

> The Dynamics of e-Crime

Rt Hon James Brokenshire MP

Shadow Crime Reduction Minister
Member of Parliament for Hornchurch

Mr. Mike Humphrey

Head Of Information Assurance & Accreditation
Serious Organised Crime Agency

Prof. Howard Schmidt

President & CEO
Information Security Forum Ltd. UK

Nick Selby

VP & Research Director, Enterprise Security
The 451 Group

> Agenda

- Some definitions and ground rules
- E-Crime trends
- How this affects citizenry
- What government can do
- Opportunities for the private sector



Some ground rules...

- We assume you've read a magazine in the last 5 years
 - “It's not about script kiddies anymore”
 - “Malware industrial complex”
 - Organised criminal gangs creating and distributing malware
 - Fraud, theft, money laundering

> Some statements...

- E-crime targeting citizens or businesses seeks to exploit lack of understanding, weak defences, social engineering etc. All exploits probably involve people at some point.
- It is likely that economic conditions lower the threshold to which people may resist criminal temptation or corruption.
- Likewise, resistance to temptation to fall for 'get rich quick' scams and phishing exploits to get you to disclose passwords is lower.
- Falling for these scams adds to financial burdens.
- All this will increase the pool of potential vulnerable people for organised criminals to exploit.

> Citizenry

- Should industry recognise these trends and increase their vigilance on potential insider compromise?
- How do enterprises educate staff about the dangers of scams and other traps that could turn their employees into insiders?

> Citizenry

- What does e-crime mean to the citizen?
- - Ask 100 people and get considerably varying answers.
- - Is it a pure series of offences or a modus operandi to existing crime?
- How do we measure it?

> Citizenry

- The Water Board man
- IAAC (Information Assurance Advisory Council) in their Identity Assurance Programme 2006-8 Conclusions paper raised the notion of a need for the equivalent of a Highway Code for the citizen using the Internet.

> Government

Because law enforcement resources must be targeted effectively, small scams don't get the attention that large operations do. Yet the Internet is designed in such a way that no agency has jurisdiction over sufficient territory to take blanket action. How can we target e-crime without attempting to boil the ocean while using our resources efficiently? Surely this is not impossible?

> Government

- The state of affairs with inter/intra-departmental understanding of e-crime issues
- Training of LEO/military/corporate security personnel to recognize and handle e-crime

> Opportunities

- Open source intel services for both enumeration by and defence against
- criminals
- i) cyber-intel services beyond traditional brand protection (ie
- digital clipping services)
- ii) distribution control/piracy
- iii) Information sharing on industry vertical basis
- iv) Information sharing between industry and law enforcement

> Opportunities

- Social networking as it relates to targeted physical/logical attacks and industrial or nation-state espionage
 - Criminal cyber-intel for executive stalking or
 - reverse-engineering commercial intent ('My dad's in France for some Airbus thing')
 - Targeted malware attacks against social networking sites to harvest corporate creds
 - iii) ...?