: large firms have both the staff to take preventative action and the money to invest adequately in licensing software and purchasing hardware of adequate quality.

Virus and spam damage

Another type of incident showing a diminution of frequency with company size is virus attack. The reason, here again, is probably the greater ability to invest in software and IT departments capable of introducing appropriate measures which causes the decrease in damaging incidents with size revealed in the e-Business Survey 2005.

Damage from spam attack shows a different pattern. Apparently, despite their lack of access to resources to combat security threats, the smallest organisations are *less* prone to damage by spamming attacks than larger enterprises. Well under 10% of micro enterprises report damage through spam, whereas well over 10% of those with at least 10 employees report significant damage from this security threat. It seems unlikely that the threat of spam damage rises as strongly with the number of employees in an organisation as does, say, employee negligence. One possible explanation is that available protection is poor and therefore that having greater IT resources represents little advantage. There are indications from other data in the survey that spam protection is

³⁹ A calculation based on a propensity to act negligently of 0.2% p.a. results in expected annual incidence levels of 63.2% for enterprises with 500 employees and 1% for those with 5 employees.

not improved significantly by increasing the know-how or resources applied to protective measures. Therefore ineffectiveness of known controls may be part of the explanation for the lower incidence among the smallest enterprises.

Another factor possibly affecting the frequency of spam damage suffered relates to Internet presence. One of the principal sources of address lists for spam generators is published web information. Today, most medium-sized and large enterprises have their own information published on the Web, and these web-sites usually hold e-mail address information on which spammers feed. The extent of web publication is much lower in micro enterprises, whose address data may as a consequence not so often get into the hands of spam generators. Furthermore, many micro enterprises do not run their own e-mail service, relying on free public providers such as msn, hotmail or gmx. These providers have introduced quite effective spam filtering, so that these – effectively outsourced – controls may also be contributing to a relatively low level of spam damage in the smallest organisations. It is of interest to see if the larger corporations introduce similar controls on-site in future, changing the pattern of spam damage in European enterprise.

Unauthorised access

As with security threats relating to employee behaviour, the threat of damage from unauthorised access could be expected to rise with size of organisation. The overall trend across three of the four size categories shows such a rise, but again the reported levels of incidence in the largest size categories do not conform to a simple model - each employee creating an equal additional risk. There is a strong impression that larger companies are effectively countering a greater level of threat with appropriate measures, including physical access controls such as employing security personnel to monitor access to sites, and more sophisticated security architectures and software.

The modest trend of increasing frequency of reported incidents with size is broken in the small enterprise category, where reported incidence is higher than in any other. A higher rather than lower incidence in smaller organisations would be consistent with the general explanation that the larger the enterprise the more effective the controls, however, it would raise the question as to why micro enterprises report so few cases of damage through unauthorised access compared to small enterprises.

If the peak of incidence in the small enterprise (10-49 employee) category is not just a statistical artefact, it could be speculated that this is a size range where some advantages of small size is lost before the controls affordable by larger companies are introduced. Micro-enterprises potentially have an advantage that the very low number of access points and the intimacy of a small group of people can reduce the risk of third parties gaining unauthorised access. The safety of close peer control may well break down as staff numbers approach 20 or more, and at this size the greater risk does not yet attract enough resources from management to police access more thoroughly, to provide employee training or to improve hardware and software defences.

Legislative impact

The statistics in the data table above show a near three-fold increase over the size categories in the proportion reporting significant costs due to new legislation, including national transposition of EU regulations (e.g. on digital signature), and tightening requirements of national legislation to secure personal data and combat fraud.

Inadequate confidentiality and costly new legislation are linked: maintaining confidentiality is a primary requirement of data protection legislation. It may indeed be that many firms address confidentiality as a compliance issue, rather than an issue of trust of their trading partners which, arguably, should motivate them independently of legislation.

Either of two effects may underlie the observed increasing incidence with size: it may well be that smaller organisations more often take the risk of not complying with all legislative requirements, and secondly in some cases legislation exempts smaller enterprises from certain liabilities or from the requirement to introduce expensive measures.

Failure of services by third parties is in a category of its own. There is only a marginal increase of reported incidence visible with size of enterprise. The reason for this may be that a quite large proportion of enterprises in the larger size categories risk relying on few suppliers, or even on a single supplier, for critical network services, including Internet. Where there is a one to one enterprise-provider relationship, as is almost universally the case in a micro-enterprise, the client enterprise loses all network services if there is a failure of that single provider. With the increasing dependence on network services, enterprises in this position will typically suffer at least 'significant' economic damage if their supplier fails for any length of time. Common reliance on one or a small number of suppliers independent of size may underlie the lack of variation of incidence of significant damage with size.

The remaining slight tendency for incidence to rise with size may point to a stronger dependence on third-party ICT services among the larger enterprises. For instance, relatively short interruptions of communications between partners in large-volume supply chains might cause significant (to very significant) economic loss, as the dependency on single systems is greater, the staff with know-how smaller in number and, therefore, the capacity to temporarily work around a failure reduced.

2.1.3 Variation by country

In terms of variation by country, the greatest incidence of significant **damage** to a business **through spamming** is in the United Kingdom, with nearly 20% of enterprises reporting this kind of incident; Italy and Germany follow at only half this frequency.

Despite the apparent similarity of the threat of damage by spammers to that by viruses and other malicious software, the pattern of reported incidence is different, with Italy rather than the UK the most strongly affected. Countries clearly differ quite markedly either in their relative exposure to these two threats or in their success at responding to them, at national or enterprise level.

Comparatively lower exposure to **virus damage** compared to spam is common to firms of countries such as the UK, Germany and the Czech Republic, but the opposite is true of France, Italy and Poland. Neglecting for the time being differences between these countries in sectoral composition and in the distribution of sizes of enterprises, differences in damage levels may also be due to language. The most prevalent language for spam is English, and Spanish spam is also quite frequently observed, perhaps against the background of the language communities in the USA as the principal target of attack. This language distribution may help to explain the relatively low levels of damage for French companies, in particular.

The measure of the incidence of virus damage used in the e-Business Survey 2005 is of course neither a pure measure of the rate of incidence of viruses nor a measure of the lack of deployment of software and other security controls to counter virus attack: it is a combination of the two. Exposure to virus attack varies with the type of business, increasing for instance in businesses using information retrieval from the Web intensively or with a high volume of incoming e-mail from a broad audience. Where B2B enterprises may communicate with a small range of suppliers and customers, B2C enterprises today often communicate by e-mail to a broad audience, and in these cases legitimate mail and spam or malicious mail may be more easily confused.

Damage through incidence of **hardware and software failure** is most prevalent for enterprises from Poland; incidence is similar across the countries from the former EU15 but lowest in the Czech Republic. It can be speculated that lively uptake of software in Polish firms coupled with low budgets for hardware and software might be contributing to this impact, but this view is to some extent questioned by the particularly low level of incidence in the other new Member State in the e-Business survey 2005, the Czech Republic. It is difficult to imagine that budgets for software and hardware investment would be significantly higher there compared to Poland, and there is no evidence to suggest that levels of ICT uptake are to such a great extent dissimilar between the two countries.

The pattern of variation of other incidence of damage or other costs in relation to security threats does not suggest any very strong trends, differences in levels of threat or variation in access to appropriate

measures between the countries. The cost of introduction of new ICT security **legislation** has no very significant impact in any country, but is lowest for companies from France and the Czech Republic. This pattern also applies to the impact of **employee negligence** and **unauthorised access** to systems. In the case of **failure of services provided by third parties**, firms from Italy, the United Kingdom and Poland seem to suffer disproportionately compared to other countries. The lowest incidence here is again in France and the Czech Republic.

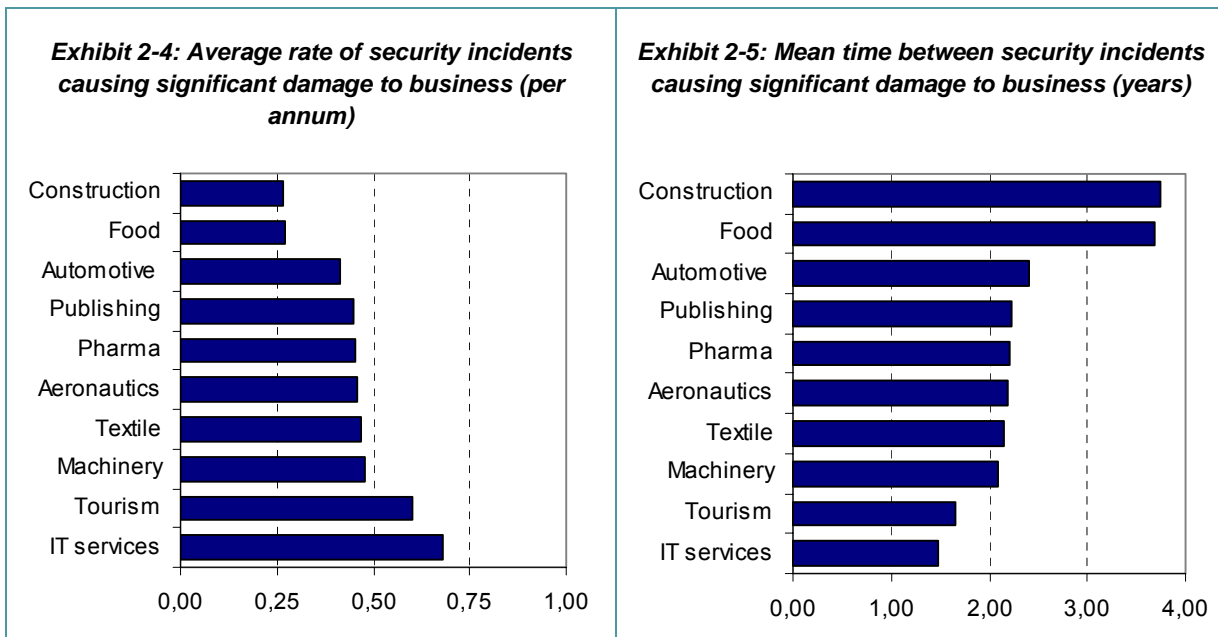
2.1.4 Variation by sector

Overall levels vary strongly by sector

Across the sectors, incidence of damage through security incidents varies strongly. It can be seen that the most common threat causing significant damage, spamming, affects over 20% of enterprises in the IT services sector.

The overall picture is complex; Exhibit 2-1 ("Companies having experienced ICT security incidents with a significant impact on the business") has 13 cells in which incidence of significant damage lies at over 10% of enterprises per year. These have no immediately apparent pattern, yet as will be seen, much important variation is there to be commented on.

To gain overview we first build an overall sectoral comparison.



Unweighted figures.

Source: e-Business W@tch (e-Business Survey 2005)

The mean time between incidents varies from just over a year to nearly four years, as shown in Exhibit 2-5.

Overall, enterprises in the IT services sector report the greatest number of incidents causing significant damage, nearly three times as many as in the construction or food & beverages sectors. Whereas the rate of incidence in tourism is nearly as high as in IT services, other sectors are in mid field. The fact that there is no consistent relationship between overall levels of incidence and average size of enterprise in a sector means that sector-specific communication and ICT deployment structures are likely to be a more important covariant of the frequency of security failures and security-related costs than size of enterprise.

Tourism and IT services appear particularly prone to damaging incidents. In the former case a high volume of communication with a wide audience in a B2C environment might be a contributory factor.

In the other, underlying causes are more likely to be the vulnerability of strongly ICT-based production processes to breaches of ICT security.

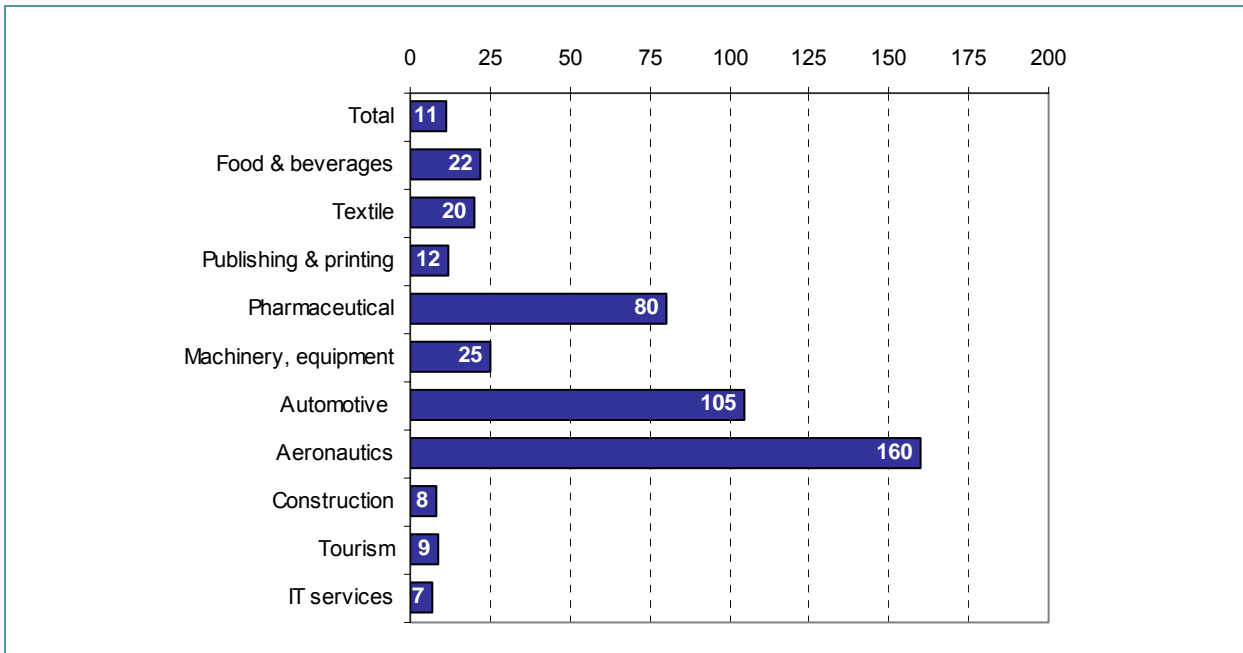
The opposite factors may contribute to the relatively low level of incidence in the construction and food and beverages sectors: a low level of IT use and physical rather than virtual outputs offer less opportunity for ICT-based threat. In addition, in both cases there are a relatively small number of clients involved in any time period.

As can be seen by comparing sectors close in overall ranking such as construction and automotive, this overall picture masks considerable and interesting divergence across the specific security domains. For instance, the automotive sector is one of the most affected by spam attack but construction is bottom of this ranking, and software malfunction has the opposite pattern, causing more frequent damage in construction than in automotive industry. In the following discussion, conformance to and divergence from the overall pattern is used as one way of highlighting features of the distribution of security breaches across sectors.

Component malfunction most prevalent in small enterprises

Damage through **hardware and software failure** reflects to some extent the prevalent size of enterprises in a sector, with smaller enterprises being more prone to damage.

Exhibit 2-6: Average firm size in the 10 sectors surveyed (according to survey)



Source: e-Business W@tch (e-Business Survey 2005)

This pattern is illustrated by the automotive and aeronautics sectors, which each exhibit large average size and a relatively low incidence of damage through hardware failure. This pattern should be contrasted with the one shown by the tourism and publishing and printing sectors, where a much higher incidence of damage coincides with a relatively small average size of enterprise.

However, this pattern is by no means consistent. There is a relatively low incidence of damage from hardware failure despite small average size of enterprise in textiles, food and beverages, IT services and particularly in construction. It is likely that these low levels of incidence are simply the result of less prevalent use of IT hardware and lower dependence on IT in all named sectors except IT services, and that there is therefore resistance to 'significant impact' of hardware failure on the respective business. In the case of IT services, the low incidence is likely to be the result of know-how advantages and purchasing policies. The opposite divergence from the size-related pattern, i.e. relatively high levels of incidence for quite large average size, is to be found in the pharmaceuticals sector.

Though incidence of hardware and software failure is clearly correlated, in the publishing and printing, the picture differs between hardware and software failures. Whereas companies from this sector report a high incidence of hardware failure, damage through software failure is lower than would be expected. Given the maturity of packaged software for publishing, it may be that reliable software is available on the market at a cost enabling the smallest enterprises access and therefore protecting them from the levels of damage suffered by enterprises of similar size in other sectors. The exposure of enterprises in printing and publishing to hardware malfunction is not known to be dependent on any comparable sector-specific supply situation.

The automotive industry is among the lowest ranking with respect to incidence of both hardware and software malfunction. In a sector with a strong presence of large enterprises the size effect discussed already will contribute to this result. In addition it is likely that large manufacturers in the supply chain contribute to a sectoral improvement by driving and managing the software engineering process underlying supply chain interconnection. According to this view, large manufacturers in the automotive sector are being particularly effective at setting standards for hardware and software and ensuring that quality hardware/software solutions are introduced into and used throughout their supply chain. Other enterprises, including the smaller ones, would profit from such sectoral initiatives and exhibit low levels of security failure and cost compared to size peers in other sectors.

Virus and spam damage greatest in B2C businesses

The cross-sectoral picture for **viruses and spam** is particularly interesting. Incidence of significant damage from spamming is greatest in IT services and in the automotive and aeronautics industries. Aeronautics is among the sectors most affected by malicious software, joined this time by textiles, pharmaceuticals, machinery and equipment and, at the top of the range, tourism.

As in the case of software and hardware malfunction, these two types of incident show some similarity in their pattern of incidence across the sectors, which in this case may be linked to similarities in the deployment of e-mail in business processes.

One important form of exposure to malicious software (viruses, trojan horses, worms etc.) is through the use of the Web for information access, and another through receipt of email attachments. High levels of email use, particularly from a broad and fluctuating audience, would expose an enterprise disproportionately to both spam and viruses. It may be that the use of Web information in business is strongly correlated to use of broad-audience email. However, if use of these two ICT technologies varies independently, the correlation in incidence suggests that email rather than Web access is the primary source of viruses, at least such which do cause significant damage.

Thus, in general, sectors with high levels of wide-spread communication, especially as part of a B2C business model, show the highest incidence of damage from these causes. A high degree of use of email to a broad audience (rather than to a small group of companies) increases the danger of infection and the rate of spam reception. Narrow-audience, B2B mail audience is the likely reason for the low levels of damage through unsolicited mail and malicious software in sectors such as construction and food and beverage manufacture. At the other end of the scale, tourism suffers extensively from damage from both viruses and spam.

This analysis alone, however, fails to explain the relatively high levels of damage incidence in the textiles, pharmaceuticals and aeronautics industries - and of spamming in the automotive sector. Some explanation for these levels may be found in differences in competence at deploying controls. In both IT services and, to some extent, the automotive sector, the level of incidence of spam damage is much higher than the incidence of damaging virus attack. This may indicate that both these sectors have been more successful than their peers in other sectors in combating viruses. As already observed, the IT services sector has good access to expertise, and the automotive sector appears to be one of the most effective in deploying high quality software.

Despite IT services having particular expertise in the area of software controls, the incidence of spam damage in the sector is very high. This suggests that even software experts find it difficult to protect

their own organisations against this security threat. This finding underlines the need for action to control spam at its source, which is increasingly being recognised in policy initiatives globally.

Costs of legislation: pharmaceuticals strongly affected

The highest level of impact of legislation across sectors was reported by enterprises in the tourism, IT services and pharmaceuticals sectors. One source of legislation impact is data protection, where customer data must be protected against unauthorised access. The impact of this legislation on costs is higher for enterprises operating on a B2C model with many customers. This may well be the background to relatively high levels of impact in the tourism sector. Sectors reporting a particularly low incidence of significant costs from legislation such as textiles, aeronautics, M&E and construction support this position, as a majority of enterprises operate on a B2B model or, as in areas of the construction sector, have a large proportion of turnover with few customers, reducing privacy compromise risks.

In the case of pharmaceuticals, working almost exclusively on a B2B model, the explanation probably lies either in specific regulation attached to drug development or in sector-specific operations other than sales. Certainly, the privacy implications of some sector-specific operations, in particular carrying out large-scale clinical trials or receiving data about drug impact on particular patients from doctors, are very significant and introducing adequate controls a daunting task.

Little difference in impact of employee negligence and unauthorised access across sectors

No clear pattern is visible in the very low variation of incidence of damage through breach of system integrity either through unauthorised access to systems or through employee negligence. These threats do not appear to have a strongly sector-related impact, except in the case of confidentiality breaches in the machinery and equipment sector, for which, however, no explanation can yet be offered.

Third party service failure hits IT services and integrated supply chains

Textiles, IT services, aeronautics and machinery and equipment manufacture top the list of sectors most frequently reporting significant damage through third party system failure. It may well be that the risks of depending on a small number of suppliers and systems in large high-volume and high-value supply chains are exposed in the results from sectors such as automotive, aeronautics or machinery and equipment manufacture. Due to restrictions in the way questions are put, it is not immediately clear from the results whether reported failures are of third party ICT services supporting supply chain interconnection or of supply-chain and other services closer to the production process. However, risks and impact can be similar.

The failure of services provided by third parties in the IT services sector is a special case, as many players in this sector are in a software production supply chain. Here 'components' in the production process are also software modules and services built into the overall output failure of these suppliers would legitimately be recorded here, raising incidence levels in comparison with other sectors.

Summary

Main findings: Incidence of security breaches and security-related costs

- The **mean time between security-related incidents** with significant impact on an enterprise is **well under 2 years** in the most vulnerable sectors in Europe, such as tourism and IT services.
- **Malicious software** and **unsolicited e-mail** currently have the greatest impact, followed by failures of hardware or software.
- Incidence of damage from breaches of security and other security-related costs **vary with size of enterprise**, but the trends of incidence with size are **mixed in direction**.
- From a sector perspective, enterprises in the **IT services** sector report the greatest number of incidents.
- The **automotive industry** is an interesting case, exhibiting very low levels of incidence of both hardware and software malfunction.
- However, the **pattern is not consistent** for all items. It is likely that low levels of incidence in some sectors are simply the result of less prevalent use of ICT hardware and lower dependence on ICT in respective sectors.
- It appears that **no sector can lay claim to universal best practice** in avoiding damage.

2.2 Deployment of ICT security controls

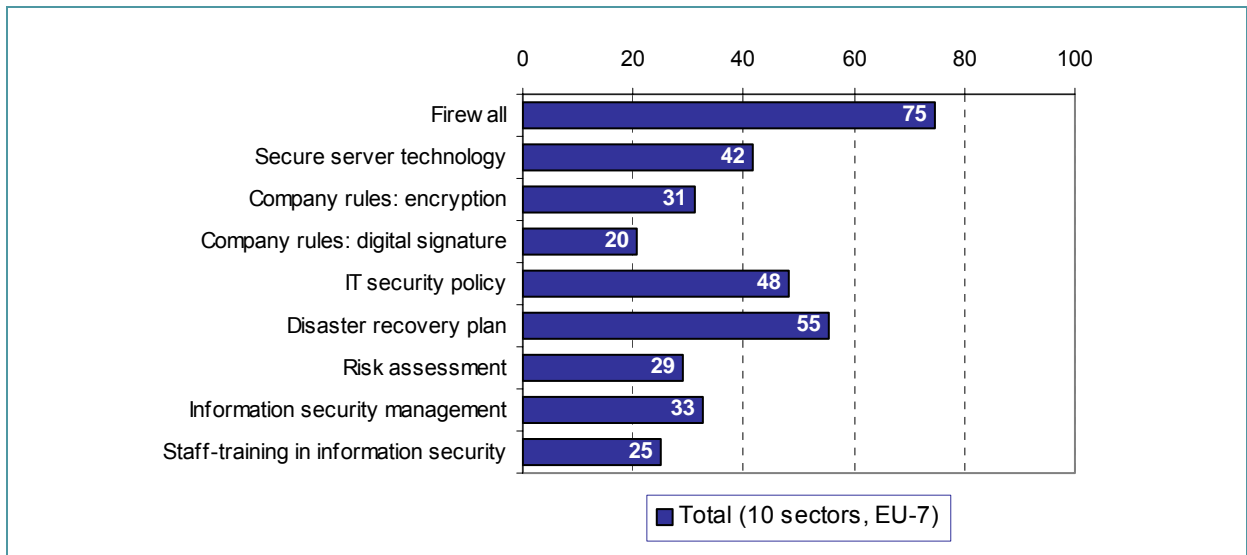
2.2.1 Introduction: data tables and questionnaire reference

This chapter features the results of survey question D12: "Does your company have any of the following IT security measures in place? Do you have / use ... [item (a)-(i)]?"

- (a) a firewall
- (b) secure server technology, such as SSL protocol
- (c) company rules relating to encryption of data
- (d) rules that specify the use of digital signature or Public Key Infrastructure
- (e) an IT-security policy
- (f) a disaster recovery plan in place
- (g) a risk assessment using a pre-defined methodology
- (h) an information-security management system
- (i) a staff-training programme in information security awareness

An overview of the results by firm-size and country is presented in Exhibits 2-7 to 2-9. These results are then analysed and discussed in detail.

Exhibit 2-7: ICT security measures used by companies (EU-7, 10 sectors)



Base: All enterprises using computers. N = 5218.
 In "% of employment", i.e. firms representing ...% of employment.

Source: *e-Business W@tch* (e-Business Survey 2005)

Exhibit 2-8: Companies with ICT security measures in place (I)

Weighting:	Firewall		Secure server technology		Company rules: encryption of data		Company rules: digital signature / PKI		IT security policy	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Total (10 sectors, EU-7)	75	56	42	25	31	15	20	11	48	23
1-9 empl.		54		24		14		11		21
10-49 empl.		65		31		22		14		32
50-249 empl.		84		43		31		21		57
250+ empl.		94		61		50		36		79
By sector (EU-7)										
Food & beverages	76	47	40	17	31	8	25	12	52	20
Textile	74	45	36	17	26	11	24	13	48	20
Publishing & printing	85	60	45	22	28	15	23	11	54	22
Pharmaceutical	94	67	49	28	41	21	34	19	85	41
Machinery, equipment	87	59	43	23	31	15	20	12	59	25
Automotive	96	64	76	24	63	20	36	15	88	32
Aeronautics	62	75	55	34	36	19	3	13	70	42
Construction	63	52	31	24	21	11	14	10	31	16
Tourism	69	51	37	22	29	15	15	11	41	22
IT services	96	93	69	48	53	38	36	19	74	57
By country (10 sectors)										
Germany	87	70	47	24	38	19	18	13	49	17
Spain	63	53	42	37	28	16	27	18	46	28
France	70	46	31	11	19	12	17	6	50	25
Italy	65	53	30	26	16	7	18	9	39	20
United Kingdom	86	78	53	33	48	27	19	10	63	33
Czech Republic	56	38	38	13	20	14	15	9	42	17
Poland	63	39	39	25	30	21	34	19	33	10
Base (100%)	all		all		all		all			
"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country "% of firms" = % of firms as legal units, irrespective of their size PKI = Public Key Infrastructure										

Source: e-Business W@tch (e-Business Survey 2005)

Exhibits 2-7 and 2-8 show that **firewall technology** is well diffused, with three quarters of employees working in enterprises of all sizes already equipped with it. At 42%, the prevalence of **secure server** technology is much lower, reflecting the fact that more enterprises access Internet services than provide them on their own hardware.

The second most commonly implemented ICT security control is the drafting of a **disaster recovery** plan. An effective plan is not simply a document but includes preparation for disaster recovery, including such measures as initiating off-site back-up or hardware duplication.

Exhibit 2-9: Companies with ICT security measures in place (II)

	Disaster recovery plan		Risk assessment on predefined methodology		Information security management system		Staff-training in information security awareness	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Total (10 sectors, EU-7)	55	34	29	15	33	19	25	15
1-9 empl.		33		14		18		14
10-49 empl.		42		17		22		18
50-249 empl.		60		26		37		26
250+ empl.		83		46		50		37
By sector (EU-7)								
Food & beverages	60	30	28	10	30	14	22	12
Textile	53	24	21	9	30	15	23	11
Publishing & printing	63	33	28	14	31	17	23	13
Pharmaceutical	81	51	54	25	53	32	32	24
Machinery, equipment	64	41	27	16	34	19	29	11
Automotive	92	42	61	20	46	24	49	17
Aeronautics	62	51	38	21	73	25	40	22
Construction	43	29	18	11	23	13	18	13
Tourism	44	30	28	17	32	21	22	14
IT services	80	71	45	32	54	41	42	30
By country (10 sectors)								
Germany	52	21	29	13	19	9	25	11
Spain	55	38	22	18	42	29	23	24
France	66	42	24	12	29	14	15	10
Italy	36	23	26	15	40	23	25	15
United Kingdom	70	59	47	24	41	22	33	19
Czech Republic	57	38	22	8	33	11	24	5
Poland	43	24	13	5	26	11	27	9
Base (100%)	all		all		all		all	
<p>"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country "% of firms" = % of firms as legal units, irrespective of their size</p>								

Source: e-Business W@tch (e-Business Survey 2005)

In terms of penetration into European enterprise, countering security risks by implementing an **IT security policy**, although ranking third, drops just under the half-way mark: less than half of European employees work in enterprises with a security policy in place. This is a surprising statistic, one which suggests at first sight that many managers even of larger companies do not see the need to respond to evident threats with a coherent policy approach. This is despite consensus across standardisation bodies and advisors to management that such a policy is an essential first step to ensuring adequate protection from growing security threats.

Three other measures which are again in the domain of organisation rather than technology are the implementation of **information security management**, the associated **risk assessment**, without which the magnitude of threat and potential damage from security breaches remain speculation, and **staff training** in information security, which is the principal way in which the human factor in security breaches can be addressed. This applies to negligence, unintended damage and working around security controls, though not to malicious activity. Though these measures have been implemented by less than 20% of firms, due to their above average size they represent 25%- 33% of employment.

Not surprisingly given their complexity and the scarcity of expertise in drawing them up, organisational rules on **digital signature** are the least widely spread security control in European enterprise. It is more surprising, however, and in terms of risks faced by European enterprise much more worrying, that **encryption** is so seldom mandated by management in the form of company rules. Only in 15% of firms, representing about a third of employment (in the sectors and countries included in the survey), are such rules in place.

A relatively new challenge stems from the spread of mobile technologies, notebooks and PDAs with large storage devices, and the frequent practice of copying all files, including sensitive and personal information, onto archive tapes to be taken off-site (for security reasons). In this context, failure to encrypt information routinely lays a majority of enterprises open to malicious attack, to industrial espionage and to compromise of the privacy of individuals, including customers, whose personal data are stored there.

2.2.2 Variation by size of organisation and principal component analysis

Exhibit 2-10 clearly shows how all measures to improve ICT security in European enterprise are most widespread in the largest enterprises. The commonest measure, the introduction of a firewall, is close to 100% saturation penetration in the largest enterprises, and exceeds 50% even in the micro-enterprise category. For organisation and process measures (policy, plans, risk assessment, management systems and training), the difference in penetration between the lowest and highest category amounts to a factor of at least 2.5 and in some cases approaches 4.

To further simplify the analysis, particularly in respect of sectoral and country variation, principal component analysis (PCA)⁴⁰ was used to model the underlying covariance structure. The analysis revealed three factors, which are indeed helpful for interpretation of patterns. The first factor, "**Management and Policy**", reflects, in order of factor loading, the following items:

- risk assessment using a pre-defined methodology
- information-security management system
- staff-training programme in information security awareness
- IT-security policy
- disaster recovery plan in place

The second and third factors reflect two main items each. "**Secure Components**" reflects

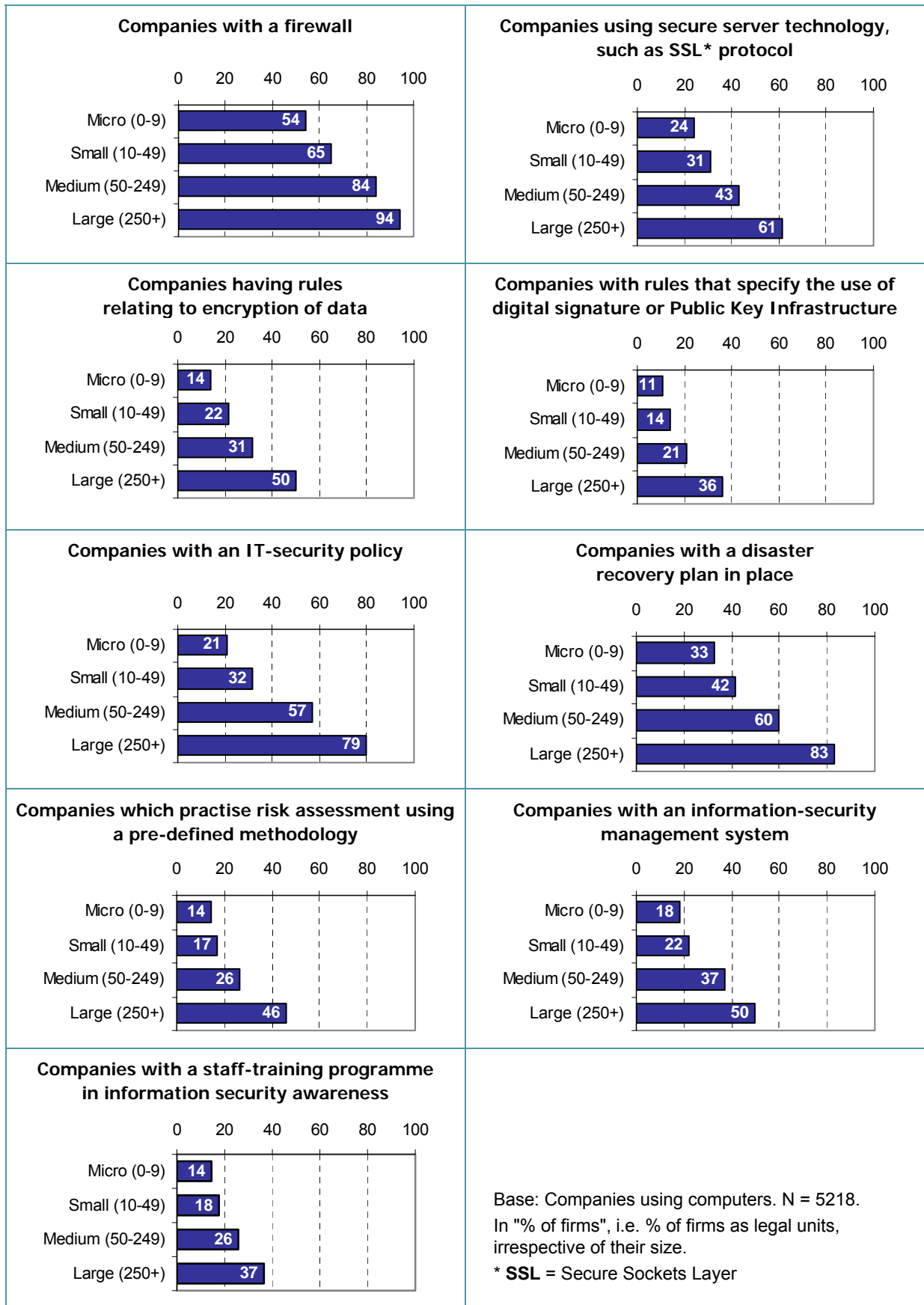
- firewall, and
- secure server technology, such as SSL protocol, while

"**PKI and Encryption**" mainly embodies the remaining two security controls:

- rules that specify the use of digital signature or PKI, and
- company rules relating to encryption of data.

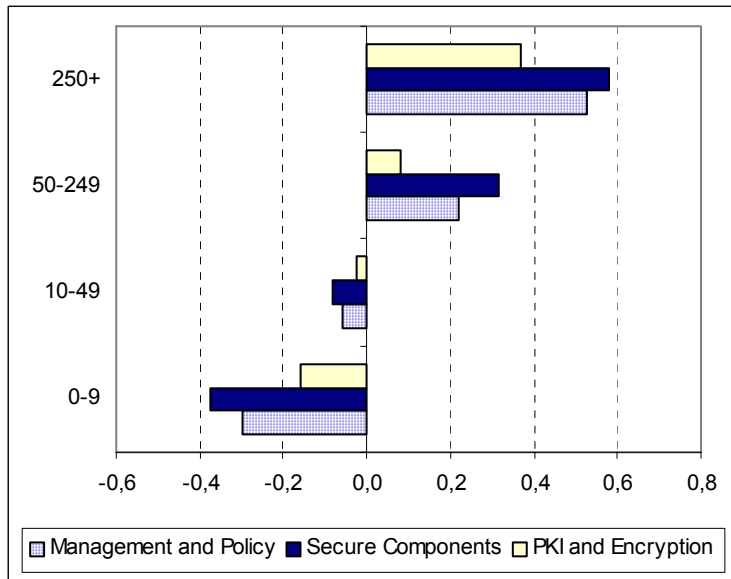
⁴⁰ Principal component analysis (PCA) involves a mathematical procedure that transforms a number of (possibly) correlated variables into a (smaller) number of uncorrelated variables called principal components. The first principal component accounts for as much of the variability in the data as possible, and each succeeding component accounts for as much of the remaining variability as possible.

Exhibit 2-10: Prevalence of ICT security measures by size-band



Source: e-Business W@tch (e-Business Survey 2005)

Exhibit 2-11: Correlation of security measure penetration with size of enterprise



Unweighted sample

PKI = Public Key Infrastructure

Source: *e-Business W@tch* (e-Business Survey 2005)

Exhibit 2-11 confirms the correlation of security measure penetration with size of enterprise, and shows in addition that this applies to all three underlying factors. Clear economies of scale mean that large enterprises are able to afford more controls to improve ICT security. This is practically confirmed by results of the e-Business Survey 2005 which provide evidence that action is actually being taken in line with ability to afford it.

It is perhaps surprising that some of the cheapest measures - deploying a firewall or an SSL server, reflected by the **Secure Components** factor - are most dependent on size; however, the correlation is only marginally different to that of **Management and Policy**, which carries in it measures which consume considerable management resources and may involve expensive consultancy. It was therefore to be expected that Management and Policy would be strongly dependent on size.

It is particularly noteworthy within this group that specific **training** to staff is so little provided in European enterprise. The high cost of absenting staff from their work-place for traditional types of training may be one factor, another perhaps the inherent uncertainty about pay-off from such measures, which mean that even in the largest size category only 37% of enterprises offer such training.

The weakest variation with size is shown in the case of **PKI and Encryption**. These measures are only marginally more likely to be deployed in medium sized enterprises than in small enterprises, though there remains a very significant contrast between the largest and smallest categories. This lower level of variation with size possibly reflects a situation where adoption is not driven by individual cost-benefit decision making, but by market or legislative imperatives. Cost is not an issue - and therefore size has no impact - where market participation and consequently survival depends on adoption.

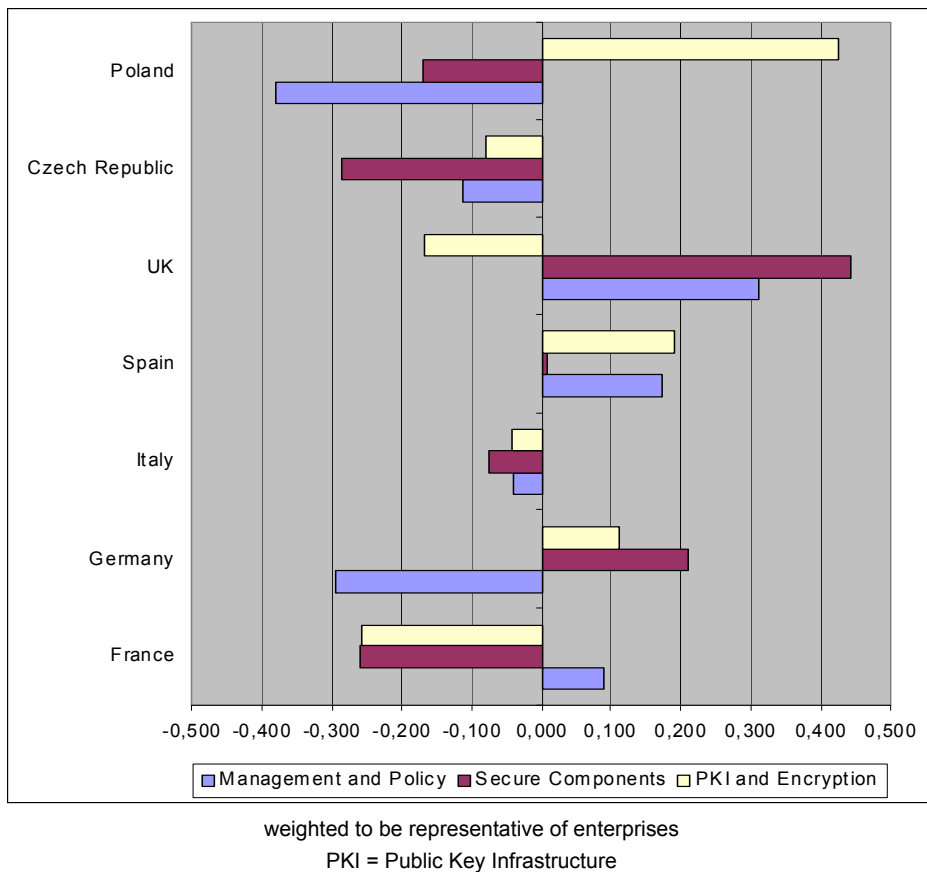
More importantly, in light of the critical role of encryption in avoiding high risks in current distributed and mobile ICT use, small enterprises should be strongly encouraged, possibly through relevant EU policy measures, to mandate use of encryption by their employees in data storage and transmission.

2.2.3 Variation by country

The analysis of the main factors in control deployment by country shows no such simple structure as the correlation with size, but carries some interesting messages for European and national policy-makers. Attention to the area of **Management and Policy** is reported strong to be very strong among firms in the UK, Spain and France, whereas these techniques for countering ICT security threats are least employed in German and Polish enterprises. The case of Germany is particularly surprising in this context, as governmental bodies researching ICT security and developing standards and guidelines are generally highly regarded and active in this country.

European leadership goes to the UK companies in this respect, possibly as a result of the attention paid by UK standards bodies to organisation and process topics in tackling security threats. It may be also that the second part of the British Standard BS 7799⁴¹ standard, which describes a security management system for organisations, has had a direct impact in that country. If so it could be expected that the adoption of similar organisational and process standards at European or global level - e.g. extending ISO 17799 - would help bringing the levels of security controls across Europe up to match those in the UK.

Exhibit 2-12: Correlation of security measure penetration with location of the firm



Source: *e-Business W@tch* (e-Business Survey 2005)

Companies in Germany, though weak in Management and Policy, are - along with the UK firms - the strongest performers in introducing **Secure Components**. Lower levels of penetration of Security Components (firewalls, secure server technology) in the two new Member States are less surprising

⁴¹ Part one of the standard - BS ISO/IEC 17799:2005 (BS 7799-1:2005) Information technology. Security techniques. Code of practice for information security management. ISBN 0 580 36958 7. www.bsi-global.com. - has been fully adopted as an ISO standard, see: ISO/IEC 17799:2005, Information technology -- Security techniques -- Code of practice for information security management. Technical committee / subcommittee: JTC 1/SC 27; ISO Standards. www.iso.org. Part two has yet to acquire international status.

than those exhibited by French companies, possibly indicating weaker national policy in encouraging introduction of such protective components.

Finally, in terms of **PKI and Encryption**, it is possibly a surprise to find companies from Poland leading the EU7 field. Firms in Spain, but also in Germany, seem to be particularly strong in introducing rules for these cryptographic methods. Companies from France again show clear weaknesses, this time shared by their counterparts in the UK. It may be that the reservations that exist about the centralised structures underlying some forms of digital signature - identity management by Certification Authorities in particular - have an impact here on management reluctance to introduce digital signature based on PKI. Nevertheless, in the case of the UK penetration of formal rules for encryption is high, and the low score on this factor is due entirely to a low level of activity on digital signature.

2.2.4 Variation by sector

The picture by sector shows the clear dominance of enterprises in the **IT services sector** in the introduction of security controls in the areas of Secure Components and Management and Policy. It may be that the threats faced by this sector are greater than elsewhere, given the nature of their business processes and products discussed in section 2.1.4. However, it is abundantly clear that enterprises in this sector are comparatively very well-placed to deploy sophisticated controls. IT services enterprises can draw the know-how needed to select, implement and maintain secure systems from their mainstream value-adding business units. Enterprises in other sectors must set up and pay for ICT services; for them, ICT is a cost centre and not a profit centre.

In terms of **Secure Components**, the strongest contrast with the leading IT services sector is companies in food and beverages, textile Industries, tourism and construction. As the above table shows, these latter sectors are among those with the smallest average size, from which follows that they have a particularly large proportion of small and micro enterprises, whose behaviour dominates the statistics. The interpretation given in section 2.2.2 above of the impact of enterprise size is also applicable here: small enterprises suffer from diseconomies of scale and cannot expect an adequate payoff from introducing security controls such as Secure Components.

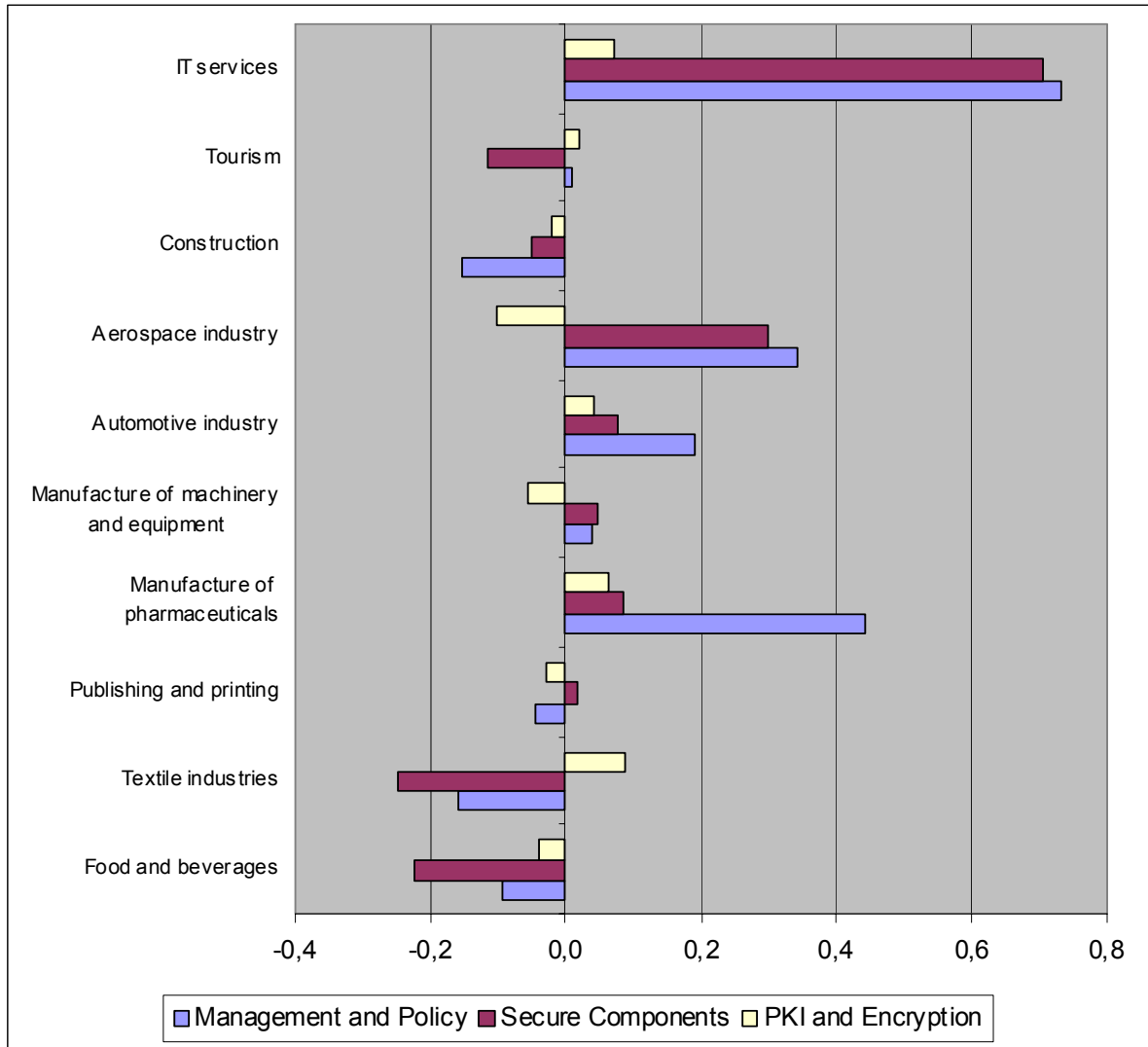
This analysis is flawed in respect of two sectors in particular – IT services and publishing and printing - which are also at the low end of the size spectrum. The special case of IT services has already been discussed; in the case of publishing and printing, it is apparent that strong investment in Secure Components has taken place disproportionately to size. Possibly there is an in-house know-how factor at play here, too: as publishing and printing processes increasingly involve software and communications skills, so that in such enterprises, again, resources for ICT security controls can be drawn from mainstream business units rather than cost-centres or external providers. It may be also that threats to electronically published products force these enterprises to spend more on Secure Components than their size would otherwise warrant. An alternative explanation arises from the observation that the production value per employee in the sector is relatively high, twice as high as in tourism (see Exhibit 2-14). This suggests high capital expenditure and that ICT security measures would form a smaller part of total capital expenditure and could more easily be financed in publishing and printing compared to, say, tourism.

Other sectors lie above the average for Secure Components. Companies in aerospace show a particularly high level activity, but companies in the automotive sector seem to score low in view of the large average size of enterprises in that sector (see Exhibit 2-14) and, surely, commensurate resources.

The inter-sector pattern in the case of the **Management and Policy** factor is broadly similar to that of Secure Components. Expenditure on Management and Policy measures to address security threats is perhaps more consistently related to size, with the exception of IT services. Again with the exception of IT services, there is little evidence of a know-how factor. automotive and pharmaceuticals enterprises score more strongly positively on this factor, and the same set of sectors with a particularly

large proportion of small enterprises exhibit the lowest rates of adoption (e.g. textiles and construction).

Exhibit 2-13: Correlation of security measure penetration with sector



weighted to represent all enterprises. PKI = Public Key Infrastructure

Source: *e-Business W@tch* (e-Business Survey 2005)

Finally, in the case of the factor **PKI and Encryption**, much less variation by sector is evident. If the variation is driven by market imperatives, as was mooted in section 2.2.2, then this lack of variation is surprising. The co-variation by sector matches that of the two other factors to a large extent, but the match is broken in the case of textile, aerospace, machinery and equipment manufacturing – and, marginally, tourism. Whereas in the case of the textile industry a sectoral, supply-chain related pressure to adopt digital signature techniques may be at work, causing the rate of adoption of digital signature to rise in this sector, this kind of explanation cannot be fielded to explain the particularly low scores in other manufacturing sectors such as aerospace or machinery and equipment manufacturing. In-depth research into sectoral practice and management planning would be required properly to interpret these differences.

Exhibit 2-14: Average firm size in the 10 sectors surveyed (according to survey)⁴²

	Average firm size (employees) in EU-7	Production value per employee in EU-25
Weighting:	% of firms	% of firms
Total (10 sectors)	11	164
Food & beverages	22	76
Textile	20	126
Publishing & printing	12	243
Pharmaceutical	80	131
Machinery, equipment	25	266
Automotive	105	250
Aeronautics	160	93
Construction	8	54
Tourism	9	109
IT services	7	164

Sources: *e-Business W@tch* (e-Business Survey 2005); Eurostat New Cronos / DIW Berlin

Summary

Main findings: Deployment of ICT security controls

- Basic components such as **firewalls** and **secure servers** already exhibit high levels of penetration.
- Low application levels are reported for **data encryption** and deployment of **public key infrastructure**. This could hamper the development of distributed and mobile computing environments, and the evolution of interoperable solutions for many e-business processes.
- Also low proportion of enterprises reporting that they train their staff in security awareness, carry out risk assessment or, in particular, have put a security management system in place.
- Clear dominance of enterprises in the **IT services** sector in the introduction of security controls in the areas of 'secure components' and 'management and policy'.
- In contrast, low endowment with security controls in **food and beverages**, **textile** industries, **tourism** and **construction**. However, this is partly explained by the dominance of small firms in these sectors.

⁴² see also Exhibit 2-6.

2.3 Summary

According to the e-Business Survey 2005 results, breaches of security which have had a significant impact on an enterprise have **rarely been reported by more than 10% of firms**, independently of their category or the type of security incident. However, the impact on European enterprises should **not to be underestimated**, given a general motivation to under-report damage and taking into account that the mean time between incidents with significant impact comes down to well under 2 years in the most vulnerable sectors, such as tourism and IT services.

Malicious software and unsolicited e-mail currently have the greatest impact, followed by failures of hardware or software and problems faced by providers of services to the enterprise, such as leased lines or Internet access. Though not by any means negligible in scale, the impact of employee misconduct or unauthorised access to systems is reported to be at much lower levels than damage from spam or component failure. Many forms of regulation impart costs of compliance on European enterprise, which, as the survey shows, weigh heavily in some sectors. Legislation increases enterprise liability, e.g. if the security of data entrusted to the enterprise is compromised. Significant impact from these aspects of ICT security is comparatively infrequent, but the overall cost is likely to be high.

The analysis of security controls and other measures applied by European enterprises to counter security threats shows that **basic components** such as firewalls and secure servers (for those enterprises that require them) **already exhibit high levels of penetration**. Major deficits in security controls in European enterprise are evident in the reported **low levels of data encryption** application, which is generally regarded as essential in distributed and mobile computing environments. The yet lower levels of deployment of public key infrastructure could represent an obstacle in the evolution of interoperable solutions for many e-business processes, particularly those with strong contractual content such as the transfer and agreement of large liabilities.

Given the importance of the human factor in breaches of security, the **low proportion of enterprises reporting that they train their staff in security awareness**, carry out risk assessment or, in particular, have put a security management system in place, should be a cause for concern among policy makers. Though the proportion of larger enterprises which have drafted disaster recovery plans and developed a security policy is over 70% (in each case), the picture is much **bleaker among smaller businesses**. Only 21% and 33% respectively of micro- and small enterprises reported having an ICT security policy in place, despite strong consensus among security consultants and standards-setting bodies that such planning is essential in building a proper response to security threats. If the commonly quoted saying "*to fail to plan is to plan to fail*" is applied here, then a majority of European SMEs appear to be planning to fail by default.

The lower levels of control deployment found in smaller enterprises have a **clear economic foundation**. The ability to profitably deploy resources in combating security threats tends to be a function of the size of a business, particularly in larger enterprises where key ICT functions are centralised. These economies of scale can be clearly seen in the behaviour of enterprises in respect of the security controls included in the survey.

The lower levels of security control in smaller enterprises are also evident in the levels of security breach reported in the study: in some cases, the **frequency of security incidents actually decreases with size of enterprise**, even though in many cases the scale of threat increases with size. In one case, in respect of damage caused by employee negligence, a plausible argument is presented that *micro enterprises may be suffering 20 times more damage from this type of security lapse than they would if they were part of a centrally managed, larger unit*.

Some of the structural differences exposed in this study can be responded to by public policy. Initiatives should aim at **improving the cost-benefit equation for SMEs**, for example by reducing the cost of controls through standardisation. Other possible strategies include encouraging market offerings, and promoting inter-enterprise cooperation or the sharing of resources.

Part B: Electronic payments and e-invoicing activities in European enterprises

3 Electronic payments and e-invoicing activities in European enterprises

Introduction

This chapter provides recent empirical evidence on the development and uptake of electronic invoicing and payments. These processes are key components of electronic transactions between businesses, the public sector and consumers. The use of e-invoicing and e-payment methods promises to save costs for both parties involved (invoicing entity and receiving entity), as processing invoices in a standardised, electronic format can be accomplished much faster compared to the often cumbersome handling of printed invoices.

Typically, e-invoicing & e-payment systems that are used by companies involve technical functionalities related to the following component processes:

- Delivery of the invoice from the seller's computer system to the buyer's system in electronic format, without mailing any printed document;
- Handling billing disputes electronically;
- Electronic payment, normally through both the buyer's and supplier's financial institutions, and
- Integration with applications such as accounts payable, accounts receivable and a company's ERP (enterprise resource planning) system.

The cost saving potential obviously depends on the number of invoices that have to be processed. Particularly for companies and organisations that have to process a very large number of structurally similar invoices⁴³, e-invoicing promises substantial benefits. In essence, the benefits arise from partial automation of work processes related to billing and invoicing that needed to be accomplished manually in case of paper-based invoices, for example entering the data into the accounting system, and archiving an invoice. In a way, e-invoicing can be compared to the electronic processing of insurance policies and claims. For insurance companies, digital processing of policies and claims is a key cost saving opportunity. Therefore, most firms work on strategies to migrate from paper-based processing of documents to electronic processing.⁴⁴

The envisaged cost savings arise from direct and indirect time savings. Direct time savings are the reduced time needed by staff to process an invoice in the first place. Indirect time savings arise, if the error rate can be reduced compared to manual, paper based processing of documents. This reduces the follow-up effort for tracking errors and correcting them.

The chapter is structured in two parts (see Exhibit 3-1). The first part features evidence on the adoption of e-invoicing and payment systems among enterprises, based on the e-Business Survey 2005 by *e-Business W@tch*. The second part focuses on e-payment behaviour by consumers, based on a study of real e-transactions conducted by Pago eTransaction Services.⁴⁵

⁴³ If the type of goods, or the structure of individual invoices differs widely from one another, electronic standardisation of the invoicing format can be a challenge.

⁴⁴ e-Business Sector Studies on the Insurance Sector, July 2002, January 2003. [Hwww.ebusiness-watch.org](http://www.ebusiness-watch.org) ('resources')

⁴⁵ Pago eTransaction Services GmbH (Cologne, Germany) is an international acquiring & payment service provider for e-commerce businesses, shops (point-of-sale) and mail-order business. Since 2002, Pago has

Exhibit 3-1: Structure of chapter 3: ICT adoption and e-payment acceptance

	Chapter 3.1: Use of ICT for invoicing and payments processes	Chapter 3.2: Consumer behaviour and risks in e-payment transactions
Perspective	ICT adoption among companies	E-payment acceptance among consumers
Focus	<ul style="list-style-type: none"> • Readiness of enterprises for e-invoicing and e-payments • ICT systems implemented in firms 	<ul style="list-style-type: none"> • B2C e-commerce transactions • Consumer (buyer) behaviour in making e-payments
Data source and method	<i>e-Business W@tch</i> : Representative enterprise survey (e-Business Survey 2005)	Pago eTransaction Services GmbH: Analysis of real e-transactions conducted on the Pago platform
Reference year for data	2004/05	2004

3.1 Adoption of e-invoicing and e-payment activity by EU enterprises

Revitalising an 'old' concept: from EDI to e-invoicing

Although e-invoicing has only recently gained momentum and attracted considerable attention in policy, the idea of processing invoices in B2B transactions electronically is not new. The concept dates back at least 20 years, as it can be traced to EDI (Electronic Data Interchange). Transforming invoices into standardised electronic files and delivering this file to the receiver over dedicated communication channels is an integral part of EDI. One of the reasons for the surge in popularity is that the internet was projected to surpass EDI as the primary pathway for trading partners to present and manage invoices and payments within a few years.

EDI has been effective in achieving some of the objectives related to electronic invoicing. However, it is not a solution that has been widely spread and deployed, mainly because EDI frameworks are comparatively complex and expensive to build and maintain. Typically, EDI is used in point-to-point networks between large enterprises, which is confirmed by results of the e-Business Survey 2005 (see Exhibit 3-2). The effort which is needed to connect to additional suppliers is significant, since each transaction set must be customized.

been publishing an annual research report ("Pago Report") based on the analysis of real purchasing transactions. See chapter 3.2.

Exhibit 3-2: Use of EDI-based standards

Firm size		Use EDI-based standards
Micro	1-9 employees	2
Small	10-49 employees	4
Medium	50-249 employees	14
Large	250+ employees	43
TOTAL		19
Base: enterprises using computers from EU-7, 10 sectors. N = 5218. In % of firms from a given size-band. TOTAL: weighted by employment EDI = Electronic Data Interchange		
Source: <i>e-Business W@tch</i> (e-Business Survey 2005)		

EDI is a domain of large companies. Only 2-4% of micro and small enterprises say they use EDI-based systems, about 14% of medium-sized and more than 40% of large companies. Differences by size are thus much more pronounced for than those by sector. Among the industries studied in 2005, EDI is most widespread among the automotive, aerospace and pharmaceutical industry (about 10% of firms in each of these sectors where the presence of larger firms is more dominant than in others).

Modern Electronic Invoice Presentment and Payment (EIPP) solutions are based on new standards (mainly XML-based standards) and promise to be less costly to implement and maintain, and be coming more attractive also for SMEs than traditional EDI systems. Solutions offered by service providers are usually deployed on a web-based infrastructure and use the internet as the main presentation, interaction and messaging channel. By relying on web-based programming techniques, service providers claim that their EIPP solutions *"have eliminated the complexity and rigidity inherent in the old EDI structure"*.⁴⁶ However, if this involves the redesign of legacy systems, it can be a complicated and cost-intensive activity.

Successful deployment of electronic invoicing will depend on favourable technical framework conditions, which requires some coordination of activities among stakeholders. In particular, the analysis, design and development of protocols, electronic data formats and messages for the interoperation of applications should be promoted, on the basis of international standards (e.g. XML, ebXML, ebisXML, EC/UN), also considering legal and statutory frameworks for electronic transactions.⁴⁷

⁴⁶ Cf. Electronic Invoice Presentment and Payment (EIPP): A Win-Win Proposition. White Paper by CheckFree iSolutions (2003), p. 6.

⁴⁷ *ibid*

Project description:

The PRAXIS project – a Greek B2B initiative

The Greek **PRAXIS project**⁴⁸ has studied emerging systems and services for e-invoicing and B2B collaboration in Greece. PRAXIS points at some key issues that have to be addressed so that SMEs can successfully engage in B2B transactions via the internet:

- # **Application-to-application (A2A) integration** is seen as a key aspect, also for SMEs, since it is a requirement to realise everyday transactions with minimum effort and maximum security and reliability.
- # The **framework** for such an interoperability improvement (leading to the necessary processes, the XML schemes, and the relative infrastructure) is **practically non-existent in most of the EU and CEE (Central and Eastern Europe) countries**.
- # A2A integration and Enterprise Application interoperability must engulf systems of the **enterprises, the government and the intermediaries** (e.g. banks, IT service providers, consortia).
- # Since the redesign and re-development of existing enterprise and legacy systems can involve a tremendous effort, **new approaches** are required for the 'retrofit' of the various systems, based on emerging standards. The objective is that these approaches lead to a selection of easy to implement frameworks, low cost architectures and easily adoptable business processes.

Source: Presentation by Yannis Charalabidis e-Business W@tch Workshop on e-Invoicing, Athens, 31 May 2005.

The e-invoicing maturity ladder: readiness – adoption – impact

While framework conditions as outlined above are clearly important, ultimately it will be the enterprises themselves that decide whether or when to start using e-invoicing. As with many e-applications, it can be expected that the large firms will go first and SMEs will follow. Furthermore, in some sectors the motivation and/or preconditions for adoption are better than in others. This depends on typical customer-supplier-relationships (B2B, B2C, average number of customers and suppliers), the general e-maturity of enterprises, and the lock-in to legacy systems such as EDI.

Against this background, the adoption curve of e-invoicing activity among firms can be studied on three levels of maturity: first, the general preparedness and **readiness** for adoption; second, the level of actual **activity**; and finally, the **impact** level, i.e. the outcomes of e-invoicing activity (see Exhibit 3-3). The results of the e-Business Survey 2005 provide some evidence on the readiness of companies for using e-invoicing, and on the actual use of ICT for e-invoicing. The available evidence is presented in this chapter as follows:

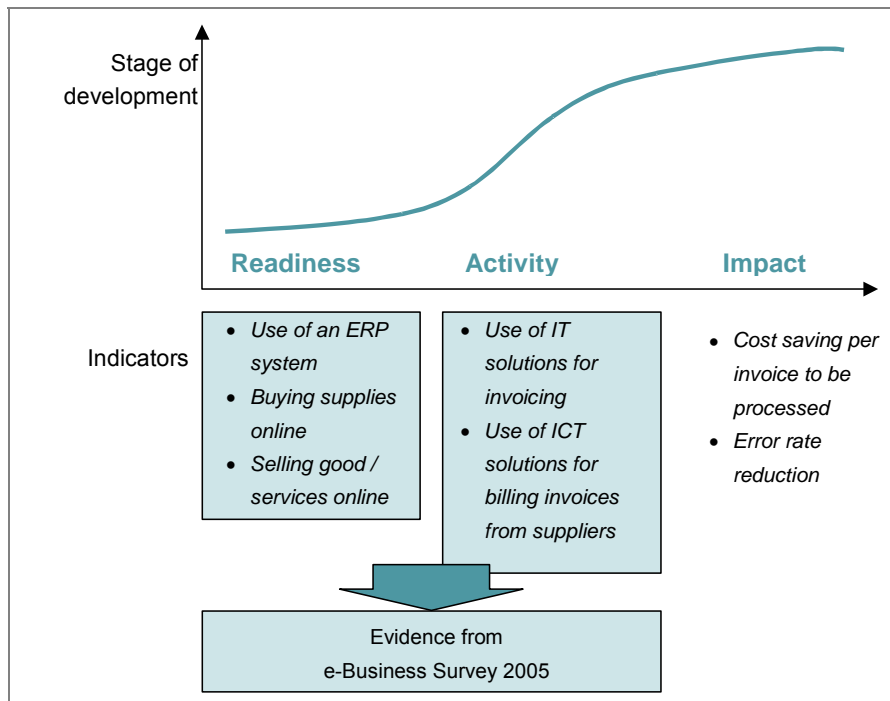
- First, an assessment of the general preparedness of EU enterprises (by sector and size) is presented, based on the diffusion of ERP and CRM systems, and on e-procurement and online sales activity. It is assumed that companies with an ERP system, and possibly with some experience in online trading, should be more inclined to adopt e-invoicing, since these activities and the underlying ICT systems are closely linked to each other.

⁴⁸ See: presentation by Yannis Charalabidis at the e-Business W@tch Workshop on e-Invoicing, Athens, 31 May 2005: "Emerging Systems and Services for e-Invoicing and B2B Collaboration in Greece: The PRAXIS Project". Available at [Hwww.ebusiness-watch.org/H\('events'\)](http://www.ebusiness-watch.org/H('events')). For more information, see [Hwww.praxisnet.gr/H](http://www.praxisnet.gr/H)

- Second, evidence on the current state of e-invoicing adoption is presented. Indicators for this stage are the use of ICT systems for billing invoices of suppliers, and for invoicing customers, as demonstrated by replies to the respective questions of the survey.

There is no information available from the survey, however, on impacts of e-invoicing, for instance on cost savings or error rates (which could be indicators for impacts). It is quite likely that it would be most difficult to obtain this information: most companies, particularly SMEs, are unlikely to have exact figures about cost reductions, but could give an estimate at best. This was also confirmed by the attitude of the majority of interviewees in the case studies conducted by the *e-Business W@tch* in 2004 and 2005, who were either reluctant or unable to provide such figures (not only an e-invoicing but, practically, on any type of e-activity).⁴⁹

Exhibit 3-3: Development stages in e-invoicing – from readiness to impact



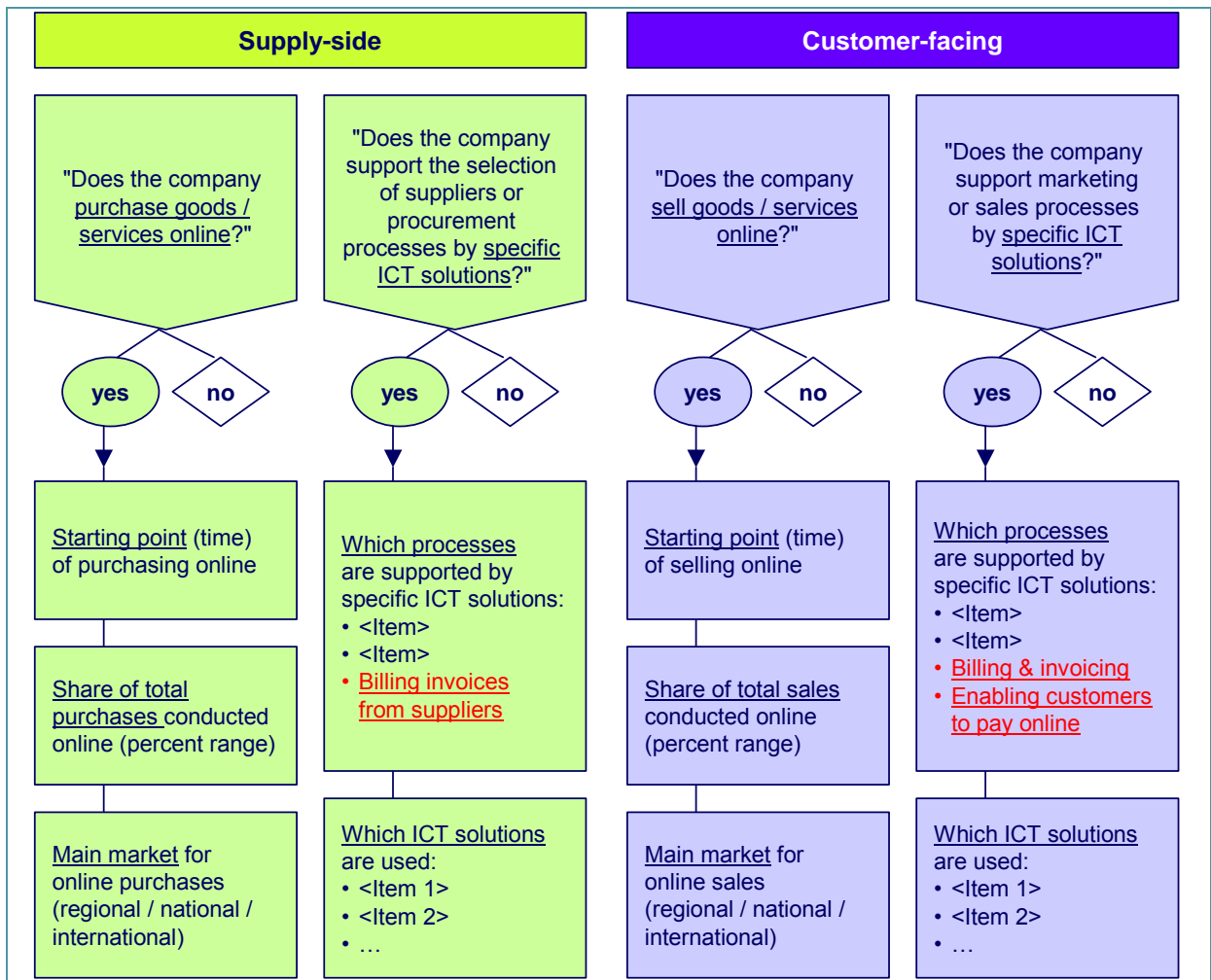
Source: *e-Business W@tch* (2005)

All data presented in this chapter are taken from the e-Business Survey 2005. Exhibit 3-4 visualises the structure of questions from the respective modules of the questionnaire which inform about e-invoicing and e-payment activity. *e-Business W@tch* asked all companies that participated in the survey whether they "support the selection of suppliers or procurement processes by specific ICT solutions", and, if so, if they used these systems for "billing invoices from suppliers". Similarly, companies were asked if they "support marketing or sales processes by specific ICT solutions", and, if so, if they used these systems for "billing and invoicing" and for "enabling customers to pay online". These questions were introduced in the e-Business Survey 2005⁵⁰ and yielded some interesting results.

⁴⁹ Moreover, it is difficult to obtain such figures in ad-hoc interviews as used in representative surveys, because firms are either reluctant to give away this information, or interviewees do not have it readily available during the interview. The same applies, for instance, to figures on ICT investments.

⁵⁰ They were not used in the surveys of 2002 and 2003.

Exhibit 3-4: Questions on e-commerce and e-invoicing in the e-Business Survey 2005



Source: e-Business W@tch (2005)

3.1.1 Readiness for e-invoicing and e-payment processing

Diffusion of ERP and CRM systems

E-invoicing systems are often integrated with the **ERP** (Enterprise Resource Planning) system of a company. Against this background, the existence of an ERP system in a company can be regarded as a facilitator for taking up e-invoicing activities. ERP diffusion can, hence, be regarded as an indicator for e-invoicing readiness.

Similarly, there are close links between e-invoicing and the **CRM** (Customer Relationship Management) system of a firm. Electronic invoicing can be regarded as a component of the overall customer management of a company, and related data will also be stored and used in the CRM system. In fact, EBPP software providers are working on improved integration of EBPP with CRM systems.⁵¹ The rationale is that EBPP "should be seen and categorized as a logical extension to (...) existing CRM initiatives"⁵², since the introduction of EBPP will position the company to drive customer service interaction to a its web presence. This is not unlikely, as a good deal of inbound customer service calls is invoicing related.

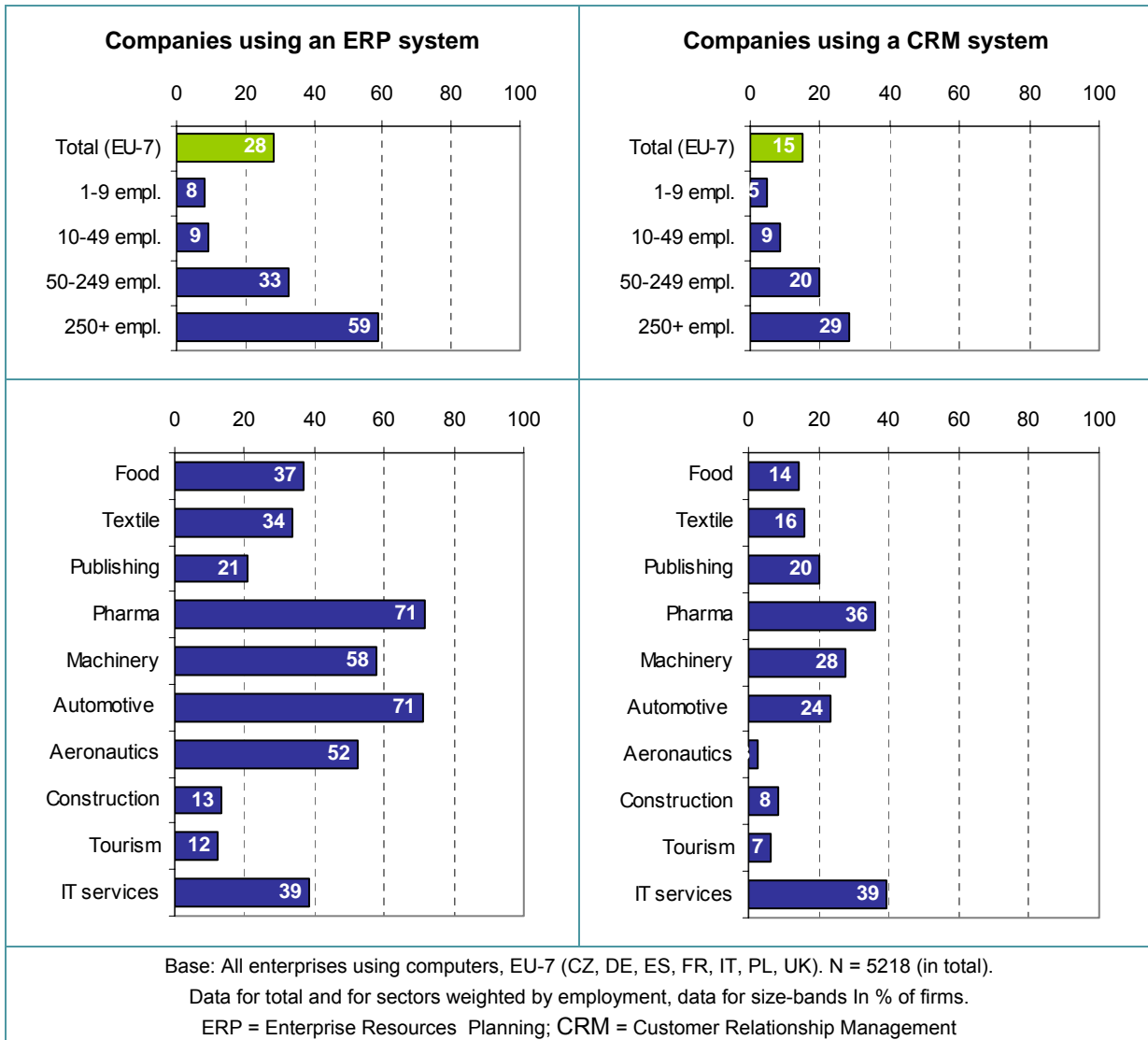
⁵¹ See, for example: "MaxBill Announces Launch of MaxCare's Web-based CRM", press release by MaxBill, 7 March 2005. The new system is announced to "integrate customer product instances, billing information, CRM and order management information in one single, easy-to-use, front end HTML framework". http://www.maxbill.com/pr05_MaxCare.html (July 2005).

⁵² See: "ROI through Electronic Invoice Presentment and Payment (EIPP)", by CheckFree iSolutions (2003)

However, if electronic invoicing is to be tied to CRM initiatives, only a fraction of companies is currently in a position to add e-invoicing (EBPP) functions, as the installed base is comparatively small. Only about 5% of all firms surveyed by the *e-Business W@tch* reported using a CRM system in 2005. Diffusion increases quite linearly by firm size and reaches significant adoption rates among medium-sized firms (about 20%) and large companies (close to 30%).

There are also variations by sector. The IT services and the pharmaceutical industry are the sectors where CRM appears to have the highest significance among the 10 sectors compared in the 2005 survey. This holds true for employment-weighted adoption rates (see Exhibit 3-5, right column), but also for SMEs. In % of firms, these are the only sectors where more than 10% of all companies reported using a CRM system (24% in IT services, 12% in the pharmaceutical industry). In the other sectors, diffusion has reached between 4-8% of firms, but goes up when measured in terms of employment-shares of those companies.

Exhibit 3-5: Diffusion of ERP and CRM systems among European enterprises



Source: *e-Business W@tch* (e-Business Survey 2005)

ERP systems are relatively more widespread than CRM systems, but they are also mainly used by medium-sized and large enterprises. About one in three medium-sized firms and about six out of ten large firms from the 10 sectors surveyed use an ERP system, while less than 10% of micro and small firms do.

ERP systems are modular software solutions for the planning, management and controlling of enterprise resources. They were originally developed for use mainly by large companies in manufacturing, wholesale or retail, which have to manage complex inbound and outbound supply chain logistics. In the past few years, as the large company markets are starting to reach saturation, many ERP software manufacturers are increasingly targeting small and midsize businesses as customers. Moreover, an increasing number of standardised software packages for specific industries such as engineering are reaching the market. The ERP software market is dominated by a few large software companies (including, for instance, SAP, Peoplesoft, Oracle and Microsoft), but there are also many regional solution providers which have specialised in niche markets (by offering for instance solutions that are optimised for specific industries).⁵³

ERP systems can be critical for electronic invoicing in the B2B area. Here, the e-invoicing interface should normally be integrated with the ERP system so that processes can be linked within the company (e.g. between the sourcing and accounting departments). A precondition to achieve this objective is the definition of standards for such interfaces, so that data can be exchanged between companies (ERP-to-ERP connectivity). This requires coordination with software vendors and could be an action point for business and trade associations.⁵⁴

At least for B2B processes, the penetration of ERP systems is therefore a useful indicator for the e-invoicing readiness of an industry. The 10 sectors studied by *e-Business W@tch* in 2005 can be grouped in 2 categories according to ERP penetration:

- sectors with a high penetration, where about 20% of all firms have an ERP system (pharma, machinery, automotive, aeronautics, IT services), and
- sectors with a comparatively low penetration of about 6-8% of firms (food, textile, publishing, construction tourism).

This dichotomy is partly an 'artefact' of the industry structure in terms of average firm-size, but has also to do with business activities and supply chain structures. A possible scenario for the deployment of B2B related e-invoicing activity is that uptake will be hampered among small firms in sectors with a low ERP diffusion. Thus, it could take longer to reach critical mass in those sectors, which is important for triggering fast growth in the adoption process.

Adoption of electronic commerce activity

Another indicator for the readiness of sectors for e-invoicing and e-payment is the amount of e-commerce activity. It can be argued that electronic billing, invoicing and payment is a logical step to be taken by companies which have already started buying and/or selling electronically. Although electronic invoicing is not necessarily restricted to transactions that have been accomplished electronically over computer-mediated networks, related activities are closely linked to each other.

Electronic commerce activities in the sectors under study are featured in detail in the *e-Business Sector Studies*.⁵⁵ This chapter presents a comparative synthesis of key indicators stemming from these reports.

Exhibit 3-6 summarises evidence on online purchasing activity in the 10 sectors studied by *e-Business W@tch* in 2005. In contrast to many other e-business indicators (such as CRM and ERP, as outlined above), the size of a firm does not make a good predictor for online buying. If the minimum threshold of online purchasing is set at 5% of the total volume of supply goods, firms of all size-bands behave very similar. About 25% of companies say that they buy more than 5% of their supplies online, about 10% of firms procure more than 25% of supplies online and results are fairly consistent across size-classes.

⁵³ Several web portals and IT specialist magazines feature overviews and links to ERP software providers. See, for example, [Hwww.softguide.de/software/erp.htm](http://www.softguide.de/software/erp.htm).

⁵⁴ see Austria as an example, chapter 1.2.3

⁵⁵ See [Hwww.ebusiness-watch.org](http://www.ebusiness-watch.org), ('resources')

Differences by sector, however, are more pronounced. Interestingly, it was not companies from the manufacturing sectors with large dominant players and deep supply chains which reported the most intensive use of online purchasing. The IT services sector is outstanding in this regard (with more than 40% of firms saying that they buy at least 25% of supplies electronically). In tourism, publishing & printing, and in aeronautics, the share of firms that buy at least 5% of their supplies online is also significant (about 30%). It appears that service sectors and sectors where a lot of digital goods and components are traded (publishing) have surpassed typical manufacturing sectors on the more intensive levels of e-purchasing.

Exhibit 3-6: Companies purchasing supply goods online

	Make online purchases		Buy more than 5% of supplies online		Buy more than 25% of supplies online		Use specific ICT solutions for e-procurement	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Weighting:								
Total (10 sectors, EU-7)	51	44	27	25	10	10	19	11
1-9 empl.		43		26		11		11
10-49 empl.		46		20		6		10
50-249 empl.		54		26		8		22
250+ empl.		58		29		11		30
By sector (EU-7)								
Food & beverages	43	22	16	7	4	1	18	5
Textile	44	30	15	11	3	2	14	8
Publishing & printing	57	48	32	28	10	9	16	8
Pharmaceutical	48	38	29	19	8	7	32	14
Machinery, equipment	53	36	22	18	5	4	18	10
Automotive	60	41	34	17	2	5	39	13
Aeronautics	43	65	38	36	2	11	63	16
Construction	43	36	18	17	4	2	16	9
Tourism	57	49	36	30	17	14	14	14
IT services	76	81	60	64	37	44	29	19
By country (10 sectors)								
Germany	62	56	35	36	10	16	22	11
Spain	46	50	25	31	7	13	23	23
France	40	26	19	15	7	5	21	7
Italy	35	37	13	18	4	5	11	7
United Kingdom	68	63	44	41	20	21	22	11
Czech Republic	49	42	23	21	7	7	15	8
Poland	37	39	8	15	4	6	8	3
Base (100%)	all		all		all		all	
"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country "% of firms" = % of firms as legal units, irrespective of their size								

Source: *e-Business W@tch* (e-Business Survey 2005)

This finding is somewhat put into perspective when another indicator for e-procurement activity is used as a 'corrective': the use of specific ICT systems for supporting electronic sourcing and procurement processes. Here, the typical progression of adoption by firm size can be found (from about 10% of micro-firms up to about 30% of large firms), and sector deployment is closer to what could be expected from the type of business activity. In total, about 10% of firms (and 20% by employment) use special ICT solutions to support e-procurement processes, a finding which indicates that electronic sourcing and procurement play an important role in these companies. From an industry perspective,

such solutions are mostly used in the IT services sector, in automotive and aeronautics, in the pharmaceutical industry, but also in tourism.

Thus there is a wide gap between the use of e-procurement systems and the share of companies that buy online. The most likely explanation is that a good deal of online purchasing activity consists in making occasional purchases from websites of suppliers, rather than applying special procurement systems for this purpose.

The gap is much smaller, however, when customer facing e-commerce activities are studied (see Exhibit 3-7). There, the use of special ICT systems for electronic marketing and sales corresponds closely to the share of companies that make online sales, with the exception of micro-enterprises. The most plausible explanation behind this evidence is that companies that sell their goods or services online *themselves* require some type of e-commerce system (e.g. a shop system on the web), and thus have a specific ICT solution for online marketing or sales.

Three sectors are standing out in terms of the relative importance of online sales, namely the two service sectors in the sample (IT services and tourism), and – to a lesser extent – publishing & printing. In the IT services and tourism industries, about one in five firms report that online sales already account for more than 5% of their total sales volume; for one in ten firms, online sales represent even more than 25% of sales. This is plausible, considering for example the increasing importance of online reservations and online ticketing in tourism. In publishing, 'online sales' can refer to websites where users have to pay for the download of articles (for instance for access to the online edition of a newspaper or magazine). Such offers are often linked with micro-payments.⁵⁶

In the tourism industry, many firms (for instance many hotels) have outsourced the operation of an online reservation system to third party service providers (online travel and hotel reservation platforms). Thus they make 'online sales' (which means they enable customers to make an online reservation), without having a respective ICT system for e-commerce. This may explain the outstanding discrepancy of figures for this industry, where 31% of firms said that they sell online, but only 12% use respective ICT systems. There is also a clear gap in the publishing industry. In all other sectors, the share of companies that report online sales corresponds closely to the diffusion of related systems.

From a broader perspective, an interesting finding is that the three sectors where companies buy the highest shares of supply goods online are the same sectors that report the highest shares of online sales. Only in IT services, tourism and publishing more than 10% of firms say that they make more than 5% of their revenues from online sales. From this evidence, and in the context of this report, it can be concluded that these sectors could have a high propensity to adopt e-invoicing because of their comparatively broad and intensive use of electronic commerce, both in terms of supply-side and customer-facing activity (see summary and Exhibit 3-12 in the following chapter).

⁵⁶ See *e-Business W@tch* Sector Report on Publishing & Printing, September 2005. [Hwww.ebusiness-watch.org](http://www.ebusiness-watch.org) ('resources')

Exhibit 3-7: Companies selling products or services online

	Make online sales		Sell more than 5% of goods online		Sell more than 25% of goods online		Use specific ICT solutions for online marketing / sales	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Weighting:								
Total (10 sectors, EU-7)	17	15	10	10	3	4	17	8
1-9 empl.		15		10		4		8
10-49 empl.		14		8		3		11
50-249 empl.		16		10		2		20
250+ empl.		21		9		3		28
By sector (EU-7)								
Food & beverages	12	8	4	2	1	0	15	6
Textile	14	10	4	6	1	1	14	7
Publishing & printing	37	18	17	10	3	4	27	9
Pharmaceutical	18	13	8	6	3	2	26	12
Machinery, equipment	11	5	4	2	0	1	17	8
Automotive	6	11	2	5	1	2	24	9
Aeronautics	8	12	n/a*	n/a*	n/a*	n/a*	6	14
Construction	4	3	2	1	0	0	8	3
Tourism	36	31	26	21	10	10	19	12
IT services	25	25	14	19	7	12	40	23
By country (10 sectors)								
Germany	19	25	9	15	2	5	23	13
Spain	13	15	8	7	3	3	17	12
France	11	8	6	5	3	3	17	6
Italy	15	13	11	11	4	4	8	3
United Kingdom	24	16	14	11	6	7	21	13
Czech Republic	14	12	7	7	3	4	9	4
Poland	15	16	7	10	2	5	9	10
Base (100%)	all		all		all		all	
<p>"All" = companies using computers. N = 5218 (Total). "% of employment" = firms representing ...% of employment in the sector(s) / country. "% of firms" = % of firms as legal units, irrespective of their size</p> <p>* Percentages only indicative, due to small number of observations (N = 16 for the Aeronautics sector).</p>								

Source: e-Business W@tch (e-Business Survey 2005)

3.1.2 E-invoicing and e-payment activity

After having investigated the readiness of different sectors for the future growth of electronic invoicing, this section features some evidence on the current state of adoption. According to Gartner Group, of all B2B transactions conducted in the United States, only 14% of invoices and 17% of payments were processed electronically in 2003. Out of those, more than two-thirds were processed using EDI, and only 5% used the internet. The internet was projected, however, to surpass EDI as the primary pathway for trading partners to present and manage invoices and payments within a few years.⁵⁷

It is difficult to compare these figures for Europe, as they cannot be directly 'translated' into the structure of the questionnaire used in the e-Business Survey 2005. However, e-Business W@tch has

⁵⁷ Quoted from: "Making e-invoicing pay" by Bryan Houston, Partner, IBM Business Consulting Services, Financial Services Sector. January 2004. Published as an IBM news bulletin at <http://www-1.ibm.com/industries/financialservices/doc/content/news/newsletter/991324103.html> (download: June 2005)

evidence that about 50% of those companies that used special ICT systems for e-procurement or e-sales used them for billing and invoicing (see Exhibits 3-8 and 3-9).

In most sectors about 5% of firms (accounting for about 10% of employment) used ICT to invoice customers electronically, and also about 5% to bill invoices from suppliers electronically in early 2005. Activity clearly increases in both cases by firm size. 11% of medium-sized and 17% of large companies invoiced customers electronically, according to these figures.

As there is no information on the total amount of invoices that are processed by the companies, it is impossible to calculate or assess the share of invoices that are processed electronically. While Gartner reports for the USA that digitisation of payment processes has reached a higher level than for invoicing,⁵⁸ *e-Business W@tch* findings indicate that fewer companies use their ICT system for enabling customers to pay online than for billing and invoicing (see Exhibit 3-9, second chart). Diffusion of ICT systems that are used for processing payments electronically is below 5% of firms.

This evidence is based on a follow-up question *e-Business W@tch* asked those companies that reported the use of special ICT solutions for e-procurement or e-sales. Companies were asked which e-commerce related business processes they actually supported by use of these systems. Exhibit 3-8 depicts those processes that are related to e-invoicing and e-payments. For comparison, and as a point of reference, the most common application ('ordering supply goods online') is also included in the table.

Exhibit 3-8: Companies using ICT solutions for e-invoicing and e-payment processes

	Order supply goods online		Billing suppliers' invoices		Billing and invoicing		Enable customers to pay online	
	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms	% of empl.	% of firms
Weighting:								
Total (10 sectors, EU-7)	81	83	49	54	56	44	28	33
1-9 empl.		84		55		42		35
10-49 empl.		77		44		51		26
50-249 empl.		72		51		53		15
250+ empl.		82		47		58		26
By sector (EU-7)								
Food & beverages	83	72	49	63	50	39	18	13
Textile	82	81	55	67	46	44	19	29
Publishing & printing	68	81	40	51	62	55	50	33
Pharmaceutical	74	67	58	38	78	62	6	21
Machinery, equipment	86	78	44	42	65	56	2	15
Automotive	89	73	56	48	82	56	34	27
Construction	78	84	38	33	45	50	13	17
Tourism	78	77	47	65	49	32	45	42
IT services	89	98	68	75	53	57	23	34
Base (100%)	Companies using special ICT solutions for e-procurement				Companies using special ICT solutions for marketing or sales processes			
N ~ 800 (for total). "% of employment" = firms representing ...% of employment in the sector(s) / country. "% of firms" = % of firms as legal units, irrespective of their size								

Source: *e-Business W@tch* (e-Business Survey 2005)

As can be expected, the vast majority of those firms that have e-procurement systems in place use them for directly ordering goods online from suppliers (about 80%). About every second company that has implemented ICT systems for e-commerce uses these systems for billing and invoicing (see Exhibit 3-8). This holds true for billing invoices from suppliers (as regards the use of e-procurement systems) and for invoicing customers (as regards ICT systems for e-sales). About every third company

⁵⁸ *ibid*

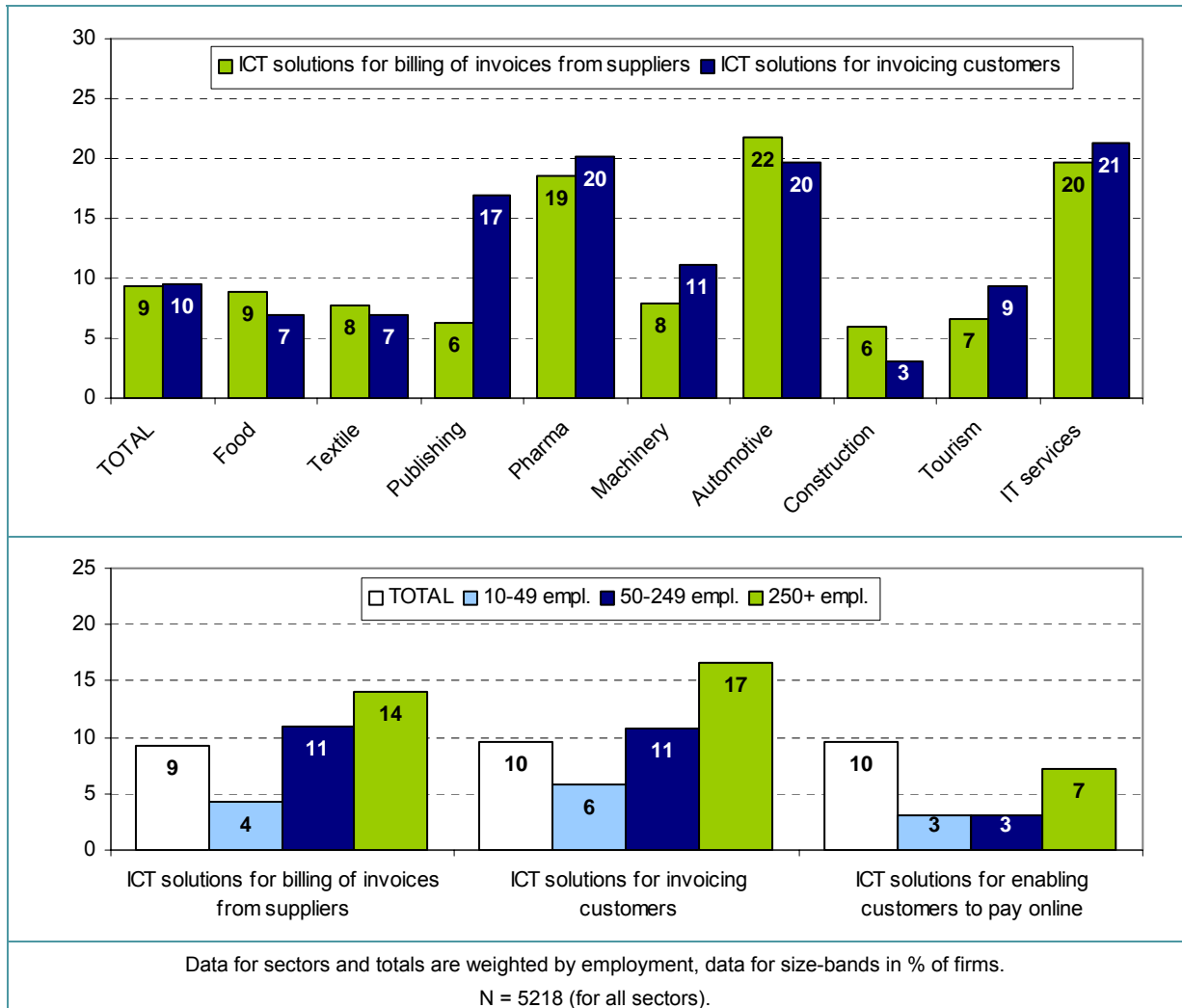
with special ICT solutions for e-commerce has included functionalities to enabling customers to pay online for goods or services ordered.

The percentages depicted in Exhibit 3-8 relate to the base of firms that use ICT solutions for e-procurement or online sales. Exhibits 3-9 and 3-10 show the adoption of e-invoicing and e-payment activities as a share of *all* companies with computers, which is obviously a much broader base. In all sectors except IT services, fewer than 10% of all firms use electronic billing or invoicing. However, the adoption of these e-commerce related activities increases by company size. About 15% of large firms used ICT systems for electronic billing and invoicing in early 2005 (see Exhibit 3-9, second chart). As a consequence, a comparatively small percentage of firms can account for a significant share of a sector's employment, notably in the automotive and the pharmaceutical industry (see Exhibit 3-9, first chart). In these sectors, companies representing about 20% of all employees have started to process invoices electronically.

In most sectors, the digitisation of invoicing customers and of billing supplier invoices appears to go hand in hand (see Exhibit 3-9, first chart). This can be expected, as e-invoicing will normally be a two-way process, at least in B2B transactions. The situation can be different for sectors which are mainly consumer oriented in their sales. In fact, the publishing industry differs from the other nine sectors in its profile in this respect: here, the automation of customer-facing invoicing processes (subscribers, advertisers) is clearly more important than billing invoices from suppliers electronically.

As explained above, the sector comparisons in Exhibit 3-9 emphasize activity in large firms. The apparently broad diffusion of related activities in the automotive and pharmaceutical industry are mainly due to the dominance of large players in these industries. Sector differences in the diffusion of e-invoicing activity are not very pronounced when weighting does not account for differences between small and large firms.

Exhibit 3-9: Use of ICT solutions for invoicing customers and billing invoices from suppliers electronically (EU-7, by sector and size-band, 2005)



Source: *e-Business W@tch* (e-Business Survey 2005)

A possible exception is the IT services sector, where about 14% of all firms reports to bill supplier invoices electronically. This is plausible, as the software industry and other sub-sectors of the IT services sector are forerunners in digitising business processes. The comparatively advanced adoption level in tourism, if measured in % of firms (9% of firms), should not come as a surprise: e-procurement activity was found to be generally high in this industry in 2005, which facilitates the readiness of enterprises for electronic processing of supplier invoices.

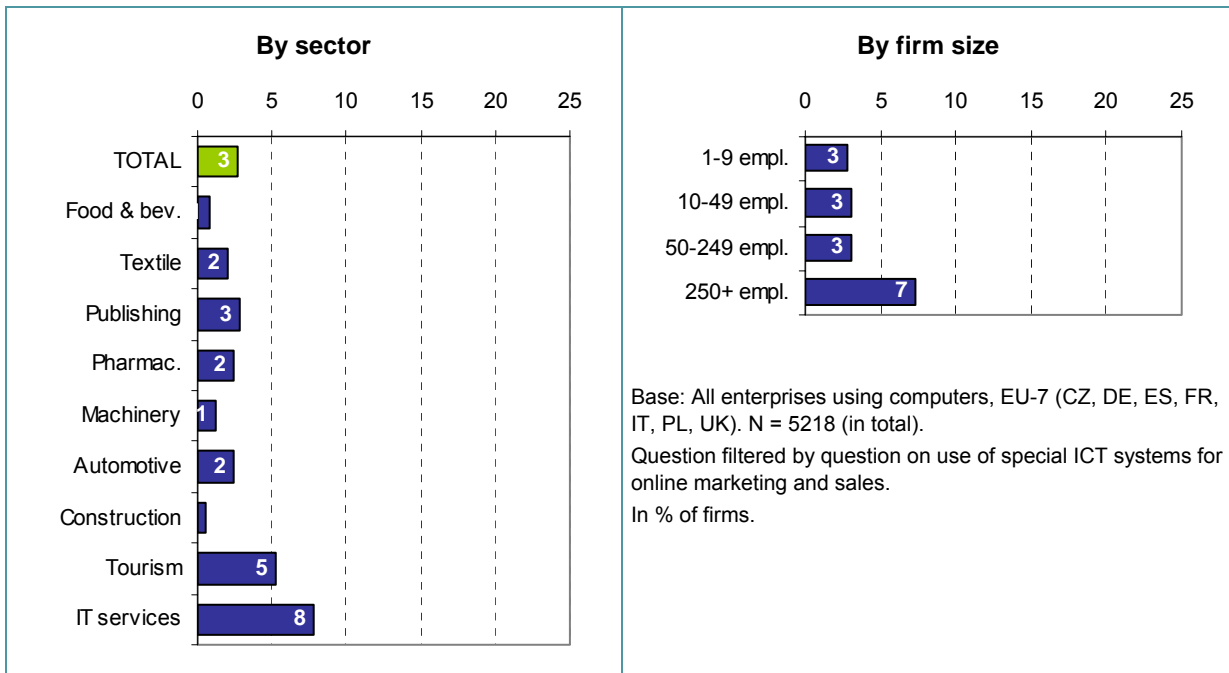
In some of the manufacturing sectors, there is a pronounced gap between small and large firms. In the automotive industry, for example, only about 2-5% of micro and small firms (with up to 49 employees) said that they use applications to bill invoices from suppliers electronically, but more than 20% of large firms did so. A similar increase of e-billing activity by firm size can be observed for the textile industry (about 16% of large companies) and for food and beverages (up to about 13% of large firms).⁵⁹

As regards electronic processing of payments, the IT services sector and the tourism industry are most advanced (see Exhibit 3-10). The finding reflects that electronic payment is closely linked to B2C electronic commerce activity, which is particularly important in both these industries. In all other

⁵⁹ Exact figures cannot be quoted due to high confidence intervals; the general trend of an increase by company size, however, is significant.

sectors monitored, currently less than 5% of firms report using ICT systems for e-payments. A closer look at some of the related processes is provided in the following chapter (3.2).

Exhibit 3-10: Percentage of firms enabling customers to pay online



Source: *e-Business W@tch* (e-Business Survey 2005)

Summary

In total, about 5% of all firms from the 10 sectors and 7 countries surveyed in 2005 have reported using ICT systems for electronically invoicing their customers. Similarly, about 5% use systems for billing invoices from suppliers electronically. Differences are not very pronounced by sector, with the possible exceptions of the IT services sector which is a forerunner in electronic billing and invoicing.

This evidence confirms that e-invoicing is a comparatively young development which is not yet widely diffused. However, it is commonly expected that e-invoicing offers prospective business value to many companies, including SMEs, as well as to the public sector. Since the adoption of e-invoicing has the potential of a win-win game for all parties involved, fast uptake across sectors is likely. This development could be further promoted by related activities of the public sector.

Exhibit 3-11: E-invoicing in the EU: readiness, potential and current state of adoption in 10 sectors

Sector	E-Invoicing readiness		E-Invoicing potential	Current state of adoption	
	Criteria	ERP & CRM installed base	E-commerce activity	Type of business activity, customer structure	Relative to other sectors
Food and beverages	★★	★	★★★(★)	●	~ 2-5%
Textile industry	★★	★	★★★(★)	●●	~ 4-8%
Publishing and printing	★★	★★★★	★★★★(★)	●●	~ 3-6%
Pharmaceutical industry	★★★★★	★★	★★★★	●●	~ 5-8%
Machinery and equipment	★★★	★(★)**	★★★★	●●	~ 3-6%
Automotive industry	★★★	★(★)**	★★★★★	●●	~ 4-8%
Aerospace industry	★★★	★(★)**	★★★★★	●●●	~ 8-12%
Construction	★	★	★★★(★)	●	~ 2-5%
Tourism	★	★★★★	★★★(★)*	●●●	~ 5-10%
IT services	★★★★★	★★★★★	★★★★★	●●●●	~ 10-15%

★ = low; ★★ = medium; ★★★ = high; ★★★★★ = high, also in SMEs
 Note: "low" / "high" is defined in relation to the average of the sectors monitored.
 ERP = Enterprise Resources Planning; CRM = Customer Relationship Management

* In tourism, the potential varies considerably by segment. While opportunities may be promising for airlines, tour operators and hotels, e-invoicing will be less relevant for example for bars or restaurants.

** Mainly e-procurement activity by larger companies, comparatively few companies selling online.

Source: e-Business W@tch (e-Business Survey 2005)

e-Business W@tch concludes that the **potential to benefit from electronic invoicing is considerable in all sectors** (see Exhibit 3-12). The main benefits to be gained are cost savings, reduced errors and improved customer relationships.

In **B2C** markets, the highest potential is seen for firms which regularly issue similarly structured invoices to a large number of customers, for example telecommunication or utility service providers, insurance companies, or publishers (subscriptions). Here, EBPP (Electronic Bill Presentment and Payment), i.e. the web based presentation of invoices and accounts to customers, will be the main platform.

In **B2B**, electronic invoicing is tightly linked and integrated with the use of ERP (Enterprise Resource Planning) systems and has a high potential particularly in sectors with deep supply chain integration and longstanding supplier-customer relationships. This applies, for example, to the automotive, the aerospace and parts of the chemical industry.

3.2 E-payment consumer behaviour and the risk of fraud

Introduction

This chapter is based on research carried out by Pago eTransaction Services GmbH (Cologne, Germany), an international acquiring and payment service provider for e-commerce businesses, shops (point-of-sale) and mail-order business.⁶⁰ Since 2002, Pago has been publishing an annual research report (the 'Pago Report') based on the analysis of real purchasing transactions.

The Pago Report 2005 has about 150 pages and provides valuable data and insights on e-commerce and e-payment activity in Europe. Analysis focuses on the demand-side in B2C (business-to-consumer) transactions. The report analyses consumer behaviour in European online shops, for example the preference of online payment methods by sector and country, and time patterns in making online payments (daily and yearly peak times when payments are being conducted). It also provides data on the risk of fraud and non-payments.

With its focus on the demand side, the analysis documented in the Pago Reports is complementary to the supply-side oriented research of *e-Business W@tch*. User behaviour, particularly in B2C transactions, is clearly important aspect in analysing electronic payments and in order to better understand e-commerce developments. This chapter summarises key results of the Pago Report 2005, continuing the fruitful cooperation and exchange between *e-Business W@tch* and Pago in the area of e-business related research.⁶¹

Background – the Pago database

The findings in this chapter are based on the analysis of around 20 million real purchase transactions which were processed through the Pago platform in the period from 1 January 2004 to 31 December 2004. All findings relating to payment behaviour are based on the payment methods processed on the Pago platform. Random sample data were extracted from the total volume of transactions and were checked to confirm that they were representative of the predetermined query.

Geographic scope: A distinction must be made between the location of a vendor (the online shop⁶²) and the consumer who purchases and pays online.

- The Pago analysis includes e-transactions conducted in European online shops, with a focus on German and UK shops. The sample of shops consisted of about 48% UK based shops, 28% in Germany, and 24% in other European countries.
- The location of users includes non-European users. Out of the transactions studied, about 25% were made by buyers located in Germany, 3% in the UK, 8% in other European countries, and 64% from non-European countries.

While the share of German online shops corresponds to the share of buyers located in Germany, it appears that UK based shops are much more frequented by international buyers. One explanation for the non-European consumer's affinity to UK online shops is the fact that the majority of these shoppers are from the USA and Canada, who prefer English language shops.

⁶⁰ Pago enables its clients to receive payments for their goods and services through electronic channels. The integration of credit card acquiring and payment processing enables Pago to allow businesses of all shapes and sizes to use all internationally and nationally relevant payment methods. The range of payment methods includes Visa and MasterCard, American Express, Diners Club, JCB, Switch/Solo as well as locally used direct debit methods. All payment transactions are processed through the Pago platform, which was established in 2000. Pago is also a licensed Visa and MasterCard acquirer for Europe. See: [Hwww.pago.de](http://www.pago.de)

⁶¹ *e-Business W@tch* has made contributions to the Pago Reports 2004 and 2005.

⁶² In the context of this analysis, the term "online shop" does not only include retail shops, but all types of electronic points of sale where products or services can be ordered and paid online. This includes specifically online casinos, electronic pharmacies, and online travel agencies.

Sectoral scope: In line with the *e-Business W@tch* approach, Pago also analyses differences between industries. Pago focused its research activities for the 2005 Report on five sectors: electronic retailing, online gambling, online pharmacies, telecommunications, e-travel. Results show that the preferred payment methods differ by sector.

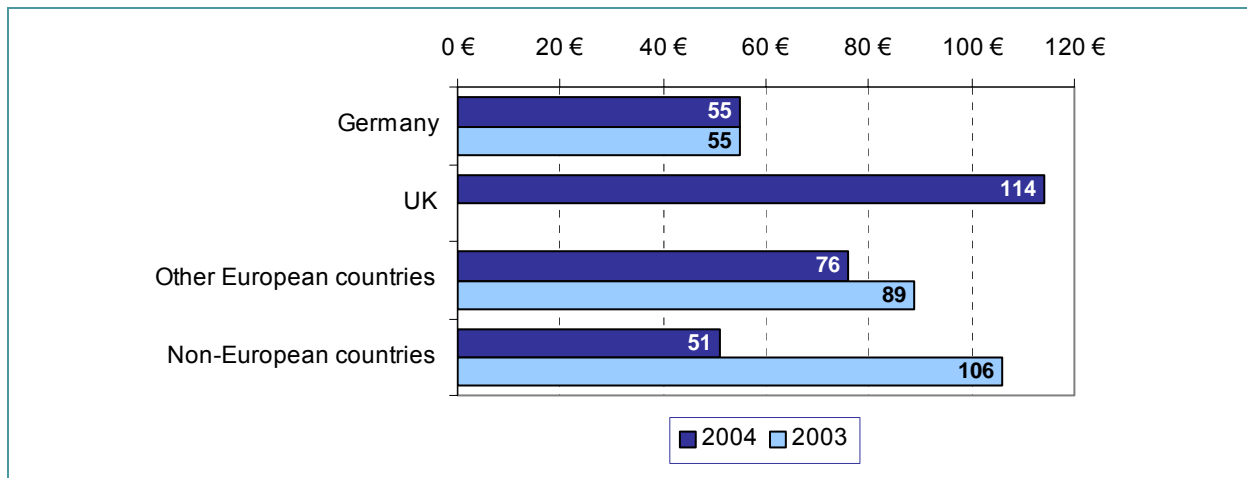
Definition of 'transaction': A purchase transaction is defined here as any transaction that involves at least a payment transaction, but can include a reminder and/or credit transaction. A purchase transaction is created when a shopper in an online shop collects items in a shopping cart and then submits and confirms his/her personal details. The purchase transaction, as defined here, is completed when either the shopping cart value has been paid in full by the online buyer or debt recovery proceedings have been started or a credit note has been issued. The result of debt recovery proceedings is not relevant, at least for the completion of the purchase transaction.

3.2.1 Consumer behaviour in making e-payments in 2004

Average transaction values

The average transaction value (shopping cart values) has changed significantly compared with 2003. In 2003, non-Europeans had the highest average value (106€ on average). They were surpassed in 2004 by UK shoppers who generated average shopping cart values of 114€. The average transaction value for German consumers has hardly changed (55€). The average value generated by purchases from consumers from the rest of Europe was lower in 2004 (76€) than in 2003 (89€). It must be noted that the comparability of figures over years is limited, as the sector configuration on which they are based was not the same in 2003 and in 2004. Therefore, results are only indicative.

Exhibit 3-12: Average transaction values in European shops by consumer origin



Source: Pago eTransaction Services (Pago Report 2005)

A closer comparison of UK and German shopping behaviour helps to understand the higher average shopping card value of purchases by UK shoppers. The percentage of UK shoppers generating average transaction values of over 500 euros is higher than in Germany (6.6% of all transactions by UK buyers have a value of 500 euros or more, but only 1.6% of transactions by German buyers do so). This could go back to the fact that online flights, package holidays and hotel booking are more popular in the UK than they are in Germany; average transaction values of over 500 euros are more typical of the e-travel business.

Preferred times for paying online

Analysis of time patterns of e-payment activity show that the day of the week and the time of the day are important parameters for e-payment activity. For companies, this is important information for modelling the respective offer and also for optimal scheduling of ICT maintenance work. Differences in

the monthly distribution of e-payments are less pronounced, with the exception of November and December (Christmas shopping).

Daily preferences: Consumer behaviour was found to vary slightly between regions. Saturday was the weakest online shopping day for German consumers, while Mondays and Tuesdays were the most popular days for online shopping. For customers from other countries, daily patterns were less pronounced, with a clear preference for week-ends from other European countries' shoppers.

Exhibit 3-13: Daily shopping preferences in European shops by country of shopper

	German shoppers	UK shoppers	Shoppers from other European countries	Non-European shoppers
	Indexed values: 100 = weakest shopping day			
Monday	152	118	109	100
Tuesday	154	109	111	100
Wednesday	146	114	113	102
Thursday	130	113	100	109
Friday	120	102	100	112
Saturday	100	111	125	115
Sunday	120	100	122	110

Source: Pago eTransaction Services (Pago Report 2005)

Monthly preferences: In contrast to the general monthly distribution pattern for all consumers in 2004, German consumers tend to show a stronger seasonal behaviour: About twice as many e-payments are made in November and December ('Christmas peak') as in other months. From January to September, differences are rather insignificant.

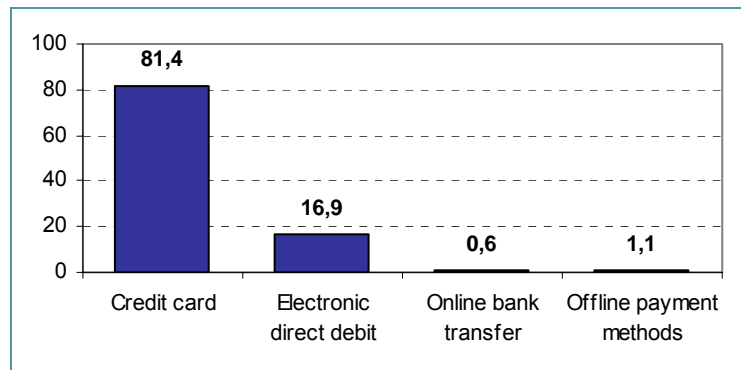
Hourly preferences: The observation of hourly shopping preferences is based on the evidence of German consumers' buying in European shops. Statistics confirm that a good deal of online shopping is probably accomplished from the office desk. About 60% of all purchase transactions by German consumers in 2004 were executed between 8 am and 6 pm. The peak time was in the late morning between 10 am and 12 noon. One figure, however, stands out in the 2004 analysis: a small, yet substantial fraction (10%) of all transactions is carried out between 6 am and 8 am in the morning.

Payment methods used

Research has differentiated between payments by credit card, use of various electronic direct debit systems, online bank transfer and offline payment methods (including purchases on invoice and advance payment).

The 2003 Pago Report clearly showed that the credit card has become by far the most important payment method in B2C electronic commerce. This also applies to 2004. However, the analysis of payments made in 2004 shows a trend toward nationally developed payment methods, which appear to become more and more popular with consumers.

This trend can be seen in the share of credit card transactions. In 2003, the credit card accounted for about 93% of all transactions, whereas in 2004 their share decreased to 81%. At the same time, the share of direct debit transactions (e.g. the electronic direct debit in Germany) has more than doubled from about 7% in 2003 to 17% of all transactions in 2004. As in 2003, offline payment methods only accounted for about 1% of all transactions.

Exhibit 3-14: Share of payment methods in European shops in 2004

Source: Pago eTransaction Services (Pago Report 2005)

There are considerable variations in the relative importance of e-payment methods by sector, by country and depending on the amount to be paid. Payments by UK consumers and by those from outside Europe for purchasing goods in European online shops are only made by credit card. Among German users, in contrast, processing payments by electronic direct debit is more popular than using the credit card online.

There is a clear pattern in the distribution of the various payment methods in relation to transaction value ranges. The electronic direct debit is used especially in transactions of under 10 euros, for example for telecommunications services. The opposite applies to credit card payment, which is used relatively seldom for smaller transactions. Among credit cards, Visa has by far the largest market share among the online shops studied. Visa was used in about 69% of all credit card transactions. Mastercard was used in about 30% of transactions, leaving only about 1% for other cards.

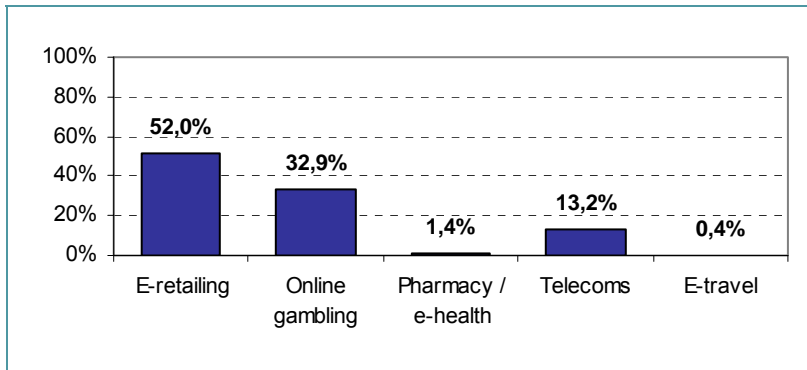
3.2.2 e-Payment sector profiles

For its 2005 report, Pago eTransaction Services analysed e-payments from an industry perspective. To this end, online shops to be studied were selected from five categories, according to the following working definitions:

- **Electronic retailing:** all online shops which offer goods, either produced by the merchant or where the merchant acts as an agent between producer or wholesaler and consumer.
- **Online gambling:** includes all merchants offering gambling, gaming and betting services.
- **Online pharmacies / e-health:** includes all merchants offering medication, drugs and similar products online
- **Telecommunications:** Telecommunication-related services include call-by-call offers, traditional fixed line and mobile services, and website hosting. These are being increasingly offered on the internet, and online billing is also increasing.
- **E-travel:** includes the sale of package holidays and trips, flights – especially so-called low-cost flights – hotel bookings, last-minute packages and flights and car rentals.

It must be noted that the distribution of e-payments (analysed in the Pago study) by sector reflects the structure of Pago customers rather than the real volume of e-transactions in each of the five sectors studied. In 2004, out of the more than 20 million e-payment transactions analysed, 52% were made in e-retailing shops, 33% in online gambling, 13% in telecommunications, 1.4% in online pharmacies and less than 1% in e-travel outlets.

Exhibit 3-15: Distribution of e-transactions in European shops by industry



Source: Pago eTransaction Services (Pago Report 2005)

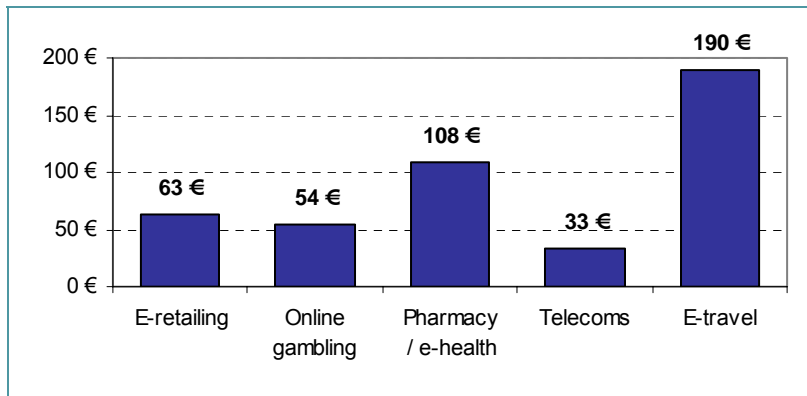
Average transaction values by sector

The average transaction value of e-payments differed significantly by sector. E-retailing purchases averaged at 63€ per transaction and online gambling transactions averaged 54€. In online gambling, this is a drop of more than 50% compared to 2003, which was probably due to the very strong expansion of the international online sport betting market in 2004.

The comparatively low average transaction value (33€) in the telecommunications industry is partly determined by the supply structure and the related payment methods. A large proportion of transactions are monthly subscriptions and fees, for instance for website hosting and ADSL access.

The average value of e-health transactions was surprisingly high (108€). Trends in this industry are largely dependant on the question of whether and to what extent common medicines are available online. In 2004, most purchases seemed to be for speciality products. The average value in the e-travel sector (190€), which appears to be low when considering the type of service that is purchased, indicates that low cost airline and hotel bookings made up the majority of transactions in 2004.

Exhibit 3-16: Average transaction values in European shops by industry



Source: Pago eTransaction Services (Pago Report 2005)

Seasonal effects

The relative weightings of transactions accomplished in the five industries analysed shifted continuously throughout 2004. In the first half of the year, e-retailing accounted for up to two thirds of all transactions, but the share fell to about 38% in the second half of 2004. The lows of August through to October could indicate reduced online shopping activity during vacation time.

Online gambling accounted for between 25% and 30% of transaction in the first half of 2004, but increased to 41% in the second half of the year. This pattern does not reflect any kind of seasonality; the increase is due rather to more attractive gambling offers and corresponds to an increase in sports betting in this sector.

There were two peaks in the e-pharmacy / e-health sector: in May, e-health accounted for more than 2% of transactions and in November nearly 3%. The relative low figures for the first four months are due to relatively few merchants in this sector being processed by Pago at that time.

The pattern of transaction volumes in the online telecommunications sector largely reflects the telecommunications industry as a whole, which experienced a slight downturn in the first half of 2004 before picking up again towards the end of the year.

The share of Telco transactions increased continuously from March 2004 and accounted for 0.4% of all transactions at the end of the year.

The total number of transactions for e-travel was relatively low. There was, however, a noticeable improvement throughout the year, with peaks during the summer vacation time from July to September. This finding suggests that e-travel bookings are to a large extent used for 'last minute' (or at least short term) reservations, rather than for vacations that are booked months in advance.

Transactions in e-travel

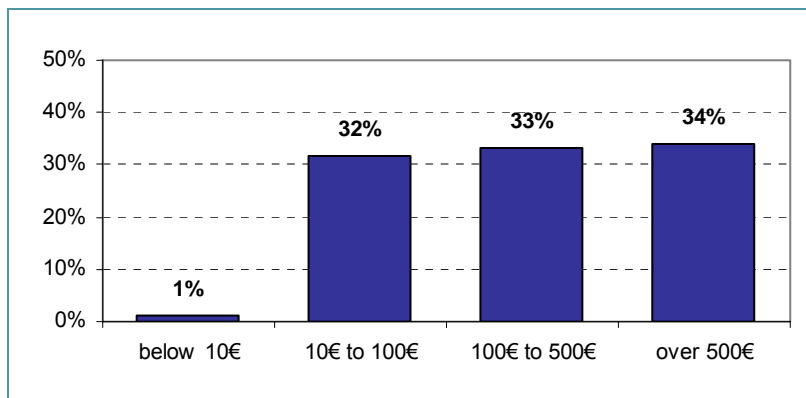
The Pago Report 2005 features a detailed analysis of electronic payments for each of the five sectors under study, including break-downs of figures by the location of customers, the monthly and weekly distribution of payments, and the market shares of credit cards used for making payments.

In this section, some results on the e-travel industry are presented as an example. Pago studied the online travel industry for the first time in 2004. The number of transactions in this sector was relatively small. These results should consequently, be seen as indicative trends only. However, the online travel industry is probably the fastest growing sector in e-commerce.

Whereas offers used to be restricted to last-minute packages and flights a few years ago, nowadays all important airlines, travel agencies and package providers are offering their full range of services online. Consumer acceptance has always been relatively strong, but seems to be growing further.

The distribution of average transaction values is shown here only for the UK, because the absolute number of transactions from other countries was too low. UK travel consumer purchases follow a very typical pattern: the segment under 100€ includes low-cost flights and car rentals; package holidays and scheduled flight bookings are usually to be found in the segment from 100€ to 500€, while the segment over 500€ includes more expensive package holidays, cruises and long-distance flights. The distribution of transactions in these three segments was roughly equal.

Exhibit 3-17: Distribution of transactions by transaction value in the UK e-travel industry



Source: Pago eTransaction Services (Pago Report 2005)

Credit card payment is used in 100% of all online travel bookings. This is due mainly to the fact that the vast majority of travel providers offer only this payment method. Visa had a market share of about 66%, Mastercard of 34%.

3.2.3 The risk of fraud and non-payment in online credit-card transactions

Concepts for measurement

The analysis of non-payment risk is restricted to purchases in which credit card payment was used (81% of all payments). In case of credit card payment, risks are inherent in the card-not-present (CNP) domain, where the merchant has to decide whether to accept or reject a credit card payment that is based only on the order information (name and address) given by the purchaser and the credit card details (card number, expiry date, verification number) supplied.

Pago has calculated non-payment risk based on two decisive parameters: the success rate and the chargeback ratio.

The **chargeback ratio** is defined simply as the proportion of credit card transactions in which the cardholder objects to a payment thereby causing the payment to be reversed. There can be various reasons for such an objection: The cardholder can object to a payment because:

- he did not execute the transaction himself;
- he may not have received the goods as ordered;
- or (s)he may have returned the goods to the merchant (e.g. because of transport damage, or non-compliance with the order).

The first case is more often than not a case of attempted fraud. In the pioneer years of e-commerce, a large proportion of this kind of fraud was actually attempted by cardholders themselves. However, in recent years, fraudsters have stepped in, illegally obtaining credit card details, and then systematically defrauding online merchants. The chargeback ratio remains an accurate measure of successful fraud attempts.

The so-called '**success rate**', on the other hand, is more difficult to understand conceptually. The starting point of a credit card transaction is the authorisation, resulting finally in the successful collection of the payment amount. All credit card transactions, were further examined, looking at if and at what attempt authorisation was successful. Authorisation is successful if the given details match the system's details. The degree of matching, however, is largely dependant on the individual credit card brands and varies with their authorisation procedures. Successful transactions are defined as those that are successfully authorised in the second attempt, at latest. The success rate (or, inversely, the 'failure' rate) does not, therefore measure fraud, but is rather a criterion to measure the effectiveness of fraud prevention mechanisms.

The combination of success rate and chargeback ratio allows the most accurate conclusions about non-payment risk to be drawn. A high success rate combined with a low chargeback ratio indicates little attempted fraud, whereas a low success rate and a high chargeback ratio point to a large proportion of successful fraud attempts.

Reasons for credit card objections

The analysis of credit card payment objections shows that the most common reason is incorrect authorisation, for example because of a missing or incorrect verification number. However, the relative percentage has decreased compared to 2003, which indicates that cardholders have got used to this mechanism thus making fewer mistakes by users.

The percentage of 'suspected interference', although still small, has increased. This happens when credit card details do not match with the address details given, thereby indicating that this value is probably an accurate measure of unsuccessful fraud attempts.

Exhibit 3-18: Reasons for credit card transaction rejections (in % of rejected transactions)

Rejection reason	2004	2003
Authorisation rejected	56	62
Card blocked	15	13
Suspected interference	7	4
Card invalid	4	4
Card stolen	1	1
Expiration date exceeded	1	1
Verification number not set or invalid	1	3
Other	11	10
Total	100	100

Source: Pago eTransaction Services (Pago Report 2005)

Success rates and charge back rates

The comparative overall success rate for accomplishing credit card payments in the shops monitored in 2004 was about 73%, up from 66% in 2003. The overall chargeback rate remained nearly unchanged at 0.8% (both in 2003 and 2004). The figures are situated in a scenario of 'medium success rate / medium chargeback rate'.

Exhibit 3-19: Success rate and chargeback ratio categories

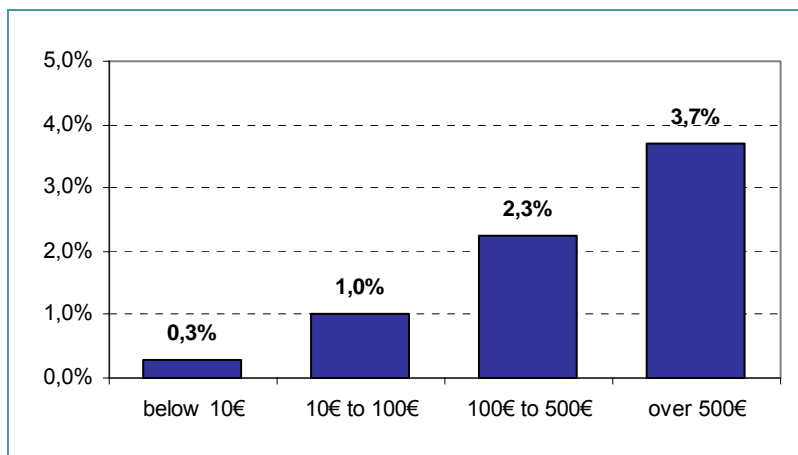
Category	Success rate	Chargeback rate
low	less than 70%	less than 0.5%
medium	70% - 90%	0.6% - 1.0 %
high	more than 90%	more than 1.0%

Source: Pago eTransaction Services (Pago Report 2005)

This indicates that there was an average amount of attempted fraud with relatively good fraud prevention mechanisms in place.

However, analysis of chargeback rates in combination with transaction values shows an interesting and alarming trend. Compared with a (satisfactory) overall chargeback rate of 0.8%, the figure for transactions of between 100€ and 500€ is 2.3% and 3.7% for transactions in excess of 500€.

Exhibit 3-20: Chargeback rates by transaction values



Source: Pago eTransaction Services (Pago Report 2005)

This means that 37 out of every thousand transactions of over 500€ result in chargebacks. This is obviously a timely reminder to companies which offer goods in this price segment or allow shopping carts to add up to these kinds of totals, to make sure that proper anti-fraud mechanisms are in place.

Summary

The Pago Report 2005 presents a statistical analysis of around 20 million real purchase transactions which were processed through the Pago payment platform in 2004.

- In total, about 80% of electronic payments were made by credit card. However, there are considerable variations in the relative importance of **e-payment methods** by sector, by country and depending on the amount to be paid. Payments by UK consumers and by those from outside Europe for purchasing goods in European online shops are only made by credit card. Among German users, in contrast, processing payments by electronic direct debit is more popular than using the credit card online.
- The **average transaction value** of e-payments differed significantly by sector. The average value was highest in the e-travel sector (190€), e-retailing purchases averaged at 63€ per transaction, online gambling 54€ and telecommunication services 33€. The average value of e-health transactions was higher (108€).
- The comparative overall **success rate** for accomplishing credit card payments in the shops monitored in 2004 was about 73%, up from 66% in 2003.
- Analysis of **chargeback rates** in combination with transaction values shows an interesting and alarming trend. Compared with a (satisfactory) overall chargeback rate of 0.8%, the figure for transactions of between 100€ and 500€ is 2.3% and 3.7% for transactions in excess of 500€. This means that 37 out of every thousand transactions of over 500€ result in chargebacks, possibly due to fraud.

4 Policy conclusions

4.1 Information and network security

4.1.1 Policy objectives and measures

As part of the Lisbon process, the European Commission has in recent years set a high priority on strengthening the security of ICT applications and their use. This priority was particularly apparent in the eEurope 2002 and the eEurope 2005 Action Plans.⁶³

In January 2002, the European Union Council of Ministers adopted a resolution “*on a common approach and specific actions in the area of network and information security*”. This Resolution defines a common European strategy and identifies a number of targets and deadlines for policy. In January 2003 the EU took a further step through the Council Resolution on a European approach towards a culture of network and information security.

The concept of a “culture of security”⁶⁴ was introduced by the OECD to emphasise the recognition that countering security threats is not merely a matter of improving technological responses but must involve business and society in a much wider way. The OECD approach includes both “*security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks*”.

The view is comprehensive, network and information security is taken to mean that every single part of interconnected networks, from the single household to large enterprises and the government, is secure. The intended culture of security is to engender trust among ICT users, to ensure continued and increased use of these technologies by enterprises and their customers.

The challenge is seen as maintaining the functioning of global ICT infrastructure. This infrastructure is highly critical to the operation of society generally, as it underlies the functioning of other critical systems such as energy, transportation, and financial networks. Secure ICT infrastructure is also highly critical to European enterprise, as e-Business connectivity and the functioning of multiple business processes is increasingly dependent on reliable public ICT infrastructure.

4.1.2 Policy deficits and requirements

Current policy across the EU consists of a fragmented set of initiatives. This signals a need for action to ensure that successes of national programmes are promoted across the EU, and adopted into EU policy instruments where appropriate. Such a pan-European approach should address all aspects of the requisite culture of security, taking into account the specific structure of European industry and paying special attention to the difficulties which companies, SMEs in particular, have in defending their systems against growing ICT security threats (see sections 2.1.2 , 2.2.2 and 2.3 above).

Policies have to take the evident conflicts of goal in the domain fully into account; for example, cybercrime can lead to severe financial loss. Combating cybercrime, however, tends to impose constraints on business freedom and potentially prejudices the privacy of business information. In particular, interception of communication may be desirable for prosecution and prevention as well as the ability to access communication content, reducing the ability to protect such content.

Policies should promote improvement in the awareness and understanding of risks across all sector players. It may be that benchmarking exercises or other models of exchange of best practice between **sectors** would be profitable, in parallel with an exchange of best practice at national level in respect of

⁶³ The eEurope 2002 Action Plan was agreed by Heads of State and Government in Feira in June 2000. In May 2002, the Commission adopted a follow-up Action Plan to eEurope 2002, eEurope 2005 (COM(2002) 263 final), running from 2003 to 2005.

⁶⁴ OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, 2002. OECD

policy measures. Such activities would help improve our understanding of the variation across sectors of the incidence of damage from security-related sources and in this way enable one sector to profit from lessons learned in another. For example, improving understanding of the way companies in the automotive sector reduce damage from software malfunction may be found useful by their counterparts in, say, machinery and equipment manufacture (compare section 2.1.4 above).

4.1.3 Possible actions

General measures to improve the culture of security

Policy measures already initiated in Europe, based on the goal of achieving a culture of security, include the setting up of a task force and a security agency. The European Union Council requested that the Commission set up a Cyber Security Task Force to “*build on national efforts to both enhance network and information security and to enhance Member State’s ability, individually and collectively, to respond to major network and information security problems*”.

In 2003, the European Commission adopted a proposal for a regulation establishing a European Network and Information Security Agency (ENISA). This agency is to help increase information exchange and co-operation between different stakeholders in Europe, with the aim of ensuring a high level of network and information security within the Community and to contribute to the development of a culture of network and information security. ENISA has now taken up operational work from headquarters in Heraklion (Crete, Greece).

Measures to achieve a culture of security include

- raising ICT users’ **awareness** and responsibility⁶⁵ through information campaigns, education and training and promotion of best practice;
- ENISA has an advisory and **co-ordination** role to ensure international functions are provided⁶⁶;
- public / private co-operation, more specifically an **information exchange** between public and private units, to accelerate legislation, standardisation and certification procedures;
- regular review and updating of the **legal framework** for e-security to adapt to changing requirements;
- a European **Warning and Information System** incorporating CERTs (Computer Emergency Response Teams) to react directly to possible e-security threats;
- Ensuring that necessary **R&D** into security components is carried out and that security products, such as encryption software, are freely available and affordable.

Specific measures to improve enterprise ICT security

Apart from addressing the requirements mentioned in the previous section, there is a need to coordinate and better profit from national initiatives, e.g. British Standard BS 77993, which helps organisations to assess their information security procedures as well as the ones of their partners, and the handbooks developed by the BSI, the German public information security institute. The baseline BSI security handbook provides industry with a detailed approach to risk management. The UK Department of Trade and Industry provides a useful input to enterprise-level risk analysis by regularly sponsoring surveys on security breaches to help businesses in risk assessment (www.dti.gov.uk/industries/information_security).

Standards for risk analysis, security controls and management can significantly reduce the cost to enterprises of proper security policy implementation. Standardisation here can reduce the decision

⁶⁵ Network and Information Security: Proposal for a European Policy Approach, 2001. European Commission, p.15/16

⁶⁶ Establishing the European Network and Information Security Agency: Proposal for a regulation of the European Parliament and of the Council, February 2003. European Commission

load on management to acceptable levels for smaller enterprises. The adoption of standards by software and service suppliers will increase competition and market size, reducing the cost of solutions to customer enterprises as economies of scale are passed on.

Standards can be agreed through a number of channels. The working group ISO / IEC JTC1/SC27 has the remit to standardise IT security methods and techniques, including risk assessment. An alternative channel for standards in Europe is through the work of CEN, potentially taking effect through a CEN Workshop Agreement. Given the danger of increasing costs of compliance, these costs should continue to be monitored in the standardisation process. European or global standards can draw on national initiatives, e.g. on work sponsored by the UK Department of Trade and Industry in 2004 on standardising risk analysis methods and metrics.

An example from the USA might be followed, where the Homeland Security Secretariat is supporting the extension of **quality processes** to the field of security. The so-called "Baldrige processes" are designed to support on-going improvement of quality in manufacturing in multiple sectors. The planned extension to security is to support improvement of quality through the measurement of organisational risk-preparedness. This enterprise-level action is seen as complementing ICT infrastructure security, itself an objective of US national security policy⁶⁷.

A set of possible measures specifically addressing enterprise ICT security in Europe is the following:

- promoting **exchange of best practice** in measures addressing ICT security at national level across the EU;
- strengthening national initiatives to improve **awareness** on security issues among employees and to develop and consolidate a culture of security in the workplace;
- encouraging **benchmarking** and exchange of best practice between sectors of European industry in respect of measures to counter security threats, to accelerate introduction of secure digital communication and to reduce the rate of failure of mission-critical software packages;
- supporting **international dialogue** on regulation and legislation which impact on enterprise security measures and
- ensuring that the impact on enterprises, particularly SMEs, in terms of the **cost of compliance**, is fully taken into account in legislative action.

Other possible public sector responses which have been identified in specific areas of survey results include the following:

- In light of the low use of encryption and its critical role in avoiding high risks in current distributed and mobile ICT use, **small enterprises** should be strongly encouraged to mandate use of encryption by their employees in data storage and transmission.
- The low levels of provision of **specific training to staff** could be investigated further to understand better the costs and benefits as seen by enterprise management. Potentially there is a role for public sector policy to explore training options and communicate findings on optimal training approaches, or to encourage exchange of best practice in training.
- Current patterns of use of **PKI and encryption** are difficult to interpret in terms of potentially sector-specific practice and circumstances, calling for **more detailed research** into sectoral practice and management planning.
- The low level of use of security controls among SMEs could be addressed by further or more **rapid standardisation** and promotion of conformant products to improve the cost-benefit equation for SMEs. Another technique might be to promote inter-enterprise cooperation and the sharing of resources.

⁶⁷ Network and Information Security: Proposal for a European Policy Approach, 2001. European Commission, p.4

Action to be taken at enterprise level

To address their increasing vulnerability to security threats, enterprises should carry out a risk assessment and introduce appropriate measures or controls. To address their increasing vulnerability to security threats, enterprises should carry out a risk assessment and introduce appropriate measures or controls. The international standard ISO 17799:2005⁶⁸ recommends the introduction of a security management system (SMS)⁶⁹, comprising risk assessment and control deployment, in enterprises of all sizes.

Risk assessment means taking into account the damage each breach of security could wreak, up to causing the business to fail. Critical areas of operation are identified, the types of threat which might prejudice these activities are identified and the level of threat determined. This risk assessment step is then basis for selecting appropriate security controls, taking account of cost – payoff considerations. Implementation of controls and continuous review of risks and controls completes the security management system.

Various steps in the introduction of an SMS can require support. For instance, risk analysis and assessment is difficult when the incidence of threats is not known. Insurers can be a source of information about the level of threat. CLUSIF⁷⁰ was set up by French insurers to provide risk analysis method with metrics, using data on real incidence of damage. Statistics can be provided on very specific categories of threat and damage such as the failure of telecommunications relay, switching or cellular base stations due to flood.

Business continuity planning is part of an SMS and consists of a set of measures to ensure that an organisation remains operational after an ICT failure. This is not the same as disaster recovery planning, which is complementary and also required, and consists in organising recovery activities when disaster has happened.

The following table summarises proposed policy measures relating to improving EU enterprise ICT security.

⁶⁸ ISO/IEC 17799:2005: Information technology – Security techniques – Code of practice for information security management.

⁶⁹ ISO/IEC 27001:2005: Information technology - Security techniques - Information security management systems - Requirements.

⁷⁰ Club de la sécurité des systèmes d'information français.

Policy objective	Suggestions for policy actions	Potential initiator(s)
Improve enterprise-level ICT security	<ul style="list-style-type: none"> Promote exchange of best practice in measures addressing ICT security at national level across the EU; Strengthen national initiatives to improve awareness on security issues among employees and to develop and consolidate a culture of security in the workplace. 	Regional and national government
	<ul style="list-style-type: none"> Encourage benchmarking and exchange of best practice between sectors of European industry in respect of measures to counter security threats, to accelerate introduction of secure digital communication and to reduce the rate of failure of mission-critical software. 	EU, e.g. through e-BSN
	<ul style="list-style-type: none"> Accelerate standardisation and standards adoption in the area of ICT security and promote conformant products. 	Industry associations ICT services industry
	<ul style="list-style-type: none"> Ensure that the impact on enterprises, particularly SMEs, in terms of the cost of compliance, is fully taken into account in legislative action. 	National and regional government, EU (directives)
	<ul style="list-style-type: none"> Encourage SMEs to mandate use of encryption by their employees in data storage and transmission, e.g. by publishing interviews with best practice SME managers and articles illustrating dangers. 	Business intermediaries (chambers of commerce, associations)
	<ul style="list-style-type: none"> Support international dialogue on regulation and legislation which impact on enterprise security measures 	European Network and Information Security Agency (ENISA)

4.2 Promoting the diffusion of electronic billing, invoicing and payments

The opportunities that arise from developments in the area of electronic invoicing have some implications for policy and, broadly speaking, for the public sector as a whole. It is strongly recommended that public authorities on all levels from local to European, should consider whether and how to use e-invoicing themselves in order to save costs. In addition, particularly at the European level, monitoring and benchmarking activities could stimulate the transfer of best practices and thus promote the uptake of electronic invoicing throughout the EU.

Policy objective	Suggestions for policy actions	Potential initiator(s)
Save costs in the public sector through e-invoicing	<ul style="list-style-type: none"> Consider strategies for introducing e-invoicing in the public sector. 	Regional and national governments
	<ul style="list-style-type: none"> Monitor and assess e-invoicing related policy initiatives; Exchange of experiences between member states in policy networks; Promote transfer of best practices. 	EU as the coordinator (e.g. through e-BSN) Member states / regional representatives as participants in networks
Promote and accelerate adoption of e-invoicing and e-payment activity among enterprises	<ul style="list-style-type: none"> Public sector can act as a first-mover and role model by introducing e-invoicing; Check existing legal frameworks in terms of their compliance with e-invoicing developments and consider adaptations, if necessary. 	Regional and national governments EU (as far as implementation of relevant EU directives by member states is concerned)
	<ul style="list-style-type: none"> Promote standardisation and interoperability, as much as possible on a European level. 	Business intermediaries (chambers of commerce, associations) to coordinate and promote agreements Software vendors (e.g. of ERP systems)

Consider options for electronic billing and invoicing in the public sector

It has often been stated with regard to electronic procurement that the public sector could or should act as role model and, thus, stimulate the use of ICT by enterprises. The same consideration applies to the electronic processing of invoices, which can be considered as part of procurement related processes.

Motivation for the public sector to start processing invoices electronically is high. All evidence currently available concludes that electronic billing and invoicing offers a substantial and realistic potential to save costs. If this is the case, then the public sector is obliged to consider approaches for exploiting this potential, given the huge number of invoices treated by governments.

It is unlikely that the same approach will work in all regions and countries. The existing regulatory frameworks, for example with regard to the use of digital signature, and differences between EU member states in their administrative structures, will call for different strategies and approaches. A

radical approach such as adopted by Denmark (see chapter 1.2.3) may work in this country, but not necessarily in another.

Therefore, a specific approach neither can nor should be recommended; regional and national governments will have to consider different options for themselves and decide on the appropriate **strategy that fits best the legal and cultural specificities**. The European Commission could act as a coordinator for the exchange of experiences and best practices between Member States in this context.

Monitoring, best practice identification, coordination

Since e-invoicing is a rather recent development (if EDI is not considered), there is still a lot of uncertainty of what will be the best way to introduce it. **Monitoring, benchmarking and the identification of 'good practices'** are all useful instruments to promote successful national and regional programmes in the area of e-invoicing. The European Commission has a role in coordinating such activities at the European level and in facilitating the transfer of lessons learned between Member States.

The e-Business Support Network (www.e-bsn.org), a policy-makers forum established and sponsored by the European Commission, DG Enterprise & Industry, has already recognised the importance of the topic and started relevant activities in this domain. It is recommended that these activities are continued, since electronic billing and invoicing could be a topic where the approach of the e-BSN fits very well and helps to accentuate the European dimension of the issue.

Besides promoting good practices, policy has also a role in supporting and **coordinating standardisation** processes on the European level. It was pointed out in this report that a lack of standards could lead to national systems for electronic invoicing and payments and thus hamper the use in international trade. Banks, for example, are currently working on their national standards for e-invoicing, which could replicate a situation that existed for making payments to another country. Ideally, electronic invoicing and payment systems have a great potential to facilitate cross-boarder trade within the European Union, in particular for SMEs. To achieve this potential, however, requires international coordination and agreement on standards. European and national business organisations, such as chambers of commerce and trade associations, certainly have a role here in coordinating and promoting agreements on common interfaces. Software companies, for example vendors of ERP systems, should be consulted and integrated in this process.

References

- Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (30.04.2004)
- Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (30.04.2004).
- Directive 1999/93/EC of the European Parliament and the Council of the European Union (Electronic Signature Directive).
- Electronic Invoice Presentment and Payment (EIPP): A Win-Win Proposition. White Paper by CheckFree iSolutions (2003), www.checkfree.com
- "Elektronische Rechnung spart Milliarden", Computerwoche, 14 Dec. 2004, www.computerwoche.de (July 2005)
- "ERP auf Electronic Payment gefasst", Computerwoche, 24 Feb. 2003, www.computerwoche.de (July 2005)
- European Commission (2004a). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Action plan for the implementation of the legal framework for electronic public procurement. 13 December 2004.
- European Commission (2004b). Commission Staff Working Document: Impact Assessment of the Commission on an Action Plan on electronic public procurement. 13 December 2004
- European Commission (2003). Establishing the European Network and Information Security Agency: Proposal for a regulation of the European Parliament and of the Council, February 2003.
- European Commission (2001a). Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 2001.
- European Commission (2001b). Impact and Priorities - A communication to the Spring European Council in Stockholm, 23-24 March 2001 - Communication to the European Parliament and the Council, 2001.
- European Commission (2001c). Network and Information Security: Proposal for a European Policy Approach, 2001. European Commission, p.5-12.
- European Parliament and the Council (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.
- European Parliament and the Council (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, 2002. OECD
- Pago-Report 2005: Success and risk factors in international E-payment. Recommendations on real purchasing transactions in 2004. Published by Pago eTransaction Services GmbH.
- ROI through Electronic Invoice Presentment and Payment (EIPP). White Paper by CheckFree iSolutions (2003). Available online at www.newmetrics.co.uk/downloads/pdf/ROIThroughEIPP.pdf (July 2005)

Web based resources

- **Fact-box**, chapter 1.2.2, example "industrial espionage":
 - <http://informationweek.com/story/showArticle.ihtml?articleID=163702020>
 - <http://www.ynetnews.com/articles/0,7340,L-3091900,00.html>
 - <http://www.computerweekly.com/Articles/2005/06/07/210254/FirmswarnedtheymaybetargetsofTrojanspies.htm>

- **Fact-box**, chapter 1.2.2, example Pgp coder
 - http://news.zdnet.com/2100-1009_22-5718678.html
 - <http://www.newscientist.com/article.ns?id=dn7426>
 - <http://abcnews.go.com/Technology/wireStory?id=787172&CMP=OTC-RSSFeeds0312>

Annex I: The e-Business Survey 2005 – Methodology Report

The *e-Business W@tch* collects data on the use of ICT and e-business in European enterprises by means of representative surveys. The e-Business Survey 2005, which was the third survey after those of 2002 and 2003, had a scope of 5,218 telephone interviews with decision-makers in enterprises from seven EU countries (Czech Republic, France, Germany, Italy, Poland, Spain and the UK).⁷¹ Interviews were carried out in January and February 2005, using computer-aided telephone interview (CATI) technology.

Questionnaire

The general design of the questionnaire builds on the ones used in the previous surveys of 2002 and 2003 in order to ensure a basic continuity of the research approach. However, new modules on security and interoperability have been added, while other modules have been reduced (mostly the ones on perceived impacts of e-business, where little new evidence was to be expected compared to the findings of 2003).

New questions were also introduced in the e-commerce related modules, reflecting the developments in electronic business and changing perspectives in research, in particular the emphasis on electronic business processes. An important focus of the 2005 survey was on the use of ICT systems to support e-procurement and online sales processes. These questions complement the previously used questions on online purchasing and selling activity.

The questionnaires of all three surveys (2002, 2003, 2005) can be downloaded from the *e-Business W@tch* website at www.ebusiness-watch.org/about/methodology.htm.

Population

In contrast to the surveys of 2002 and 2003, the 2005 survey considered only **companies that used computers**. Thus, the highest level of the population was the set of all computer-using enterprises which were active within the national territory of one of the 7 countries covered, and which had their primary business activity in one of the 10 sectors specified on the basis of NACE Rev. 1.1 categories.

Evidence from previous surveys shows that this does not make a noticeable difference for medium-sized and large firms, as the share of firms that use computers can be expected to be 99% or more in all sectors and countries covered. Differences are relevant, however, for micro and small enterprises, in particular in the food and beverages industry, the textile industry, construction and tourism. In these four sectors, 10-30% of micro enterprises and 4-15% of small firms (depending on the country and sector) do not use a computer.⁷² Therefore it makes a difference if a figure represents a percentage of "all companies" (as in 2003) or a percentage of "companies using computers" (as in 2005). Differences are much less pronounced, though, when figures have been weighted by employment.

The 10 sectors that have been selected for the 2005 survey are extremely heterogeneous in terms of their size. Construction is by far the largest with about 2.3 million enterprises in the EU-25. At the other end of the range are the aerospace and pharmaceutical industries with only about 2,200 and 3,900 firms respectively in the EU-25. This is a factor of about 100 between the largest and smallest sector. This imbalance has clearly implications for the achievement of survey quota and the impact of weighting on sector data and on aggregate results.

⁷¹ These seven countries are frequently referred to as the "EU-7" in this report. They account for roughly 75% of the EU-25 population and GDP.

⁷² Non-computer users include typically small craft firms (textile, construction), bars, restaurants or pensions (in tourism), and small food producing companies.

Table 1: Population coverage of the e-Business Survey (2005)

No.	NACE Rev. 1.1		Sector name (as used by <i>e-Business W@tch</i>)
	Section	Division / Group	
01	DA	15	Manufacture of food products and beverages
02	DB	17, 18	Manufacture of textiles (17), wearing apparel; dressing & dyeing of fur (18)
03	DE	22	Publishing, printing and reproduction of recorded media
04	DG	24.4, 24.5	Manufacture of pharmaceuticals (24.4), soap and detergents, cleaning and polishing preparations, perfumes and toilet preparations (24.5)
05	DK	29.1 – 29.5	Manufacture of machinery and equipment (not included: Manufacture of weapons and ammunition, domestic appliances)
06	DM	34	Manufacture of motor vehicles, trailers and semi-trailers
07	DM	35.3	Manufacture of aircraft and spacecraft
08	F	45	Construction
09	H, I, O	55, 62.1, 63.3, 92.3+5	Tourism, including hotels and restaurants (55), parts of air transport (62), travel agencies and tour operators (63.3), and parts of recreational, cultural and sporting activities (92)
10	K	72	Computer and related activities

Sampling frame and method

No cut-off was made in terms of minimum size of firms. The sample drawn was a random sample of companies from the respective sector population in each of the seven countries, with the objective of fulfilling minimum strata with respect to company size class per country-sector cell. Strata were to include a 10% share of large companies (250+ employees), 30% of medium sized enterprises (50-249 employees), 25% of small enterprises (10-49 employees) and up to 35% of micro enterprises with less than 10 employees. Samples were drawn locally by fieldwork organisations based on widely recognized business directories and databases (see Table 2).

Table 2: Directories from which samples were drawn (2005)

Country	Directory / database	
CZ	Czech Republic	Albertina Business Database (database of economic subjects with >1m entries)
DE	Germany	Heins und Partner Business Pool
ES	Spain	Dun & Bradstreet
FR	France	SIREN file from INSEE (the French National Statistics Institute)
IT	Italy	Dun & Bradstreet
PL	Poland	Kompass Polska
UK	United Kingdom	Dun & Bradstreet

The survey was carried out as an enterprise survey: data collection and reporting focus on the enterprise, defined as a business organisation (legal unit) with one or more establishments. In some of the sectors, target quota in the larger enterprise size-bands could not be accomplished in each of the countries. In these cases, interviews were shifted to the next largest size-band (from large to medium-sized, from medium-sized to small).

Fieldwork

Fieldwork was coordinated by the German branch of Ipsos GmbH (www.ipsos.de) and conducted in cooperation with its local partner organisations (see Table 3) on behalf of *e-Business W@tch*. Pilot interviews prior to the regular fieldwork were conducted with 12 companies in Germany in December 2004, in order to test the questionnaire (structure, comprehensibility of questions). The survey had a scope of 5,218 interviews, evenly spread across the seven countries covered. About 565 interviews per sector were conducted (see Table 4), except for the aeronautics and the pharmaceutical industry. Due to the small population of firms in these sectors, it was not possible to achieve the target quota. In the aerospace industry, only 163 company interviews could be realised in the seven countries covered. In this sector, practically the entire population of companies was contacted.

Table 3: Market research companies having conducted the fieldwork in the e-Business Survey 2005

Country	Fieldwork organisation
CZ	Czech Republic
DE	Germany
ES	Spain
FR	France
IT	Italy
PL	Poland
UK	United Kingdom

Table 4: Number of interviews conducted by sector and country (2005)

Sector	CZ	DE	ES	FR	IT	PL	UK	TOTAL
Food and beverages	85	80	82	80	86	83	75	571
Textiles and clothing	85	76	81	80	81	83	75	561
Publishing and printing	84	80	82	80	79	83	75	563
Pharmaceutical industry	54	83	81	76	81	82	75	532
Machinery and equipment	85	80	81	77	84	83	75	565
Automotive industry	85	80	81	80	81	83	75	565
Aerospace industry	20	38	15	39	23	3	25	163
Construction	84	81	83	80	80	83	75	566
Tourism	84	80	82	80	82	83	76	567
Computer related services	84	80	82	78	82	84	75	565
TOTAL	750	758	750	750	759	750	701	5218

Table 5: Interview contact protocol: completion rates and non-response reasons (2005)

		CZ	DE	ES	FR	IT	PL	UK	Total
1	Sample (gross)	2632	7247	8796	10123	5082	7825	13104	54809
1.1	Telephone number does not exist	126	880	680	373	340	959	870	4228
1.2	Not a company (e.g. private household)	42	130	220	200	44	214	115	965
1.3	Fax machine / modem	40	56	10	0	359	248	116	829
1.4	Quota completed > address not used	191	361	3357	1623	351	1161	3856	10900
1.5	No target person in company	57	344	186	98	72	109	691	1557
1.6	Language problems	2	16	14	14	1	0	0	47
1.7	No answer on no. of employees	10	8	3	1	0	0	8	30
1.8	Company does not use computers	11	80	194	332	41	30	567	1255
	Sum 1.1 – 1.8	479	1875	4664	2641	1208	2721	6223	19811
2	Sample (net)	2153	5372	4132	7482	3874	5104	6881	34998
2.1	Nobody picks up phone	212	366	335	892	1080	1333	6	4224
2.2	Line busy, engaged	60	52	6	68	60	438	0	684
2.3	Answering machine	42	133	20	1208	79	137	463	2082
2.4	Contact person refuses (refusal at reception, switchboard)	472	931	2010	2024	755	1613	1695	9500
2.5	Target person refuses	388	2125	184	693	142	122	2591	6245
2.6	No appointment during fieldwork period	42	13	395	202	0	261	298	1211
2.7	Open appointment	77	935	363	1584	968	371	1008	5306
2.8	Target person is ill / not available	10	3	47	0	2	0	0	62
2.9	Interview abandoned	91	56	22	57	28	79	119	452
2.10	Interview error, cannot be used	9	0	0	4	1	0	0	14
	Sum 2.1 – 2.10	1403	4614	3382	6732	3115	4354	6180	29780
3	Successful interviews	750	758	750	750	759	750	701	5218
	Completion rate (= [3] / [2])	34.8%	14.1%	18.2%	10.0%	19.6%	14.7%	10.2%	14.9%
	Average interview time (min : sec)	17:07	19:06	17:29	17:15	20:51	21:15	19:53	19:00

Non response: In a voluntary telephone survey, in order to achieve the targeted interview totals, it is always necessary to contact more companies than just the number equal to the target. In addition to refusals, or eligible respondents being unavailable, any sample contains a proportion of "wrong" businesses (e.g., from another sector), and wrong and/or unobtainable telephone numbers. Table 5 shows the completion rate by country (completed interviews as percentage of contacts made) and reasons for non-completion of interviews. Higher refusal rates in some countries, sectors or size bands (especially among large businesses) inevitably raises questions about a possible refusal bias. That is, the possibility that respondents differ in their characteristics from those that refuse to participate. However, this effect cannot be avoided in any voluntary survey (be it telephone- or paper-based).

Feedback on the fieldwork

No major problems were reported from the fieldwork with respect to interviewing (comprehensibility of the questionnaire, logical structure). The overall feedback from the survey organisations was that fieldwork ran smoothly and that the questionnaire was well understood by most respondents. The main challenge was the fulfilment of the quotas, which was difficult or impossible in some of the sectors, in particular among the larger size-bands. Specific remarks from fieldwork organisations, however, point at some differences in the local situation (see Table 6).

Table 6: Comments by national fieldwork companies on their experience (2005)

Country		Comments
CZ	Czech Republic	<ul style="list-style-type: none"> It was more difficult to complete interviews with very small companies. They were less willing to participate in an interview. Respondents often felt that questions about a firm's profit or turnover are not adequate. The interviewers mentioned that these questions were several times a cause of abandoning the interview.
DE	Germany	<ul style="list-style-type: none"> In total fieldwork ran smoothly and the questionnaire was easy to understand and interesting for most of respondents. Answering the question about turnover as well as the investment on ICT was often problematic for the respondents and yielded a high proportion of non-replies. Respondents of small companies often had difficulty in answering questions related to specific technical terms and application. In cases where they used only one or few computers, some questions (e.g. regarding networks) were not relevant for them. Positive resonance comes from the respondents when they know that the survey is being done on behalf of the European Commission. The reference to the website at the end of the interview was welcome and helpful.
ES	Spain	<ul style="list-style-type: none"> Interviews in very small companies were more difficult to complete due to the lack of knowledge about ICT. On the other hand, the participation of respondents in big companies was difficult to achieve. Generally the questionnaire was easy to understand. About a quarter of the firms contacted have subcontracted most of their ICT tasks, which made it difficult for the respondents to answer specific technical questions. Questions regarding the turnover and investments were difficult to answer for the respondents and yielded a high proportion of don't know responses. This is also often experienced in other B2B surveys.
FR	France	<ul style="list-style-type: none"> Small companies often do not have much ICT equipment. Respondents therefore sometimes had difficulty in answering some of the questions, since the questionnaire was not adapted to these companies. Small companies often answered "don't know" to more detailed questions. Respondents from larger companies had difficulty answering questions concerning turnover, benefits and other financial issues. These questions would be better put to somebody from the financial department. As more and more companies outsource their IT department, it is difficult to identify a responsible person within the company to answer the questions.

IT	Italy	<ul style="list-style-type: none"> • The questionnaire was considered long, but quite easy to answer. • However, a few sections (mainly D and E) were considered more complicated than others. In particular technical terms that referred to security and to online services were difficult to understand. • Interviews were carried out without any problems in medium-sized enterprises where it is easier to identify and contact an IT manager. Those respondents had the best grasp of what was being talked about in the interview. • The financial questions were difficult to answer for most of the respondents, especially the question on ICT investments.
PL	Poland	<ul style="list-style-type: none"> • Respondents from small companies often had difficulties in answering questions related to specific technical applications. • Companies are quite reluctant to provide financial information, so respondents often answer DK to the financial questions. • In many companies, IT people are not allowed to say anything about internal matters of the company. • Many companies outsource their IT department and its activities.
UK	United Kingdom	<ul style="list-style-type: none"> • As with previous surveys carried out in the context of the <i>e-Business W@tch</i> programme, fieldwork ran relatively smoothly. • However, the anticipated strike-rate was severely affected by the substantial length of the interview (20 minutes). • Gathering turnover and investment details again yielded a high proportion of don't know responses. • As a final point, it is becoming increasingly difficult to secure interviews with IT/DP professionals, and we suspect that this situation will only worsen in the future.

Weighting schemes

Due to stratified sampling, the sample size in each size-band is not proportional to the population numbers. If proportional allocation had been used, the sample sizes in the 250+ size-band would have been extremely small, not allowing any reasonable presentation of results. Thus, weighting is required so that results adequately reflect the structure and distribution of enterprises in the population of the respective sector or geographic area. *e-Business W@tch* applies two different weighting schemes: weighting by employment and by the number of enterprises.⁷³

- Weighting by employment: Values that are reported as employment-weighted figures should be read as "enterprises comprising x% of employees" (in the respective sector or country). The reason for using employment weighting is that there are many more micro-enterprises than any other firms. If the weights did not take into account the economic importance of businesses of different sizes in some way, the results would be dominated by the percentages observed in the micro size-band.
- Weighting by the number of enterprises: Values that are reported as "x% of enterprises" show the share of firms irrespective of their size, i.e. a micro-company with a few employees and a large company with thousands of employees both count equally.

The use of filter questions in interviews

In the interviews, not all questions were asked to all companies. The use of filter questions is a common method in standardised questionnaire surveys to make the interview more efficient. For example, questions on the type of Internet access used were only asked to those companies that had replied to have Internet access. Thus, the question whether a company has Internet access or not serves as a filter for follow-up questions.

⁷³ In the tables of this report, data are normally presented in both ways, except for data by size-bands. These are shown in % of firms within a size-band, where employment-weighting is implicit.

The results for filtered questions can be computed on the base of only those enterprises that were actually asked the question (e.g. "in % of enterprises with Internet access"), but can also be computed on the base of "all companies". In this report, both methods are used, depending on the indicator. The base (as specified in footnotes of tables and charts) is therefore not necessarily identical to the set of companies that were actually asked the underlying question.

Statistical accuracy of the survey: confidence intervals

Statistics vary in their accuracy, depending on the kind of data and sources. A "confidence interval" is a measure that helps to assess the accuracy that can be expected from data. The confidence interval is the estimated range of values on a certain level of significance. Confidence intervals for estimates of a population fraction (percentages) depend on the sample size, the probability of error, and the survey result (value of the percentage) itself. Further to this, variance of the weighting factors has negative effects on confidence intervals.

Table 7 gives some indication about the level of accuracy that can be expected for industry totals (EU7 totals based on all respondents) depending on the weighting scheme applied. For totals of all-sectors, an accuracy of +/- 2 percentage points can be expected for most values that are expressed as "% of firms", and of +/- 3 percentage points for values that are weighted by employment. The confidence interval for industry totals (EU-7) is about +/- 5 percentage points (in both weighting schemes). Employment-weighted results for the pharmaceutical, the automotive and the aeronautics industry have higher confidence intervals, because these sectors are more sensitive to weights due to their structure (i.e. the dominance of large firms in a comparatively small population). In the aeronautics industry, employment-weighted figures should not be used.

The calculation of confidence intervals is based on the assumption of (quasi-) infinite population universes. In practice, however, in some industries and in some countries the complete population of businesses consists of only several hundred or even a few dozen of enterprises. In some cases, literally each and every enterprise within a country-industry and size-band cell was contacted and asked to participate in the survey. This means that it is practically impossible to achieve a higher confidence interval through representative enterprise surveys in which participation is not obligatory. This should be borne in mind when comparing the confidence intervals of *e-Business W@tch* surveys to those commonly found in general population surveys.

Table 7: Confidence intervals for all-sector and sector totals (EU-7)

	Survey result	Confidence interval								
		Weighted by employment			Weighted as "% of firms"			Unweighted		
All sectors (aggregate), EU-7	10%	8.1%	-	12.2%	8.7%	-	11.5%	9.3%	-	10.7%
Food and beverages	10%	7.2%	-	13.8%	6.9%	-	14.3%	8.1%	-	12.3%
Textile industries	10%	7.4%	-	13.3%	6.9%	-	14.3%	8.1%	-	12.3%
Publishing and printing	10%	7.2%	-	13.7%	7.2%	-	13.8%	8.1%	-	12.3%
Manufacture of pharmaceuticals	10%	5.3%	-	18.0%	7.5%	-	13.1%	8.1%	-	12.4%
Manufacture of machinery and equipment	10%	6.5%	-	15.1%	7.1%	-	13.9%	8.1%	-	12.3%
Automotive industry	10%	4.6%	-	20.2%	7.7%	-	12.8%	8.1%	-	12.3%
Aerospace industry	10%	1.7%	-	41.3%	5.7%	-	16.9%	6.8%	-	14.6%
Construction	10%	7.7%	-	12.8%	7.0%	-	14.1%	8.1%	-	12.3%
Tourism	10%	7.2%	-	13.8%	6.9%	-	14.3%	8.1%	-	12.3%
IT services	10%	7.3%	-	13.6%	6.5%	-	15.2%	8.1%	-	12.3%
All sectors (aggregate), EU-7	30%	27.0%	-	33.2%	27.9%	-	32.2%	29.0%	-	31.1%
Food and beverages	30%	25.2%	-	35.2%	24.7%	-	35.9%	26.9%	-	33.3%
Textile industries	30%	25.7%	-	34.6%	24.7%	-	35.8%	26.9%	-	33.3%
Publishing and printing	30%	25.3%	-	35.1%	25.3%	-	35.2%	26.9%	-	33.3%
Manufacture of pharmaceuticals	30%	21.5%	-	40.2%	25.9%	-	34.4%	26.8%	-	33.4%
Manufacture of machinery and equipment	30%	23.9%	-	36.9%	25.1%	-	35.4%	26.9%	-	33.3%
Automotive industry	30%	19.9%	-	42.6%	26.3%	-	34.0%	26.9%	-	33.3%
Aerospace industry	30%	10.5%	-	61.0%	22.3%	-	39.0%	24.4%	-	36.2%
Construction	30%	26.3%	-	34.0%	24.9%	-	35.7%	26.9%	-	33.3%
Tourism	30%	25.2%	-	35.2%	24.7%	-	35.9%	26.9%	-	33.3%
IT services	30%	25.5%	-	35.0%	23.9%	-	36.9%	26.9%	-	33.3%
All sectors (aggregate), EU-7	50%	46.6%	-	53.4%	47.7%	-	52.3%	48.9%	-	51.1%
Food and beverages	50%	44.6%	-	55.4%	43.9%	-	56.1%	46.6%	-	53.4%
Textile industries	50%	45.2%	-	54.8%	44.0%	-	56.0%	46.5%	-	53.5%
Publishing and printing	50%	44.7%	-	55.3%	44.6%	-	55.4%	46.5%	-	53.5%
Manufacture of pharmaceuticals	50%	39.8%	-	60.2%	45.4%	-	54.6%	46.4%	-	53.6%
Manufacture of machinery and equipment	50%	42.9%	-	57.1%	44.4%	-	55.6%	46.5%	-	53.5%
Automotive industry	50%	37.7%	-	62.3%	45.8%	-	54.2%	46.5%	-	53.5%
Aerospace industry	50%	23.2%	-	76.8%	40.9%	-	59.1%	43.6%	-	56.4%
Construction	50%	45.8%	-	54.2%	44.1%	-	55.9%	46.5%	-	53.5%
Tourism	50%	44.5%	-	55.5%	43.9%	-	56.1%	46.5%	-	53.5%
IT services	50%	44.8%	-	55.2%	42.9%	-	57.1%	46.5%	-	53.5%
All sectors (aggregate), EU-7	70%	66.8%	-	73.0%	67.8%	-	72.1%	68.9%	-	71.0%
Food and beverages	70%	64.8%	-	74.8%	64.1%	-	75.3%	66.7%	-	73.1%
Textile industries	70%	65.4%	-	74.3%	64.2%	-	75.3%	66.7%	-	73.1%
Publishing and printing	70%	64.9%	-	74.7%	64.8%	-	74.7%	66.7%	-	73.1%
Manufacture of pharmaceuticals	70%	59.8%	-	78.5%	65.6%	-	74.1%	66.6%	-	73.2%
Manufacture of machinery and equipment	70%	63.1%	-	76.1%	64.6%	-	74.9%	66.7%	-	73.1%
Automotive industry	70%	57.4%	-	80.1%	66.0%	-	73.7%	66.7%	-	73.1%
Aerospace industry	70%	39.0%	-	89.5%	61.0%	-	77.7%	63.8%	-	75.6%
Construction	70%	66.0%	-	73.7%	64.3%	-	75.1%	66.7%	-	73.1%
Tourism	70%	64.8%	-	74.8%	64.1%	-	75.3%	66.7%	-	73.1%
IT services	70%	65.0%	-	74.5%	63.1%	-	76.1%	66.7%	-	73.1%
All sectors (aggregate), EU-7	90%	87.8%	-	91.9%	88.5%	-	91.3%	89.3%	-	90.7%
Food and beverages	90%	86.2%	-	92.8%	85.7%	-	93.1%	87.7%	-	91.9%
Textile industries	90%	86.7%	-	92.6%	85.7%	-	93.1%	87.7%	-	91.9%
Publishing and printing	90%	86.3%	-	92.8%	86.2%	-	92.8%	87.7%	-	91.9%
Manufacture of pharmaceuticals	90%	82.0%	-	94.7%	86.9%	-	92.5%	87.6%	-	91.9%
Manufacture of machinery and equipment	90%	84.9%	-	93.5%	86.1%	-	92.9%	87.7%	-	91.9%
Automotive industry	90%	79.8%	-	95.4%	87.2%	-	92.3%	87.7%	-	91.9%
Aerospace industry	90%	58.7%	-	98.3%	83.1%	-	94.3%	85.4%	-	93.2%
Construction	90%	87.2%	-	92.3%	85.9%	-	93.0%	87.7%	-	91.9%
Tourism	90%	86.2%	-	92.8%	85.7%	-	93.1%	87.7%	-	91.9%
IT services	90%	86.4%	-	92.7%	84.8%	-	93.5%	87.7%	-	91.9%

confidence intervals at $\alpha=.90$