**Response to the Call for Evidence: Ransomware**

**Dr Matthew Robert Shillito (Lecturer in Law)**

**The School of Law and Social Justice, University of Liverpool**

**Biography**

Dr Matthew Shillito is a Lecturer in Law at the University of Liverpool. His research identifies and develops issues and themes in the areas of financial and dark web crime, with a particular focus on how the law regulates the use and abuse of digital currencies. In September 2016, he completed his PhD thesis, entitled ‘*Criminal abuse of non-traditional payment methods: A comparative analysis of the application of anti-money laundering and counter-terrorist financing frameworks in the UK, US, and Australia*’. The thesis specifically focussed on how the law was developing in each jurisdiction to tackle the emerging threat of Bitcoin and other digital currencies. Dr Shillito is developing a book on this area, in light of developments since his thesis was completed. He also has a meaningful body of publications and conference presentations focussing on legal issues surrounding the use of crypto-assets, and in 2016/17 through a joint N8 funded research project with Greater Manchester Police and colleagues at other academic institutions, helped to develop a handbook for the Metropolitan Police on how to deal with cryptocurrencies uncovered during the course of criminal investigations. Dr Shillito teaches an undergraduate Banking Law course to circa 250+ students and has developed several lectures on cryptocurrencies, which have a particular focus on a range of different crypto-assets and the risks they present to consumers due to the lack of regulation and protection in the area.

**Topic 1: The extent and nature of the ransomware threat (including sources), modes of extortion, and how the threat could evolve in the future.**

Ransomware is arguably the most insidious threat facing UK businesses today. Attacks can be targeted (i.e., at specific businesses) or indiscriminate (designed to exploit common weaknesses meaning the victim is not the concern of the criminal). Each type of attack poses its own challenges, but the ease with which indiscriminate attacks spread is a particular challenge (e.g., if it exploits a weakness in an operating system utilised by thousands of companies). So, attacks can be large both in terms of the size of the ransom and the volume of individuals / organisations it impacts. The largest source of vulnerability is without doubt outdated or unpatched software / hardware. These vulnerabilities are easily exposed by criminals. Additionally, employees are another layer of weakness largely due to human error and lack of care when for instance dealing with email attachments or setting passwords, allowing criminals to instal malware on their systems in that way. Once ‘inside’ the business, the criminal often threatens to: publish sensitive data, destroy files, or permanently withhold access to key systems / websites if the ransom is not paid.

Primarily at present, extortion is by means of the use of cryptocurrencies due to quick transaction times, cross-border utility, and the pseudonymity they afford. Depending on the cryptoassets used for extortion, traceability can be difficult or impossible in terms of a ‘follow the money approach’ to investigations – e.g., Monero provides greater anonymity to criminals than Bitcoin. Criminals have also been known to utilise other types of payment, e.g., pre-paid cards or informal value transfer systems as a means of extortion, largely for the same anonymity driver. Where crypto has more utility is that it can be more widely used than a pre-paid card.

In terms of the evolution of the threat, it is unlikely that the initial stages of it would need to evolve. There are too many weaknesses to exploit, and human error will remain. It is however likely that the extortion element will continue to evolve. In the cryptocurrency era, we have already seen criminals move from Bitcoin to more privacy focussed coins like Monero due to it having a more hidden blockchain meaning that it is harder for law enforcement to investigate. As crypto further develops, or new payment mechanisms emerge, it is guaranteed that criminals will appraise their utility as an extortion mechanism. This would also nullify the impact of blockchain investigative firms to assist law enforcement. It is also likely that criminals will advance their encryption methods to make it harder for victims to recover files without having paid the ransom. Ultimately, as the crime evolves and becomes harder to track / recover funds, criminals will begin to place more emphasis on targeting larger businesses and critical national infrastructure due to the ability to demand larger ransoms.

**Topic 2: Levels and sources of vulnerability of UK organisations to ransomware, including operators of critical national infrastructure.**

The level of vulnerability of UK organisations to ransomware entirely depends on how we judge ‘impact’. For instance, low to mid-sized businesses are likely to have weaker cyber security and therefore be more impacted / not have a pre-planned response to such an attack that allows them to carry on with their business and so in that sense they are most at risk. However, in terms of criminal revenue this is likely to be lesser than a successful attack on a large organisation or on national infrastructure due to the impact this can have on national security and public safety. Smaller businesses are also more likely to attempt to deal with the situation themselves by making a payment to the criminal before coming forward to law enforcement.

That said, it is likely that businesses that either deal with high levels of data (be it sensitive or valuable) or that play a key role in national infrastructure (e.g., health, education, energy etc) are most at risk of a ransomware attack because attackers seen them as more attractive targets due to the fact, they can demand a larger sum. Again, this entirely depends on the criminal’s motivation e.g. high ransom or quick payment.

Large organisations are also at risk due to the number of employees they have and the corresponding diligence of each employee in terms of cybersecurity.

**Topic 3: The UK victim experience, including sources of support for prevention, detection and recovery, public private partnerships, the role of media, access to and availability of insurance cover, and regulatory requirements placed on ransomware victims.**

The UK victim experience in the UK is incredibly different depending upon who they are (e.g., individual, small business, large business, governmental organisation) and what the nature of the ransomware attack is (e.g. is related to embarrassing activity or playing on fear, or simply blocking access to critical infrastructure). The result is that some cases of ransomware are ‘dealt with’ early, some are long term, and others never come law enforcements attention. Within those categories, the type of support needed will vary significantly depending on with the victim is emotionally impacted, whether it impedes essential activity, and whether they have already advanced funds to the criminal.

In terms of prevention, individuals and businesses are largely left to their own devices in terms of creating secure environments in which they hope to avoid a ransomware attack, more could definitely be done in this regard, see e.g., the example from UAE in response to topic 7, below. In terms of critical government-run infrastructure, these can often be exposed due to under-resourcing or inadequate training of staff.

Moving to detection, this is largely reliant on individuals and businesses coming forward to report a ransomware attack. In that sense, there is likely an underappreciation as to the scale of the problem. Where instances are reported, detection is fairly straightforward in the sense that the crime has visual markers that make it evident. However, actually identifying the perpetrator can be incredibly difficult due to geographical location and law enforcement resources.

Public-private partnerships have the potential to do significant good in this area, particularly where funds have already exchanged hands. There is now a wealth of blockchain analysis firms in the UK who specialise in the tracing and recovery of cryptoassets which are the subject of crime. Coupling with these private entities increases law enforcement’s ability to tackle ransomware crime and gives the victim a greater chance of funds being returned. There is of course the potential for private firms to play a role earlier in the process, prior to funds being passed to the criminal, in terms of liaising on how to best deal with a ransomware attempt, or even better in the provision of security software that is harder for criminals to crack.

Media could play more of a role in promoting the threat of ransomware and how to treat it. Through family experience, I know that individuals can 1) be unaware of ransomware until it is too late; 2) be unsure how to deal with it; and 3) think that payment results in a solution. Bringing good practice to the attention of the public is essential to try and stop criminals from profiting. It would also be useful in terms of highlighting that ransomware criminals rarely have the kind of information on an individual that they claim to have.

Cybercrime insurance is becoming increasing difficult to find (in terms of it covering all a business’s needs) and increasingly expensive. For instance, in the US it is estimated that the cost of cybercrime insurance rose 96% in 2021.[[1]](#footnote-1) Those that can afford it struggle to find cover for ransomware attacks, and those that cannot (the majority) are likely to be the ones that need it most / are most at risk of an indiscriminate attack. In terms of individuals, it is unlikely that an individual would be seeking insurance for this kind of crime.

**Topic 4: The effectiveness of the response to ransomware by Government, law enforcement agencies and other state actors, including key operational challenges and ministerial oversight.**

**Topic 5: Reforms that might enhance the UK’s resilience to ransomware, reduce the economic and societal damage that it causes, and / or support the law enforcement response.**

The response to these two topics is dealt with together.

In terms of reforms, the government should focus its efforts on enforcement and victim support. Whilst improvements in a regulatory sense could be achieved, this is not where real gains are to be made – broadly speaking the mechanisms to prosecute individuals and recover funds are sufficiently developed, save for the known caveats around their effectiveness.

However, an area of weakness though it has improved in recent years, is in relation to law enforcement capabilities and the resources they are afforded. Given that 1) the types of businesses targeted are of critical importance either because of the outcomes they achieve e.g., hospitals / education providers or their contribution to the economy; and 2) that ransomware, and cryptocurrency crime generally, involves the laundering of incredibly large sums of money; then increasing government spending in this area would pay for itself. Indeed, it can be noted that recent government cuts to tackle the national debt, also impact this area, but this is a false economy as tackling crime in this area has large potential to pay for itself either directly or indirectly. Indeed, there is an acute problem that as tech develops and law enforcement struggle to keep up, efforts to counter tech-enabled crime in this country are reliant on officers upskilling themselves creating inconsistencies in approach across the country and leaving law enforcement open to the prospect of losing those skilled staff to the private sector (e.g., we have seen this routinely happen in relation to crypto-crimes, with skilled officers taking up positions in tech investigative firms). Furthermore, if sufficient resource is not put in, law enforcement will be forever reliant on the private sector to assist them in tech investigations.

Given likely limitations in resources and the problem of retaining skilled officers, it is essential to turbo-charge the use of public-private partnerships in this area. But this should not be seen as a substitute for proper investment in law enforcement capabilities, rather as a complimentary step. This of course requires its own resources and careful selection and managing of partnerships. Furthermore, there would need to be careful consideration given to data protection laws and how these can be construed to ensure that these partnerships are as effective as they can be.

Outside of formal partnerships, the UK should be looking to previous successes in this field, notably the Joint Money Laundering Intelligence Taskforce (JMLIT) which was once considered industry leading. How could a model like this be reinvigorated in this new tech-crime era? For instance, can new gateways for information / intelligence sharing be created, can artificial intelligence / machine learning capabilities be shared?

**Topic 6: The scope for international cooperation to combat the global ransomware threat more effectively, including on crypto-currency regulation;**

International cooperation to combat the global ransomware threat is not just needed, it is **essential**. One of the fundamental difficulties in tackling any kind of cybercrime is that it can be committed in any location from anywhere in the world. The problem is further exacerbated where cryptocurrencies (or other globally accessible payment methods e.g., certain types of pre-paid cards) are utilised as the extraction method, as the funds can cross international borders swiftly and it can add to the cross-border evidential difficulty (i.e., the funds could be located in a country other than where the criminal is based). Furthermore, where the ransomware is distributed indiscriminately e.g., where it looks to exploit tech security weaknesses irrespective of the victim, then any investigation would likely necessitate international cooperation. This can also be true of ‘targeted’ ransomware attacks, though an international element to the crime is not necessarily guaranteed.

To this end, Interpol and Europol play key roles in facilitating international cross-border investigations. The UK is often at the forefront in these efforts, and it should make every effort to ensure this is always the case. That said, Interpol and Europol are limited in terms of competence, they can only play a coordinating role not a leading one and are reliant on their members to bring prosecutions. Ceding any additional power to these institutions in terms of prosecutions / enforcement powers is likely to be unpalatable from a sovereignty perspective, however perhaps they could be given more investigatory autonomy and larger resource. Particularly, as crime across the board is becoming more global in nature. Perhaps, given their role in terms of being the international standard setter for anti-money laundering and counter-terrorist financing, consideration should be given as to how the Financial Action Task Force (FATF) Recommendations can be better tailored to assist in the fight against ransomware. For instance, could their Recommendations around international cooperation do more? Meanwhile, whilst their work on cryptocurrencies should be applauded, and will be of use to law enforcement the world over in tackling this type of crime, they are still in their infancy, and guidance makes little mention of ransomware beyond some case study examples of criminal usage.

Outside of this, international cooperation in criminal matters is heavily reliant on bi-lateral mutual legal assistance treaties. The limits of these are many and varied. First, their existence does not guarantee assistance at all, never mind effective assistance. Secondly, where assistance is provided, there are routinely factors that impede successful cooperation e.g., priority afforded to the request, resources, language barriers etc. There is undoubtedly scope here for the international community to recognise that mutual legal assistance requests, as they relate to ransomware could and should be met with the utmost urgency.

Further to this, whilst expanded the FATF remit (suggested above) will improve mechanisms available to law enforcement in tackling ransomware attacks, it still leaves a significant gap around the sharing of best practice in tackling ransomware distribution. Consideration should be given to how this could be best facilitated.

Finally, cooperation is a two-way process, and as is the case with other financial crimes, weaknesses in other jurisdictions impede the quest to effectively tackle the crime. It is therefore imperative that all jurisdictions consider how they can support one another, particularly how we assist those in the global south who may be disproportionately impacted by ransomware and less able to react.

**Topic 7: Lessons that could be learned from other countries’ approaches and responses to ransomware.**

Government may consider harnessing the expertise of the private sector in a similar way to the approach adopted in the United Arab Emirates (UAE).

This would require greater use of public-private partnership as a method of tackling ransomware (and indeed all cybercrime) through the sharing with law enforcement of private sector knowledge, software, and other capabilities. The UK has some good examples of this e.g., work between the NCA, police and cryptocurrency investigative firms like Chainalysis, but this needs to become more routine and fully facilitated by Government / regulators. At present, there are too many limits to what they can achieve.

A second fundamental concept of the UAE approach is to sign agreements with tech-leading companies and promote their usage by business operating there (an outsourced service-centric model), rather than focussing on each individual business building up their own tech capabilities where there would be disparities in strength. Such a move should result in a consistently higher level of protection to ransomware across the board, something we recognise as being essential given that criminals seek to exploit any weakness in the system.

1. For more, see: <https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html#:~:text=Cyber%20insurance%20pricing%20in%20the,and%20the%20largest%20since%202015>. [↑](#footnote-ref-1)