Security and Privacy Lab
Institut für Informatik
Universität Innsbruck

E-CRIME Policy Brief

The Costs of Consumer-facing Cyber Crime in Europe

Markus Riek, Rainer Böhme[1]

In an increasingly connected world cyber crime has affected almost everyone, from individual consumers to big companies, at some point in time. The proliferation of online services which require financial transactions, such as online banking and shopping, opens unprecedented opportunities and attracts specialized profit-oriented criminals.

The E-CRIME Project (the economic impacts of cyber crime) is a three year project that started in April 2014 and will end in March 2017. The aim of the project is to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of the European society, while also identifying and developing concrete measures to manage and deter cyber crime. (Website: `http://ecrime-project.eu`).

Victimization Survey In order to build effective measures against cyber crime based on empirical evidence, an essential part of E-CRIME concerns the measurement of cyber crime prevalence and the estimation of the social and economic impact. Empirical data on the costs of consumer-facing cyber crime has been collected through representative victimization surveys in six European countries: Germany, Estonia, Italy, the Netherlands, Poland, and the UK (in protocol order). The results focus on the costs borne by consumers, but also uncover businesses implications for non-ICT sectors.

Key results

- Germany and the United Kingdom are most affected by cyber crime.
- Monetary losses of cyber crime victims are zero-inflated, i. e. many victims lose nothing.
- Loss distributions are skewed, i. e. most victims lose small amounts and a few lose a lot.
- Victims of identity theft typically receive substantial compensation payments.
- Scams have the severest impact on the victims.
- Time loss is a substantial factor of the economic costs of cyber crime.
- Consumers' protection expenses are considerably higher than their losses to cyber crime.

This brief introduces the E-CRIME survey (Sec. 1), reports cybercrime prevalence (Sec. 2), describes the estimation of victim losses (Sec. 3), and finally reports national cost estimates (Sec. 4). Information beyond this brief can be found in the working paper: *How to estimate the costs of consumer-facing cyber crime: An instrument and representative data for six EU countries* by Riek et al. 2016 (`http://informationsecurity.uibk.ac.at/people/markus-riek/`).

[1]Security and Privacy Lab, Institute of Computer Science, University of Innsbruck (UIBK), Austria

1 E-CRIME survey

Data collection The aim of the E-CRIME survey is to collect first-hand data on EU citizens' experiences with cyber crime, to measure its prevalence and estimate its economic costs. A telephone survey was carried out by IPSOS in six EU member states (in protocol order): Germany (DE), Estonia (EE), Italy (IT), the Netherlands (NL), Poland (PL), and the United Kingdom (UK), between July 2015 and October 2015. The target population for the survey was the general population, aged 18+, who use the Internet for personal purposes at least on a monthly basis. Overall $6\,394$ responses have been collected. Because cybercrime victims are relatively rare, 256 additional victims were included in a second sampling phase (oversampling), leading to an overall subpopulation of $(1\,242)$ victims.

Population surveys are best suited to study crimes with a direct relationship between the victim and the criminal. Table 1 shows the seven types of (profit-oriented) consumer-facing cybercrime which are covered in the survey along with the original wording of the question.

Table 1: Consumer-facing cyber crimes with original question wording

Thinking of the past 5 years, have you ever personally experienced any of the following?	
Identity theft wrt. online banking	*Someone getting access to your bank account password (to buy something in your name, take money from your account, open a credit etc.)*
Identity theft wrt. bank cards	*Someone getting access to your bank card security numbers (to buy something in your name)*
Identity theft wrt. PayPal	*Someone getting access to your PayPal password (to buy something in your name, or take money from your account)*
Identity theft wrt. online shopping	*Someone getting access to your online shopping account (e. g., Amazon etc.), to buy something in your name*
Online shopping fraud	*Products or services which you have purchased online not being delivered, being defective or of different quality than advertised*
Extortion	*Someone extorting money from you to recover access to an account or your computer*
Scams	*Someone tricking you to transfer money to a fraudulent website*
Malware infections	*Do the following statements apply to you? During the past 5 years, I have had malware/viruses on my computer*

Cost estimation To improve the quality of estimates and derive meaningful results from the survey-based data, E-CRIME uses a systematic framework, which distinguishes different aggregate cost categories and cost factors. The cost categories comprise *victim losses* and *expenses for preventive protection measures*. Within both categories the money and the time that is lost are estimated and aggregated. Furthermore, different estimation methods are evaluated in order to derive robust cost estimates, which respect the distributional characteristics of the costs.

2 Cyber crime prevalence

Table 2 shows the prevalence of cybercrime in the six surveyed countries. Each cell represents the percentage of adult Internet users who reported to have experienced any type of cybercrime during the last five years.[2]

Total cyber crime is most prevalent in Germany and the UK, with approximately $22\,\%$ of adult Internet users reporting at least one incident. This is driven by the highest incident rates for extortion ($5.1\,\%$), scams ($5\,\%$), and IDT wrt. to online shopping ($4.3\,\%$) in Germany. The UK is most affected by cyber crimes associated with financial accounts, with the highest incident rates for IDT wrt. online banking ($3.3\,\%$), bank cards ($4.8\,\%$), and PayPal accounts ($2.3\,\%$). The Netherlands have the highest prevalence of online shopping fraud ($10.3\,\%$). Overall, Italy ($12.1\,\%$) and Estonia ($13.2\,\%$) are least affected by cyber crime. We surveyed malware inf

Table 2: Incident rates of cybercrime by type and country

	Internet users victimized in the last 5 years						Losses	
Cybercrime	DE	UK	NL	PL	EE	IT	Money	Time
IDT wrt. o. banking	$1.4\,\%$	$3.3\,\%$	$1.4\,\%$	$1.2\,\%$	$1.0\,\%$	$1.1\,\%$	$34.1\,\%$	$97.7\,\%$
IDT wrt. bank cards	$3.5\,\%$	$4.8\,\%$	$2.0\,\%$	$0.9\,\%$	$1.7\,\%$	$2.7\,\%$	$34.4\,\%$	$98.5\,\%$
IDT wrt. PayPal	$2.0\,\%$	$2.3\,\%$	$0.7\,\%$	$0.8\,\%$	$0.4\,\%$	$0.9\,\%$	$24.4\,\%$	$97.6\,\%$
IDT wrt. o. shopping	$4.3\,\%$	$4.1\,\%$	$1.1\,\%$	$0.9\,\%$	$0.8\,\%$	$1.9\,\%$	$17.4\,\%$	$98.6\,\%$
O. shopping fraud	$8.4\,\%$	$9.0\,\%$	$10.3\,\%$	$9.7\,\%$	$9.1\,\%$	$5.0\,\%$	$90.9\,\%$	$90.3\,\%$
Extortion	$5.1\,\%$	$2.8\,\%$	$1.1\,\%$	$1.4\,\%$	$0.6\,\%$	$1.5\,\%$	$13.3\,\%$	$93.4\,\%$
Scams	$5.0\,\%$	$4.4\,\%$	$2.3\,\%$	$3.4\,\%$	$1.7\,\%$	$2.4\,\%$	$45.1\,\%$	$95.0\,\%$
Total	$22.2\,\%$	$21.6\,\%$	$15.7\,\%$	$13.9\,\%$	$13.2\,\%$	$12.1\,\%$		

Germany (DE), United Kingdom (UK), Netherlands (NL), Poland (PL), Estonia (EE), Italy (IT)

Cyber crime impact The last two columns of Table 2 provide further information on the impact of each type of cyber crime (across all countries), reported by victims for the severest incident. Consumers report a loss of time for the vast majority of incidents ($> 90\,\%$). This holds for all seven types of cyber crime, with up to $98.6\,\%$ for incidents of IDT wrt. online shopping. Monetary losses are less common. Even though data is collected for the severest incidents, the majority do not lead to a monetary loss. This is particularly true for extortion and IDT wrt. online shopping, for which less than $20\,\%$ of the incidents lead to monetary losses. Online shopping fraud is an exception, because consumers reported monetary losses in more than $90\,\%$ of the incidents. Note that this number is largely driven by our identification of victims of online shopping fraud, which used monetary losses as a proxy variable to identify victims. Across all crimes, only a minority of victims reports personal ($13.4\,\%$), professional ($3.8\,\%$), or other problems ($10.5\,\%$) resulting from cyber crime.

[2]The numbers include multiple victimization. However, with 79.2 %, the majority of the victims reported one single incident. 15.5 % experienced two incidents and only 5.3 % fell victim to more than two types of cybercrime.

3 Victim losses

Distribution of monetary losses Summary statistics of the losses of victimization are estimated for each type of cybercrime across all six countries. The left part of Figure 1 shows the distribution of initial losses of the 199 scam victims. The empirical distribution of the losses (histogram) shows that the majority of victims does not lose money, resulting in a *zero-inflated distribution*. Losses (if not zero) are is skewed to the right, meaning that most victims lose little, but a few lose a lot. This situation makes the mean (e. g., $488\,€$ for scams) and median (e. g., $0\,€$ for scams) unreliable and requires a more robust approach. E-CRIME estimates monetary losses using a "harmonized loss indicator", which scales the distribution-based median of positive losses by the probability of losses. This indicator produces estimates which are robust against the zero-inflation and large value outliers ($89\,€$ for scams).

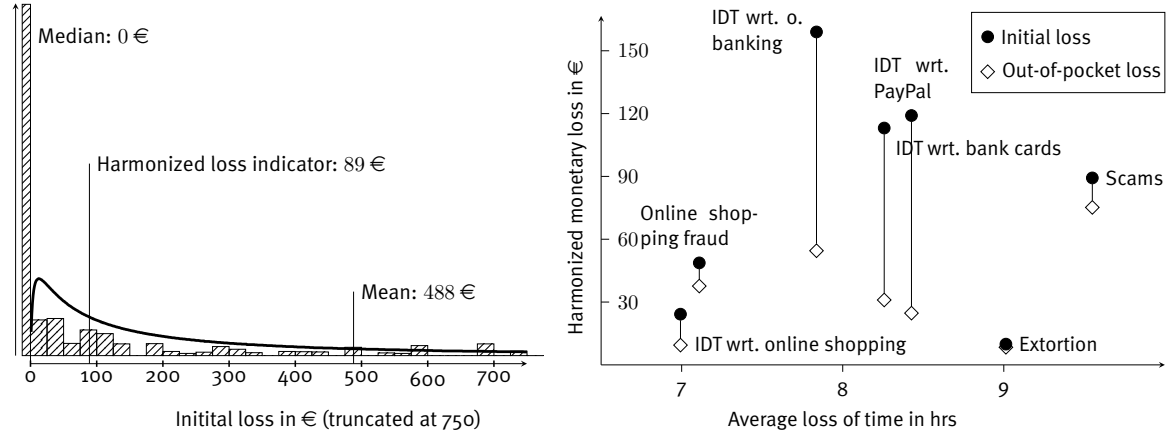

Figure 1: Losses of scam victims (left) and cyber crime impact map (right)

Cyber crime impact map The right part of Figure 1 orders the seven types of cyber crime according to their impact on the victim. The harmonized monetary loss defines the location of a crime on the y-axis and the average time lost defines the location on the x-axis. In addition to initial monetary losses (black circles), the out-of-pocket (OOP) losses (white diamonds) represent the ultimate losses after the reception of potential compensation payments. Obviously, cyber crimes in the upper right part of the map have a more serious impact on the victim, i. e. they result in bigger losses.

The impact map illustrates that the seven types of cyber crime fall into three categories, corresponding to third party involvement. The first category comprises incidents related to online shopping and is characterized by the smallest losses for consumers. The second category relates to financial services, comprising IDT wrt. online banking, bank cards, and PayPal. These crimes lead to the highest initial losses, but service providers bear large parts of the costs through compensation payments. Consequently, the OOP losses are comparable to the other types of cyber crime. While we suspected that receiving compensation requires more time, we could not find evidence for this effect in our data. The third category of crimes – extortion and scams – does not involve a third party. These crimes turn out to be most time-consuming and victims do not receive any compensation.

4 National cost estimates

Cyber crime losses, protection expenses, and total cyber crime costs are aggregated to the country level. We present two types of estimates for each country: α represents the costs per Internet user for the last five years in €, along with 90 % confidence intervals. β represents the annual costs per country in million euros.[3] All monetary cost estimates are based on the harmonized loss indicator, but a pure mean-based estimate is reported for comparison. The time lost is converted to monetary costs using the minimum wage in each country.

Table 3: Aggregate costs per country

	Germany		Estonia		Italy		NL		Poland		UK	
	α	β	α	β	α	β	α	β	α	β	α	β
Victims losses (base: cyber crime losses: 1 242 victims)												
Initial	18.66 [16:27]	270	10.19 [9:13]	2	10.91 [9:15]	90	12.78 [11:17]	41	11.94 [10:16]	64	22.87 [19:35]	275
OOP	10.11 [9:19]	146	6.00 [5:10]	1	5.58 [5:11]	46	7.36 [6:13]	23	7.51 [7:13]	40	11.13 [9:25]	134
Time	20.43 [19:21]	295	2.74 [3:3]	1	9.02 [8:9]	75	13.47 [12:14]	43	3.47 [3:4]	18	19.62 [19:21]	236
Total	39.09 [35:47]	565	12.93 [12:16]	3	19.92 [18:24]	165	26.25 [24:31]	83	15.42 [14:20]	82	42.49 [38:55]	512
Protection expenses (base: full sample 6 242 respondents)												
Monetary	84.48 [77:89]	1221	17.73 [13:19]	4	54.79 [48:59]	453	78.90 [73:86]	251	49.26 [45:53]	262	106.13 [97:112]	1279
Time	178.08 [168:194]	2573	29.07 [29:36]	7	110.09 [102:122]	910	172.27 [157:189]	547	40.29 [39:46]	214	119.54 [115:141]	1440
Total	262.57 [249:280]	3794	46.80 [43:53]	11	164.89 [153:177]	1363	251.17 [234:270]	798	89.55 [85:96]	476	225.67 [217:248]	2719
Total cyber crime costs												
Harm.	301.65 [288:322]	4359	59.73 [57:67]	14	184.81 [173:198]	1528	277.42 [261:297]	881	104.96 [101:114]	558	268.16 [261:296]	3230
Mean	396.19 [249:280]	5725	98.74 [43:53]	23	252.14 [153:177]	2085	344.24 [234:270]	1094	167.32 [85:96]	890	383.62 [217:248]	4621

α: Costs per Internet user for the last 5 years in €; β: Annual costs per country in million €; Out-of-pocket (OOP)

While Table 3 contains many insights, we only summarize a few key findings. **Cyber crime is time consuming**. The monetary equivalent of the time spend on protection is at least twice the monetary expenses in Germany, Italy, and the Netherlands. Only Polish consumers spend more money than time on protection. The results for victim losses are mixed, but tend towards more losses of time, when considering out-of-pocket losses. **Consumers are protective.** Protection expenses are substantially higher than cyber crime losses in all countries. This even holds if we only consider monetary expenses, which are at least twice the overall cyber crime losses in all countries except Estonia. **Protection efforts differ between countries.** The highest cyber crime prevalence in Germany and the UK correlates with the highest cyber crime losses. However, while German consumers mainly spend time on protection, UK consumers rather invest into protection measures. Dutch consumers spend comparatively much on protection considering the medium prevalence of cyber crime in the Netherlands.

[3] β is derived by multiplying α with the absolute population of Internet users in each country and dividing by 5.

About E-CRIME

Project type: Collaborative research project
Funding scheme: European Union Seventh Framework Programme (SEC-2013.2.5-2)
Start date: 1 April 2014
End date: 31 March 2017
Coordinator: David Wright – Trilateral Research & Consulting (TRI)
Grant agreement number: 607775
EU contribution: hm?

Project description

E-CRIME (the economic impacts of cyber crime) is a three year project that started in April 2014 and will end in March 2017. The aim of the project is to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of European society, while also identifying and developing concrete measures to manage and deter cyber crime. Further information can be found on the official website (`http://ecrime-project.eu`).

Contacts

Policy Brief Author: Markus Riek and Rainer Böhme (UIBK)
University of Innsbruck (UIBK), Austria
`markus.riek@uibk.ac.at`
Project Coordinator: David Wright
Trilateral Research & Consulting (TRI), UK
Dissemination: Timothy Mitchener-Nissen
Trilateral Research & Consulting (TRI), UK
`tim.nissen@trilateralresearch.com`
Website: `http://ecrime-project.eu`