Economic Cybercrimes and Policing Responses

Mike Levi

Cardiff University

Levi@Cardiff.ac.uk

Cambridge Cybercrime Colloquium 2016

Typology of reported frauds in NFIB last quarter 2014 data

Fraud type	No. of frauds	Percent total reported frauds
Banking and credit industry fraud	34,913	32.7%
Cheque, plastic card and online bank accounts (not PSP)	19,127	18%
Application fraud (excluding mortgages)	10,091	9.5%
Non-investment fraud	30,490	28.6%
Online shopping and auctions	12,405	11.6%
Computer software service fraud	8,455	7.9%
Advance fee payments	15,065	14.1%
Other advance fee frauds	7,498	6.7%
Lender loan fraud	2,078	1.9%
No identified category	12,404	11.6%
Categories as % of total	92,872	87%
Total	106,681	100%

Offender first contact with victims in NFIB cases

Contact method	No. of frauds	Percent of total reported frauds
Phone call, text message or similar	31,088	35%
Visit to a website	15,587	18%
Other	11,625	13%
In person	10,932	12%
Letter or fax	10,159	11%
Email	6,859	8%
Web forum, chat room or similar	1,582	2%
TV, radio or online advert, or flyer	462	1%
Newspaper, magazine	179	0%
Total	88,473	100%

Selected Action Fraud category/sub-categories	% Cyber-involvement
Dating scam	88%
Online shopping and auctions	86%
Rental fraud	74%
Ticket fraud	72%
Mortgage related fraud	48%
Fraudulent applications for grants from charities	44%
Business trading fraud	31%
Charity fraud	27%
Pyramid or Ponzi schemes	24%
Cheque, plastic card and online bank accounts	18%
Consumer phone fraud	18%
Fraudulent applications for grants from government	17%
Bankruptcy and insolvency	17%
HM Revenue and Customs (HMRC) fraud	17%
Lender loan fraud	17%
Inheritance fraud	15%
‘419’ advance fee fraud	15%
Door to door sales and bogus tradesmen	14%
Share sales or boiler room fraud	11%
Corporate procurement fraud	9%
Lottery scams	8%
Time shares and holiday club fraud	7%
Application fraud (excluding mortgages)	7%
Retail fraud	7%
Fraud by abuse of position	6%
Pension liberation fraud	5%
Telecom industry fraud (misuse of contracts)	4%
Corporate employee fraud	3%

Some data

- The remorseless rise
  - in e-crime 'data' in different countries or globalised via 'Guardians'
  - In fears about identity theft and state-sponsored espionage/attacks
  - In suspicions that the fall in crime is not real but is an 'e-transplant'
- > half UK adults aware of mass-marketing frauds, but 2.6 million individuals victims in lifetime; 800,000 in 2012
- A quarter of those scammed were repeat victims
- All of these have potential demands on policing

Public and Private Policing Responses, England and Wales

NCA
National Crime Agency

FALCON
FRAUD AND LINKED CRIME ONLINE

DCPCU
Dedicated Card and Payment Crime Unit

TEAM CYMRU

FFA
Financial Fraud Action UK
Working together to prevent fraud

cifas
Leaders in fraud prevention

GET SAFE ONLINE .org

Get Safe Online
Free expert advice

Met and City of London Priorities

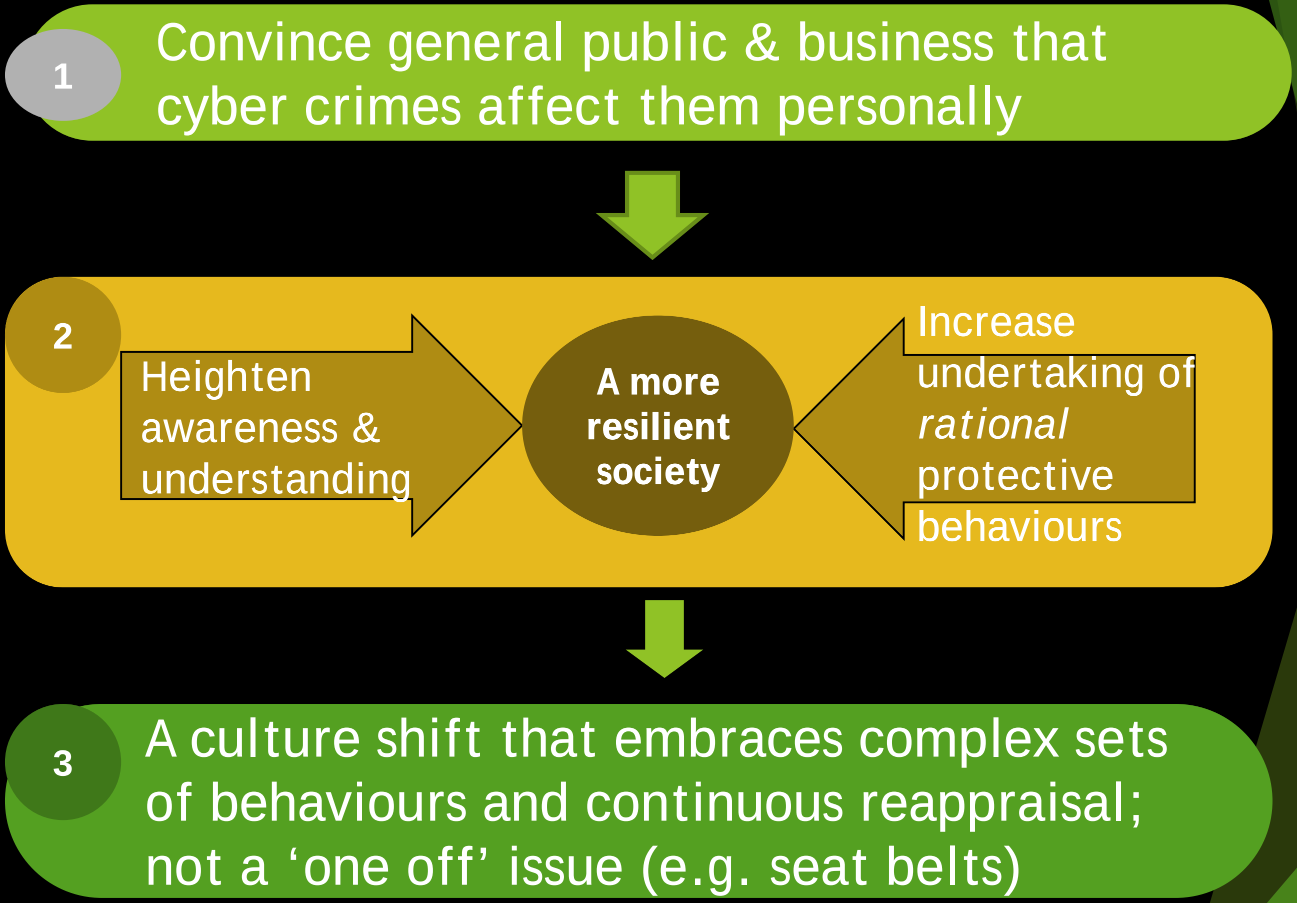
- Industry-funded DCPCU Strategic Tasking & Co-ordination Group Priorities:
- **1. Remote Payment Fraud - 6012**
  - To work with bank investigators to target those criminal gangs responsible for remote payments.
- **2. Staff Integrity**
- **3. Social Engineering - Telephony**
  - To identify criminal groups…who are targeting largely vulnerable individuals and businesses.
- **4. ATM**
  - To proactively target organised gangs committing fraud at ATMs.

- **FALCON Mission: To reduce the harm caused by fraud and cyber criminals in London.**
- Ensure all Action Fraud (AF) referrals to the MPS are effectively responded to by dedicated fraud / cyber investigators
- Provide excellent victim care and seek compensation for our victims wherever possible
- Significantly increase the numbers of arrests and charges relating to fraud and cyber crime
- Proactively target cyber criminals and fraudsters, focusing on stemming the harm caused by the most prolific Organised Crime Groups
- Work in partnership with businesses to improve our response to fraud and cyber crime affecting London's businesses
- Undertake targeted prevention work with industry partners that designs out crime, tackles the enablers of cyber crime & fraud and raises awareness within the public and businesses

Reassurance Policing & the 4 Ps

- *Feeling* safer and/or *being* safer
- What are our objectives for which sectors & behaviours against which *effectiveness* can be judged?
- Who needs Pursue *by the police* and for what sorts of offenders and what behaviours is this realistic?
- How can we sell these limitations to the public?
- Who are we using for ‘third-party policing’?

The challenge for Government, police and ‘nudgers’



1 Convince general public & business that cyber crimes affect them personally

2 Heighten awareness & understanding

A more resilient society

Increase undertaking of *rational* protective behaviours

3 A culture shift that embraces complex sets of behaviours and continuous reappraisal; not a ‘one off’ issue (e.g. seat belts)

Public and private policing

- The mission of the police is “protect the weak, support the fearful and vulnerable, thank the helpful and lock up the bad guys” then Met Police Commissioner Sir Ian Blair (3 July 2005)
- Require private sector to be unpaid army of informants (AML SARs regime)
- Get private sector to pay for policing of crimes for which they find *public* police powers useful
- Corporate investigation agencies for more complex e-crime cases/’self-cleaning’ – but when does this happen?
- What technologies of policing are available and are actually used for ‘financial crimes’?

Some models for action

- The targets for cyber-fraud/extortion are very widespread
- Need more understanding of teachable moments to divert offending
- Prevention should be built-in with minimal effort or administered in a more bottom-up way through peer groups, community level bodies and charities, to help individuals and SMEs adopt easy security processes - regular efforts from them are not practicable.

Public/private partnerships

eCrime Partnership Mapping Study

(Levi & Williams 2011)

- Perceptions and measures of eCrime prevalence largely symmetrical
- Significant gaps in cooperation frequency and quality between government and finance sector and private sector other (SMEs?)
- Third sector organisations and local government on the periphery of the UKIA network

- **Major changes in some areas since then**
- **Cabinet Office fraud profession development**

Some Thoughts for the Future

- Offline and online strategies differentiated
- Disruption strategies – including take-downs of websites, botnets and dark markets – may reduce harm, especially if websites are taken down early
- but we know little yet about the longer-term signalling and market reduction effects of these ‘whack-a-mole’ measures
- Scope for experiments, e.g. warning ‘pop ups’ on screen for those who fall victim to offers that could have been fraudulent or fake, though need careful management of media concerns.
- More focused Internet Governance could deal with these Global Bads, but the politics of international opportunity reduction are very hard to achieve.

Modern Crime Prevention (Home Office 2016)

- Up to 80% of cyber crime can be prevented if members of the public & businesses take simple precautions, equivalent to locking front doors.
- Campaigns will focus on three simple steps everyone can take that will prevent crime:
  1. Using strong passwords made up of three random words (e.g. fur-dis-bat);
  2. Installing security software on all devices; and
  3. Downloading software updates which contain vital security upgrades to correct bugs or vulnerabilities that hackers and cyber criminals can exploit.
- Working with online financial and retail services to help the public to better understand key online security principles, that will reduce their risk of being a victim of crime (particularly fraud), and help them to make an informed choice about where to take their business.

Stop refunding victims of online fraud MPS Commissioner *Bernard Hogan-Howe said that the public were being "rewarded for bad behaviour"*

Commander Chris Greany said that the public should take as much care online as in the real world. "I think there will be cyber-insurance in the future…home insurers will not pay out if you do not lock your front door. There needs to be a conversation in society. If people choose not to take sensible precautions with their property, will they in the future be refunded?"