Improving the UK's resilience to ransomware

RISCS held an online policy workshop on 2nd December 2021 with 33 participants from Government, academia, and the wider community as part of the RISCS Cybercrime theme led by Dr Maria Bada.

Context

Whilst ransomware isn't a new problem, criminals have exploited the COVID-19 pandemic, which offered more opportunities and left people and organisations more vulnerable to ransomware. For example, the requirement to work from home left organisations with less oversight over where their assets and vulnerabilities are (such as people using personal devices or home routers).[1] There were also attacks on many public sector organisations, including the University of Oxford while it was working on COVID-19 vaccine research.[2]

The aim of this workshop was to establish the latest thinking amongst the cybercrime community on understanding the scale of the ransomware problem, preventing and mitigating ransomware attacks, and to understand gaps in knowledge where further research is needed. This report summarises the discussions from the workshop and highlights possible research questions to explore that were identified during this session. We invite members of the RISCS community to consider taking forward research to address these gaps and would be happy to discuss opportunities for collaboration on any of them.

Key Points

- A better understanding of perpetrators could help prevent and improve recovery from ransomware attacks. Attackers possess a range of motivations and adopt different specialisms and tactics.
- Current under-reporting limits our ability to analyse and investigate the scale and implications of ransomware attacks. Ransomware victims may not understand why or how to report, or they might not feel incentivised to do so.
- The social impacts of ransomware are considerable but poorly understood. Tracking these can be challenging as surveys struggle to keep up with the pace of change in ransomware.
- Phishing is the main vector for ransomware. It is unsurprising that organisations struggle to repel attacks that arise from employees opening malicious links or attachments in emails.
- SMEs are likely to have a lower availability of expertise and support than larger organisation. For example, IT asset management (including traditional PCs and servers, or cloud-based databases) is too expensive for SMEs and the use of personal devices for work makes this more difficult.
- Organisations don't always connect business continuity and cybersecurity - i.e. business critical systems could be severely disrupted should a ransomware attack occur. In cases where organisations rely on outsourcing of software and IT infrastructures, their recovery may be out of their control entirely.
- There is a limited time window to investigate the cause of an attack, which needs to be balanced with undertaking the recovery process.

1 RISCS, 2021. Remote working and (In) Security: https://www.riscs.org.uk/new-publication-remote-working-and-insecurity/

2 NCSC Annual Report 2021: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/resilience/ncsc-response-to-covid

1. Understanding the offenders

Current understanding of who conducts ransomware attacks and their motivations is limited. Improving this may progress prevention and recovery efforts. Perpetrators include individual cybercriminals, organised criminal gangs, and state-sponsored or state-condoned attackers. Their motivations span a wide range of political, technical and economic reasons.

Behind each ransomware attack there is an ecosystem of cybercrime, where individuals and groups provide different specialisms and tactics to tailor attacks towards different sectors and organisation types. Both attackers and victims can be transnational. The ransomware ecosystem is becoming increasingly complex with the emergence of ransomware as a service (RaaS), which involves ransomware authors offering 'pay-for-use' ransomware. This complicates efforts to understand who offenders are and how they operate.

Possible questions to explore

- Where are ransomware attackers actually based? Are there any UK-based agents?
- Are different types of organisations (such as public, private or service providers) or organisations of different sizes subject to different types and volumes of attacks?
- What are the emerging threats in ransomware and who are the emerging attackers? Should we be concerned about AI-driven ransomware?
- How can post-attack forensics help us to understand the attacker(s) and their motivation(s)?
- Would more direct disruption of attackers' activity improve understanding of the scale and impact of ransomware attacks?

2. Organisational preparedness

Ransomware became the most significant cyber threat facing the UK in 2021.[3] Despite this, participants discussed that organisations often don't perceive themselves to be at risk. This could be a result of the media's tendency to highlight cases where large, multinational companies are ransomware victims, rather than portraying the issue as something that may affect organisations of any size or character. Organisations may not think they have anything of value to be taken, choosing instead to prioritise 'business as usual' issues that they perceive to be more likely to cost them money, but the reality is that any organisation with financial assets is at risk.

Cyber Essentials[4] is a Government backed certification scheme designed to guard organisations against the most common cyber threats and demonstrate their commitment to cyber security. According to the 2021 Cyber Security Breaches Survey,[5] the vast majority of organisations are not aware of the Cyber Essentials scheme and only 4% of businesses and charities report adhering to Cyber Essentials.

Equally, organisations may be overconfident and overestimate their preparedness for a ransomware attack. Some organisations who have achieved Cyber Essentials may feel they have 'ticked the compliance box'. Participants discussed that the most helpful

3 UK National Cyber Strategy 2022: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040805/National_Cyber_Strategy_-_FINAL_VERSION.pdf

4 NCSC Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials/overview

5 The Government's 2021 Cyber Security Breaches Survey found an overall low awareness of Cyber Essentials among both the business (14%) and charity (10%) populations: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

understanding for organisations to have is that while prevention strategies like obtaining Cyber Essentials won't always work, good is better than nothing.

It is not possible to fully protect an organisation from malware and it can therefore be assumed that at some point malware will infiltrate the organisation. For this reason, participants discussed whether more emphasis should be placed on mitigating an attack's impacts than prevention.[6]

Possible questions to explore:

- How do we reach SMEs and other organisations who aren't aware of Cyber Essentials or the potential risks of ransomware and incentivise them to take action?
- How can cyber security be embedded within an organisational culture and who has (or should have) the responsibility to promote cyber security and enhance resilience within an organisation?

3. Responding to an attack

When an attack happens, it's not a given that organisations will know immediately, let alone know who the right person to respond is. Participants raised examples of cases where organisations had not realised that malware had been on the system for months, rather than days. Research into cyber security culture within organisations can focus on the Chief Information Security Officer (CISO) but they may not always be the right person to respond, for example if they lack the organisational visibility or direct channel to the management team. Board level decisions may be required, but board members may not have sufficient knowledge and understanding about the incident and the required next steps to make an informed decision. The CISO needs to be able to convey the security risks appropriately through direct communication channels with management.

Organisations may not appreciate what needs to happen when an attack takes place: in particular, who they should report to, how long the recovery process might take, and what it could cost. Participants suggested that a clearer appreciation of these factors may aid the immediate response and decision making process.

Possible questions to explore

- How can we communicate the reporting and recovery process?
- Do organisations understand what happens following an attack and the guidance to inform their response?
- How can we improve our understanding of what happens after a ransomware attack is reported and what is the 'customer journey' for victims of ransomware?

4. Reporting

Under-reporting is a major obstacle in tackling ransomware as it obscures the scale of the challenge and limits investigation and analysis. Existing data is considered insufficient as it can rely on victims labelling their own experience as ransomware. This may be inaccurate if victims have a lack of understanding about what ransomware is, or if data collection methods lead to victims describing their experience as a cyber attack rather than specifically as ransomware. Participants raised a number of challenges in reporting. Organisations might not know who to

6 NCSC guidance on mitigating malware and ransomware attacks: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

report to between their insurance company, the police or the NCSC, nor what the process of reporting will look like or how long it will take.

There may be conflicts of interest between different stakeholders. For example, organisations with insurance cover for ransomware attacks might contact their insurers and be subsequently disincentivised from reporting the incident to law enforcement due to fears that doing so may slow down their pay out/support package from the insurer and the organisation's recovery to business as usual. Similarly, insurance companies may avoid reporting ransomware attacks to law enforcement if doing so might slow down their investigation of an attack.

Fear or embarrassment may shape an organisation's behaviour after an attack if there is uncertainty about what is happening, what could happen, or that individuals may be assigned blame. They may be confused or unsure of what happens after reporting an attack to the police or whether reporting may result in a GDPR fine. Amongst organisations affected by an attack, it may be unclear who is responsible for reporting where there are multiple actors involved, such as SMEs or outsourced IT companies. Full understanding of the scale and impact of ransomware may also be hindered by difficulties in information sharing between relevant actors – such as the police and the ICO.

Possible questions to explore

- Is there a stigma to reporting a ransomware attack? Does this differ between organisations of different sizes or in different sectors?
- How do data protection concerns affect reporting and how can these be balanced against the interest in reporting ransomware attacks?
- How can we incentivise reporting of ransomware attacks? For example, would a frictionless reporting system or the design of a 'safe harbour' help?
- Can we connect recovery assistance or an elimination or reduction in fines to reporting?
- How can recovery assistance be connected to improving baseline standards and reducing the likelihood and potential impact of future attacks?
- What can be learned from organisations/sectors with a strong reporting culture?

5. Financial impacts of ransomware attacks

The financial implications of an attack to a business depends on a number of factors: including the cost of paying a ransom (if they opt to do this), the costs of disruption to a business, and the cost of the recovery process. Some organisations may have insurance in place which is specific to cyber incidents, or seek to cover the costs through a broader insurance policy. NCSC have provided guidance regarding cyber insurance[7] and the government is working with the sector on sharing more robust cyber risk impact information. However, recent work by RUSI suggests that the positive effects of cyber insurance on cyber security are currently limited.[8]

Ransomware payments were a recurring discussion item. Participants shared the view that paying the ransom perpetuates the problem of ransomware, given that it helps to fund the attacker's activities and does not guarantee that data will be returned. Law

7 NCSC Cyber insurance guidance: https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

8 RUSI Occasional paper: Cyber insurance and the cyber security challenge: https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

enforcement do not encourage, endorse, nor condone the payment of ransom demands.[9]

The cost of business disruption will to some extent depend on whether adequate back-up mechanisms are in place, such as offline back-up systems or cloud based systems, which could allow some critical business functions to be restored. If this is not the case, or if backup systems have also been compromised, organisations may be unable to continue with any functions.

Organisations will need to scan back-up systems for malware before restoring files and prioritise business critical activities and reinstating physical servers. This could take several weeks depending on the scale of attack. Simultaneously, organisations need to deal with responding other elements of recovery, such as strategies for internal and external communications about the attack, any legal obligations to regulators and potential insurance claims. It was suggested during the discussion that organisations could underestimate the scale of the financial implications of a ransomware attack, and the steps required to prevent a repeat attack (for example, if the attackers know about vulnerabilities in back-up systems which they could exploit later).

Possible questions to explore

- What happens to lost data, particularly when there are legal implications (such as for sensitive data)?
- Why do some organisations decide to pay the ransom?
- What is the role of cyber insurance?
- Should the focus be on prevention strategies, or mitigation of these financial impacts?
- How does support for victims of ransomware attacks need to vary depending on organisation size and sector?

6. Social impacts of ransomware attacks

There can be a multitude of other impacts of ransomware attacks, on individual victims, organisations and society. For example, the considerable impact that the WannaCry ransomware had on the UK healthcare system. As well as financial implications, there can also be emotional and psychological impacts on victims. For example, affected individuals may feel shame or experience increased levels of stress in the aftermath of a ransomware attack. There is little support available for victims, who may also be prioritising the practical response to the attack rather than the well-being of their employees or customers.

Possible questions to explore

- How can different actors involved in tackling ransomware work together to address the social impacts of ransomware?
- How are data collected on the social impacts of ransomware?
- How do we ensure our response to a reported ransomware attack avoids causing additional harms to victims?

9 Same as footnote 6

- Could a system of 'best practice' and information sharing help reduce the social and financial impacts of ransomware, and could this be mandated? If so, who should be responsible for establishing these kind of practices – industry or Governments?
- How could story-telling and victim journey-mapping help understand and address the social impact of ransomware?

Participants list by organisation

- Accenture
- Cambridge University
- Cardiff University
- De Montfort University
- Eastern Region Cyber Resilience Centre
- Home Office
- University of Kent
- University of Leeds
- National Crime Agency
- NCSC
- University of Nottingham
- Oxford Brookes University
- Police Digital Security Centre
- QMUL
- Royal Holloway
- RUSI
- Talion
- UCL
- Westtek Solutions

Contributors

This workshop and report were produced in partnership with Florence Greatrix in UCL Engineering's Policy Impact Unit (PIU) and with Niamh Healy UCL as part of the Research Institute for Sociotechnical Cybersecurity (RISCS) Fellowship on Cybercrime led by Dr Maria Bada, QMUL. The team is particularly grateful for contributions and engagement from NCSC & Home Office with this work.

This workshop series on the RISCS Fellowship themes is funded by the UCL EPSRC Impact Acceleration Account and by RISCS.

Contact us

Dr Maria Bada, Lecturer in Psychology, Queen Mary University of London
RISCS Fellow for Cybercrime. M.Bada@qmul.ac.uk

For more information on the PIU, please visit: https://www.ucl.ac.uk/steapp/collaborate/policy-impact-unit-1