Measuring Cybercrime

Richard Clayton

Ballarat
4th December 2012

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory

Some large estimates being made

- McAfee (2009) cybercrime costs $1000bn (1 trillion) worldwide
  - very dubious multiplication
- Symantec (Sep 2012) $110bn worldwide ($20bn in US)
  - doesn't include remediation ($274 bn) or IP theft
  - but Symantec stands behind it: based on consumer surveys…
- Feb 2011: Detica (part of BAE plc) estimated cost of cybercrime to the UK economy was $43 billion / annum (~ 1.8% of GDP)
  - biggest part of this was IP theft (estimated as % of turnover)
  - our 2008 report for ENISA had drawn attention to the limited number of reliable sources of data and MOD Chief Scientist asked us to update this and comment on the Detica report
- Florencio and Herley "Sex, Lies and Cybercrime Surveys"
  - this WEIS 2011 paper points out how outliers affect results (single loss of $50K in a 1000 person survey becomes $10bn scaled up)

Measuring the Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Michel J.G. van Eeten [5] Michael Levi [6] Tyler Moore [7] Stefan Savage [8]

Abstract

In this paper we present what we believe to be the first systematic study of the costs of cybercrime. It was prepared in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem. For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole. We distinguish carefully between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly. As far as direct costs are concerned, we find that traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/Euros/dollars a year; transitional frauds cost a few pounds/Euros/dollars; while the new computer crimes cost in the tens of pence/cents. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society. Some of the reasons for this are well-known: cybercrimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local, and the associated equilibria have emerged after many years of optimisation. As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.

[1]Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. ross.anderson@cl.cam.ac.uk
[2]UK. chris@vnworks.net
[3]University of Münster, Department of Information Systems, Leonardo-Campus 3, 48149 Münster, Germany. rainer.boehme@wi.uni-muenster.de
[4]Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. richard.clayton@cl.cam.ac.uk
[5]Faculty of Technology, Policy and Management, Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, Netherlands. M.J.G.vanEeten@tudelft.nl
[6]School of Social Sciences, Cardiff University, Cardiff, CF10 3XQ, UK. levi@cf.ac.uk
[7]Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX 75275, USA. tylerm@smu.edu
[8]Department of Computer Science and Engineering, University of California, San Diego, CA 92093, USA. savage@cs.ucsd.edu

http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Joint work!

- Ross Anderson, Richard Clayton
  - U of Cambridge : work on card losses, phishing etc!
- Chris Barton
  - Cybercrime expert, ex-Symantec now with Cloudmark
- Rainer Böhme
  - University of Münster, ex: ICSI, cyberinsurance, audits, privacy
- Michel J.G. van Eeten
  - Delft U of Technology, work on botnets and cleaning up malware
- Michael Levi
  - U of Cardiff: criminologist, with much work on white collar crime
- Tyler Moore
  - Southern Methodist, Dallas: phishing & other ecrime topics
- Stefan Savage
  - UCSD, extensive study of underground economy, pharmacies etc

What is cybercrime?

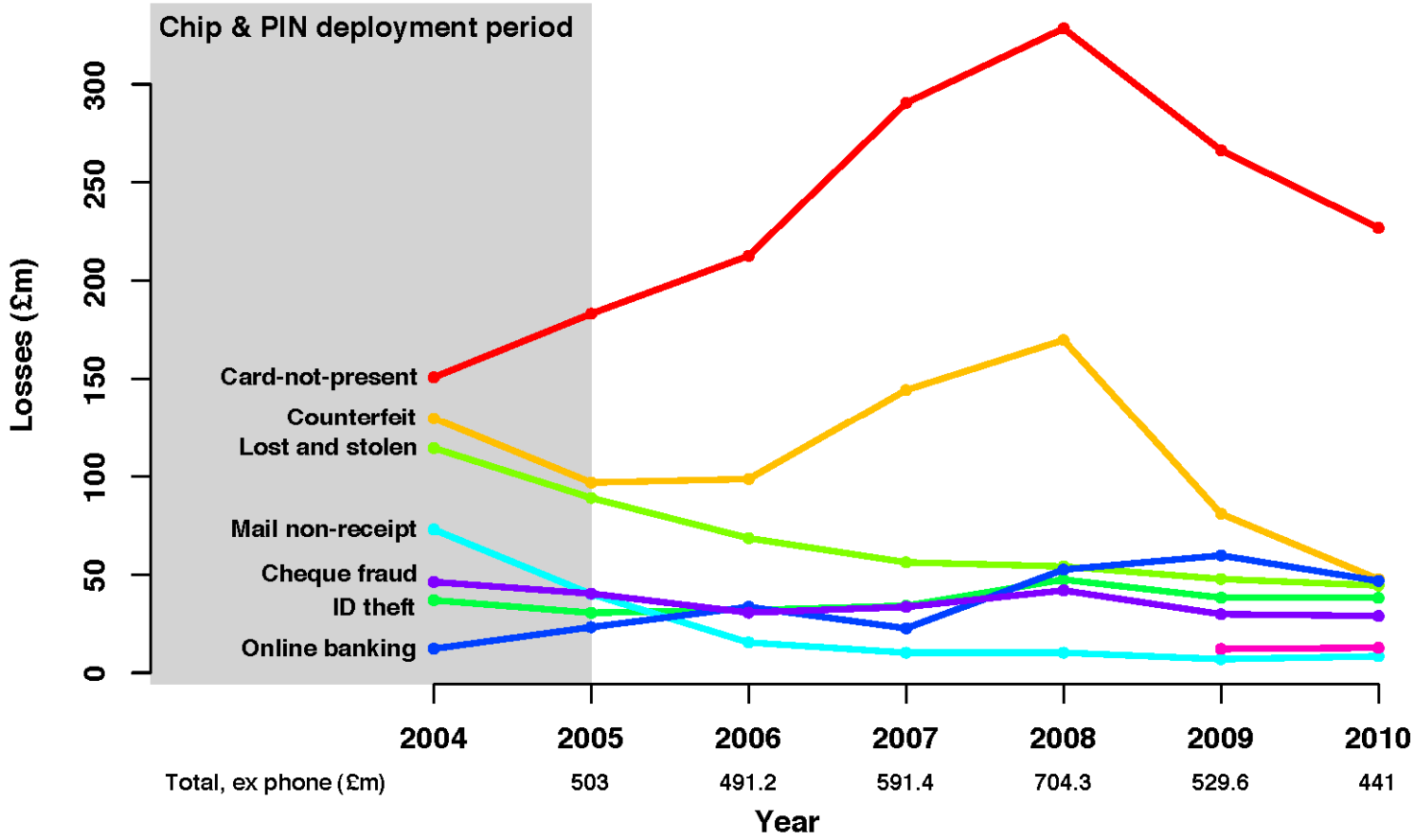
- EU Commission definition:
  - traditional crime (fraud/forgery &c) performed online
  - publication of illegal content online (eg child sexual abuse images)
  - uniquely online crime (hacking, (D)DoS etc)
- We follow this, but immediately note a problem, in that lots of activities are going online
- eg: UK welfare budget is $243bn and fraudulent claims account for 0.8% of this. This will all be online in 2013!
- Income tax fraud (evasion) costs $5 .. $13 bn/annum
- Carousel (missing trader) VAT fraud cost $8bn in 2005/6 when the system wasn't really online... it is now!

Our analytical framework

- Criminal revenue
  - How much ends up in the pocket of criminals (may be spread out when a pharmacy operation has to pay for hosting, spamming &c)
- Direct losses
  - What it costs the victim (may be more than criminal revenue, consider theft of copper wires)
- Indirect losses
  - What it costs, whether or not the crime succeeds. e.g. Loss of confidence in online banking, cost of malware clean-up, inability of banks to use email and save on communications costs
- Defence costs
  - Cost of anti-virus, spam filtering, security training, cost of cyber-police etc – can be hard to ascribe to a particular crime, but they are costs that are incurred because crime is occurring

What we know about: Carding & Phishing

- In the UK we have reliable data from UK Payments Association (a trade group) broken down by fraud type



Carding : indirect losses

- Indirect losses to this $43bn market are hard to quantify
  - 14% of UK consumers are too frightened to buy online
  - so they probably buy offline (but for more £s?)
  - but their searching costs are higher
  - however, some of the online shopping is abroad
  - we estimate loss to the UK economy at $720m
- Merchants also affected
  - they lose 1.8% of revenues to chargeback (1/3 is fraud)
  - But they reject 4.3% of orders through fear of fraud!
  - Some issues with the source of these numbers (a company selling fraud detection products to merchants), but with some caveats a figure of £1bn indirect loss looks plausible
- Online banking saves the banks money (!)
  - ~$70/customer, but 16% don't use it: so $720m indirect cost

Phishing

- Research (Moore/Clayton, Florencio/Herley) suggests worldwide phishing losses in 2007 of c $320m (a sixth of other estimates)
- Phishing now less important – “man in the browser” malware is now what scares the banks
- Oct 2010 : zeus arrests, FBI says one gang stole $70m
- Ongoing FBI cases investigating corporate bank account takeover (ACH etc) with total value of $85m
- So little evidence for “billions” and worldwide losses ~ $300m
- Defence costs (calculators, apps etc) are more!
  - Turnover of relevant companies is ~ $500m
  - Add to that internal costs at banks of the same magnitude

What we know about: Fake Anti-Virus

- Visit a web page that tells you of an infection, and offers to sell you an anti-virus product to fix it
- Access to sales databases (see Stone-Gross et al, WEIS 2010) for 3 different gangs yielded exact information about sales, conversion rates, prices paid etc etc.
- Total criminal revenue (worldwide) for these 3 gangs (2007-2010) was $97m/annum
- There may be more gangs – but if so, they are much lower profile and hence this estimate is pretty reliable

What we know about: Unlicensed pharmacies

- Viagra costs $$ from Pfizer and ¢ (brand infringing) from India
- The opportunities for arbitrage drive for this (and many other drugs) underpins a substantial industry
- Indirect costs include handling spam ($1.31bn in 2005)
- But we have good estimates of criminal revenue
- Inference from invoice numbers (and data about shopping cart contents) shows monthly revenues around $6m worldwide
- Leaked databases show that a major affiliate program had gross revenues of $67m (2009) of which 6.4% was in the UK
- Putting this all together suggests total criminal revenue worldwide of $288 and $14m in the UK

What we know about: Copyright infringement

- Copyright infringing software
  - 2004 BSA survey (1000 worldwide) => 12 million buyers in UK
  - 2011 survey (using inference techniques on invoice numbers) estimated 37000 buyers/month worldwide
  - on reasonable assumptions, total turnover ~$22m
  - consistent with marketplace changes (cost of Office, cloud services)
- “Pirated” music & video
  - In UK is civil issue, not “crime”
  - Studies show increased purchases, and net social gain (!)
  - We conclude that incorporating figures from rights holders into our study cannot be justified
  - But we can count the money made by the “cyberlocker” sites; Megaupload had $50m in assets seized – so on some plausible assumptions total criminal revenue ~$150m worldwide

What we know about: Stranded traveller

From friend: ***"I write this with tears in my eyes. I had to travel to London at short notice and last night I was mugged at gun point. They have stolen all my cash, credit cards and mobile phone. Fortunately my passport and airline ticket was in my hotel room, but the manager will not let me check out until I settle my bill. Please will you spare me $1,900 to pay the hotel, I will reimburse you as soon as I get back."***

- Estimate (from unpublished 2010 data) is that overall criminal revenue worldwide is ~$10m
- Much of the money (in 2010) flowed via Western Union to the UK (!) but final destination is most likely to be West Africa
- Total UK victim cost might be $1m at most

What we know about: Fake escrow scams

- Also known as “auction fraud”
- Many gangs have connections to Romania
- Victim buys cheap car/motorbike/boat on auction site
- Inveigled into using a third party escrow service run by criminal
- Pays money to the third party – and no car ever appears
- ~100 active websites at any given time
- Data suggests perhaps only one victim per website per week
- Overall turnover ~$200m/annum, so UK “share” perhaps $10m

What we know about: Advanced Fee Fraud (419)

- Deceased dictators, lottery scams, dying philanthropists
  - Scam is that a small advance payment must be made to release the big money (and there is a never-ending need for bribes, taxes, fees for bank accounts and so on)
- Some big individual losses (7 figure $ sums), but lottery scams can net just $1200
- Remarkably few reliable statistics – 2001 estimate of $240m in the UK, but this was not all cyber
- We wave our hands and suggest $50m for the UK, but it is one of the vaguest figures we have
- Note that biggest cost may be to the legitimate Nigerian economy, because of the impact of the country's reputation

What we know about: PABX fraud

- Communications Fraud Control Association (CFCA) does regular study – experts fill in web questionnaire and they crunch the numbers best they can
- 2011 estimate for all types of telecoms fraud is $40bn worldwide (with actual losses reported by responders of $2bn)
- This is a decrease of a third on their 2008 figure
- BUT 98% of responders said fraud was static or increasing!
- Specific estimate for PABX fraud (unauthorised calls made when PABX accessed over Internet and reconfigured) is $4.96bn worldwide (Europe: $1.28bn, so UK $185m)
- Note that this may not be actual loss to companies (who may negotiate and pay wholesale values, or just a %age)

What we know about: Cyber-espionage & extortion

- These topics were a big part of the Detica report's totals
  - $15bn/annum lost by "companies that create significant quantities of IP or whose IP is relatively easy to exploit"
  - $12bn/annum lost by failing to win tenders and consequent stock price movements
  - $3.5bn/annum lost to "extortion"
- No reliable evidence for any of this, so although our framework admits of it's existence we cannot offer any numbers
- About the only data we have is of a 2004 extortion case involving DDoS against online casinos – payments were $4m

What we know about: Fiscal fraud

- False claims for tax rebates matter in the USA
  - 2010: 1.5m fraudulent filings, for a loss of $5.2bn
- UK has a more robust filing scheme for identification
- Nevertheless news reports suggest $960m loss in 2011
- BUT reply to Parliamentary question: “HM Revenue and Customs do not have an estimate of the cost of tax refund payments being fraudulently redirected as a result of websites that impersonate Government websites.”

What we know about: Botnets

- Best estimate of bot-herder income ($0.50 / machine / annum) makes this too small a value to consider further
- BUT we do know something about remediation:
  - UK: about 1 million households have a machine in a botnet/year
  - (this is a robust number from 2 different methodologies)
- Cost to fix each machine estimated at $100 (US 2007) but this is undoubtedly high – and machine replacement (a common strategy) is now rather cheaper
  - we estimate UK cost of remediation to be $500m/annum
  - also UK spends ~$170m/annum on AV and other security products
- Note: studies of “pay per install” systems show that their turnover too small to consider $2.5m, but it also means that botnets are cheap for the criminals to replace

What we know about: Cyber-policing

- Headline figure that UK spending $1040m of “new money” on dealing with cybercrime
- Look carefully and you see this is over 4 years
- Look carefully and you bulk of the money goes to GCHQ
- New money for policing is just $15m/annum
- Which still means real hiring by Met eCrime … but this is one of the smaller numbers in these slides

Take-aways on the numbers

- You could add up “true cybercrime” to get $170m
- But this is smaller than the next figure (card fraud)
- And that’s way smaller than the figures for tax/benefit &c fraud
- And many of the numbers are rough estimates…
- We can conclude:
  - Traditional frauds cost citizens a few hundred dollars per year
  - Transitional frauds cost citizens a few tens of dollars per year
  - New cybercrimes net criminals tens of pence per citizen per year
- BUT the indirect costs and defence costs (and especially cleanup costs) for new crimes are more than 10x the criminal revenue

Data on traditional crimes

- Canada has good data on traditional crime such as burglary and car theft (figures across whole economy for 2003):
  - Victim costs estimated at $47bn
  - Criminal justice system costs $13bn
  - Defence costs estimated at $10bn
  - Other countries show similar ratios
- UK robbery costs (Home Office 2005)
  - £109 stolen
  - £438 health service cost
  - £1011 lost output
  - £3048 “distress”
  - £2601 costs in the criminal justice system
  - BUT for burglary, £846 stolen, but justice spend is £1137

Data on cybercrimes

- Sentences for robbery and higher than for burglary
- Cybercrooks get much shorter sentences than either
- Fraudsters (unlike terrorists) don't set out to annoy you!

- The British Crime Survey shows 2% reporting burglary or car theft – but double that number report a fraud incident (they didn't distinguish types of fraud, but online fraud undoubtedly the majority of this)
- ie: cybercrime now the typical volume property crime in the UK
- So maybe more policing is justified… albeit, it's not an easy task to tackle

Conclusions

- Cybercrime figures are often grossly inflated
- Our recent work has provided some rather more realistic estimates – but remember that they are estimates
- Our main contribution is our framework – and the way that we try to distinguish the different types of cost
- We intend to revisit this work in the future with a view to improving accuracy and coverage; so we're always looking for more and better data

http://www.lightbluetouchpaper.org

http://www.cl.cam.ac.uk/~rnc1/publications

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory