Plus Ça Change:
Cybercrime, Past Present and Future

Dr Richard Clayton

Director, Cambridge Cybercrime Centre

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Cambridge
24th July 2019

My background

- I’ve been looking at online abuse (spam, phishing, malware, DDoS etc) for two decades
- My general approach is data driven (I count things)
- I have obtained many datasets from industry under NDAs and that has underpinned the work I have done (in collaboration with some very smart people)
- BUT this is a long and tedious process, and we’re beginning to realise that no papers in this field can be reproduced (data cannot be shared, results cannot be compared, conclusions cannot be validated)
- This does not really look like science…

Cambridge Cybercrime Centre

- I have 5 years funding from EPSRC (+ some other money)
- Currently 6 of us + PhD students & UTOs
  - Computer Science, Criminology & Psychology
- We collect & collate cybercrime datasets
  - and then do world class work on it
- AND we also share this data with other academics
  - this is not "open data", you have to sign paperwork
  - but we make data available at an early stage (even realtime)
  - over 25 research groups now signed up
- I'll share your data too if you like !
  - we already have appropriate legal agreements
  - "one stop shop" – we do all the due diligence & paperwork!

What I’m talking about today

- WEIS 2012 “we” wrote “Measuring the Cost of Cybercrime”
  Anderson, Barton, Böhme, Clayton, van Eeten, Levi, Moore, Savage
- Established a framework and then added measurement data
- Headline numbers:
  - tax fraud, VAT fraud, benefit fraud — $100s / person
  - fraud that had moved online (banking etc.) — $10s / person
  - “cybercrime” — 10¢ / person
- BUT: spending ~$100 / person for defence costs
- WEIS 2019: “Measuring the Changing Cost of Cybercrime”
  - added three authors (and subtracted two)
  - Anderson, Barton, Böhme, Clayton, Gánañ, Grasso, Levi, Moore, Vasek
- … and we get pretty much the same result !
- BUT the differences and trends are very interesting …

Victim surveys

- Back in 2012 we thought that cybercrime was about half of all "property crime"
- Victim surveys since then show that we were right !
  - USA (10% of population had an unauthorised debit in 2016)
  - UK (Oct 2018: 3.5m fraud offences/year – similar to theft)
  - Belgium (over half of businesses experiencing cybercrime)
  - France (3m cybercrime events/year, affecting 4% of population)
  - Australia (2017 survey suggests losses in the $100s/person/year)
  - E-CRIME EU project: 6 countries, 10Euro/person/year
- Unfortunately little consistency re questions or methodology
- Nevertheless, victim surveys much prized by criminologists because many crimes underreported, but care needed when scaling results to population levels…

Since 2012…

CHANGES

- Android / iPhones replacing Windows (& Macs)
- Services are moving to the cloud
- Social networks pretty much ubiquitous
- Internet of Things (IoT)

UNCHANGED

- Law Enforcement budgets
- The key role of technology firms
- Botnets
- Malware

Payment fraud

- UK: card-not-present fraud has doubled in volume & value
- UK: e-commerce events rising, mail & telephone falling
- UK: lost/stolen card fraud tripled in volume but doubled in value
- BUT: payment volume has more than doubled
  - in fact better analytics plus chip-and-pin means we're winning!
- Same pattern can be seen in US & Europe
- European Central Bank data shows bank fraud also rising, but the amount is highly correlated with usage levels and so varies widely from country to country
- There's currently an uptick in SMS-related fraud (banks use this as a "second factor", but no reliable data yet…)

Business Email Compromise (BEC)

- Multiple scams affecting businesses:
  - invoice replacements (send payment to this bank account instead)
  - CEO fraud (messages asking for wire transfers)
  - gift cards ("I want to reward staff with a surprise bonus")
- Also affecting individuals (especially real estate transactions)
  - termed "Authorised Push Payment" fraud in UK, and "Email Account Compromise" fraud in USA
- Internet Complaint Centre (IC3 == FBI) publishes stats

– 2014	$226m	2 417 complaints
– 2015	$246m	7 837 complaints
– 2016	$361m	12 005 complaints
– 2017	$676m	15 690 complaints
– 2018	$1298m	20 373 complaints

- Worldwide now $12.5bn since 2013

Ransomware & Cryptocrime

- This wasn't in our 2012 paper (though by 2012 prepaid money cards were already being used by ransomware)
- Ransomware generated $16m criminal revenue 2015-17
  - actual losses will be several orders of magnitude higher
- Many other cryptocurrency enabled crimes
  - $7.1m ponzi scams; $52m mining scams; $36.3m fraudulent ICOs; $6m fraudulent cryptocoins; $5m fake cryptocurrency services
  - this SEC data undoubtedly underestimates the issue
    - BitConnect may have cost investors $1bn
- Cryptomining malware has generated profits of $56m since 2012 (4.32% of Monero mined through subterfuge)
- Exchanges lost $1bn to hackers in 2018
- Overall the cost is somewhere in $2bn/annum range!

PABX fraud

- Back in 2012 global cost of telecoms fraud was $40bn
  - much was people not paying bills, but $4.96bn was PABX fraud
- But phone calls (often VOIP) are now cheaper !
- So headline figure is now down to $29.2bn
  - and dropped 23% from 2016 to 2017 (the most recent data)
- PABX fraud now $3.88bn and is now mainly calls to premium rate numbers rather than reselling service to expats
  - “Yes, I will accept the charges for a call to Zaire”

Industrial espionage & extortion

- There still is no compelling evidence as to the level of losses but nevertheless this topic still talked up by Governments
- Also nothing to support wild claims about extortion losses
  - yes, DDoS extortion is a thing, but amounts are small
- HOWEVER Wannacry & NotPetya did real damage:
  - overall losses perhaps $1bn to $2 bn
  - BUT examine the data with caution! original TSMC (Taiwan chipmaker) losses of $255m later scaled back to $84m
- Mondelez is claiming $100m under their policy from Zurich Insurance for NotPetya losses – but this has been refused under an "act of war" clause (& simply because cyber not covered under property & casualty). The courts may settle this one.
- Most state activity not linked to financial losses …

Summary of the current state

- Payment fraud is up, but transactions are up even more
- Cryptocurrencies enabling new scams (but the big money is being lost in schemes resembling traditional investment frauds)
- Structural change has markedly reduced telecoms fraud
- Some crimes disappearing, others appearing
  - anti-virus fraud almost disappeared
  - tech support scams growing very rapidly
- Plus ça change!
  - the big money is still in tax fraud, VAT fraud, welfare fraud etc
  - defence costs outweigh actual losses
  - criminals still don't think they'll be caught (and are mainly correct)
- Tech has changed markedly, but economics is much the same

Predictions for the future

- Short term
  - deep fakes and AI will sound very scary
  - criminals will continue to concentrate more on companies
  - the big money will still be in tax, welfare and VAT fraud
- Medium term
  - BEC will fall once the accountants regain the upper hand
  - insurers will stop paying out ransoms
  - WORM devices will become *de rigeur*
  - the big money will still be in tax, welfare and VAT fraud
- Long term
  - politicians will allow law enforcement to operate across borders
  - cybercrime will finally start to fall
  - the big money will still be in tax, welfare and VAT fraud

blog: https://www.lightbluetouchpaper.org

Cambridge Cybercrime Centre

data: https://cambridgecybercrime.uk/process.html

UNIVERSITY OF CAMBRIDGE
Computer Laboratory