



Improving resilience to ransomware

Dr Maria Bada
Queen Mary University of London

 m.bada@qmul.ac.uk

Threat Landscape



Threat landscape



Ransomware attacks continued to be the preferred method of attack in 2022 (Forbes, 2022).

435% increase in such attacks in 2020 alone (WEF Global Risks Report, 2022).

Cybersecurity failure now frequently ranks as a top-five risk in East Asia and the Pacific as well as in Europe.

Four countries—Australia, Great Britain, Ireland, and New Zealand—ranked these attacks as their number one risk.


\$10T Global Cybercrime Damage Predicted by 2025.

Forbes (2022). Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. <https://www.forbes.com/sites/chuckbrooks/2022/06/03/ alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/? sh=5e343ee77864>

WEF (2022). The Global Risks Report 2022, 17th Edition. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

UK Cybersecurity Breaches Survey (2020).

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf



Improving resilience to ransomware attacks

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.

What can we do to improve resilience to ransomware?

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.

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>

Key Points

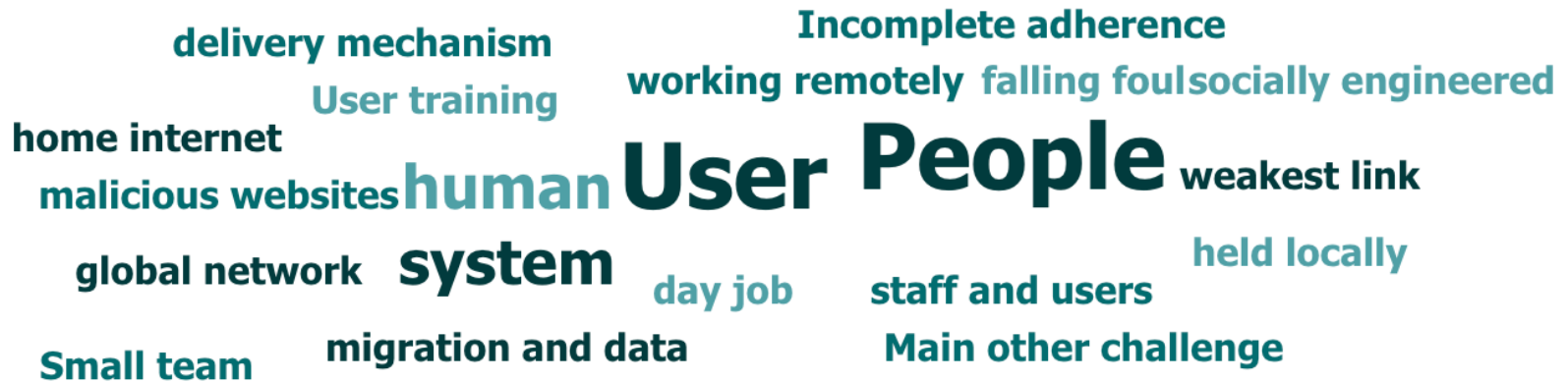
- A better understanding of perpetrators could help prevent and improve recovery from ransomware attacks. Attackers possess a range of motivations and adopt different specialisms and tactics.
- Current under-reporting limits our ability to analyse and investigate the scale and implications of ransomware 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.

Improving the UK's resilience to ransomware (December 2021)

AIM:

- a) To establish the latest thinking & practices around ransomware attacks.
 - b) Identify further research needs to inform new policy responses and/or change how organisations prevent and mitigate ransomware attacks.
-
- **Workshop: 33 participants** (Government, academia, business and the wider community).
 - **Online survey: 28 participants (SMEs)**

Biggest challenge for an organisation being resilient to ransomware



A word cloud of terms related to ransomware challenges. The most prominent words are 'User' and 'People'. Other significant words include 'system', 'weakest link', 'Incomplete adherence', 'socially engineered', 'working remotely', 'falling foul', 'day job', 'staff and users', 'Main other challenge', 'held locally', 'migration and data', 'Small team', 'global network', 'malicious websites', 'home internet', 'delivery mechanism', and 'User training'.

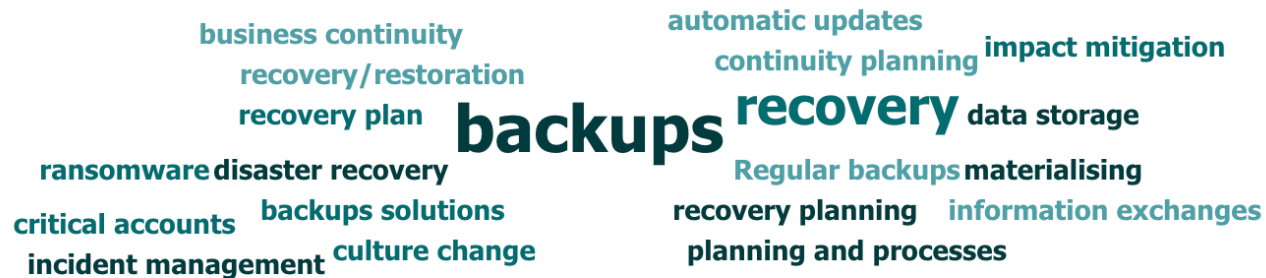
delivery mechanism **Incomplete adherence**
User training **working remotely** **falling foul** **socially engineered**
home internet **malicious websites** **human** **User** **People** **weakest link**
global network **system** **day job** **staff and users** **held locally**
Small team **migration and data** **Main other challenge**

Measures taken to prevent ransomware



A word cloud of cybersecurity measures. The most prominent word is "Training". Other significant words include "cyber security", "Firewalls", "ransomware", "security architecture", "SIEM monitoring", "security controls", "security awareness", "security job", "security event", "EDR", "malware protection", "malware solutions", "box solutions", "endpoint protection", "security services", "Security via our IT provider", "solutions", "protection culture", "network and infrastructure", and "security architecture".

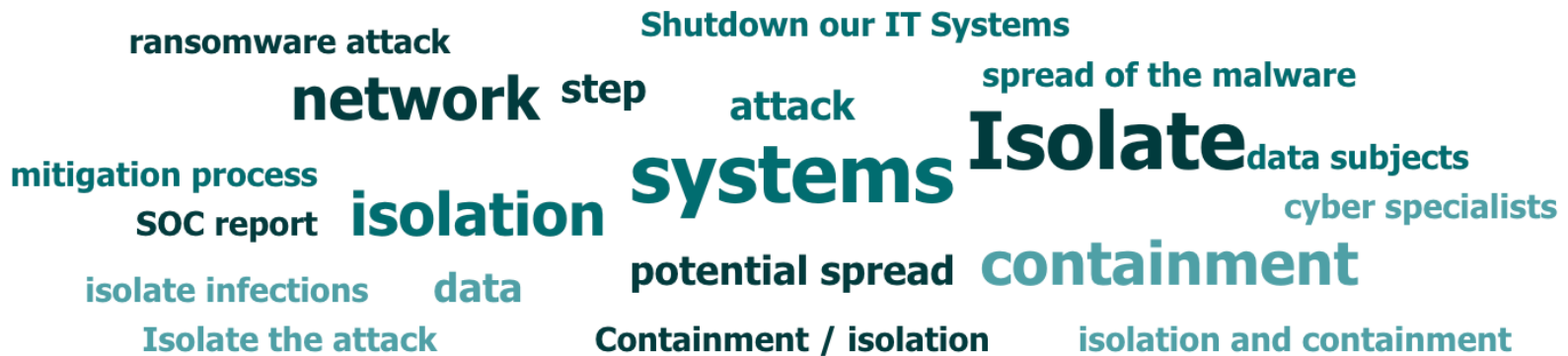
malware solutions SIEM monitoring security controls
Security awareness security job
box solutions security event **Training** **cyber security**
malware protection EDR solutions protection culture
endpoint protection security services Firewalls ransomware network and infrastructure
Security via our IT provider security architecture



A word cloud of recovery and continuity measures. The most prominent words are "backups" and "recovery". Other significant words include "disaster recovery", "regular backups", "materialising", "information exchanges", "planning and processes", "business continuity", "recovery/restoration", "recovery plan", "critical accounts", "incident management", "culture change", "automatic updates", "continuity planning", "impact mitigation", "data storage", "ransomware", "backups solutions", and "culture change".

business continuity automatic updates impact mitigation
recovery/restoration continuity planning
recovery plan **backups** **recovery** data storage
ransomware disaster recovery Regular backups materialising
critical accounts backups solutions recovery planning information exchanges
incident management culture change planning and processes

1st step in mitigating ransomware attacks



Communication Strategy



Reporting a Ransomware Attack to the Police



To Pay or Not to Pay



- The risk management and leadership teams face a critical decision: ***Should we pay the ransom?***
- Several factors should go into this decision:
 - the criticality of affected data and systems,
 - availability and integrity of data backups,
 - cost of the ransom versus the estimated cost of restoration,
 - the likelihood of successful restoration (whether the ransom is paid or not),
 - and regulatory implications

Identifying Key Gaps on Ransomware



Defending Against Ransomware Attacks

Ensure you have antivirus and firewall installed on all endpoints within the organization

Backup your data

Restrict admin rights on endpoints

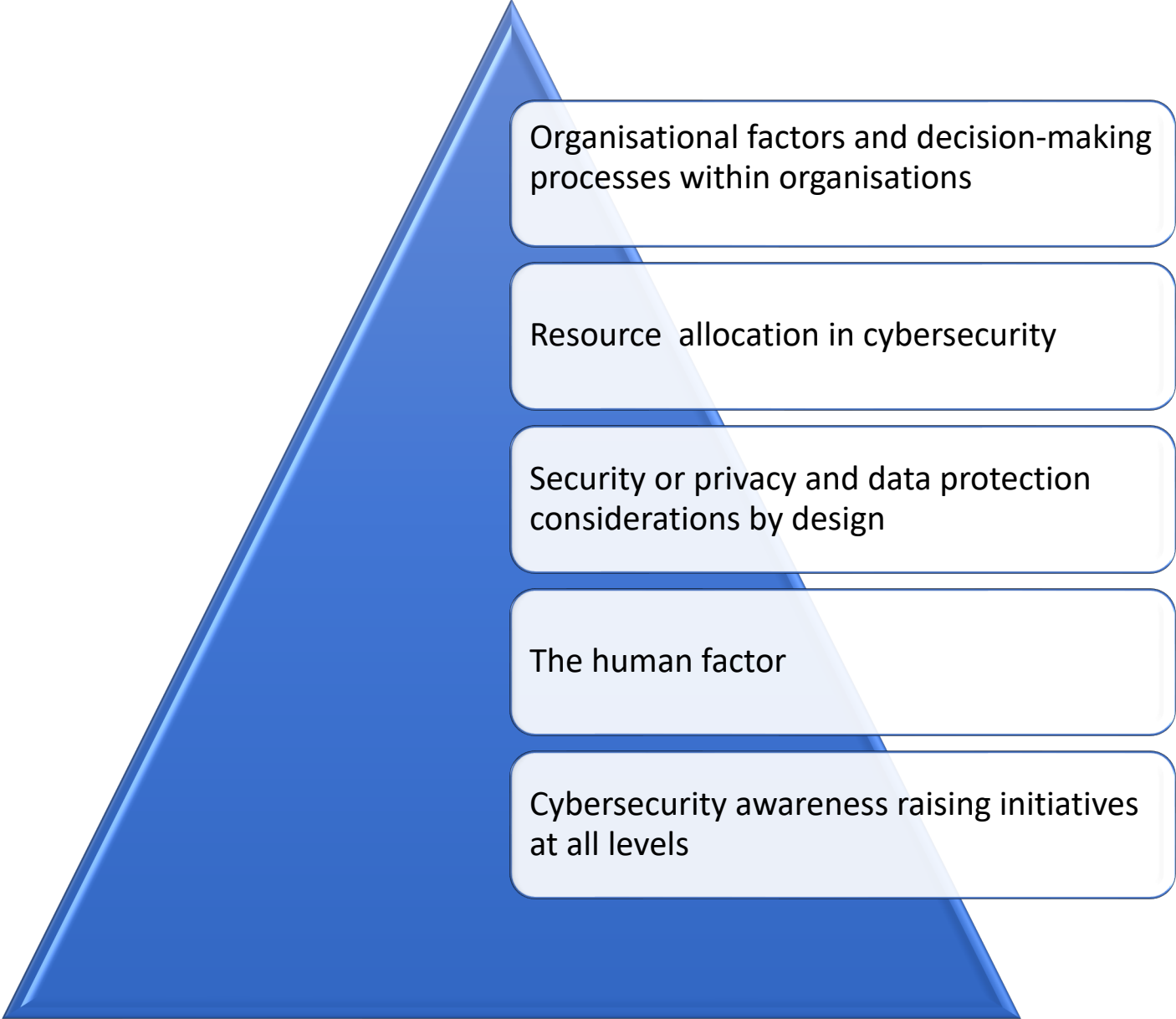
Keep commonly exploited third-party applications updated

Run a risk assessment

Invest in auditing & monitoring

Invest in cybersecurity awareness training tools for employees

Recommendations



Organisational factors and decision-making processes within organisations

Resource allocation in cybersecurity

Security or privacy and data protection considerations by design

The human factor

Cybersecurity awareness raising initiatives at all levels



Improving resilience to
ransomware with cybersecurity
capacity building



Improving Resilience to Ransomware with Cybersecurity Capacity Building

November 2022

Participants





A total of 36 participants took part in this study. Interviews were conducted with representatives from:

- Public sector
- Private sector
- Finance sector
- Academia
- Law enforcement
- Incident Response
- SMEs
- NGOs
- Non-profit organisations

Challenges in Managing Ransomware

Policy Recommendations

 Governance	 Criminal infrastructure
 Incident response capacity	 Cyber Insurance
 Legislation and law enforcement	 Trust and collaboration
 Certification schemes	 Societal impact
 Skills and training	

Cluster 1	Build effective partnerships for ransomware defence	
Cluster 2	Develop a community-based resilience architecture	
Cluster 3	Uplift cybersecurity skills and capacity	
Cluster 4	Define a regulatory response to ransomware	

Thank you!

Dr Maria Bada



m.bada@qmul.ac.uk



@MariaBadaCC