D6.2 Executive summary and brief: The economic impact of cyber crime on non-ICT sectors

Deliverable submitted on 15 February 2016 in fulfilment of the requirements of the FP7 project, E-CRIME Economic Impact of Cyber Crime

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n°607775

ecrime The Economic Impacts of Cyber Crime	E-CRIME Coordinator:Trilateral Research Consulting (TRI)	Crown House 72 Hammersmith Road London W14 8TH	T: +44 207 559 3550	www.ecrime-project.eu

Project Acronym	E-CRIME
Project full title	The economic impacts of cyber crime
Website	www.ecrime-project.eu
Grant Agreement #	607775
Funding Scheme	FP7-SEC-2013-1
Deliverable number:	D6.2
Title:	Executive summary and brief: The economic impact of cyber crime on non-ICT sectors
Due date:	31/01/16
Actual submission date:	15/02/16
Lead contractor:	Delft University of Technology
Contact:	Michel van Eeten
Authors:	Michael Ciere Carlos Gañán Michel van Eeten
Reviewers:	TRI
Dissemination Level:	Public

Contents

Executive summary

Cyber crime is a problem that exists in our society and affects not only citizens but also all sectors and is driven by its profitability. Despite the increasing prevalence of cyber crime, the understanding of its economic impact is limited to cost estimates that do not capture all the repercussions that cyber crime imposes to society.

This study provides an assessment of the economic impact of cyber crime on non-ICT sectors. It is based on a theoretical framework that was published separately (D4.1 of the E-CRIME project). The current study concentrates largely on cyber threats identified as prominent by industry experts in these sectors. Different economic impacts have been measured using the E-CRIME survey of victims, industry interviews with cyber security experts and estimates of industry turnover and costs. Resource cost estimates for the criminal justice system have been derived using public budgets and selective interviews with relevant law enforcement agencies. Figures used in this reports represent estimates based on the best available evidence, but nevertheless they should be used cautiously.

A detailed description of the methodology used to construct these results can be found in D6.3 "Detailed appendixes on the economic impact of cyber crime on non-ICT sectors". However, a high-level description of the results is offered in this report.

In order to get a true picture of the impact of cyber crimes in the selected non-sectors, we assess the short-term implications and the long-term distortions for each of the five following non-ICT sectors.

Heath Care As information technologies like Electronic Health Records (EHRs) and patient and provider portals become standard issue in health care organizations, security breaches are escalating in frequency. Consequently, medical institutions are implementing physical and technical safeguards to guarantee the security of private-sensitive data. These security controls do not come for free and highly impact the productivity of practitioners in the sector. Hence the main economic impact of cyber crime in the

health care sector comes as *anticipation*. Unauthorised access to private-sensitive data represents the main security concern. However, the economic consequences of potential data breaches are often overshadowed by the costs of acquiring, implementing, and keeping up-to-date security controls in place. Altogether, cyber crime slows the adoption of EHR due to privacy and security concerns, reduces the productivity of the sector due to the extra security safeguards and obstruct data sharing among the different companies within the sector.

Financial Services Financial institutions were one of the earliest adopters of IT and, therefore, remain the most attractive target for cyber criminals. The sector is ahead of many industries in terms of prevention and detection of cyber incidents, but at the expense of deploying state-of-the-art security controls and, thus, reducing the productivity of their employees. However, despite the huge amount of investment to mitigate cyber crime, financial institutions are not exempt of its consequences. They suffer from different types of fraud, regulatory sanctions and litigation costs which altogether lead to revenue loss. Hence cyber crime imposes multiple long-term distortions in the sector: (i) the essential in-house knowledge of fraud and risk management creates an entry barrier; (ii) innovative services are delayed due to the uncertainty of potential risks, and (iii) consumers avoid some services due to fear of cyber crime.

Retail Online retailers represent a common target of cyber criminals due to massive amount of payment and customer information they handle. The investment on security controls highly varies across the different entities in the sector. Most of the costs come from complying with current regulations such as PCI DSS. A minority of retailers also acquire cyber insurances to cover potential losses due to cyber incidents. Besides data breaches and the consequent penalties, business disruption is one of the main concerns in the sector. But the retail sector also suffers from long-term disruptions due to cyber crime. As the E-CRIME survey shows, consumers avoid using online retail as their fear of becoming a victim of cyber crime increases. Secure payment authentication procedures deter potential consumers from shopping online and, at the same time, disincentivise retailers from adopting innovative payment methods.

Transportation As the transportation industry relies on information technologies to conduct business electronically, they are directly in the cross-hairs of cyber criminals. Basic services such as in-transit visibility, asset tracking, video surveillance and smart ticketing, can be compromised. Cyber criminals leverage this large attack surface to carry out different types of crime, e.g., cargo theft, extortion, personal data theft and e-

ticketing fraud. Consequently, companies in this sector deployed basic countermeasures to comply with generic security standards (e.g. ISO 27000 series) and, thus, mitigate the economic impact of cyber crime. However, the security controls in place are not enough, and the companies suffer loss of value due to cargo theft, loss of income and even a temporary interruption of the supply chain. All in all, cyber crime slows downs the adoption of innovative technologies as well as creating efficiency losses due to avoidance of data sharing.

Energy Increasing automation in the energy sector and more reliance on the digital world for its operations increases its vulnerability to cyber-attacks. Companies have implemented not only sophisticated security controls but stringent access control policies that limit the impact of cyber crime. Air gaping policies, real-time system monitoring, connectivity restrictions are examples of safeguards the industry has in place to prevent cyber crime. However, the sector is characterised but the immeasurable consequences that a cyber attack could cause. SCADA and distributed control systems handle critical information for the correct functioning of the energy generation and transmission. Infiltrating these control systems could lead not only to financial losses but also to injuries and casualties. Extortion and the loss of intellectual property also appear as consequence of cyber crime. Additionally, the sector is reluctant to publicize cyber incidents as it would create bad PR and loss of confidence among consumers and employees. Thus, cyber crime distorts the efficiency of the energy industry and delays the introduction of innovative services.

Introduction

Understanding the economic impact of cyber crime has never been as critical as it is today. Criminal statistics, industry and individual victim surveys show that cyber crime is on the rise, while the rates for other types of crime are decreasing. However, the assessment of the economic impact of cyber crime is incomplete and weak. Other than cyber security vendor data and third party surveys, we depend on victims identifying and communicating their experience of a cyber crime and their understanding of the attack vectors. Companies are reluctant to disclose information about cyber incidents they have suffered.

Based on the model designed in the previous report (see deliverable D6.1), the purpose of this report is to identify, define and examine some of the key issues and complexities surrounding cyber crime on non-ICT sectors. Combining reliable and available information with the data collected during industry interviews, a European consumer survey and non-ICT industry players' feedback, the report shows how non-ICT sectors are affected by cyber crime. We present a description of specific economic effects that cyber crime is having on non-ICT sectors at different levels of European society (i.e., individual, industry players, sectors, states, society) and participants in the value network (comprising non-ICT industry players, cyber security providers, end users). This multi-level and multi-stakeholder investigation opens the doors to create a meaningful and economically-sound base to identify concrete opportunities that exist to fight against cyber crime. We specifically focus on the economic losses and other damages that citizens and companies suffer as result of cyber crime; the behavioural and attitudinal changes produced by cyber crime, or the fear of cyber crime; the effects that counter-measures might have on citizens and companies; and the roles that citizens and industry players could have in fighting cyber crime.

Mapping the different impacts of cyber crime on the different non-ICT sectors provides a snapshot of where cyber crime is prevalent now, and how society and industry are organised against its various dimensions. This allow us to qualitatively compare the five non-ICT sectors in terms of the economic impact they suffer due to cyber crime. Quantitative assessments of some of these impacts are presented where accurate data is available and act as a basis for discussion only. Finally, this report also analyses qualitatively the society's response to cyber crime and how the criminal justice system is affected by cyber crime.

Estimates reported in this study are best estimates of the economic impacts given the information available, but are inevitably imprecise. As shown in D6.1, high-quality data is not always available and some sectors are inherently reluctant to publicise evidence of cyber attacks. Moreover, some figures are based on estimates from other fields of research. Therefore, the impacts estimated in this report are sensitive to changes in assumptions made or to improvements in the quality of the supporting data.

1.1 Objectives and outline of the report

The report's objectives are:

1. Qualitative assessment of the economic impact of cyber crime on non-ICT sectors based on the model developed in Task 6.2;
2. Quantitative assessment of the key economic impacts of cyber crime on non-ICT sectors with the data collected through WP4 and 5 and the suitable external data sources as assessed in Task 6.1;
3. Comparison of the economic impact of cyber crime across the selected non-ICT sectors.

The remaining chapters of this report correspond to these objectives. Chapter 2 presents a high level description of the impact of cyber crime on each of the non-ICT sectors as well as the quantification of the economic impacts of cyber crime for the key cyber threats affecting each non-ICT sectors as identified from the industry interviews. Chapter 3 presents the economic impact of cyber crime on the society's response. Finally, we conclude by reflecting on the qualitative assessment of the different non-ICT sectors.

The economic impact of cyber crime on five non-ICT sectors

While every business in every sector faces a unique set of cyber security risks, the mere use of connected devices exposes them to generic forms of cyber crime such as ransomware, data theft, and online banking fraud. These cyber security risks are generally not of the greatest concern or interest, compared to the more advanced, targeted and sector-specific risks. Therefore, in the following sections on each of the five sectors we look closer at such risks. Additionally, for the sake of completeness in the detailed appendices we review these generic cyber crimes and what we know about their costs.

2.1 Health care

2.1.1 Use of IT

The adoption and use of information and communication technologies are increasingly seen as support, redesign and improvement tools for health care delivery, especially in primary care. Patient care involves a large amount of data, ranging from test results and radiological images to patient histories and billing information. The health care sector uses IT for storing, processing and sharing these data. Health care organisations outsource most IT development by procuring an Electronic Health Record (EHR) system — essentially a customised database management system with several applications built on top of it. This may include features that help physicians to quickly retrieve patient histories and order diagnostic tests, but also e-health portals that allow patients to access their own medical records and get help with self-administered treatments. An important

use of IT is automating the ordering, dispensing and administering of medication, with the intention to prevent medication errors. There is a strong demand for interaction between EHR systems of different health care providers that allows for quick sharing of information.

The adoption of EHR systems in hospitals and medical offices is not yet universal but seemingly the pace of adoption has been accelerating [32]. However, not every country in the EU is adopting EHRs at the same rate. Table 2.1 shows the status of the EHR adoption in each one of the countries analyzed in the E-CRIME project. Even within Europe, different countries face different legislation on EHR systems. Estonia and The Netherlands present the highest rates of adoption, while Polish hospitals have barely integrated electronic patient records in their systems. This is also explained by the significant variability in the general use of computers across and within hospitals in different countries [8]. Table 2.2 shows the different ways IT is used among different practitioners across different countries, i.e., (i) record keeping; (ii) drug prescriptions; (iii) storing of tests results; (iv) making appointments; (v) communication with other parties; and (vi) searching medical information. All these usages require the exchange of private-sensitive data that needs to be done in a secure way. Central and Northern European countries (e.g., Germany) enjoy mature e-health strategies. In contrast, Southern and Eastern EU countries are mostly at the planning stage or only now implementing e-health applications. Among Eastern European countries, Estonia represents a positive example also in terms of strategic e-health applications [8].

2.1.2 Cyber security risks

The primary cyber security risk in the health care sector is that patient records are stolen. For those with malicious intentions, patient records are a valuable commodity that can be sold for $50 per record on online black markets [35]. Buyers of these stolen records use them for identity fraud, getting prescription drugs and medical treatments billed to unaware victims.

Besides losing patient records, cyber security threats to the health care sector include the disruption of IT systems (through DDOS attacks, for instance), as well as generic threats like ransomware, banking fraud, and cyber extortion. In this report we focus on the most prevalent threat of data breaches.

2.1.3 Costs in anticipation of cyber crime

Country	Stage of implementation	Legal context
Estonia	Full implementation of shared EHR systems (ENHIS) [15] since 2008	Specific and comprehensive legislation on EHR systems
Germany	No shared EHR systems. Several policy initiatives underway	General provision setting the general framework for the development of EHR system. Reliance on general data protection and health record legislation
Italy	Deployment phase of EHR system at regions and autonomous provinces	Legal obligation for region and autonomous provinces to develop EHRs. Draft law specific on EHR
Netherlands	Several shared EHR systems being deployed. Deployment of a shared EHR system (LSP) [55] since 2011 that has the potential of being a nationwide system.	No specific legislation on EHRs but a proposal is under discussion Reliance on general health records legislation and data protection rules
Poland	Shared EHR system under development foreseen by 2017	Specific legislation on shared EHR system Reliance on general health record legislation, patients' rights and data protection rules
UK	Full implementation of a shared EHR system in the UK countries - England (SCR [25] in 2008), Scotland (ECS [31] in 2006, ePCS [27] in 2009, KIS [40] in 2013), Wales and Northern Ireland (ECS [26] in 2008, NIECR [52] in 2013)	Only few legal provisions specific on EHRs Reliance on an information governance framework which includes; general health record legislation, data protection legislation and medical rule. Institutional guidelines on EHRs

Table 2.1: Stage of implementation of shared EHR systems and legal approaches [37]

	Estonia	Germany	Italy	Netherlands	Poland	England	Euro-31
Making appointments	73.64%	55.32%	25.23%	100.00%	25.45%	98.82%	51.33%
Issuing invoices	79.84%	93.62%	8.26%	94.47%	27.73%	60.95%	42.01%
Issuing drug prescr.	92.25%	99.15%	99.08%	100.00%	50.00%	99.41%	80.99%
Keeping records	96.12%	87.66%	85.32%	100.00%	44.09%	99.41%	77.40%
Sending ref. letters	82.17%	99.15%	55.50%	98.72%	21.36%	98.22%	70.47%
Storing test results	93.80%	88.94%	88.53%	99.57%	30.45%	98.22%	73.85%
Searching med. info	97.67%	71.49%	78.90%	99.15%	59.09%	98.82%	82.18%
Sending prescript. to phar.	96.90%	16.17%	13.30%	95.32%	4.09%	44.97%	31.60%
Cases	129	235	218	235	220	169	6301

Table 2.2: Use of computers in primary care (QUALICOPC survey) [8]

Cost of security products and services

Since the development of most IT applications is outsourced, so are many of the technical security controls. At its core, an EHR system is a database management system, and its primary security layer is a standard access and privilege management system.

Development and maintenance of these security features is indirectly payed for by health care organisations via license and support fees. As such, these costs do not show up in the budgets and bookkeeping of health care organisations, and are unlikely to be included in self-reported estimates of security investment in surveys. However, since the development and maintenance costs of EHR systems are shared by a large number of customers, the costs for a single organisation that one may attribute to these security controls is relatively small. To illustrate, Epic Systems, the number one EHR vendor in the United States, offers an EHR system that is built on top of the Intersystems Caché database platform, which has several built in security features such as encryption and system event logging [30]. The costs of these features are shared not only by the hospitals and primary care practices that use Epic Systems, but by all customers of the Caché database platform. The homogeneity of health care organisations in the way they use IT significantly brings down the costs of security controls.

At the user level, however, health care organisations still need to implement and manage basic security controls to prevent network intrusions and malware infections. To encourage this, regulators have set guidelines and created standards and best practices. In Section 2.1.6 we present estimates of the costs of implementing and maintaining the security controls typically recommended in such guidelines for both hospitals and primary care practices.

Productivity losses due to security policies

There are well-documented anecdotes of physicians in hospitals writing their login credentials down on sticky notes or simply leaving themselves logged in on devices to convenience their colleagues. Interviews with health IT experts carried out earlier in the E-CRIME project confirmed the prevalence of such behaviour. This is often attributed to a general lack of understanding of IT security in the health care sector, but it may in fact be explained in part by an unfavourable trade-off between security and productivity. In Section 2.1.6 we give some estimates of the productivity losses due to typical security policies and provide a quantitative perspective on this issue.

Recent reports have shown that EHR have both positive and negative impacts on primary-care outpatient practices [28]. Concerns around the privacy and confidentiality of the EHR system have systematically appeared [10, 38]. But the main barriers that are slowing the adoption are the costs when implementing EHR, i.e., financial costs and loss of productivity due to training.

Administering EHR systems takes a lot of time. Physicians complain a lot about how tedious and unproductive EHR systems are. Security is probably responsible for some part of that lost time, but only a small part given the actual complaints (e.g., "we just could not do it because they want a portal, they want a connection with an HIE, they want secure messaging and we are not able to do it.") [24].

2.1.4 Costs as a consequence of cyber crime

As in any sector, a data breach may lead to disruption of processes and may require significant efforts to investigate and repair the breached systems to restore normal operations. The lack of security expertise at many health care organisations makes this challenging. An IT professional working at a large German hospital who was interviewed for the E-CRIME project revealed that only 2 of the 80 IT professionals were designated

security officers. Smaller hospitals, clinics and primary care practices often have no security expertise at all. When such organisations experience a security breach, they need to procure external IT security consultants, at considerable cost.

The actual victims of a data breach, however, are the people whose personal records are lost. The responsible health care organisation suffers to the extent that the victims or regulators make them — through litigation, penalties, notification rules, or loss of trust. It is important to be careful in labelling these costs as a consequence of a cyber criminal incident. Regulatory fines may only apply when the health care organisation was non-compliant with regulatory guidelines, and litigation may only take place if the organisation was severely negligent. In the U.S., for instance, hospitals are exempted from the notification rule if the stolen records are encrypted. It is therefore not always appropriate to add these costs up to estimate the total impact of data breaches on the health care sector. One might consider regulatory fines as the result of non-compliance, rather than the result of a data breach. This distinction matters when one wants to use impact estimates in cost-effectiveness or cost-benefit analyses of existing or newly proposed policies.

2.1.5 Long term implications

Despite of evidence to the contrary, it is a common belief among practitioners that there are more security and confidentiality risks involved with EHRs than paper records [34]. The amount of data breaches that reach social media is polarizing privacy concerns and thus, slowing down innovation and the adoption of new technologies such as EHRs. Cyber incidents, though most of the times are due to human errors, increase the concern for privacy, confidentiality, and security for computerized patient information.

On the other hand, while EHRs were introduced to increase the productivity of practitioners, the demands for security and usability are often contradictory. Privacy regulations introduce a number of checks to ensure that users are authorised to use the system but at the expense of usability. Practitioners take more time to get started with the system which reduces the amount of patients they can visit per day. A 2011 study reported on the financial and nonfinancial costs of implementing a commercial EHR in a health care network in Texas [19]. They estimated that the end-users (defined as the physicians, clinical staff members, and nonclinical staff members) required 134 hours per physician to become familiar enough with the EHR that they could comfortably use it with patients. Moreover, studies have also shown a loss of productive due to the change in workflow after the EHR implementation. For instance, the use of central station desktops was

found to be inefficient increasing the work time 238.4%.

Despite the progress in adoption EHR systems within individual health care sector, the level of electronic information sharing across such systems has failed [23]. The roadblocks slowing information sharing arise from the nature of the health care market, in which patient information resides where care and services are delivered, such as the offices of primary care physicians and specialists, hospitals, laboratories, pharmacies, health plans, as well as with the patients. Also slowing adoption are infrastructure costs associated with exchange, a dearth of standards and systems interoperability, privacy and security, as well as liability concerns.

2.1.6 Quantifying the key economic impacts

As mentioned in section 2.1.2, the main threat that the health care sector faces is the unauthorised access to patient records. In this section we estimate quantitatively to what extent data breaches represent the main economic impact.

To that end, we use the number of data breaches in the US during 2012 and linearly extrapolate those to the European countries based on two variables: population size and national health expenditure. The number of data breaches is not publicly available. The ePrivacy Regulations 2011 (S.I. 336 of 2011) have spawned somewhat recent laws in many countries that require network service providers to notify national regulators of data breaches within 24 hours (and affected individuals without undue delay), but expansion of the directive and laws to include enterprises, like in the US, has not happened yet [57].

	Population (millions)	Health spending ($PPP per capita)	Total health spending (billions)	No. of breaches (method 1)	No. of breaches (method 2)	records lost (thousands) (method 1)	records lost (thousands) (method 2)
US	322	8845	2848	170	170	5200	5200
NL	17	5358	91	9	5	276	166
IT	61	3209	196	32	12	985	358
UK	63	3495	220	33	13	1017	402
EE	1	1385	1	1	0	16	2
DE	81	4617	374	43	22	1308	683
PL	39	1489	58	21	3	630	106

Table 2.3: Estimates of the number of data breaches in the health care sector and the number of records lost

Table 2.3 shows the estimates of the number of data breaches in the health care sector and the number of records lost. According to these estimates, Germany is the country where more data breaches would occur as it is the country with the highest population. However, the Netherlands, despite being the country that spends the most on health

care, would suffer less numbers of data breaches than in Germany or in the UK. As Estonia has the smallest population and the lowest expenditure on health care, it will suffer no more than a couple of data breaches.

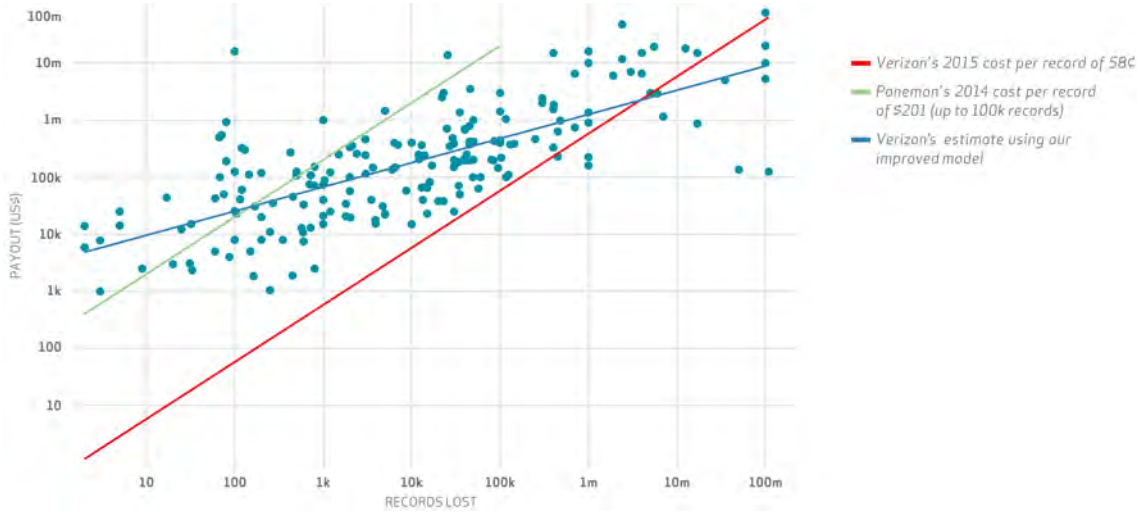

Figure 2.1: Total claim amount by records lost

To monetize the estimated number of data breaches, we use Verizon's report on data breaches [56]. Figure 2.1 shows the total claim amount by records lost based on the different estimations of the record cost. Combining both the average record cost with the estimate of the number of records lost, we can estimate the cost of data breaches for the European countries shown in table 2.3. For instance, in the Netherlands the losses due to data breaches in the health care sector will range from 1k€-1M€.

Though several million Euros might seem a significant amount of money, this is not the main cost that cyber crime imposes on the health care sector. Implementing an EHR system could cost a single physician approximately $163,765 [43]. Of course, the whole cost of an EHR system is not fully attributable to security, but even only considering 10% of this cost is due to security, the cost will overshadow the losses due to data breaches. Again, one could argue whether EHR also increase the productivity [20] but this is not always the case when they are implemented to follow privacy laws.

One evident loss of productivity is the amount of time that practitioners spend logging in and out of the EHR. According to the Health Insurance Portability and Accountability Act (HIPAA) [54], a covered entity should activate a password-protected screensaver that automatically prevents unauthorized users from viewing or accessing electronic protected health information from unattended electronic information system devices. This is an addressable implementation specification, so timeouts and log out features will relate to size of covered entity and degree of access to electronic information system devices. As a benchmark, it is recommended to wait a 10-minute timeout period before the log out

capability locks the device and makes information inaccessible. Devices in high-traffic areas a timeout of 2 to 3 minutes is recommended.

When estimating quantitatively this loss of productivity with monetary estimates, one realizes that these costs outweigh the losses due to potential data breaches. As an example, let us assumes that the average time to logging into an EHR system take an average of 30 seconds[1]. According to a 2014 survey by the American Academy of Family Physicians [1] doctors see 20 patients a day on average. Assuming € 150/hour wage costs and 240 working days per year, the loss of productivity due to logging in and out of the system will amount to € 6000 per physician per year. Extrapolating these costs to a country-level:

- The Netherlands has roughly 60k physicians, around half of which work in a hospital € 6000×30000 physicians $=$ 180 million Euros a year;
- UK: € 1 billion;
- Germany: € 1.8 billion.

Even though the accuracy of these estimates is based on the aforementioned hard assumptions, these figures are 2 or 3 order of magnitude higher than the losses due to data breaches. This evidences that the loss of productivity due to the security controls in place to comply with current security regulations can easily overshadow the cost of potential data breaches.

2.2 Financial services

2.2.1 Use of IT

The financial services sector was one of the earliest adopters of IT. Perhaps at first the reason for adopting IT solutions was simply to reduce overhead costs, allowing banks to close branches and to cut costs in customer service, communication, and transaction processing. However, the wide-spread adoption of the Internet opened the doors to new services, new delivery channels, and new market players. This includes crowd funding platforms, crypto-currencies, online banks without physical branches, and payment services offered by technology companies.

[1]Note that this is a lower bound, as depending on the specific software that the practitioners need to run it might take several minutes [5].

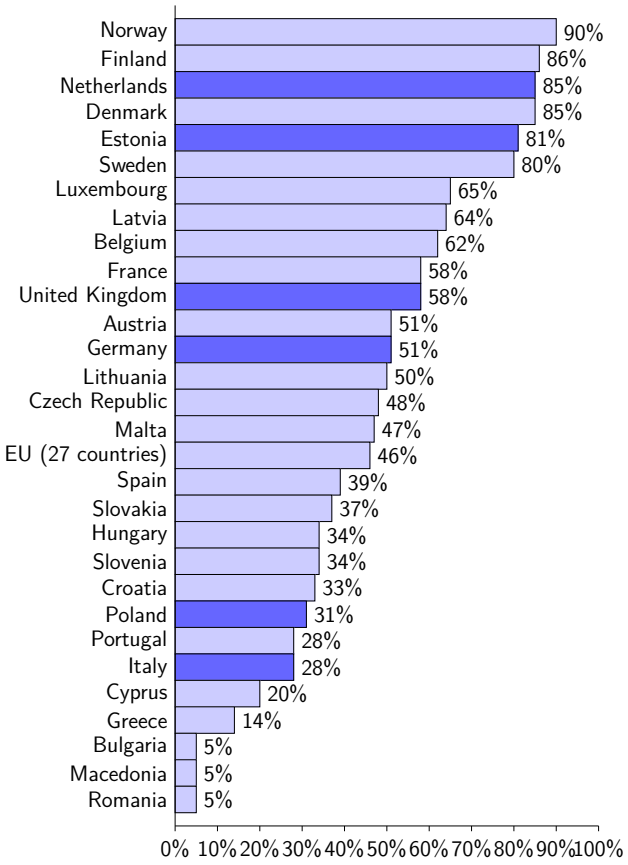

Figure 2.2: Online banking penetration in selected European markets in 2015 [49]

IT has also provided the financial sector with the wherewithal to deal with the challenges the new economy poses [44]. IT has been the cornerstone of recent banking industry reforms aimed at increasing the speed and reliability of financial operations and of initiatives to strengthen the banking sector. Many of these new services — as is often the case with technology — effectively 'cut out the middle man'. The result is that an ever larger part of the ICT infrastructure in the financial services sector is no longer controlled by the traditional banks. This has shifted the responsibilities and incentives in the fight against cyber crime.

2.2.2 Cyber Security Risks

The financial services sector continuously faces attacks by financially motivated and strategically thinking cyber criminals. Attacks are mostly designed to exploit the trust of people — either employees or customers — by means of phishing, pharming, and malware.

Traditional risks in the financial sector — fraud, bank robbery, scams, and so on — all have their cyber criminal equivalents. Digital assets can be stolen by cyber criminals who

manage to infiltrate the intranet of a bank and transfer assets to their own accounts — the modern equivalent of a bank robbery. Man-in-the-middle attacks on online bank transactions are similar to the now ancient crime of cheque washing, in which a signed cheque is intercepted in transit, the ink dissolved, and a new transaction written down. Similar analogies can be drawn for other types of fraud. The online channels through which financial services are offered have simply increased the scale and effectiveness at which criminals operate.

The online payment infrastructure, in terms of functionality, is conceptually simple. An asset is an entry in a database, and a transaction is a record in a ledger. The main cyber security risks for the online payment infrastructure start with some form of identity theft, originating from theft of personal payment information or from attacks targeted at consumers in which credentials are stolen.

2.2.3 Costs in anticipation of cyber crime

In anticipation of cyber crime, businesses in the financial services sector have two tasks: (1) securing their own network, on which they store and process sensitive data like personal records, account balances, and transaction data, and (2) protecting consumer payment systems against fraud.

Cost of security products and services

Banks actively pursue the best possible security using state-of-the art technical controls, such as SIEM and intrusion detection systems. Their security policies and expenditures go beyond generic standards and best practices.

To some degree, cyber security is a marketable product for financial services companies. As one E-Crime interviewee noted, a bank protecting its internal network is hardly different from a bank protecting its physical vault. IT has not changed the demand for secure storage of value. Hence, when considering the cost of technical security controls at banks, pension funds and credit unions, one should view them in proportion to the cost of the more traditional security controls that they have replaced, and also consider their marketable value.

In addition to technical controls, organised staff training is common in the financial services sector.

Businesses in the electronic payment network — credit card companies, payment service providers, banks — have extensive fraud departments. These efforts are not aimed at completely stopping fraud, but rather limiting it to acceptable levels. The number of fraudulent transactions prevented is generally an order of magnitude smaller than the number that gets through.

Productivity losses due to security policies

With online payments there is a trade-off between security and convenience. More advanced authentication and authorisation procedures tend to reduce the number of transactions. We will explore this issue further in our discussion of the retail sector. Of relevance to financial services companies is the effort required to process a transaction.

2.2.4 Costs as a consequence of cyber crime

Not much is known about cyber security breaches on the internal networks of financial services businesses, aside from anecdotal evidence. The financial services sector has the biggest data centres, the most transactions and the highest IT security and regulatory compliance risk exposure. One only has to look at a sampling of data breaches to know that confidential customer data and proprietary intelligence is increasingly subject to theft [50]:

- JPMorgan Chase (83 million accounts);
- Heartland Payments Systems (134 million accounts);
- Global Payments, Inc. (1-1.5 million accounts);
- Citigroup (360,000 accounts).

Fraud losses are also better documented, and financial fraud can come in many forms, e.g:

- Tax evasion and money laundering;
- Debit/credit card fraud;
- Identity theft;

- Transaction fraud.

Nowadays, fraud might not result in a loss to the customer if national laws require financial institutions to bear this cost instead. Costs to the organisation might be much more severe and could include liability costs that are not always covered by corporate insurance policies. Litigation or prosecution can also represent important costs.

2.2.5 Long term implications

While established financial businesses and services are now quite successful in minimising the damage of fraud and other cyber crime, this has taken years of investment to achieve. Disruptive innovative services launched by start-ups and non-traditional businesses are often held back by the risks and costs imposed by cyber criminals.

Fraud in the financial services sector may also reduce the use of online banking services. It can also cause reputation damage of corporate and/or national companies which could eventually lead to other firms or countries avoiding doing business with them.

2.2.6 Quantifying the key economic impacts

Financial services by nature are a traditional target for cyber criminals. To mitigate the losses due to cyber attacks, financial institutions invest in state-of-the-art security controls and deployed their own incident response teams. Thus, the anticipation costs constitute a significant part of any financial institution's budget. Table 2.4 shows the cyber security spending of banks where we observe that the spending highly varies per bank. In any case, the major banks spend at least more than 200 million Euros on cyber security. According to the latest report published by Homeland Security regarding the 2015 U.S. financial services cyber security market [29], this market will reach $9.5 billion in 2020, making it the largest non-government cyber security market. In addition, the report concludes that this market will be the fastest growing non-government cyber security market, exceeding $77 billion in cumulative 2015-2020 revenues.

Besides anticipation costs, financial services also suffer from the consequences of fraud. As an example, Table 2.5 presents card fraud levels for the countries selected for the E-CRIME project [16]. As expected, countries with a mature card market experienced higher fraud levels, e.g., the UK, Germany and The Netherlands are the countries with higher fraud levels. In order to monetise, fraud levels we used the total value of card

	Total assets (billions)	#employees	Cyber security spending (millions)
UK banks	€7,000	425k	€900
American banks			
Bank of America	€1,940	224k	€370
JP Morgan	€2,320	240k	€460
Citigroup	€1,670	241k	€280
Wells Fargo	€1,570	265k	€230
EU28	€43,440	3 million	??

Table 2.4: Cyber security spending of banks

payments [17]. As a result, Figure 2.3 shows the total value of card fraud per country. Note that only the losses due to this type of fraud exceed the expenditure on cyber security. Thus, the economic impact on the financial services sectors comes both from the anticipation costs as well as from the consequence.

		Transactions per card		**Transactions per inhabitant**		**Fraud per transaction**		**Fraud per 1000 cards**		**Fraud per 1000 inhabitants**	
Country	**Cards per inhabitant**	**value**	**volume**	**value**	**volume**	**value**	**volume**	**value**	**volume**	**value**	**volume**
GB	2.5	5633	92	13830	226	0.063%	0.032%	3312	27.5	8132	67.5
DE	1.6	4315	44	7039	71	0.024%	0.014%	1112	5.9	1813	9.7
NL	1.8	4977	108	9022	195	0.023%	0.005%	1129	5.4	2046	9.8
IT	1.2	4387	43	5158	51	0.022%	0.012%	1104	5.9	1298	7.0
EE	1.3	4098	149	5478	199	0.013%	0.002%	532	3.5	711	4.7
PL	0.9	2940	64	2646	58	0.005%	0.002%	139	1.2	125	1.1
EA-17	1.4	4684	69	6760	100	0.034%	0.019%	1648	12.8	2378	18.5
SEPA	1.4	4660	74	6376	101	0.039%	0.020%	1899	14.9	2599	20.3

Table 2.5: Card, transaction and fraud levels from an issuing perspective

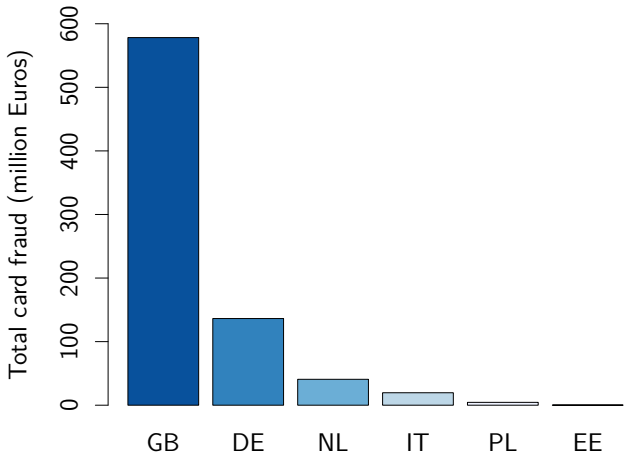

Figure 2.3: Total value of card fraud per country

On the other hand, consumers also suffer the consequences of cyber crime in the finan-

cial sector. Estimates of the costs of identity theft (IDT) to the financial sector from the consumer perspective are collected through the E-CRIME survey by measuring the victimisation and the reported costs for citizens in the surveyed countries. Table 2.6 shows the combination of both parts of the two-part model (see details in the Appendices), before and after the compensation payments. Overall Table 2.6, shows that large parts of the losses are compensated by the industry. IDT with respect to online banking has the severest impact on citizens. With the highest percentage reporting an initial loss of money ($32.56\,\%$) after the incident and the highest median loss ($551\,€$), leading to a combined overall median loss of $179\,€$. This holds even after the subtraction of the compensation payments. The last column shows the median losses of IDT to the financial sector, which is the equivalent of the money given to the victims as compensation. The highest loss ($121\,€$) is also found for IDT with respect to online banking.

Identity theft	Initial monetary loss			Remaining monetary loss			Industry loss
wrt. bank cards	$31.8\,\%$	$367\,€$	$117\,€$	$17.7\,\%$	$191\,€$	$34\,€$	$83\,€$
wrt. o. banking	$32.6\,\%$	$551\,€$	$179\,€$	$16.7\,\%$	$348\,€$	$58\,€$	$121\,€$
wrt. PayPal	$24.4\,\%$	$495\,€$	$121\,€$	$11.9\,\%$	$210\,€$	$25\,€$	$95\,€$

Probability of loss (1st.); Median loss (2nd.); Combined loss (Comb.); Based on the severest incident

Table 2.6: Structure of financial losses after identity theft

Table 2.7 shows the average costs of the three types of IDT in the financial sector per citizen over the last five years. The costs are further broken down by citizens and the industry in each country. Table 2.7 illustrates that the financial industry pays the major part of the bill of IDT in each country. For every country and type of IDT the financial industry losses at least twice as much as the victims. PayPal on average even covers about four-times more than the victims. IDT with respect to bank cards causes the highest losses throughout all countries, for both citizens and industry. Driven by the low incidence rates of IDT with respect to online banking, the total costs are comparably smaller than the costs of IDT with respect to bank cards. On average, IDT with respect to online banking is the "most expensive" type of IDT, but less frequent than IDT with respect to bank cards. On average all three types of IDT are more expensive to Germany and the UK. This is exclusively driven by their prevalence, as the costs of each type of crime have been measured across all countries. Italy and Estonia lose the least.

2.3 Retail

for ...	due to IDT wrt. ...	Upper bound of costs					
		UK	DE	NL	PL	IT	EE
Citizens	bank cards	1.49	1.06	0.85	0.48	0.38	0.28
	online banking	1.78	0.72	0.58	0.58	0.39	0.61
	PayPal	0.53	0.44	0.21	0.12	0.07	0.17
Industry	bank cards	3.67	2.62	2.09	1.17	0.94	0.7
	online banking	3.71	1.49	1.2	1.21	0.82	1.28
	PayPal	2.01	1.67	0.8	0.46	0.29	0.64

Upper bound of the costs in €, based on severest incidents in the last five years

Table 2.7: Financial loss after identity theft

2.3.1 Use of IT

A large part of business-to-consumer trade is conducted in electronic markets and online stores. The economic benefits of these channels include intensified competition, reduced search costs for consumers, and the ability for retailers and customers to transact at any time and any place.

The behaviour of (potential) customers on e-commerce websites is often tracked and used for targeted advertising. Brick-and-mortar stores also collect large amounts of customer data, either by storing payment information or with loyalty programmes. There is a strong incentive for collecting this information for purposes of marketing and sales forecasting. In addition, IT is used by retailers to manage their supply chain, with semi-automated storage and retrieval systems, real-time tracking of logistics operations, and inventory management systems.

2.3.2 Cyber security risks

E-CRIME interviews with experts in the retail sector revealed that the most concerning threats are acts of phishing and malware attacks, usually targeted at customers so as to steal their credentials, and DDoS attacks that take web shops offline.

Even though many e-commerce businesses outsource their payment infrastructure to third party payment service providers, they may still be liable for the costs of fraud. When the number of fraudulent transactions conducted on a retailer's website passes a certain threshold, the credit card companies and banks — who initially suffer the costs of fraud — often find ways to get the merchant to pay for the damages. The power imbalance in dealings between merchants and payment infrastructure providers forces retail businesses to comply with certain rules and standards, most notably the Payment

Card Industry Data Security Standard (PCI-DSS). This is not always simple, especially for smaller web shops, as evidenced by the existence of specialised PCI-DSS compliance consultants.

Another indirect cyber security risk for the retail sector is that cyber criminals may purchase products online with stolen money as a cashing-out strategy.

2.3.3 Costs in anticipation of cyber crime

Many retailers are guided in their cyber security efforts by the PCI-DSS. This standard is mandated by the major credit card schemes — retailers not compliant with their rules are subject to fines, may be held accountable for malicious chargebacks, and may in the worst case be excluded by the credit card companies altogether.

Cost of security products and services

Many e-commerce businesses procure the necessary software from a third party. This software allows retailers to set up a front-end website and manage its contents. This sometimes comes with a license fee, some part of which can be attributed to the development and maintenance of security features, but there is also open source software like Magento, which releases security patches for free. The homogeneity of retail websites creates economies of scale in developing secure software. To illustrate, Magento is used by more than 200,000 e-commerce businesses, and as a result the cost of its security features are spread out so much that they are effectively negligible.

Productivity losses due to security policies

More secure payment methods hurt conversion rates. Visa and MasterCard's now require merchants to use their 3D Secure payment protocol, but some merchants (like Amazon) prefer paying the fines to adopting the system. This trade-off between customer convenience and security is the key to understanding the costs of cyber crime in the retail sector.

One interesting aspect is how consumers change over time. Two-factor authentication was at first quite controversial, but consumers have gotten used to it. The same may happen for any other kind of security protocol. Hence, while drop-out rates are interesting, they might be a temporary, and not a long term impact.

Cost of security assessments

Merchants are required by PCI-DSS to have an annual PCI compliance assessment and a quarterly network security scan. The security scans need to be conducted by an Approved Scanning Vendor for all merchants. Smaller merchants, processing up to 6 million a year, are allowed to do the compliance assessment themselves. Large merchants and those who have suffered a data breach in the past need to get a Qualified Security Assessor carry out or sign off on the assessment. This assessment can be quite extensive and costly.

2.3.4 Consequence costs

Direct damages in the sector include down-time of online stores due to disruptive cyber attacks. An online retailer subjected to a (D)DoS attack could be shut down for several days or weeks while determining the attack's origin and taking corrective action.

For a small companies, customer information theft can paralyse operations or put a company out of business. Proprietary information, such as product designs, customer records, company strategies or employee information, is often compromised or stolen outright. All of these assets have incalculable value to a business, and thus can inflict crippling losses. A single incident could compromise the integrity of a retailer's electronic storefront could result in unrecoverable losses. Subsequent indirect costs such as fines imposed, litigation, damages and a decline in sales, as customer confidence is dented and brand reputation is tarnished.

Regulatory fines add to the direct expense bills. The Information Commissioner's Office (ICO), for example, recently issued a fine of £250,000 against a large entertainment company for a breach of the Data Protection Act (DPA) [36]. Over the past decade, merchants have been particularly hard hit due to alleged PCI non-compliance. Visa imposed $13.3 million in non-compliance fines and assessments on two acquiring banks [51], which processed the payment card information in a breach incident. The banks paid the fines, and then collected the total from a specialty retailer in line with an indemnification agreement. The fines assessed stemmed from the breach of the retailer's payment processing network due to a criminal cyber attack.

2.3.5 Long term implications

A 2012 National Cyber Security Alliance study showed that 36 percent of cyber attacks are conducted against retailers [39]. Of those, up to 60 percent go out of business within six months of an attack. Thus, cyber attacks against the retail sector directly impact on the market efficiency and create competition imbalances.

On the other hand, cyber crime also slows down the deployment of new technologies such as contactless payments. Most retailers will improve control by upgrading point-of-sale (POS) systems and introducing contactless payment to speed up the purchasing process. However, the need to assess the risks that introducing these new payment methods drags out the adoption process.

2.3.6 Quantifying the key economic impacts

To measure the impact of IDT on service providers in the retail sector from the citizen's perspective we used the E-CRIME consumer survey results. Online shopping victims were asked for the compensation payments they have received or how much of their losses they were able to recover, respectively. With $64.65\,\%$ the majority of all IDT victims who lost money were able to recover something and $47.47\,\%$ where able to recover all money that was lost. We estimated the loss distributions for the victims after compensation payments. Figure 2.4 illustrates the results by comparing the loss distributions before and after compensation payments. The blue line in Figure 2.4 represents the initial losses and the orange line the remaining losses for the victims. The difference between the distributions represents the losses that are covered by service providers in the retail (and financial) sector.

Figure 2.4 illustrates that large parts of the losses of IDT are compensated by the financial industry. The average compensation in the retail sector is comparably small $33\,€$. Table 2.8 shows the combination of both parts of the two-part model, before and after the compensation payments. The initial losses shared almost equally by the citizens and the retail industry.

Identity theft	Initial loss of money			Remaining loss of money			Industry loss
o. shopping	$15.5\,\%$	$169\,€$	$26\,€$	$8.7\,\%$	$136\,€$	$12\,€$	$14\,€$

Based on the reported severest crimes

Table 2.8: Financial loss after identity theft

Table 2.9 shows the costs of the three types of IDT in the financial sector broken down

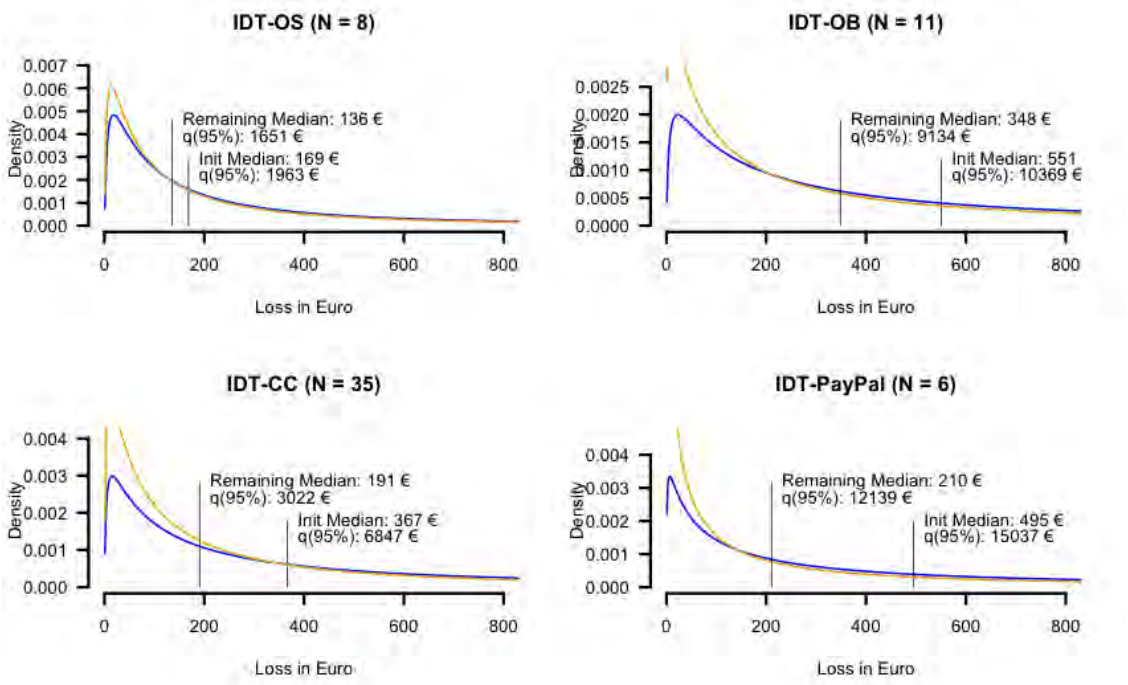

Figure 2.4: Loss distributions after compensation IDT

by citizens and the industry in each country. Table 2.9 illustrates that, the costs of IDT to retail sector are small compared to IDT in the financial sector. Furthermore, they are rather equally divided between citizens and the industry. On average, the highest costs of IDT wrt. online shopping are found in Germany, closely followed by the UK. The costs reported in Table 2.9 are not all costs to the retail sector originating from IDT. Additional costs are passed on by service providers in the financial sector.

		Upper bound of costs					
for ...	due to IDT wrt. ...	UK	DE	NL	PL	IT	EE
Citizens	**online shopping**	0.45	0.46	0.21	0.09	0.06	0.09
	credit card	1.49	1.06	0.85	0.48	0.38	0.28
	online banking	1.78	0.72	0.58	0.58	0.39	0.61
	PayPal	0.53	0.44	0.21	0.12	0.07	0.17
Industry	**online shopping**	0.54	0.55	0.25	0.11	0.08	0.11
	credit card	3.67	2.62	2.09	1.17	0.94	0.7
	online banking	3.71	1.49	1.2	1.21	0.82	1.28
	PayPal	2.01	1.67	0.8	0.46	0.29	0.64

Upper bound of the costs in €, based on severest incidents in the last five years

Table 2.9: Financial loss after identity theft

2.4 Transportation

In our discussion of cyber crime in the transportation sector we distinguish between the *transportation of goods* and the *transportation of people*.

2.4.1 Use of IT

In the transportation of goods sector, the main driving force behind IT innovation is the economic incentive to optimise supply chains. The transportation sector uses IT for sharing of information between processes to ensure smooth coordination from consignor to consignee. The challenges are: to get the shipment to its destination on schedule, with the appropriate degree of tracking in route; to minimize delays in transferring from mode to mode; and to achieve these at a competitive price without damage to the product shipped. Tracking and tracing systems using barcodes or RFID tags as well as GPS trackers enable logistics providers and their clients to retrieve background information on a shipment throughout every step in the supply chain and identify its location. The transportation sector is one of the earliest adopters of the Internet of Things.

Large companies today are likely to have sophisticated models of their operations, known as enterprise resource planning (ERP) systems [42]. ERP systems may include scheduling modules for manufacturing plants, which would allow the company to automate major portions of the decision processes in transportation or other aspects of the value chain for that plant. The use of such modules (in finance, logistics, manufacturing, human resources, or supplier management) helps the company improve the way it does business by increasing efficiency and reducing human error.

Harbours, terminals and airports are increasingly adopting robotic systems for moving cargo. These semi-automated systems promise to reduce payroll expenses, increase efficiency, avoid accidents caused by human error, and improve labour conditions.

These IT solutions are currently still being developed and optimised. The Rotterdam Harbour, one of the most important logistics hubs in Europe, is taking initiative in creating a platform for real-time data sharing between different logistics businesses. Businesses have been collecting these data for quite some time, but they are not yet used optimally. Similar initiatives exist, for instance, in Norway.

Many public transportation companies have introduced electronic ticketing smartcards, either at a regional or national level, such as the OV-chipkaart in the Netherlands, the

Oyster card in London, and the Rejsekort in Denmark. There are many other such systems throughout Europe, and further plans to have them completely replace paper tickets. Some of these systems employ cloud-based solutions.

2.4.2 Cyber security risks

Cyber-adversaries in the transportation of goods sector include cargo thieves, blackmail and extortion schemers, competitors, and Personally Identifiable Information thieves. In addition, there may be adversaries motivated to disrupt the transportation infrastructure.

Cargo theft has always imposed large costs to logistics companies, but these costs have been contained by the limited number of opportunities available to thieves. Cargo thieves are mostly interested in high value freight, containing electronics, food, or apparel, and they typically wait for it to be stored in a terminal with low security or left unattended in a parking lot. By hacking their way into real-time track-and-trace systems, allowing criminals to track valuable freights from port to destination, the number of opportunities for cargo theft greatly increases. Furthermore, cyber criminals may obtain release codes that allow them to impersonate legitimate individuals and businesses and simply pick up loads from containers.

For public transport organisations, the main cyber security risk revolves around the personally identifiable information they keep. There is no specific reason why these data should be more attractive to cyber criminals than the data stored by retailers, for instance, but the sheer amount of data, the many point-of-sale terminals, and the demand for quick access puts these organisations at risk.

Public transport e-ticketing systems have suffered from many cyber security issues. To illustrate, the MIFARE Classic RFID chip originally used in the Dutch OV-chipkaart was found to be hackable with equipment worth less then €100, allowing people to travel for free [22].

In addition, in the online sale of tickets, transportation companies face the same threats as online retailers: DDOS attacks, fraud, website defacement, and so on. In fact, these threats are so similar that we will not consider them in this section on the transportation sector.

2.4.3 Costs in anticipation of cyber crime

According to E-Crime interviewees, most transportation businesses use and maintain standard technical countermeasures, such as anti-virus software, network monitoring, firewalls, and so on. Security policies are generally based on generic standards like the ISO 27000 series.

2.4.4 Costs as a consequence of cyber crime

Cyber attacks on transportation networks could take several different forms, with varying consequences and probabilities. Incidents of destructive attacks — aimed at disrupting automated systems by corrupting industrial control systems — are mostly unheard of. The industry experts interviewed for the E-Crime project expressed some concern about the mere possibility of such attacks, but a commonly heard question is why individuals with malicious intentions would choose cyber criminal attacks on the transportation sector over more convenient and effective disruptive attacks?

There are several documented attacks on transit and road operators, such as the hacking of websites and in-the-field traffic control devices, limited primarily to hacks to roadside Dynamic Message Signs (DMS) where there is likely very little impact on public safety [41]. Though these attacks are not usually financially motivated, they disrupt the normal operations of the transport system.

Transportation systems also deal with a significant amount of privacy-sensitive data that could be potentially leaked. For instance, in the summer of 2011, a coordinated protest and cyber-attack was carried out by "Anonymous" against a major metropolitan transit system. As a consequence of the attack personally identifiable information (PII) including customer names, addresses, emails, ID numbers, and passwords for more than 2,000 customers were stolen by the attackers and posted online [45].

An important issue is the so-called *displacement effect*: prevention efforts often result not in thwarting criminals, but only in changing their modus operandi [12].

2.4.5 Long term implications

The long term economic implications of cyber crime on the goods transportation sector could be substantial if security concerns impair supply chain innovation, or if they lead

businesses to avoid sharing data on shipments. The resulting inefficiencies could easily overshadow the costs of the occasional stolen freight or data breach.

There is greater concern that as the sophistication of attacks grow, the costs of securing, and ultimately, deploying Intelligent Transportation Systems (ITS) will grow disproportionately and potentially choke-off innovation. Similarly, new e-ticketing systems are being slowly deployed due to the security concerns and the uncertainty that new technology may introduce new unknown vulnerabilities.

2.4.6 Quantifying the key economic impacts

The main economic impact on the transportation of goods sectors comes from cargo theft. Thieves continue stealing trucks in parking lots and rest stops, but as the trucking industry is widening its use of GPS devices, high-tech locks and other advanced security measures, traditional criminals have been force to adopt new methods by leveraging the cyber domain.

One of the techniques cyber criminals are using is a type of identity theft by which criminals impersonate a trucking firm. Freight security firm CargoNet says that fraud has played a role in about 10% of all cargo theft in recent years [3]. In 2014, the average value of a load lost to a fictitious pickup was more than $140,000. Some estimates put total cargo theft losses at $15 billion and up. Others say theft adds as much as 20% to the cost of consumer goods.

To estimate the impact of cyber crime on cargo theft, we consider only fictitious pick-ups where criminals impersonate truck drivers so that they fool companies into willingly turning over loads to them. They use on-line load posting sites to win transportation bids, or simply show up as drivers with fake credentials, claiming to be assigned to a load [3]. The Internet has increased the ease with which criminals can set up fake companies and acquire motor truck cargo insurance, and fictitious pick-up schemes are proliferating.

As there are no official statistics available internationally on the phenomenon of cargo theft, we show the statistics collected by Transported Asset Protection Association (TAPA) [18]. However, TAPA have created an Incident Information System (IIS), supporting its members and accessible also for law enforcement. Table 2.10 shows the losses due to cargo theft and the estimates of cyber fictitious pick-ups. We consider two bounds (3%-8% of the total cargo value) in order to monetize the losses due to cyber fictitious pick-ups. It is surprising that the UK is suffering 5 times more cargo theft than

any other European country.

Country	IIS Losses [€]	TAPA Losses Billion of Euro	Losses due to fictitious pickups [€] Lower bound	Upper bound
GB	232,767,928	83,941	6,983,038	23,276,793
NL	46,794,607	60,875	1,403,838	4,679,461
FR	47,737,308	18,647	1,432,119	4,773,731
DE	32,286,594	9,719	968,598	3,228,659
IT	11,429,184	5,430	342,876	1,142,918
PL	1,150,265	2,737	34,508	115,027
EE	12,457	425	374	1,246

Table 2.10: Cargo theft loss rate per Billion Euro of GDP

On the other hand, the transportation of persons is also highly affected by cyber crime. In the following, we use e-ticketing fraud, as an example of the economic impact of cyber crime. In particular, we will estimate the impact of cyber attacks on smart cards. As aforementioned, the OV-chipkaart is a type of smart card introduced in the Netherlands In December 2005, the OV-chipkaart was successfully introduced in the public transport system of Rotterdam, The Netherlands. In May 2008, the government assigned a commission to evaluate the potential increase of the cost budget [2]. The result of the research shows that the original starting budget of the OV-chipkaart was €249m but the extra overrun cost €100m in 2006-08. In addition to this, the NS has spent €726m for the introduction of the OV-chipkaart on the rail network. This results in a total cost of almost €1.1bn. However, due to successful hacking attempts [46] that allowed the passengers to travel for free [9], the cards had to be replaced. Travelers had to pay €7.5 for replacing their chip cards. But that is not the only cost the sector suffered.

The introduction of a new chip to solve the security issues also led to human costs as well as productivity losses. Table 2.11 presents the main indirect costs due to this replacement. It is worth noting that the costs of the replacement have probably overshadowed the losses due to potential fraud.

2.5 Energy

In this section we explore the economic impact of cyber crime on all businesses in the various energy industries; that is, those businesses involved in the generation, production, transmission, distribution, or sales of energy in Europe.

Indirect human costs	**IT cost factor**
Management/staff resource	Integrating computerised administration and control into work practices.
Management time	Devising, approving and amending IT/IS and marketing and procurement strategies.
Cost of ownership: system support	Vendor support/trouble-shooting costs.
Management effort and dedication	Exploring the potential of the system.
Employee time	Detailing, approving and amending the computerisation of estimating, cost planning and project/contract administration
Employee training	Being trained to manipulate vendor software and training others.
Employee motivation	Interest in computer-aided estimating and planning reduces as time passes.
Changes in salaries	Pay increases based on improved employee flexibility.
Staff turnover	Increases in interview costs, induction costs, training costs based in the need for skilled human resource.
Organisational costs	**IT cost factor**
Productivity losses	Developing and adapting to new systems, procedures and guidelines.
Strains on resources	Maximising the potential of the new technology through integrating information flows and increasing information availability.
Process re-design	The re-design of organisational functions, processes and reporting structures.
Organisational re- structuring	Covert resistance to change.

Table 2.11: Costs due to OV-chipkaart replacement [4]

2.5.1 Use of IT

The nature of the energy sector is mechanical, and that will not change. IT is used to operate mechanical processes, with Industrial Control and SCADA systems. These systems monitor and control every process from exploration, production, transmission, to distribution to end-customers.

A key challenge in the energy sector is the matching of supply and demand. Energy demand fluctuates heavily on an hour-by-hour, day-to-day, and season-to-season basis. Supply is uncertain due to natural disasters, political conflicts, the inherent uncertainty in exploration, and the resulting fluctuations in energy prices.

Peaks in demand require excess capacity or excess storage of energy, both of which are very expensive. There is a key role for IT in coordinating supply demand, with potentially major efficiency gains.

Moreover, modern energy systems are becoming more complex. There are supervisory control and data acquisition (SCADA) or industrial control systems (ICS) that sit outside of traditional security walls [58]. And as smart grid technology continues to gain momentum, more new energy systems will be connected to the Internet of Things, which opens up new security vulnerabilities related to having countless connected devices. In addition to this, many countries have started to open the energy market and add smaller contributors to the electric power grid, such as private water power plants, wind turbines or solar collectors [58].

Like other sectors, businesses in the energy sector use ICT for internal communications and human resource management. Several E-Crime interviewees have mentioned the importance of such systems from a cyber security perspective, due to the sensitivity of internal communications and the possibility of blackmail, extortion, and bribery of employees.

2.5.2 Cyber security risks

Advanced cyber criminal adversaries have shown the ability to infiltrate critical Industrial Control Systems. These are generally considered low-probability threats, but due to their potentially catastrophic impact and the risk-averse nature of the sector, such threats have a big influence on decision-making and workforce management policies. Furthermore, the mere threat of a disruptive cyber attack can be used to extort money from energy

businesses.

In the energy sector, cyber security risks are often considered in the greater context of *operability*. A cyber attack is in many ways similar to a system failure, a software bug, or even a mechanical failure. Risk management policies, security and safety departments, and contingency plans that were already in place have over the years been updated to incorporate cyber security risks.

Petroleum companies also are also at risk of industrial espionage. Considering the large investments in exploration missions and the high stakes of negotiations, this is a formidable threat.

2.5.3 Costs in anticipation of cyber crime

For power utilities, cyber security is to a large extent a matter of careful procurement. Petroleum companies often develop IT solutions in-house, and they are not implemented before an extensive and often lengthy security assessment.

The potentially catastrophic impact of cyber attacks, the societal importance of stable energy supply, and the high ratio of expenses to employees in the energy sector have led to particularly cautious IT security management. Restrictive security policies are much easier to justify than in, for instance, the health care sector which is more dependent on the productivity of employees. These policies bring about substantial efficiency losses, and although this is accepted and considered to be inevitable, several E-Crime interviewees have said that these indirect costs are larger than the direct costs of technical anticipation measures.

Like we have seen in other sectors, E-Crime interviewees consider employees to be the weakest link in their cyber security programme. This is reflected in restrictive access management — in both physical and cyber-space — internal monitoring of communications, and limiting device management.

2.5.4 Costs as a consequence of cyber crime

The energy sector is vulnerable to the same threats as other sectors. Cyber criminals seeking financial gain can easily dupe an unsecured smart grid into reporting fake consumption figures, overbilling targeted victims, or simply stealing victims' identities and payment information for their personal use. Smart grids manage utility production and

distribution processes by automatically sensing, analysing and controlling machine functionality, temperature, pressure, etc. But when cyber attacks on the grid occur and automatic safety measures fail, the consequence can range from power outage through loss of life. When the cyber criminals manage to get unauthorised access to the utility grid, there would be not only the cost of repairing the immediate damage, but also the cost of the disruption to homes, businesses and services that rely on electricity. However, the likelihood of disruption is lower and the more likely result is bad PR and embarrassment for the breached company. Anecdotal cases exist, like the recent attack using the BlackEnergy Trojan to disrupt the Ukrainian electric power industry that resulted in a major power cut [21].

Cyber attacks on the grid can also go after intellectual property and trade secrets. As an example, recall the case of the worm called Flame that was used by the US government to infect Iranian computer in 2010 [33]. This malware collected and sent back critical information on military and scientific secrets. But in most cases it is difficult to know which information the attacker accesses, and what the attacker will do with this information.

But cyber espionage is not the only attack vector cyber criminals are using to target the energy sector. Extortion has become a more prevalent cyber threat than espionage and sabotage to the global energy sector as criminals gain access to the systems of utility companies and demand ransoms to avoid causing damage. The amount of ransom has climbed to hundreds of millions of dollars [53].

2.5.5 Long term implications

The loss of intellectual property impacts companies' productivity and, in turn, harms the national economies of countries hosting them. Losing IP erodes the returns on innovation and slow economic growth because of the negative impacts on the energy sector. However, the impact of IP theft to society does not have to be prejudicial *per se*.

Cyber attacks also disrupt the way new technology is adopted in the energy sector. For instance, at the backbone of the smart grid there are programmable logic controller that came on the scene in the 1960s. Even though 'smarter' devices exist nowadays, most of the industrial control systems still employ PLCs as they have been tested for years and theirs strengths and weakness are well-known. Energy companies prefer to limit the known risks of operating with PLCs rather than deploying innovative technology that could be potentially compromised by cyber criminals.

2.5.6 Quantifying the key economic impacts

Firms in the energy sector are unable to monetize or even quantify the economic impact of any cyber incidents and its consequences. Firms do not separate security investment from IT investment. This causes a lack of evidence that hinder any quantitative assessment of the cost of cyber crime in this sectors. Only anecdotal incidents reach the public and their heterogeneity does not allow to estimate any impact for the energy sector.

The economic impact of society's response to cyber crime

The impact of cyber crime goes beyond the consequences inflicted after a cyber attack and also imposes significant costs to the criminal justice system. These include expenditures on police and other law enforcement agencies, prosecutors, judges (in criminal courts), prisons and other correctional facilities, probation officers, etc. Moreover, national and local Computer Security Incident Response Teams (CSIRTs) have to be created to manage cyber attacks. But not only that, society also spends money on crime prevention such as awareness campaigns.

Costs	**Party who bears the cost**
Police	Society/government
Prosecution	Society/government
Courts	Society/government
Legal fees	
– Public defenders	Society/government
– Private lawyers	Offenders
Criminal sanctions	Society/government
Victim and witness costs	Victim/Witnesses
Jury service	Jurors
Victim compensation	Society/government
Offender costs	
– Productivity	Offender/society
– Injury/death to offender while incarcerated	Offender/society
– Loss of freedom to offender	Offender
– Offender's family	Offender's family/society
Over deterrence costs	
– Innocent individuals accused of offences	Innocent "offenders"
– Restrictions on legitimate activities	Society
– Costs of additional detection avoidance by offenders	Offenders
Justice costs	Society
CSIRTs	Society/government

Table 3.1: Taxonomy of crime costs – response to crime (extended from [6])

The costs of society's response to cyber crime could be estimated by the law enforcement agencies' budgets. However, these will only represent a lower bound estimate of the society's total expenditure on response to cyber crime. Often, boundaries between cyber crime reducing efforts and other activities are blurred. For instance, probation officers and lawyers do not exclusively handle cyber criminals. Table 3.1 shows the main response costs and the parties that bear the cost. Though most of the response costs are borne by the society, offenders and victims also suffer from the society's response. Furthermore, as the criminal justice system is funded by the taxpayer, the impact of the society response also causes long term distortions on the economy. Society losses go beyond the mere amount of taxes.

One of the most prominent responses to cyber crime is the creation of Computer security incident response teams (CSIRTs). CSIRTs are commonly used by large companies and government agencies to help mitigate cyber threats and insulate them from future attacks. The costs of building and operating the CSIRT will depend on the number and types of services provided [48], as well as: the size of the constituency they are provided to; the administrative costs for the area or organisation; and the structure of the CSIRT. Infrastructure costs and salary/wages/benefits are the largest costs of a CSIRT. The infrastructure should incorporate all known precautions that are physically and financially possible. Common CSIRT infrastructure includes [47]:

- CSIRT networks, systems, and internal/external defences such as routers, firewalls, and IDS;
- databases, data repositories, and data analysis tools for storing CSIRT and incident information;
- CSIRT tools and applications to support incident handling and other provided services;
- mechanisms or applications for secure email and voice communications;
- physical location and security of CSIRT staff and data;
- staff office and home equipment.

Besides staff and infrastructure costs, CSIRTs also require [47]:

- incident reporting and tracking system;
- communications mechanisms:

  - hotline or helpdesk;
  - web site and/or ftp site;
  - mailing distribution lists;
  - cell phones and pagers.

- secure communications mechanisms:
  - PGP keys or digital certificates for signing CSIRT documents and mailings;
  - secure phones;
  - Intranets or extranets.

- secured access to CSIRT facilities.

Equipment expenditures usually do not constitute a significant cost except for those CSIRTs that require state-of-the-art labs to provide their services. That said, technology prices keep decreasing over time while labour rates continue increasing. This increase in labour rate is related to two more important cost centres; travel and training. CSIRTs staff need to stay up-to-date with technology changes and attack innovations. To achieve that, cyber security professionals need to develop their skills and join costly training courses. The total cost of training and travel budget is a relative pittance compared to salary and benefits. On the other hand, the legal and regulatory certification and accreditation environment can also drive significant costs.

CERT type	Estonia	UK	Netherlands	Italy	Germany	Poland
National/Governmental	1	2	2	5	4	2
Military	1	1	1	1	1	0
Research and Education	0	6	6	1	3	1
Financial Sector	0	3	3	0	4	0
Service Provider Customer Base	0	5	1	1	4	0
ISP Customer Base	0	1	2	1	2	2
Commercial Organisation	0	3	1	0	8	1
Non-ICT Sector	0	1	0	0	1	0
Local Agencies	0	0	0	2	0	0
ICT Vendor Customer Base	0	0	0	0	2	0
Total	2	22	16	11	29	6

Table 3.2: CSIRTs by Country

The number of CSIRTs vary per sectors and countries. Table 3.2 shows the distribution of CSIRTs for each of the countries of interest for the E-CRIME project. Note that the financial sector is the one with more CSIRTs. Besides the regional CSIRTs, there are also international CSIRTs (e.g. Cisco CSIRT, Interpol ISIRT, Team Cymru) that operate in several countries and European CSIRTs (e.g. CERT-EU) [14].

Finally, cyber security awareness take place at all levels of society on a broad and continuous basis as a response to cyber crime. This includes information portals dedicated to the consumer as are present in many countries such as Germany [11]. The primary purpose of security awareness is to influence the adoption of secure behaviours. These campaigns are quite costly as they aim at reaching a broad audience.

Table 3.3 shows a summary of the costs of different awareness campaigns. These costs range from several thousands of Euros to several millions. These differences are not only due to different campaign duration but also to the way the campaigns were carried out. For instance, the campaign launched by the French Ministry of the Family in 2006 consisted in broadcasting a series of 10 commercials [13] on TV.

Organizing entity	**Country**	**Total cost**	**Period**
Family en ligne (family online)	France	1 million euro	1 year
German Federal Office of IT security	Germany	222,038 euro	4 years
Center for Secure Information Technologies	Ireland	20 million pounds	5 years
National Cyber security Alliance	USA	3.75 million USD	3 years

Table 3.3: Selected awareness campaign costs [7]

In summary, the society's response to cyber crime is broad and costly. Societal response to cyber crime includes a variety of items that can be neither quantified nor monetised. While some costs are relatively easy to estimate, others are virtually impossible. Law enforcement agencies have to invest staff and dedicated equipment to fight cyber crime that amounts for several millions euros per year. The rest of the criminal justice system also suffer similar costs. Besides investigators and sworn officers, public defenders and prosecutors have to be trained to understand cyber crime. Cyber criminals have to be brought to trial and convicted which imposes more costs to society. But the society's response is not limited to the actions taken by the criminal justice system. Multiple CSIRTs and awareness campaigns have been created in different countries to mitigate the economic impact of cyber crime. In total, the society's response to cyber crime could be as costly as the potential losses.

Conclusions

The five non-ICT sectors analysed in this project suffer from cyber crime but to different degrees. The economic impact of cyber crime varies by industry segment, where financial services and energy companies experience higher impact than entities in retail, transport and health care sectors. Moreover, the short-term economic impact is not distributed uniformly across the different categories. Some sectors like financial services and retail have costs across all three categories while other sectors like health care mainly have anticipation costs. Table 4.1 presents a comparison of the short-term economic impacts per sector. The response of society also varies per sector. Again, the financial services sector is the one that experiences most of the costs.

		Health care	Financial	Retail	Transport	Energy
Anticipation	Security services and products	■ ■ ■ ■ ▫	■ ■ ■ ■ ■	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ■ ■ ▫
	Security policies	■ ■ ■ ■ ▫	■ ■ ■ ■ ▫	■ ■ ■ ▫ ▫	■ ■ ▫ ▫ ▫	■ ■ ■ ■ ■
	Security assessments	■ ▫ ▫ ▫ ▫	■ ■ ■ ▫ ▫	■ ▫ ▫ ▫ ▫	■ ■ ▫ ▫ ▫	■ ■ ■ ■ ■
	Insurance costs	■ ▫ ▫ ▫ ▫	■ ■ ■ ▫ ▫	■ ▫ ▫ ▫ ▫	■ ■ ■ ■ ▫	■ ■ ■ ■ ▫
Consequence	Stolen funds	▫ ▫ ▫ ▫ ▫	■ ■ ■ ■ ■	■ ■ ■ ■ ▫	■ ▫ ▫ ▫ ▫	■ ▫ ▫ ▫ ▫
	Pain&Suffering	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ■ ■ ▫	■ ▫ ▫ ▫ ▫	■ ▫ ▫ ▫ ▫
	Cost of disruption	■ ■ ▫ ▫ ▫	■ ■ ■ ■ ▫	■ ■ ■ ■ ▫	■ ■ ■ ■ ■	■ ■ ■ ■ ■
	Repair costs	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ▫ ▫ ▫	■ ■ ■ ▫ ▫
	Reputation Damage	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫	■ ▫ ▫ ▫ ▫	■ ■ ▫ ▫ ▫	■ ■ ▫ ▫ ▫
	IP loss	▫ ▫ ▫ ▫ ▫	▫ ▫ ▫ ▫ ▫	▫ ▫ ▫ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ■ ■ ▫
Response	Criminal Justice System	■ ■ ▫ ▫ ▫	■ ■ ■ ■ ▫	■ ■ ■ ▫ ▫	■ ▫ ▫ ▫ ▫	■ ▫ ▫ ▫ ▫
	Awareness initiatives	■ ■ ▫ ▫ ▫	■ ■ ■ ■ ▫	■ ■ ▫ ▫ ▫	■ ■ ■ ▫ ▫	■ ■ ■ ▫ ▫
	CSIRTs	▫ ▫ ▫ ▫ ▫	■ ■ ■ ■ ▫	▫ ▫ ▫ ▫ ▫	▫ ▫ ▫ ▫ ▫	■ ■ ▫ ▫ ▫

Table 4.1: Qualitative comparison of the prevalence of each short-term economic impacts per sector

On the other hand, the estimates of the costs of identity theft to the financial and retail

sector from the consumer perspective collected through the E-CRIME survey revealed that:

- the UK and Germany present the highest prevalence of identity theft while Estonia and Poland are least affected;
- the majority of cyber crime victims ($> 90\,\%$) loses time, a smaller percentage loses money ($33\,\%$);
- banks cover a large part of the loses due to cyber crime through compensation (two-times the losses of victims);
- PayPal covers the most (four-times the losses of victims). Probably, investing less into security and accepting the crime;
- online shopping providers only cover half of the costs;
- Costs are passed on from the financial to the retail sector.

Our qualitative assessments provide a significant advantage over previous estimates as they are not aligned with any particular cyber crime, population, or setting, which will permit future research to incorporate this information into any other sector. Considering the challenges and limitations noted in D6.1, greater coverage, better data, and more advanced methods are needed to improve precision of the quantitative estimates.

Based on the qualitative and quantitative assessments of the five non-ICT sectors, this report raises and considers some important questions for the policing of economic cyber crime that will be treated in the next workpackages. According to the critical economic impacts identified in this report, WP7 will look at how possible policing responses may be developed and what the future of policing might look like when addressing economic cyber crime on the different non-ICT sectors.

Bibliography

[1] American Academy of Family Physicians. Family Medicine Facts. http://www.aafp.org/about/the-aafp/family-medicine-facts.html, 2014.

[2] Peter Badcock. OV-Chipkaart roll-out creeps forward. http://www.esmc.eu/pdf/Cargo_Theft_Report.pdf, 2009.

[3] Walt Beadling and Keith Lewis. Cargo Theft by Fictitious Pick-up. http://www.kaamco.org/main/coc/docs/131205-CargoTheftByFictitiousPickup.pdf, 2013.

[4] Penpak Boonla. *Indirect Human Cost of Implementing the OV-chipcard in the Netherlands*. Erasmus University, 2011.

[5] Gordon Caldwell. Logging in and logging out: patient safety on ward rounds. *British Journal of Healthcare Management*, 17(11):547–553, 2011.

[6] M.A. Cohen. *The Costs of Crime and Justice*. Taylor & Francis, 2004. ISBN 9781135994501.

[7] Chris Connolly, Alana Maurushat, David Vaile, and Peter van Dijk. An overview of international cyber-security awareness raising and educational initiatives. Technical report, Australian Communications and Media Authority, 2011.

[8] Sabina De Rosis and Chiara Seghieri. Basic ICT adoption and use by general practitioners: an analysis of primary care systems in 31 European countries. *BMC medical informatics and decision making*, 15(1):1, 2015.

[9] V. Dekker. Journalisten reizen gratis met gekraakte ov-chip. http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1841751/2011/01/25/Journalisten-reizen-gratis-met-gekraakte-ov-chip.dhtml, 2011.

[10] Catherine M. DesRoches, Eric G. Campbell, Sowmya R. Rao, Karen Donelan, Timothy G. Ferris, Ashish Jha, Rainu Kaushal, Douglas E. Levy, Sara Rosenbaum,

Alexandra E. Shields, and David Blumenthal. Electronic health records in ambulatory care — a national survey of physicians. *New England Journal of Medicine*, 359(1):50–60, 2008.

[11] ECO. Association of the Internet Industry. https://international.eco.de/.

[12] Daniel Ekwall. The displacement effect in cargo theft. *International Journal of Physical Distribution & Logistics Management*, 39(1):47–62, 2009. doi: 10.1108/09600030910929183.

[13] ENISA. Information Security Awareness: Local Government and Internet Service Providers, 2007.

[14] ENISA. CERT Inventory of CERT teams and activities in Europe. https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe, 2015.

[15] Estonian e-Health Foundation. Estonian National Health Information System. http://www.e-tervis.ee, 2016.

[16] European Central Bank. Fourth report on card fraud. https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf, 2015.

[17] European Central Bank. Payment Statistics. https://www.ecb.europa.eu/stats/money/payments/paym/html/payments_nea_v_I00.VT.Z01.E.en.html, 2015.

[18] EUROPOL. Cargo Theft Report. http://www.esmc.eu/pdf/Cargo_Theft_Report.pdf, 2009.

[19] Neil S Fleming, Steven D Culler, Russell McCorkle, Edmund R Becker, and David J Ballard. The financial and nonfinancial costs of implementing electronic health records in primary care practices. *Health Affairs*, 30(3):481–489, 2011.

[20] Neil S Fleming, Edmund R Becker, Steven D Culler, Dunlei Cheng, Russell McCorkle, Briget da Graca, and David J Ballard. The impact of electronic health records on workflow and financial measures in primary care practices. *Health services research*, 49(1pt2):405–420, 2014.

[21] Thomas Fox-Brewstert. Ukraine Claims Hackers Caused Christmas Power Outage. http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack, 2016.

[22] Geeta Dayal. How they hacked it: The MiFare RFID crack explained. http://www.computerworld.com/article/2537817/security0/how-they-hacked-it--the-mifare-rfid-crack-explained.html, 2008.

[23] Government Health IT Staff. Why sharing data is so hard. http://www.healthcareitnews.com/news/why-sharing-health-data-so-hard, 2014.

[24] Max Green. 25 quotes that show just how fed up physicians are with EHRs. http://www.beckershospitalreview.com/healthcare-information-technology/25-quotes-that-show-just-how-fed-up-physicians-are-with-ehrs.html, 2015.

[25] Trisha Greenhalgh, Katja Stramer, Tanja Bratan, Emma Byrne, Jill Russell, and Henry WW Potts. Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. *Bmj*, 340:c3111, 2010.

[26] Trisha Greenhalgh, Libby Morris, Jeremy C Wyatt, Gwyn Thomas, and Katey Gunning. Introducing a nationally shared electronic patient record: Case study comparison of Scotland, England, Wales and Northern Ireland. *International journal of medical informatics*, 82(5):e125–e138, 2013.

[27] Susan Hall, Peter Murchie, Christine Campbell, and Scott A Murray. Introducing an electronic Palliative Care Summary (ePCS) in Scotland: patient, carer and professional perspectives. *Family practice*, 29(5):576–585, 2012.

[28] Jayna M Holroyd-Leduc, Diane Lorenzetti, Sharon E Straus, Lindsay Sykes, and Hude Quan. The impact of the electronic medical record on structure, process, and outcomes within primary care: a systematic review of the evidence. *Journal of the American Medical Informatics Association*, 18(6):732–737, 2011. ISSN 1067-5027.

[29] Homeland Security Research Corp. (HSRC). U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020. http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/, 2015.

[30] InterSystems Corporation. Caché Security Administration Guide. http://docs.intersystems.com/documentation/cache/20091/pdfs/GCAS.pdf, 2009.

[31] Chris Johnstone and Gerry McCartney. A patient survey assessing the awareness and acceptability of the emergency care summary and its consent model in Scotland. *Perspectives in health information management/AHIMA, American Health Information Management Association*, 7(Spring), 2010.

[32] Patrick Kierkegaard. Electronic health record: Wiring Europe's healthcare. *Computer law & security review*, 27(5):503–515, 2011.

[33] David Kushner. The real story of stuxnet. *Spectrum, IEEE*, 50(3):48–53, 2013.

[34] Hallvard Lærum, Gunnar Ellingsen, and Arild Faxvaag. Doctors' use of electronic medical records systems in hospitals: cross sectional survey. *Bmj*, 323(7325):1344–1348, 2001.

[35] Robert Lowes. Stolen EHR Charts Sell for $50 Each on Black Market. *Medscape Medical News*, 2014.

[36] Matt Warman. Sony pays 250,000 pounds PSN hack fine. http://www.telegraph.co.uk/technology/sony/10180338/Sony-pays-250000-PSN-hack-fine.html, 2016.

[37] Milieu Ltd. and time.lex. Overview of the national laws on electronic health records in the EU Member States. http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf, 2014.

[38] Elizabeth Mitchell and Frank Sullivan. A descriptive feast but an evaluative famine: systematic review of published articles on primary care computing during 1980-97. *BMJ*, 322(7281):279–282, 2001. ISSN 0959-8138.

[39] National Cyber Security Alliance. National small business study. http://www.connecticutbusinesslitigation.com/uploads/file/Stay%20Safe%20Online%20Small%20Business%20Study.pdf, 2012.

[40] National Information Systems Group. Key Information Summary (KIS). http://www.nisg.scot.nhs.uk/why-nisg/our-services/project-management/key-information-summary-kis, 2014.

[41] Jennie Olofsson. 'Zombies ahead!' A study of how hacked digital road signs destabilize the physical space of roadways. *Visual Communication*, 13(1):75–93, 2014.

[42] National Research Council (US). Committee on Freight Transportation Information Systems Security. *Cybersecurity of freight information systems: a scoping study*, volume 274. Transportation Research Board Computer Science and Telecommunnications, 2003.

[43] Tara O'Neill. Are electronic medical records worth the costs of implementation? http://americanactionforum.org/research/are-electronic-medical-records-worth-the-costs-of-implementation, 2015.

[44] IU Rahman. Role of information technology in banking industry. *Review of Business Research*, 7(6), 2007.

[45] Andrew Ross. The human threat. In *Intelligent Rail Infrastructure*, pages 1–26. IET, 2015.

[46] Pieter Siekerman and Maurits van der Schee. Security evaluation of the disposable ov-chipkaart v1. 7. 2007.

[47] Software Engineering Institute. Creating a CSIRT: Getting Started. http://www.cert.org/incident-management/csirt-development/resources-creating-csirt.cfm, 2016.

[48] Software Engineering Institute. CSIRT Services. http://www.cert.org/incident-management/services.cfm, 2016.

[49] Statista GmbH. Online banking penetration in selected European markets. http://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/, 2015.

[50] Symantec. Cyber Security for Financial Services. https://www.symantec.com/content/en/us/enterprise/white_papers/cybersecurity-whitepaper-financial-wp-21352892.pdf, 2015.

[51] Tim Wilson. Genesco Sues Visa Over $13 Million In PCI Noncompliance Penalties. http://www.darkreading.com/attacks-breaches/genesco-sues-visa-over-$13-million-in-pci-noncompliance-penalties/d/d-id/1139360, 2013.

[52] J Ulster Med. NIECR-a quiet revolution. *Ulster Med J*, 84(1):1–2, 2015.

[53] Frank Umbach. Electricity supplies are highly vulnerable to cyber attacks. http://www.worldreview.info/content/electricity-supplies-are-highly-vulnerable-cyber-attacks, 2013.

[54] US Department of Health and Human Services. Summary of the HIPAA privacy rule. *Washington, DC: Department of Health and Human Services*, 2003.

[55] Guido van't Noordende. Security in the Dutch Electronic Patient Record System. In *Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-care Systems*, SPIMACS '10, pages 21–32, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0094-0.

[56] Verizon. 2015 data breach investigations report. https://its.ny.gov/sites/default/files/documents/rp_data-breach-investigation-report-2015_en_xg.pdf, 2015.

[57] Rebecca Wong. *Data security breaches and privacy in Europe*. Springer, 2013.

[58] Candid Wueest. Attacks Against the Energy Sector. http://www.symantec.com/connect/blogs/attacks-against-energy-sector, 2015.