RESEARCH SUMMARY

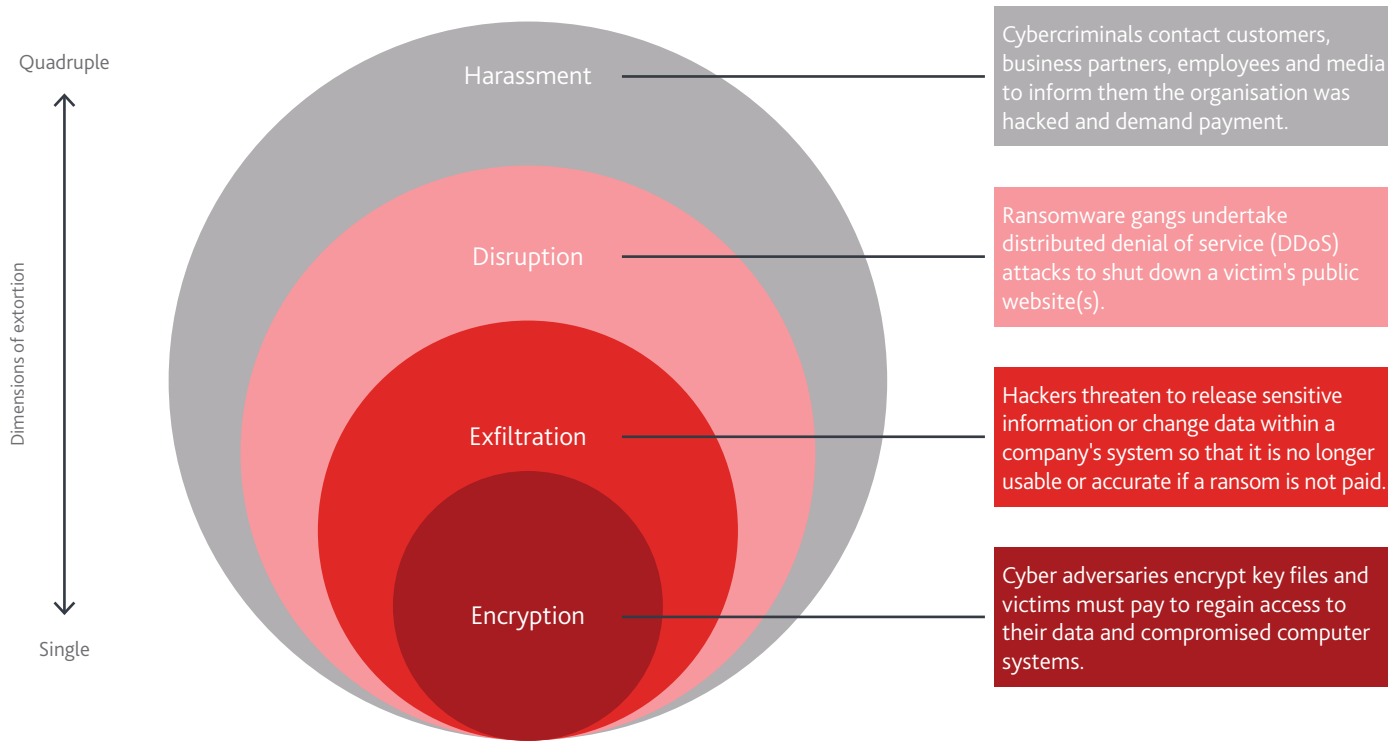
# Ransomware: An insurance market perspective

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD


**Darren Pain**, Director Cyber and Evolving Liability, The Geneva Association
**Dennis Noordhoek**, Director Public Policy & Regulation, The Geneva Association

Ransomware – a type of malicious software that gains access to files or systems and blocks user access until the victim pays a ransom in exchange for a decryption key – and other associated forms of cyber extortion have recently become a serious issue. The number of attempted intrusions and successful attacks as well as the size of ransom demands have trended sharply higher in recent years. Cybercriminals are also deploying sophisticated approaches to extort their victims. Rather than solely encrypting data/files and demanding a payment for their release, ransomware operators increasingly adopt additional extortion techniques. These include threatening to release sensitive information or taking down a firm's website if the ransom is not paid (Figure 1).

***Figure 1: Different extortion methods used by ransomware criminals***




*Source: The Geneva Association*

The development of the ransomware-as-a-service (RaaS) business model, which enables hackers to use off-the-shelf ransomware tools and services, has supercharged this field of cybercrime and enabled threat actors, even with limited technical IT skills, to launch highly disruptive attacks. A whole RaaS ecosystem has sprung up with cybercriminals now adopting specialised roles, most of which may have nothing to do with the actual launch of an attack. These include: identifying unknown vulnerabilities, gaining initial access, developing malware, processing any ransoms paid and even handling the negotiations.

## Impact on the insurance sector

Affirmative cyber insurance policies typically cover the external expenses associated with a cyberattack (for example, the costs of forensic investigations, data/system restoration and crisis management fees), business interruption costs, liabilities to third parties affected by the attack as well as any ransom paid. Ransomware has been a significant factor in the notable deterioration in cyber insurers' underwriting performance over the past two years. In aggregate, the loss ratio on U.S. cyber insurance rose from 44.6% in 2019 to 66.9% in in 2020, with ransomware accounting for three quarters of claims according to credit rating agency AM Best.[1]

More recent indicators suggest no material improvement in the claims environment, with ransomware remaining a key driver. Given the continued upward pressure on claims, cyber insurers' loss ratios remained elevated in 2021 despite a steep increase in the price of cyber insurance last year.

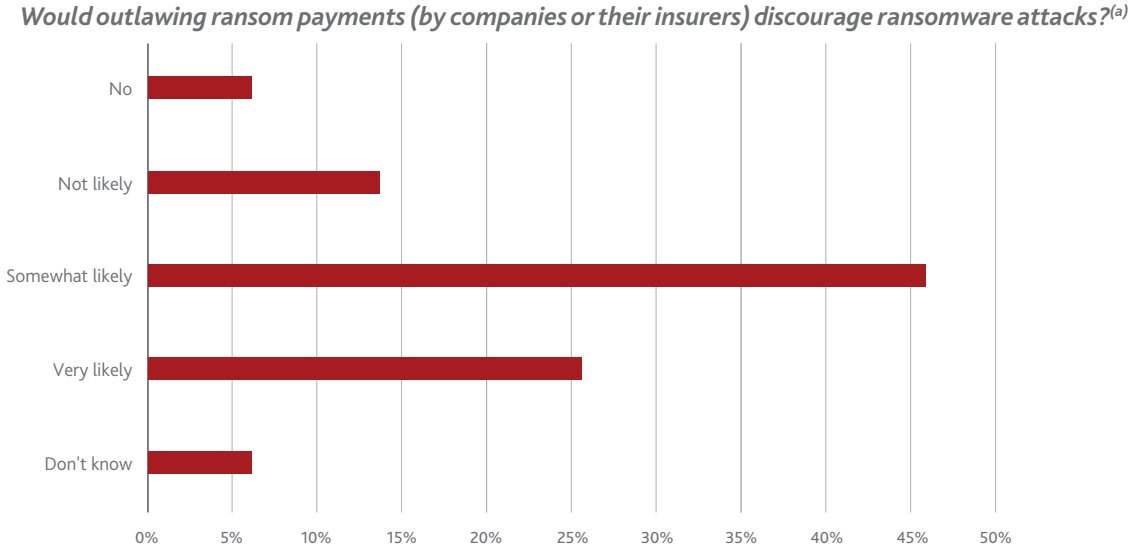
## Ongoing policy debate

By paying ransoms, firms also potentially incentivise ransomware criminals and in the process amplify the risk of future attacks on themselves or others. While this economic externality exists whether or not the victim of a ransomware attack is insured, some external commentators have expressed concern that the presence of insurance could make the situation worse by encouraging targeted ransomware attacks on those with cover. One 2021 study, for example, shows that 70% of U.K. IT security professionals surveyed believe insurance payments to companies that have paid a ransomware demand exacerbate the problem and cause more attacks.[2] Governments have also hinted at the unintentional impact that insurance may have on ransomware extortion, highlighting how the ransoms demanded are often tailored to the amount insured under the cyber insurance policy.

This has revived a policy debate about how far governments should intervene to mitigate the economic externality associated with ransoms – that is, using laws, regulations and taxes to ensure victim firms recognise that paying ransoms possibly fosters more ransomware and ratchets up future extortion demands.

Policy discussions are ongoing in a number of countries about the possibility of banning ransom payments altogether. The rationale is that if ransoms or the insurance payouts for ransom payments were prohibited, ransomware victims would be less likely to pay cybercriminals. And if ransomware targets did not pay or reduced the amount they were willing to pay (due to the lack of insurance funds as a potential source of finance), hackers' incentive to demand a ransom in the first place would also be diminished.[3]

***Figure 2: Re/insurer views on a ransom ban***




*(a) Based on a sample of 15 re/insurers active in the global cyber insurance market*

*Source: The Geneva Association*

1 AM Best 2021.
2 Talion 2021.
3 Logue and Shniderman 2021.

## Banning ransom payments is not really the answer

In practice, there are no easy solutions to ransomware and measures often involve important trade-offs, not least because of the potential for unintended consequences. For instance, an outright ban on ransom payments could drive such transactions underground and/or encourage ransomware attackers to engage in new forms of extortion, including threats to destroy property or cause bodily injury if their demands are not met.

A Geneva Association survey of cyber re/insurers reveals that, while most feel that banning ransom payments or prohibiting associated insurance payouts would probably discourage some ransomware attacks (Figure 2), such a blunt policy response may not always have the desired effect, especially if bans are not consistently applied on an international level. A ban solely against insurer reimbursements would be particularly ineffective, depriving victims of an important means of protection when other forms of risk financing may be difficult to organise. The absence of cyber insurance cover for extortion payments not only penalises the insured, but also does nothing to address the growth of RaaS, which has fuelled ransomware attacks.

Italy's experience with kidnapping in the 1990s underscores the challenges of any ransom ban. The Italian government made it illegal to pay ransoms in 1991, a move widely credited for the subsequent flattening in kidnapping rates. But the threat did not go away completely as the families of kidnapped Italian citizens simply stopped reporting crimes to authorities. If ransomware payments were outlawed, victim companies would likely look to cover up attacks and route ransom payments through unofficial mechanisms to avoid detection. This potentially means that learnings and lessons about new ransomware strains would largely go unheeded.

## Cyber insurance is part of the of the solution

While it is often ransom payments that grab the headlines, the total losses related to a ransomware attack go well beyond extortion demands. Insurance plays an important role in supporting companies that face a variety of first- and third-party losses resulting from ransomware. After an attack, cyber insurance can be a mechanism for convening the right team of experts, including legal counsel and computer forensic analysts, to assess the incident and recommend a timely response. These experts often bring in

***Table 1: Re/insurer suggestions for possible government policies to counter ransomware***

| Objective | Policy proposal |
|---|---|
| Deter | • Ensure tougher penalties against cybercriminals who carry out ransomware attacks<br>• Promote international coordination of sanctions regimes that prohibit transactions with banned entities, including sharing intelligence on re-branded ransomware strains |
| Disrupt | • Hold cryptocurrency exchanges and peer-to-peer platforms to standards for due diligence in creating accounts and monitoring transactions, including additional know-your-customer and traceability requirements<br>• Pursue, prosecute and publicise illicit activities of unlicensed exchanges and crypto-swapping services |
| Prepare | • Promote minimum cybersecurity standards and foster mechanisms to encourage best practice (for example, public resilience standards, such as minimum-security guidelines and incident response support, to help SMEs in particular)<br>• Strengthen disclosure regimes for ransomware incidents (possibly including mandatory reporting of incidents for certain sectors to the authorities, on a timetable that does not worsen the threat) and publish more threat intelligence to help businesses harden their cyber defences, raise awareness of threat actors' new TTPs and facilitate information sharing (e.g. decryptor keys)<br>• Enhance responsibilities for key network infrastructure such as cloud providers to improve overall resilience of digital assets |
| Respond | • Develop enhanced offense capabilities to pursue/prosecute the perpetrators of ransomware attacks and recover ransoms, with better consistency in coordination and action among law enforcement agencies<br>• Set up government-sponsored agencies to support cybercrime victim organisations, especially small firms<br>• Upgrade the technical knowledge and skills of public authorities and law enforcement to counter cybercrime |

*Source: The Geneva Association*

valuable negotiating skills that can be used to help lower the ransom actually paid – not least because they are well placed to assess the credibility of the threat, including the viability of decryption keys and likelihood of restoring operations.

In addition to providing ransomware victims with the operational and financial support needed to help them recover as quickly as possible, cyber insurance can make an important contribution to the overall management of cyber risk. Insurance can positively influence cyber-security standards and best practices by promoting awareness about the exposure to ransomware and other cybercrime, sharing expertise on risk management and encouraging investment in risk prevention and mitigation. For instance, carriers (directly or in collaboration with specialist cybersecurity firms) often continuously monitor the threat environment, highlighting vulnerabilities and weaknesses in a firm's networks and systems that might be unknown to the policyholder. Likewise, through the terms and conditions of available cover, re/insurers can incentivise investment in good cyber hygiene, which significantly lowers the chance of ransomware and other cyberattacks. These core benefits of insurance need to be weighed against any inadvertent, adverse-incentive effects on cybercriminals to carry out ransomware attacks.

## Governments and regulators must go further to counter ransomware attacks

There is no silver bullet for ransomware, and a multi-faceted approach will be required to reduce the underlying drivers, limit their impact and ensure business resilience. Governments, along with their regulatory and supervisory agencies, have an important role to play in improving the security of cyberspace and helping legitimate businesses gain the upper hand against cyber adversaries. Table 1 presents suggestions from re/insurers for policies aimed at deterring ransomware attacks, disrupting cybercriminals' business models, preparing organisations better against intrusions and responding to attacks more effectively.

Many of these suggestions are mirrored in measures already announced by various governments to enhance cyber security in the wake of the recent ransomware epidemic. In particular, improved mechanisms to track, monitor and share information about ransomware strains should be beneficial. The threat intelligence gathered by government-sponsored security agencies could be used to identify and track down cybercriminals. It could also provide advanced warning and guidance to victims on effective counter measures and decryptor tools to contain any spread of the malware.

Tighter cryptocurrency regulations to help identify and root out illicit transactions, enhanced cryptocurrency tracing, forensics and other blockchain intelligence tools to recover stolen funds will also be needed – especially to counter emerging trends such as the adoption of privacy-protecting coins and the use of decentralised exchanges that make investigating online crimes and enforcing sanctions difficult.[4] Together with high-profile public seizures, this will act as a deterrent: if cybercriminals know law enforcement can seize their cryptocurrency, it may lower their incentive to use it in the future.

Policy can also encourage firms to make themselves more resilient against ransomware attacks. Aggregate premiums for standalone cyber insurance represent less than 1% of the global property and casualty market, while some reports indicate that only around a third of small businesses purchase this kind of protection. With cyber exposures only set to increase, policy measures to foster this small but nascent market will help ensure the full societal benefits of cyberspace are realised.

## References


AM Best. 2021. Best's Market Segment Report: Ransomware and aggregation issues call for new approaches to cyber risk. https://news.ambest.com/presscontent.aspx?refnum=30762&altsrc=9

Clark, R., S. Kreps, and A. Rao. 2022. Shifting Crypto Landscape Threatens Crime Investigations and Sanctions. Brookings TechStream. 7 March. https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/

K. Logue and A. Shniderman. 2021. The Case for Banning (and Mandating) Ransomware Insurance. https://repository.law.umich.edu/law_econ_current/207/

Talion. 2021. Ransomware Perceptions Report, 2021. https://talion.net/wp-content/uploads/2021/08/Talion-Report_final.pdf


4 For example, Monero utilises a number of privacy-enhancing technologies, such as the obscuring of IP addresses, to obfuscate the identities of those involved in trades and improve the fungibility of tokens. Clark et al. 2022.