


Cyber Insurance and Ransomware

Dr Jason R.C. Nurse
Associate Professor in Cyber Security
University of Kent

 j.r.c.nurse@kent.ac.uk

 [jasonrcnurse](#)

 [jasonnurse](#)

 [jasonnurse.github.io](#)

What is Cyber Insurance?

... insurance [that] covers the losses relating to damage to, or loss of information from, IT systems and networks (ABI)



Cyber insurance & security: Lots said, varied evidence

Cyber-Insurance Metrics and Impact on Cyber-Security

“Sometimes we can . . . be a little bit more vigorous in using market-based incentives, working with the insurance industry, for example. . .”

DHS Secretary Michael Chertoff, April 29, 2005

“The Insurance industry has a pivotal role in play [in protecting our national infrastructure], particularly by developing cyber-insurance policies. This may be easier said than done...But carriers must begin...Somehow it can be done.”

Paul B. Kurtz, Homeland Security Council, 2003

Will Cyber-Insurance Improve Network Security?
A Market Analysis

Can Competitive Insurers Improve Network Security?

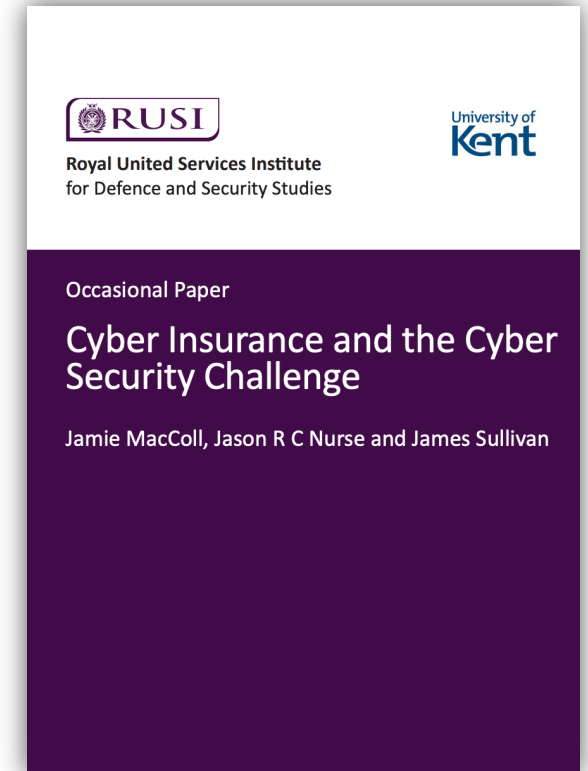
Cyber Insurance as an Incentive for Internet Security

Mapping the coverage of security controls in cyber insurance proposal forms

Can cyber insurance incentivise better security?

- Cyber insurance *could* incentivise better cyber security, but its mechanisms are imperfect in their current form/practice.
- The cyber insurance industry **faces challenges** that limit its ability to incentivise better cyber security practices.
 - Defining minimum security standards and best practices
 - Longstanding barriers to uptake
- It is **far from a silver bullet**, and insurance doesn't replace security.

(Based on 53 interviews and two workshops with professionals from the cyber insurance, government, security and government sectors)



<https://static.rusi.org/247-op-cyber-insurance.pdf>

Enter the threat of ransomware...

Companies May Be Flagging Themselves For Hackers By Buying Cybersecurity Insurance

Insurers 'funding organised crime' by paying ransomware claims

CYBER INSURANCE MAY BE MAKING RANSOMWARE WORSE, HERE'S WHY

**Cyber insurers running scared:
Ransomware “as profitable as cocaine”**

An interview with REvil's Unknown

DS: Do your operators target organizations that have cyber insurance?

UNK: Yes, this is one of the *tastiest morsels*. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

The Record.
Recorded Future® News

Is cyber insurance helping to mitigate the threat of ransomware, particularly its impacts?

Computers & Security 128 (2023) 103162

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Between a rock and a hard(ening) place: Cyber insurance in the ransomware era

Gareth Mott^a, Sarah Turner^b, Jason R.C. Nurse^{b,*}, Jamie MacColl^c, James Sullivan^c, Anna Cartwright^d, Edward Cartwright^e

^a School of Politics and International Relations and Institute of Cyber Security for Society (iCSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom
^b School of Computing and Institute of Cyber Security for Society (iCSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom
^c Royal United Services Institute (RUSI), 61 Whitehall, London, SW1A 2ET, United Kingdom
^d Oxford Brookes Business School, Oxford Brookes University, Oxford, OX3 0BP, United Kingdom
^e Department of Accounting, Finance and Economics, De Montfort University, Leicester, LE1 9BH, United Kingdom

ARTICLE INFO

Article history:
Received 20 November 2022
Revised 20 February 2023
Accepted 24 February 2023
Available online 27 February 2023

Keywords:
Cyber security
Ransomware
Cyber insurance
Security incidents
Harms
Cyber policy
Resilience
Critical national infrastructure
Malware

ABSTRACT

Cyber insurance and ransomware are two of the most studied areas within security research and practice to date, and their interplay continues to raise concerns in industry and government. This article offers substantial new insights and analysis into the complex question of whether cyber insurance can help organisations in mitigating the threat of ransomware, particularly its impacts. Having conducted an interview or workshop with 96 industry professionals spanning the cyber insurance, cyber security, ransomware negotiations, policy, and law enforcement sectors, we identify that ransomware has been a key cause of the 'hardening' of the cyber insurance market, which is exhibited at almost all levels of the market. Such hardening has been beneficial in raising the security standards required prior to purchase, but has also created a situation where some organisations may not be able to acquire viable cyber insurance at all. In presenting the outcomes of our thematic analysis of the interview and workshop outputs, the paper provides significant new empirical evidence to support the theory that cyber insurance can act as a form of governance for improving cyber security amongst organisations. Nonetheless, the hardening market does nothing to increase the penetration of cyber insurance. Questions were also raised as to the likelihood of unintended unethical – and potentially illegal – outcomes given the professionalisation of a remediation process that has to determine the most cost-effective solution to an organisation being held ransom. We conclude that insurance, at best, can help to mitigate the ransomware threat for those that can access it, as part of a wider basket of actions that must also come from different stakeholders.

© 2023 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Between a rock and a hard(ening) place:
cyber insurance in the ransomware era

<https://doi.org/10.1016/j.cose.2023.103162>



Cyber insurance supports ransomware response

- Cyber insurance offers policyholders **significant support after a ransomware attack.**
 - **Rapid access to expertise** (lawyers, to digital forensic specialists, recovery teams, data breach and data protection specialists, PR teams and negotiators...)
“...the smaller the entity, the more they need those services because **they don't know how to fix an issue...they don't have a hundred people in IT who can advise them who to speak to, to help fix it...we have it there for when clients need it.**”
 - Financial support to provide resiliency against two core risks prompted by ransomware: business interruption and data exfiltration

Mott et al., (2023) “Between a rock and a hard(ening) place: cyber insurance in the ransomware era”, Computers & Security Journal.
<https://doi.org/10.1016/j.cose.2023.103162>

Cyber insurance and ransomware: It's complicated

- **Professionals disagreed** on whether insureds were more likely to pay ransoms.
 - “no-one from the insurance industry really wants to go on the record and say, clearly it [insurance] has amplified this [ransomware]”, “[insurance] means they've got other options than just paying the ransom. It actually makes it less likely that they'd pay”
- Ransomware has hardened the market, **raising barriers for entry for insureds.**
 - “...like Dragon's Den.”, “...county councils, police authorities ... insurance has been quite a crutch for them .. So, the removal of that insurance has been a challenge”
 - Some sectors may find it significantly harder to acquire viable cyber insurance: airlines, education, public sector, hospitality, healthcare, manufacturing, CNI

Mott et al., (2023) “Between a rock and a hard(ening) place: cyber insurance in the ransomware era”, Computers & Security Journal.
<https://doi.org/10.1016/j.cose.2023.103162>

'Hot off the press' outputs

Computers & Security 128 (2023) 103162

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Between a rock and a hard(ening) place: Cyber insurance in the ransomware era

Gareth Mott^a, Sarah Turner^b, Jason R.C. Nurse^{b,*}, Jamie MacColl^c, James Sullivan^c, Anna Cartwright^d, Edward Cartwright^e

^a School of Politics and International Relations and Institute of Cyber Security for Society (ICSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom

^b School of Computing and Institute of Cyber Security for Society (ICSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom

^c Royal United Services Institute (RUSI), 61 Whitehall, London, SW1A 2ET, United Kingdom

^d Oxford Brookes Business School, Oxford Brookes University, Oxford, OX3 0BP, United Kingdom

^e Department of Accounting, Finance and Economics, De Montfort University, Leicester, LE1 9BH, United Kingdom

ARTICLE INFO

Article history:
Received 20 November 2022
Revised 20 February 2023
Accepted 24 February 2023
Available online 27 February 2023

Keywords:
Cyber security
Ransomware
Cyber insurance
Security incidents
Harms
Cyber policy
Resilience
Critical national infrastructure
Malware

ABSTRACT

Cyber insurance and ransomware are two of the most studied areas within security research and practice to date, and their interplay continues to raise concerns in industry and government. This article offers substantial new insights and analysis into the complex question of whether cyber insurance can help organisations in mitigating the threat of ransomware, particularly its impacts. Having conducted an interview or workshop with 96 industry professionals spanning the cyber insurance, cyber security, ransomware negotiations, policy, and law enforcement sectors, we identify that ransomware has been a key cause of the 'hardening' of the cyber insurance market, which is exhibited at almost all levels of the market. Such hardening has been beneficial in raising the security standards required prior to purchase, but has also created a situation where some organisations may not be able to acquire viable cyber insurance at all. In presenting the outcomes of our thematic analysis of the interview and workshop outputs, the paper provides significant new empirical evidence to support the theory that cyber insurance can act as a form of governance for improving cyber security amongst organisations. Nonetheless, the hardening market does nothing to increase the penetration of cyber insurance. Questions were also raised as to the likelihood of unintended unethical – and potentially illegal – outcomes given the professionalisation of a remediation process that has to determine the most cost-effective solution to an organisation being held ransom. We conclude that insurance, at best, can help to mitigate the ransomware threat for those that can access it, as part of a wider basket of actions that must also come from different stakeholders.

© 2023 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Between a rock and a hard(ening) place: Cyber insurance in the ransomware era

<https://doi.org/10.1016/j.cose.2023.103162>

How Cyber-Insurance Influences the Ransomware Payment Decision: Theory and Evidence***

Anna Cartwright¹[0000-0003-1965-842X],
Edward Cartwright²[0000-0003-0194-9368],
Jamie MacColl³,
Gareth Mott⁴[0000-0002-8788-769X],
Sarah Turner⁵[0000-0003-1246-1528],
James Sullivan³, and
Jason R.C. Nurse⁵[0000-0003-4118-1680]

¹ Oxford Brookes Business School, Oxford Brookes University, Oxford, UK.
² Department of Accounting, Finance and Economics, De Montfort University, Leicester, UK. edward.cartwright@dmu.ac.uk
³ Royal United Services Institute, Whitehall, London, UK.
⁴ School of Politics and International Relations, University of Kent, Canterbury, UK.
⁵ School of Computing, University of Kent, Canterbury, UK.

Abstract. In this paper we analyse how cyber-insurance influences the cost-benefit decision making process of a ransomware victim. Specifically, we ask whether organizations with cyber-insurance are more likely to pay a ransom than non-insureds. We propose a game-theoretic framework with which to categorize and distinguish different channels through which insurance may influence victim decision making. This allows us to identify ways in which insurance may incentivize or disincentivize payment of the ransom. Our framework is informed by data from semi-structured interviews with 65 professionals with expertise in cyber-insurance, cyber-security and/or ransomware, as well as data from the UK Cyber Security Breaches Survey. We find that perceptions are very divided on whether victims with insurance are more (or less) likely to pay a ransom. Our model can reconcile these views once we take into account context specifics, such as the severity of the attack as measured by business interruption and restoration and/or the exfiltration of sensitive data.

How cyber insurance influences the ransomware payment decision: theory and evidence

<https://doi.org/10.1057/s41288-023-00288-8>



Impact and reach

AP

In crosshairs of ransomware crooks, cyber insurers struggle

**ZD
NET**

Cyber insurance isn't helping with cybersecurity, and it might be making the ransomware crisis worse, say researchers

GA THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

infosecurity

Think Tank Calls for Government Review into Banning Ransom Payments

**Ransomware:
An insurance market perspective**

Ransomware Harms and the Victim Experience

This project examines the impact of ransomware on victims, economies and societies.



<https://rusi.org/explore-our-research/projects/ransomware-harms-and-victim-experience>

It's more than just money: Understanding the real-world harms of ransomware attacks

Nandita Pattnaik¹, Jason R.C. Nurse¹, Sarah Turner¹, Gareth Mott¹,
Jamie MacColl², Pia Huesch², and James Sullivan²

¹ Institute of Cyber Security for Society (iCSS) & School of Computing,
University of Kent, UK

² Royal United Services Institute (RUSI), UK
J.R.C.Nurse@kent.ac.uk

Abstract. As cyber-attacks continue to increase in frequency and sophistication, organisations must be better prepared to face the reality of an incident. Any organisational plan that intends to be successful at controlling and managing security risks must clearly understand the harm (i.e., negative impact) and the various parties impacted in the aftermath of an attack. To this end, this article conducts a novel exploration into the multitude of real-world harms that can arise from cyber-attacks, with a particular focus on ransomware incidents given their current prominence. We draw on publicly-available case data on high-profile ransomware incidents to examine the types of harm that emerge at various stages after a ransomware attack and how harms (e.g., an offline server) may trigger other negative, potentially more substantial impacts for stakeholders (e.g., the inability for a customer to access their social welfare benefits or bank account). Prominent findings from our analysis include the identification of a notable set of social/human harms beyond the business itself (and beyond the financial payment of a ransom) and a complex web of harms that emerge after attacks regardless of the industry sector. We also observed that deciphering the full extent and sequence of harms can be a challenging undertaking because of the lack of complete data available. This paper consequently argues for more transparency on ransomware harms, as it would lead to a better understanding of the realities of these incidents to the benefit of organisations and society more generally.

It's more than just money: Understanding the real-world harms of ransomware attacks, Accepted to 17th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023)


Cyber Insurance and Ransomware

Dr Jason R.C. Nurse
Associate Professor in Cyber Security
University of Kent

 j.r.c.nurse@kent.ac.uk

 [jasonrcnurse](#)

 [jasonnurse](#)

 [jasonnurse.github.io](#)