Centre for Criminal Justice Studies
School of Law

UNIVERSITY OF LEEDS

The implications of developments in cybercrime for cybersecurity and law enforcement? (AND overcoming the data-sharing paradox)

Maximising Impact from Serious Organised Crime Research, Cyber Crimes & Online Criminal Markets. University of Cambridge, Sept. 17th 2021

Professor David S. Wall,

d.s.wall@leeds.ac.uk

Source: https://www.recycleit4u.co.uk/wp-content/uploads/2014/11/data-theft.jpg

Interdisciplinary Cybercrime Research At Leeds – Work in Progress

UNIVERSITY OF LEEDS

I am interested in changes in the cybercrime threat landscape, especially the ways that offenders have become more adaptive and organised to challenge law enforcement. I am also interested in potential for offenders to develop powerful, sustainable online organised crime groups. I draw from three research projects.

- **Combatting cRiminals in The Cloud (EPSRC CRITiCal) 2015-22**
- **Ransomware and Cybercrimes of Extortion (EPSRC/ ESRC EMPHASIS)** (EconoMical, PsycHologicAl and Societal Impact of RanSomware (2017 –2019)
- **Understanding Organised Crime and Terrorist Networks** (H2020 2016-19)

A recent article relevant to this presentation is:

Wall, D.S. (2021) 'The Transnational Cybercrime Extortion Landscape and the Pandemic: changes in ransomware offender tactics, attack scalability and the organisation of offending', *European Law Enforcement Research Bulletin, 22,* (publication forthcoming) ***PREPRINT available***
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3908159

1. Cybercrime as (Transnational) modern serious organised crime

UNIVERSITY OF LEEDS

My research into cybercrime is finding that

- *Cybercrime offenders are more professional than before*.
- *More ruthless,* now *triple extortion methods, N&S, Data, DDoS*
- *The high yield is encouraging* cybercrime as a career
- *Offenders supported by, or are part of, a cybercrime ecosystem The cybercrime ecosystem system is the new face of SOC*,
- *No single Mr/Ms/Mrs Big* – multiple actors-different motivations
- *Offenders are incredibly adaptive*, C & LE rule based

2. The new challenges of cybercrime for law and enforcement

UNIVERSITY OF LEEDS

- ***Ransomware is a blended cybercrime*** as it i) comprises more than one crime and ii) combines the social with science – social engineering & negotiators.
- ***Statistically, ransomware is problematic and hard to record***. In the UK, the 'ransom' and 'ware' are recorded as different statistics. They also constitute different bodies of law and fall under different policing agencies.
- ***These agencies have untrusted relationships with industry***, especially when victims pay the ransom because they i) do not want their victimisation to become public and ii) want to resolve the matter quickly.
- ***Public and private interests often clash*** to hinder the search for justice.
- ***Need co-ownership of problem*** *to co-produce the solution*

3. The Cybercrime Data Problem (using ransomware as an example)

UNIVERSITY OF LEEDS

- *Ransomware tends to be over-reported by media* - dramatic reporting raises public expectations and distorts problem
- Gets onto the political agenda with results being demanded - taking attention from those tasked with the problem.
- *Ransomware is largely under-reported by victims* who prefer to deal with victimisation in their own interests
- *Offenders now publish victims names* – but over-report them – naming doesn't always mean victims have been affected!

The problem is getting data on (and be able to distinguish between)

a) attacks generally
b) Unmitigated attacks when an actual harm has occurred
c) Attacks where a crime has occurred - few are reported
d) Attacks where an offender is known

4. The Challenge for Law Enforcement

UNIVERSITY OF LEEDS

- *Ransomware is generally under-prosecuted*, which means little court experience across the CJS.
- *Policing ransomware becomes problematic when victims and offenders are in different jurisdictions* or more than one (see the Blackbaud case).
- *Ransomware may be big globally, but is small locally*, so local police get little experience of dealing with the crime. However, the UK ROCU model connects local and national police regionally and is fairly well regarded by police and also respected by industry.

5. Conclusions - Resolving the Public versus the Private interest problem

UNIVERSITY OF LEEDS

- ***The data sharing paradox*** *is that everyone agree on the problem but everyone disagrees on the solution.*
- ***The public and private interests often clash*** to hinder the search for justice.
  - Victims (and cybersecurity) pay the ransom because they i) do not want their victimisation to become public and ii) want to resolve the matter quickly. Cyber-insurance fans flames
- ***Lack of trust between*** victims (organisations), cybersecurity and law enforcement agencies
- **Need develop *co-ownership of problem*** *to co-produce the solution*
  - *Third party, sectoral agencies (UK payments model)*
  - *Mutual sharing of information, but not necessarily sensitive data.*