Measuring the cost of cybercrime

Ross Anderson[1], Chris Barton, Rainer Boehme[2], Richard Clayton[1], Michel J.G. van Eeten[3], Michael Levi[4], Tyler Moore[5] and Stefan Savage[6]

Computer Laboratory, University of Cambridge, UK[1]
Department of Information Systems, University of Münster, DE[2]
Faculty of Technology, Policy and Mgmt., Delft University of Technology, NL[3]
School of Social Sciences, Cardiff University, UK[4]
Computer Science & Engineering Dept., Southern Methodist University, USA[5]
Computer Science & Engineering Dept., University of California, San Diego, USA[6]

11th Workshop on the Economics of Information Security,
Berlin, Germany
June 26, 2012

Outline

How much does cybercrime cost?

Cookies | Contact us | Press Office | Subscribe | News | Resource lib

CabinetOffice

Search

About the Cabinet Office | National Security | Constitutional Reform | Government Efficiency | Transparency | Big Society | Government: How it works

The cost of cyber crime

The overall cost to the UK economy from cyber crime is £27bn per year, according to the first joint Government and industry report into the extent and cost of cyber crime across the UK, launched today by the Office of Cyber Security & Information Assurance in the Cabinet Office and information intelligence experts Detica.

With society now almost entirely dependent on cyber space, developing effective strategies to tackle cyber crime requires a better understanding of its impact. Its breadth and scale have been notoriously difficult to understand and past attempts to set cyber crime policy or develop strategies have been hampered by a real lack of insight into the problem.

"The Cost of Cyber Crime" report reveals that whilst government and the citizen are affected by rising levels of cyber crime, at an estimated £2.2bn and £3.1bn cost respectively, business bears the lion's share of the cost. The report indicates that, at a total estimated cost of £21bn, over three-quarters of the economic impact of cyber crime in the UK is felt by business. In all probability, and in line with worst-case scenarios, the real impact of cyber crime is likely to be much greater.

Downloads

The Cost of Cyber Crime - summary report

Related links

Information Management – The National Archives

Related News and Media

Crime on your street revealed

Making travel safer in cyberspac

View all n

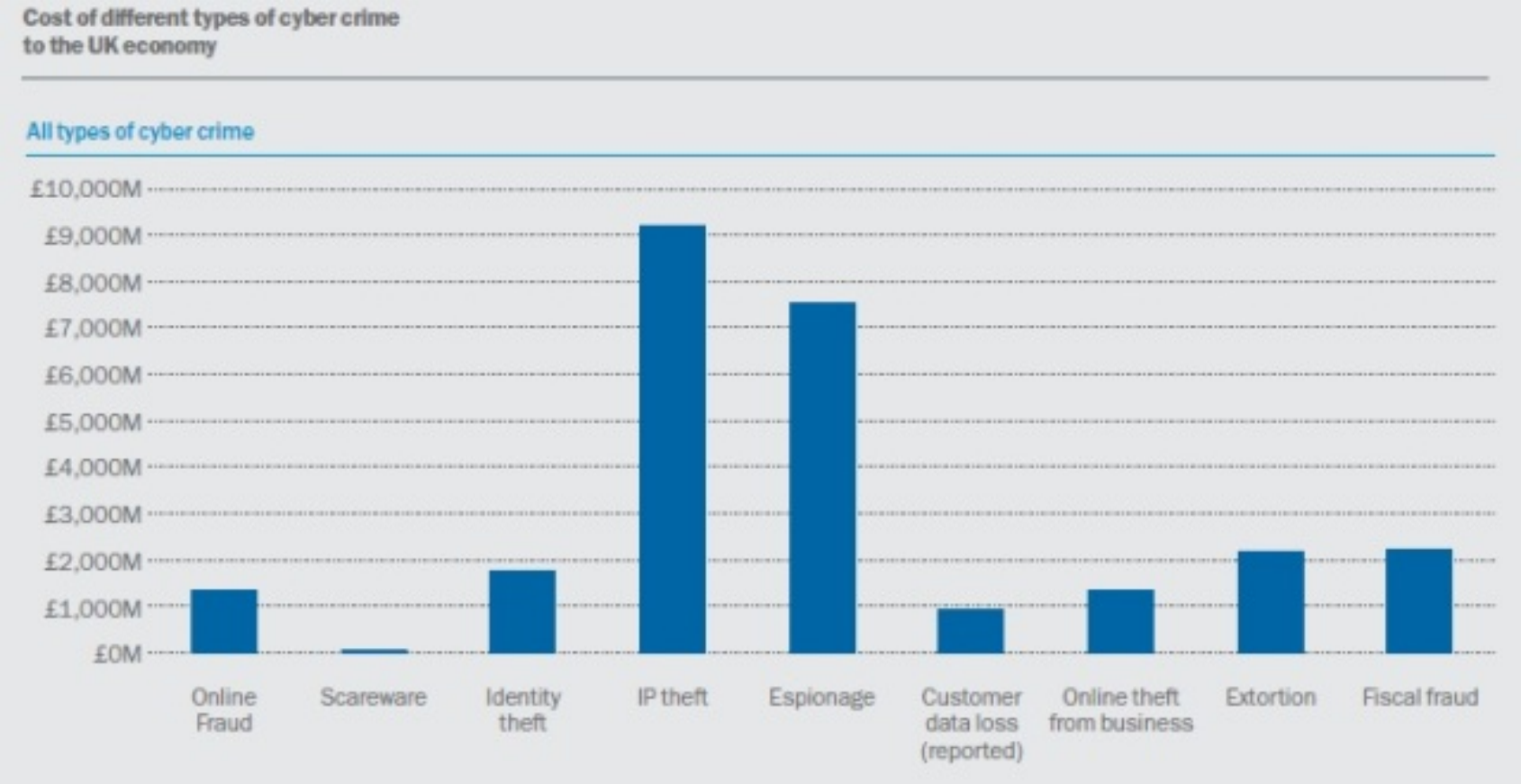
Most recent resources

1. Independent review into the barriers of public service choic
2. Individual Electoral Registratio

Can such high estimates really be right?

- In 2009 AT&T's Ed Amoroso testified before the US Congress that global cybercrime profits topped $1 trillion
- That's 1.6% of world GDP
- Detica's figure (£27 Bn) is 2% of UK GDP
- Not only are the figures eye-poppingly large, it's often unclear what is being measured
- Amoroso spoke of cybercrime 'profits', while Detica describes 'losses'

Upon closer inspection, the Detica estimates don't hold up



Upon closer inspection, the Detica estimates don't hold up

- IP theft (£9.2 Bn) and espionage (£7.6 Bn) account for 62% of the total loss estimate
- Yet the methodology for computing these estimates appears to rely extensively on random guesses
  - IP theft: buried on p. 16 of the report, the authors admit *"the proportion of IP actually stolen cannot at present be measured with any degree of confidence"*, so they assign probabilities of loss and multiply by sectoral GDP
  - Espionage: because *"it is very hard to determine what proportion of industrial espionage is due to cybercrime"*, the authors ascribe values to plausible targets and guess how often they might be pilfered

Why are poor cybercrime cost estimates dangerous?

MY TNO: Log in | Register
LANGUAGE: Nederlands | English
SEARCH

TNO innovation for life

HOME | THEMES | EXPERTISE | ABOUT US | DIRECTLY TO | WORKING AT TNO

PRESS

- Archive
- News
- Agenda
- TNO TIME
- Press Office
- Dossiers

TNO.NL › About Us › Press › News › Cost of Cyber Crime largely met by businesses

News

April 10, 2012

COST OF CYBER CRIME LARGELY MET BY BUSINESSES

Exploratory research by TNO has shown that cyber crime costs Dutch society at least 10 billion euros per annum, or 1.5 to 2 percent of our GDP. This equal to economic growth in the Netherlands in 2010. However, there are strong indications that the actual cost is two to three times higher than this. Further research is needed to identify precisely where impact is greatest and how the cost can be reduced.

TNO's findings are based on research carried out in the United Kingdom for the Home Office by consulting firm Detica. The Detica study is the first extensive study by an EU member state into the cost of cyber crime. TNO translated the findings into the situation in the Netherlands, and arrived at a figure of more than 10bn euros. Because the Netherlands is more vulnerable than the UK due to our dense cable network, advanced infrastructure and large volumes of data traffic, the actual impact is likely to be greater than this. Other research examined by TNO, including a study by Ernst & Young, confirms the suspicion that the cost is more in the region of 20 to 30 billion euros.

CONTACT

Ir. J.T. (Johan) Ruiter
+31 88 866 71 71
Contact me

› Contact & Directions

KEY WORDS

But can we do better?

- It is one thing to point out flaws in others' estimates, but it is quite another to produce a more reliable estimate of cybercrime losses
- The UK Ministry of Defence challenged us to produce a more accurate estimate
- What follows is our attempt to measure cybercrime losses using publicly available data

Outline

Outline

A working definition of cybercrime

- We adopt the European Commission's proposed definition:
  1. traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
  2. the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
  3. crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.
- The boundary between traditional and cybercrimes is fluid

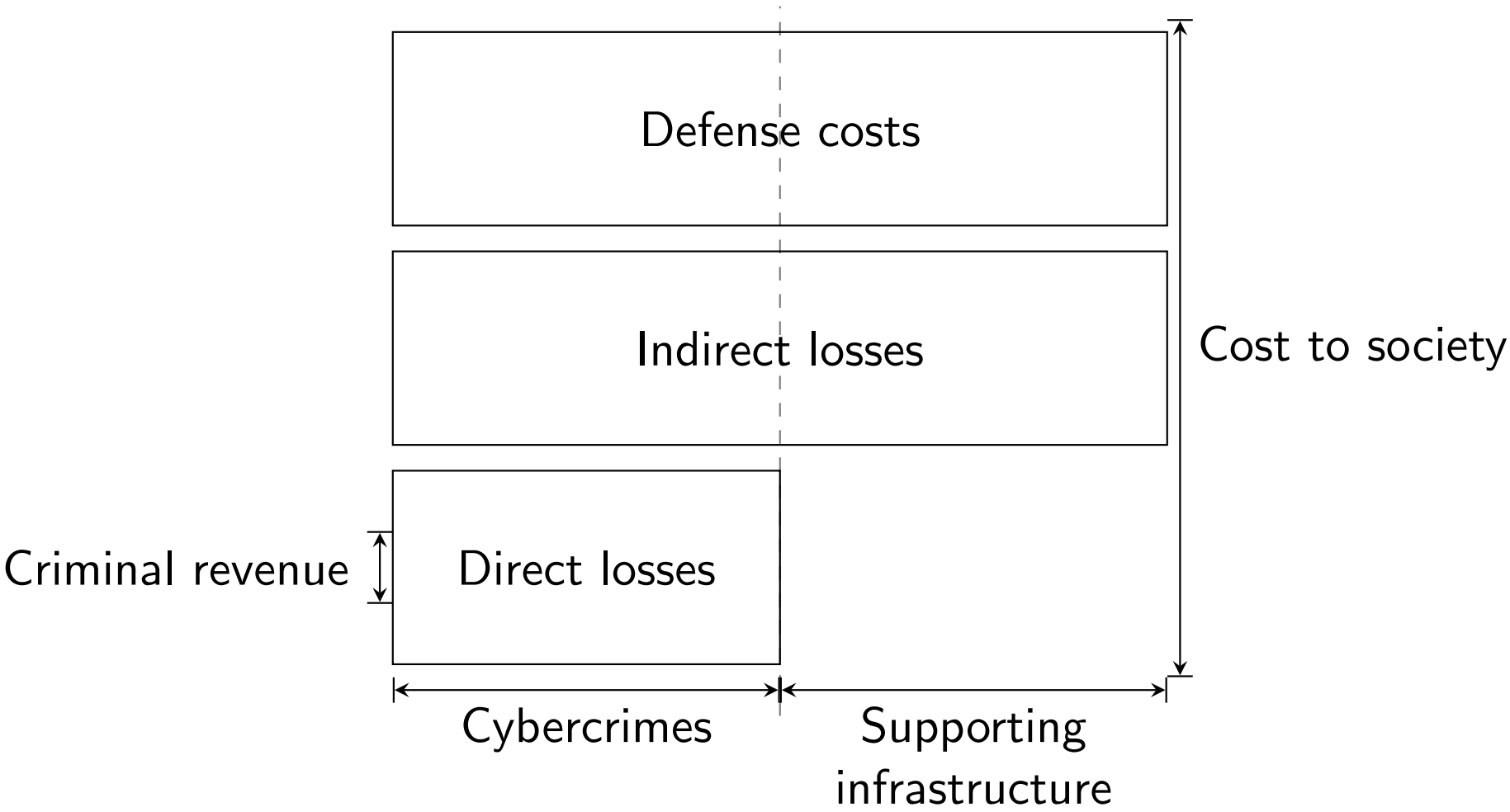
Decomposing the cost of cybercrime

- Many cybercrime measurement efforts conflate different categories of costs, which renders figures incomparable
- We break up the cost of cybercrime into four categories
  1. *Criminal revenue*: gross receipts from a crime
  2. *Direct losses*: losses, damage, or other suffering felt by the victim as a consequence of a cybercrime
  3. *Indirect losses*: losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out
  4. *Defense costs*: cost of prevention efforts
- We also distinguish between the primary costs of cybercrimes and the costs attributed to a common infrastructure used to perpetrate cybercrimes (e.g., botnets)

An example cost breakdown: phishing

- **Criminal revenue**
  - sum of the money withdrawn from victim accounts
  - revenue to spammer for sending phishing mails
- **Direct losses**
  - criminal revenue
  - time and effort to reset account credentials
  - secondary costs of overdrawn accounts (deferred purchases)
  - lost attention and bandwidth caused by spam messages
- **Indirect losses**
  - loss of trust in online banking
  - lost opportunity for banks to communicate via email
  - efforts to clean-up PCs infected with malware
- **Defense costs**
  - security products (spam filters, antivirus)
  - services for consumers (training) & industry ('take-down')
  - fraud detection, tracking, and recuperation efforts
  - law enforcement

Visualizing the component costs of cybercrime



Outline

Estimating cybercrime costs

- We investigated the literature to see what cybercrimes included data on losses
- Most data does not decompose cost by type, but rather include one or more of the types when calculating sums
- We only include crimes where annual costs exceed $10m
- We only include crimes where reliable data is available
- We distinguish between 'primary' cybercrimes and the common infrastructure used to perpetrate multiple attacks

Cybercrimes we considered

- Online banking fraud
- Fake antivirus
- 'Stranded traveler' scams
- 'Fake escrow' scams
- Advanced fee fraud
- Infringing pharmaceuticals
- Copyright-infringing software
- Copyright-infringing music and video
- Online payment card fraud
- In-person payment card fraud
- PABX fraud
- Industrial cyber-espionage and extortion
- Welfare fraud
- Tax and tax filing fraud

Cybercrimes we considered

- Online banking fraud
- Fake antivirus
- 'Stranded traveler' scams
- 'Fake escrow' scams
- Advanced fee fraud
- Infringing pharmaceuticals
- Copyright-infringing software
- Copyright-infringing music and video

} 'Genuine' cybercrime

- Online payment card fraud
- In-person payment card fraud
- PABX fraud
- Industrial cyber-espionage and extortion

} Transitional cybercrime

- Welfare fraud
- Tax and tax filing fraud

} Traditional crime becoming 'cyber'

Cost of genuine cybercrime

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Online banking fraud							
– phishing	$16m	**$320m**	2007	$\times^{?}$	$\times^{?}$		
– malware (consumer)	$4m	**$70m**	2010	$\times^{\downarrow}$	$\times^{\downarrow}$		
– malware (businesses)	$6m	**$300m**		$\times^{\downarrow}$	$\times^{\downarrow}$		
– bank tech. countermeasures	$50m	**$1 000m**	2010				$\times^{?}$
Fake antivirus	$5m	**$97m**	2008–10	$\times$	$\times$		
Copyright-infringing software	**$1m**	**$22m**	2010	$\times$	$\times$		
Copyright-infringing music etc	$7m	**$150m**	2011	$\times^{\downarrow}$			
Patent-infringing pharma	**$14m**	**$288m**	2010	$\times$			
Stranded traveler scam	$1m	**$10m**	2011	$\times^{\downarrow}$			
Fake escrow scam	$10m	**$200m**	2011	$\times^{\downarrow}$			
Advance-fee fraud	**$50m**	$1 000m	2011	$\times^{\downarrow}$			

Cost of transitional cybercrime

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Online payment card fraud	**$210m**	$4 200m	2010		(×)		
Offline payment card fraud							
– domestic	**$106m**	$2 100m	2010		$\times^{\downarrow}$		
– international	**$147m**	$2 940m	2010		$\times^{\downarrow}$		
– bank/merchant defense costs	$120m	**$2 400m**	2010				$\times^{\downarrow}$
Indirect costs of payment fraud							
– loss of confidence (consumers)	**$700m**	$10 000m	2010			$\times^{?}$	
– loss of confidence (merchants)	**$1 600m**	$20 000m	2009			$\times^{?}$	
PABX fraud	**$185m**	**$4 960m**	2011	×	$\times^{\downarrow}$		
Industrial cyber-espionage							

Case study: payment card fraud

- Criminal revenue due to card fraud is hard to estimate, but the UK banking industry does publish direct losses
  - Online payment card fraud: $210 million
  - Offline payment card fraud: $353 million
  - This only includes losses detected by the banks
  - Online fraud constitutes a large fraction but not the majority of direct losses
- Of course, direct losses are not the whole story

Case study: payment card fraud

- Indirect losses outweigh direct losses, but can be hard to precisely measure
- Consumer loss of confidence is an indirect losses
  - For consumers, we start with the Eurostat ICT survey, which finds that 14% of consumers avoided online purchases due to security concerns
  - Many simply purchased goods offline instead, but at higher search and distribution costs
  - So perhaps 10% of online purchases is foregone, implying indirect costs of $700 million due to UK consumer loss of confidence
- But merchants also lose confidence by refusing legitimate transactions

Case study: payment card fraud

- Merchants also lose confidence by refusing legitimate transactions
  - An industry survey of merchants reject 4.3% of transactions feared to be fraudulent
  - This is likely an overestimate, since the survey also finds direct losses twice as high as other sources
  - Rejecting 2% of legitimate transactions is more plausible
  - This translates to $1.6bn in lost sales

Case study: payment card fraud

- Finally, defense costs include the deployment of Chip and PIN
- Unfortunately no reliable estimates are publicly available
  - We start by noting the market leader, Ingenico, reported $907 million in sales and accounts for 38% of the market $\Longrightarrow$ $2.4 billion market
  - Total cost likely around 3 times as much, once you consider costs of integration, back-end systems, etc.
  - But the systems also offer improved functionality, not only security, so we will keep the defense cost estimate at $2.4 Bn

Returning to the cost matrix for card fraud

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Online payment card fraud	**$210m**	$4 200m	2010		(×)		
Offline payment card fraud							
– domestic	**$106m**	$2 100m	2010		$\times^{\downarrow}$		
– international	**$147m**	$2 940m	2010		$\times^{\downarrow}$		
– bank/merchant defense costs	$120m	**$2 400m**	2010				$\times^{\downarrow}$
Indirect costs of payment fraud							
– loss of confidence (consumers)	**$700m**	$10 000m	2010			$\times^{?}$	
– loss of confidence (merchants)	**$1 600m**	$20 000m	2009			$\times^{?}$	

Cost of traditional crime becoming cyber

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Welfare fraud	**$1 900m**	$20 000m	2011	×	(×)		
Tax fraud	**$12 000m**	$125 000m	2011	×?	(×)		
Tax filing fraud	-	**$5 200m**	2010	×	(×)		

The infrastructure supporting cybercrime

- Much of the cybercriminal infrastructure is used in many scams (e.g., botnets, spam)
- Furthermore, indirect losses and defense costs are also commonly affected by scams (e.g., loss of trust, antivirus software)
- To avoid double counting, we measure these separately from the primary aim of the cybercrime

Cost of cybercriminal infrastructure

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Expenditure on antivirus	**$170m**	$3 400m	2012				×
Cost to industry of patching	$50m	**$1 000m**	2010				×?
ISP clean-up expenditures	**$2m**	$40m	2010			×?	
Cost to users of clean-up	**$500m**	$10 000m	2012			×?	
Defense costs of firms generally	$500m	**$10 000m**	2010				×?
Expenditure on law enforcement	**$15m**	$400m	2010				×

What about cyber espionage?

- We chose not to include numerical estimate for cost of industrial espionage
- This is not because we think it doesn't exist
- Instead, it is because there is no reliable data available
- Furthermore, the harm caused by unauthorized data access is often less than claimed
  - No publicly reported instance of a drug firm missing out on a patent due to prior unauthorized exposure
  - Source code is made widely available by necessity – many organizations have access to Windows source code under NDA

Important caveats

- None of the data we have is perfect
- Lots of incomplete data on different costs
- Our hope is that future studies can take additional cost components into account
- We explicitly chose not to add up the costs and provide a single cost number
- Estimates are often rough, and the uncertainty in some calculations may dwarf others

Comparing costs across categories

- We can still usefully compare relative costs across categories
- Cost per citizen
  - Traditional frauds such as tax and welfare fraud: a few hundred pounds/euros/dollars a year
  - Transitional frauds such as payment card fraud: a few tens of pounds/euros/dollars a year
  - New cyber frauds such as fake antivirus: a few tens of pounds/euros/dollars a year, but the vast bulk are indirect and defense costs

Comparing direct to indirect costs

- Genuine cybercrimes don't yield much revenue for criminals: each category earns a few tens of pence/cents per citizen
- However, indirect and defense costs are roughly ten times the sum of revenue due to all new online scams
- This asymmetry is not found in many traditional crimes and for transitional cybercrime
- Consequently, more investment in law enforcement can be especially valuable if it can reduce indirect costs and defense expenditures

Conclusions

- Be wary of outlandishly large cybercrime cost estimates
- We provided the first systematic and comprehensive examination of cybercrime costs
- Indirect and defense costs dominate new cybercrimes, so increased law enforcement efforts would be a wise investment
- More research on e-crime: `http://lyle.smu.edu/~tylerm/` and `http://www.lightbluetouchpaper.org/`

To actually read the figures, look at the paper

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
Cost of genuine cybercrime							
Online banking fraud							
– phishing	$16m	**$320m**	2007	$\times^{?}$	$\times^{?}$		
– malware (consumer)	$4m	**$70m**	2010	$\times^{\downarrow}$	$\times^{\downarrow}$		
– malware (businesses)	$6m	**$300m**		$\times^{\downarrow}$	$\times^{\downarrow}$		
– bank tech. countermeasures	$50m	**$1 000m**	2010				$\times^{?}$
Fake antivirus	$5m	**$97m**	2008–10	×	×		
Copyright-infringing software	**$1m**	**$22m**	2010	×	×		
Copyright-infringing music etc	$7m	**$150m**	2011	$\times^{\downarrow}$			
Patent-infringing pharma	**$14m**	**$288m**	2010	×			
Stranded traveler scam	$1m	**$10m**	2011	$\times^{\downarrow}$			
Fake escrow scam	$10m	**$200m**	2011	$\times^{\downarrow}$			
Advance-fee fraud	**$50m**	$1 000m	2011	$\times^{\downarrow}$			
...							
Cost of transitional cybercrime							
Online payment card fraud	**$210m**	$4 200m	2010		(×)		
Offline payment card fraud							
– domestic	**$106m**	$2 100m	2010		$\times^{\downarrow}$		
– international	**$147m**	$2 940m	2010		$\times^{\downarrow}$		
– bank/merchant defense costs	$120m	**$2 400m**	2010				$\times^{\downarrow}$
Indirect costs of payment fraud							
– loss of confidence (consumers)	**$700m**	$10 000m	2010			$\times^{?}$	
– loss of confidence (merchants)	**$1 600m**	$20 000m	2009			$\times^{?}$	
PABX fraud	**$185m**	**$4 960m**	2011	×	$\times^{\downarrow}$		
...							
Cost of cybercriminal infrastructure							
Expenditure on antivirus	**$170m**	$3 400m	2012				×
Cost to industry of patching	$50m	**$1 000m**	2010				$\times^{?}$
ISP clean-up expenditures	**$2m**	$40m	2010			$\times^{?}$	
Cost to users of clean-up	**$500m**	$10 000m	2012			$\times^{?}$	
Defense costs of firms generally	$500m	**$10 000m**	2010				$\times^{?}$
Expenditure on law enforcement	**$15m**	$400m	2010				×
...							
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	**$1 900m**	$20 000m	2011	×	(×)		
Tax fraud	**$12 000m**	$125 000m	2011	$\times^{?}$	(×)		
Tax filing fraud	-	**$5 200m**	2010	×	(×)		
...							