THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

Ransomware: An insurance market perspective

July 2022

Ransomware: An insurance market perspective

Darren Pain, Director Cyber and Evolving Liability, The Geneva Association

Dennis Noordhoek, Director Public Policy & Regulation, The Geneva Association

The Geneva Association

The Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members and other stakeholders to discuss these trends and recommendations; and reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

Photo credits:
Cover page— Andrey_Popov and JMiks / Shutterstock.com

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor and Content Manager
Petr Neugebauer, Digital Media Manager

Suggested citation: The Geneva Association. 2022.
Ransomware: An insurance market perspective.
Authors: Darren Pain and Dennis Noordhoek. July.

www.genevaassociation.org

Contents

Acknowledgements

We wish to extend our gratitude to members and affiliates of the Geneva Association's Cyber and Public Policy and Regulation Working Groups, whose inputs were invaluable to the preparation of this report. Special thanks in particular go to the following colleagues for sharing their insights:

- Paul Lloyd and Tanya Kitt (AIA)
- Chuck Jainchill, Martin Hansen and Anthony Zobl (AIG)
- Scott Sayce and Marek Stanislawski (Allianz Global Corporate & Specialty)
- Max Broodryk and Hélène Chauveau (AXA)
- Matt Silley and Dan Trueman (AXIS Capital)
- Aidan Flynn and Paul Bantick (Beazley)
- Matt Prevost (Chubb)
- Paolo Madrussa (Generali)
- Anika Stehr (Hannover Re)
- Philipp Lienau (HDI Global)
- Mary Fisk-Bieker (Intact Financial Corporation)
- Neil Arklie (Lloyd's)
- Daniel Lamela Largacha and Oscar Taboada (MAPFRE)
- Diana Keegan-Dickson (MetLife)
- Martin Kreuzer and Panos Charissiadis (Munich Re)
- Simon Dejung (SCOR)
- Eric Durand, Tobias Wassmann and Sandy Codding (Swiss Re)
- Kei Kato, Harriet Gruen, Daljitt Barn and Matthew McKinnell (Tokio Marine)
- Marc Radice (Zurich Insurance)

Foreword

One ransomware attack targets a leading technology company, whose proprietary data starts appearing online. Another infiltrates an industrial powerhouse and brings global manufacturing to a halt. Yet another wreaks havoc on an entire country's civil aviation. Two separate attacks compromise two different governments, crippling core services and their ability to protect their own citizens.

And these were only in the first half of 2022.

Ransomware attacks have become even more damaging, audacious and widespread over recent years, with no obvious let-up on the horizon. The growth of this particular class of cybercrime can be tied in part to ongoing digitalisation and society's reliance on IT, which the pandemic only served to accelerate. Despite all the benefits of digital technology, the proliferation of ransomware is an unfortunate by-product.

Extortion through ransomware is only one feature of the evolving cyber risk landscape, but its potential impact on victims and their insurers, who may underwrite associated losses, demands special attention. For re/insurers, the proliferation of ransomware attacks has driven up claims, which has prompted an increase in insurance premiums. Many ransomware victims may simply find it easier and less costly to pay the ransom demand than to endure interruption to their businesses and/or incur costs to remove the malware and restore data. This is potentially creating a vicious cycle and incentivising criminals to continue carrying out ransomware attacks.

A natural reaction may be to prohibit ransom payments altogether; some governments around the world contemplate such a move. But the law of unintended consequences suggests caution, as such a ban could mean that organisations most in need of protection are even more exposed to an attack.

Instead, the future management and prevention of ransomware attacks will be a complex undertaking, requiring a multi-faceted approach. Some re/insurers have already invested in new ways to assess insureds' cyber maturity and security controls. Additionally, insurers can leverage premium discounts, co-insurance and retention arrangements to incentivise organisations to adopt essential cybersecurity best practices, reducing their susceptibility to intrusion.

For their part, governments and regulatory agencies will need to step up their efforts to dismantle cybercriminal business models and help organisations better respond to attacks. Building on the insights gained from discussions with re/insurers, this report puts forward possible policy measures that, in combination, could go a long way to boosting cybersecurity. What is clear is that countering the rise in ransomware will take commitment, innovation and a deep understanding of emerging cyber risks. The re/insurance industry is well-placed to contribute to that endeavour.

Jad Ariss
Managing Director, The Geneva Association

1. Executive summary

As a form of cyber extortion, ransomware is 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. It has become a serious issue as 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, including threats to release sensitive information or take down a firm's website if the ransom is not paid. The development of the ransomware-as-a-service (RaaS) business model has supercharged this field of cybercrime and enabled threat actors, even with limited technical IT skills, to launch highly disruptive attacks.

> Cybercriminals are deploying sophisticated approaches to extort their victims, including threats to release sensitive information.

Ransomware attacks have been a significant factor in the notable deterioration in cyber insurers' underwriting performance over the past two years. In aggregate, the loss ratio on US 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. While the bulk of ransomware claims reflect recovery and remediation costs from an attack, including business interruption, the share associated with the reimbursement of ransoms has increased. More recent indicators suggest no material improvement in the claims environment, with ransomware remaining a key driver. In the face of continued claims, cyber insurers' loss ratios remained elevated in 2021 despite a steep increase in the price of cyber insurance last year.

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. 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 either paid directly by victims or reimbursed by re/insurers; that is, the extent to which governments can use additional laws, regulations and taxes to ensure victim firms recognise the costs that paying ransoms impose on others in terms of possibly fostering more ransomware and ratcheting up future extortion demands. In practice, there are no easy solutions 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.

The challenge of economic externalities is not unique to ransomware. Similar issues arise in the context of kidnap and ransom (K&R) insurance. K&R re/insurers have developed market practices to encourage a standard approach to information exchange and resolution which works to stabilise ransoms. Although the market for cyber insurance is also concentrated, there are limited mechanisms to share intelligence about attacks, let alone impose sanctions on re/insurers that deviate from established ransom benchmarks.

By compensating victims for all insured costs of a cyber-attack, insurers make good on their promise to indemnify policyholders against any harm suffered that was beyond their control. As part of the underwriting process, insurers also expose weaknesses in an organisation's cyber defences and provide guidance for strengthening security. These core aims of insurance need to be weighed against any potential adverse-incentive effects on cybercriminals to carry out ransomware attacks. This is why it is important that the views of re/insurers on how to deal with ransomware are always part of the debate.

For a re/insurer perspective, we surveyed and/or interviewed selected Geneva Association member companies that are active in cyber insurance. The main findings are as follows:

- Banning ransom payments is a blunt, potentially ineffective instrument. Banning ransom payments by the targeted companies or prohibiting reimbursement by re/insurers would probably discourage some attacks; but such a blunt policy response may not always have the desired effect, especially if bans are not consistently applied on an international level.

- Cyber insurance provides more than cover for ransoms. Most re/insurers are not daunted by the prospect of a ban on ransom payments – the value proposition of cyber insurance would remain, especially since it serves as a key mechanism for convening experts to assess the incident and recommend a timely response.

- Involving outside experts leads to better outcomes for the insured. Independent experts help the affected organisations make informed decisions about ransomware attacks and better negotiate, potentially lowering the ransom actually paid, although the chosen response to a ransomware attack is ultimately up to the victim.

- Insurance helps improve overall cyber hygiene standards. Along with supporting the insured in the case of an attack, insurance plays an important role in encouraging good cyber hygiene and risk prevention, for example through premium discounts, co-insurance and retention arrangements as well as cover limits, all of which can vary across firms according to their overall security standards.

- Governments and regulators must go further to counter ransomware attacks. Policies aimed at deterring ransomware attacks, disrupting cybercriminals' business models (including their use of cryptocurrencies to launder funds), better preparing organisations for intrusions and more effectively responding to attacks will improve the security of cyberspace and help legitimate businesses gain the upper hand against cyber adversaries.

There is no silver bullet for ransomware. A multi-faceted approach will be required to reduce the underlying drivers, limit their impact and ensure business resilience. For that reason, cyber insurance should be seen as an integral part of the solution rather than a catalyst for ransomware.

There is no silver bullet for ransomware. A multi-faceted approach will be required to reduce the underlying drivers, limit their impact and ensure business resilience.

While outright ransom bans or restrictions continue to be discussed in some jurisdictions, such legal reforms remain subject to considerable debate and ultimately may never make it to the statute book. Instead, governments seem to be coalescing around a combination of enhanced security measures to counter the rise in ransomware. These include updating disclosure laws to increase the understanding of the crime and enable better targeting of disruption activities; tougher regulation to make it harder for criminals to use cryptocurrencies for illicit purposes; more effective mechanisms and institutional structures to exchange threat information among stakeholders, including improved international cooperation among law enforcement agencies; and measures to promote cybersecurity best practice as well as address vulnerabilities in software supply chains.

The cyber insurance market remains small but nascent. Premiums 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. To help the market develop further, policymakers should therefore avoid measures that could inadvertently discourage households and firms from buying cyber insurance. Instead, policies that aim to safeguard cyberspace, promote cybersecurity and undermine cybercriminals' business models will help to counter malware attacks and increase re/insurers' appetite to absorb cyber risks from those less able to deal with them.

2. Introduction

The ongoing diffusion of new digital technologies in everyday life and business has fundamentally affected the risk landscape facing firms and individuals. Although technological advances create many benefits that improve our lives and lifestyles, they also leave users open to cybersecurity breaches and intrusions. The response to the global spread of COVID-19 in 2020 and 2021 has only accelerated prevailing digital trends and amplified cyber risks.

According to computer software company McAfee and the Center for Strategic and International Studies (CSIS), cybercrime costs the world economy more than USD 1 trillion per year, i.e. just more than 1% of global GDP. This is up more than 50% from a similar study in 2018, which put global losses at close to USD 600 billion.[1] Similarly, Accenture reports that the volume of cyber intrusion activity globally jumped 125% in the first half of 2021 compared with the same period in the previous year.[2]

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 has recently become especially prolific. These sorts of cyberattacks have been a significant factor in the sharp 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 2020, with nearly all of the 20 largest U.S. cyber insurers reporting a deterioration in underwriting performance.[3] According to credit rating agency AM Best, ransomware accounted for 75% of all cyber insurance claims in 2020.[4]

Ransomware – a type of malicious software that gains access to files or systems and blocks user access until the victim pays a ransom – and other forms of cyber extortion has become prolific.

In the face of higher incurred losses, risk-absorbing capacity has fallen as some re/insurers have withdrawn from the cyber market and/or reduced limits and sub-limits on available cover. With demand for protection remaining strong, and even growing given heightened awareness of malicious cyber threats, this has triggered a rapid re-pricing of cyber insurance. According to Marsh, in the year to Q1 2022 the cost of cyber protection rose by more than 100% in the U.S. and the U.K. and by 80% in Continental Europe.[5] More restrictive coverage terms, including higher retentions, co-insurance and exclusions, have also become more prevalent.

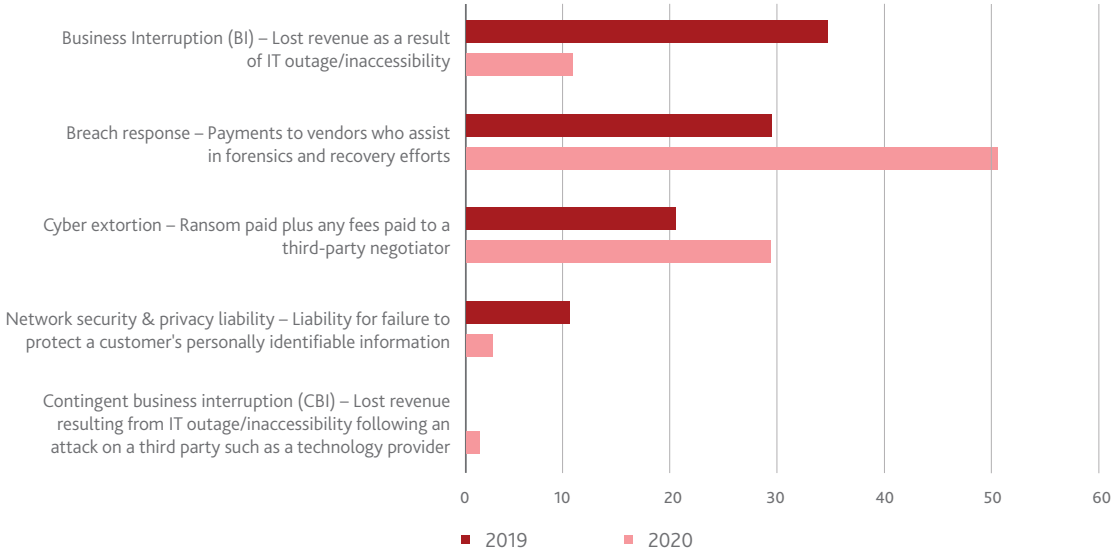
1 McAfee 2020.
2 Accenture 2021.
3 The aggregate loss ratio is based on both standalone and packaged cyber insurance policies. See NAIC 2020.
4 AM Best 2021.
5 Marsh 2022.

Improved cyber insurance pricing may have arrested the worsening in underwriting performance. But market indicators suggest no material improvement in the claims environment. More than 80% of U.S. brokers indicated that cyber claims increased in Q4 2021, up from 66% in Q4 2020.[6] Anecdotal evidence from the 1 January 2022 reinsurance renewal cycle revealed additional reported loss activity for earlier years.[7] Claims data analysed by Aon indicate that ransomware incidents contributed to losses in more than 50% of instances in each of the first three quarters of last year.[8] Equally, Willis Towers Watson highlight that ransomware is anticipated to have been the costliest loss event category in 2021.[9] Given the continued upward pressure on claims, cyber insurers' loss ratios remained elevated in 2021.

Affirmative cyber insurance policies typically cover the external expenses associated with the breach (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. While ransom reimbursements do not make up the bulk of ransomware insurance claims, their share in overall incident costs has grown in recent years, alongside breach response costs (for assistance in legal, forensics and recovery efforts). According to data from Corvus, extortion payments represented 30% of the value of ransomware claims in 2020, up from just over 20% in 2019 (Figure 1).

In compensating victims for all insured costs of an attack, including any ransoms paid, insurers make good on their core promise to indemnify policyholders against any harm suffered that was beyond their control. However, some external commentators worry that reimbursing victims for ransoms may encourage targeted ransomware attacks.[10] One 2021 study 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.[11] Governments have also hinted at the unintentional impact that insurance may have on ransomware extortion. In its recently published Ransomware Action Plan, the Australian government noted that ransom payments demanded from insured organisations are often tailored to the insured amount under a cyber insurance policy.[12]

Figure 1: Breakdown of ransomware insurance claims, by type of expense



Source: Corvus Insurance

6 CIAB 2021.
7 Johansmeyer 2022.
8 Aon 2022.
9 Willis Towers Watson 2021.
10 For example, in June 2022, IT security experts wrote an open letter to the German government highlighting how the payment of ransoms (and the reimbursement through insurance policies that cover cyber extortion) increases the likelihood of further successful attacks. Paderborn 2022.
11 Talion 2021.
12 Australian Government 2021.

Rather than act as a catalyst for ransomware, cyber insurance is an integral part of the solution.

The purpose of this report is to examine recent developments in ransomware and articulate the challenges faced by policymakers, insurers and insureds alike in responding to the enhanced threat. Drawing on discussions with re/insurers, the report makes the case that rather than a catalyst for ransomware, cyber insurance is an integral part of the solution. Any inadvertent effects on the incentives of ransomware threat actors need to be weighed against the positive contribution insurance makes by helping policyholders withstand an attack.

Cyber insurance does more than just provide vital financial protection and the operational support needed to deal with a ransomware intrusion. As part of the underwriting process, insurers often expose weaknesses in an organisation's cyber defences, provide guidance to strengthen their security posture and – through the terms and conditions of available cover – incentivise investment in best-practice cyber hygiene. Some carriers (directly or in collaboration with specialist cybersecurity firms) continuously monitor the threat environment, highlighting vulnerabilities and weaknesses in a firm's networks and systems that might be unknown to the policyholder. In many cases, those issues can be addressed quickly to prevent the firm from becoming the victim of an attack.

3. An overview of recent ransomware attacks

There is no universal or comprehensive data set on ransomware incidents and their effects. In part, this is because some victims choose not to divulge that they have been hacked, perhaps conscious of the reputational harm or third-party liability that might arise. Nonetheless, based on a range of indicators – largely captured by cybersecurity professional services from both official and unofficial sources – it is possible to discern some notable shifts in the threat landscape.

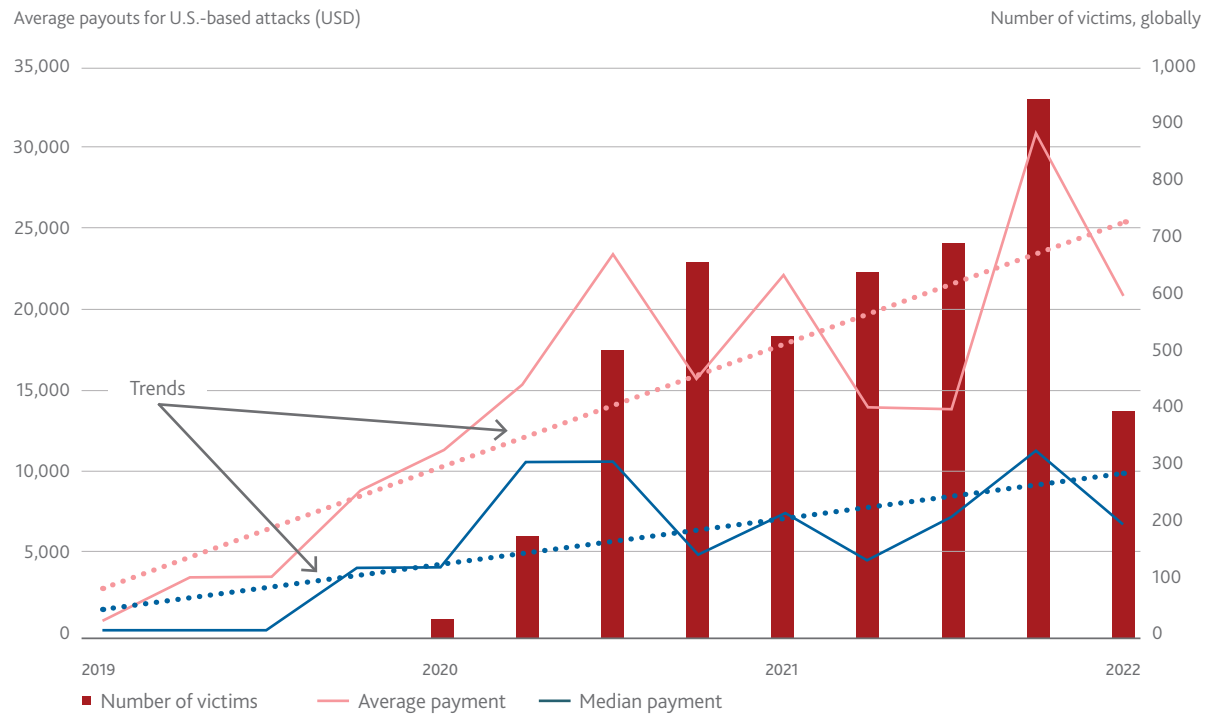
3.1 Increased incidence and bigger ransom demands

Ransomware has been around for decades, but attacks have picked up sharply over recent years in terms of both attempted intrusions – which according to some estimates more than doubled in 2021 to over 620 million[13] – and the number of victims. The amount of ransomware attacks fell in the first few months of 2022, although that could reflect the outbreak of war in Ukraine and the resulting sanctions against Russia that are making it harder for cybercriminals to organise attacks and receive ransom payments.[14] This may prove to be a temporary pause, with some cybersecurity analysts observing a noticeable rebound in ransomware activity in Q2 2022.

The number of ransomware attacks has picked up sharply over recent years, along with the size of extortion demands.

13 SonicWall 2022.
14 Zdnet 2022.

Figure 2: Ransomware attacks[(a)] and payouts[(b)]



Source: Coveware and Abnormal

The actual size of extortion demands has trended higher (Figure 2). According to one recent analysis for the U.S., the average ransom payment climbed to over USD 300,000 in the fourth quarter of 2021 up from around USD 150,000 in the same period a year earlier.[15] The distribution of ransoms is also highly skewed, with some firms reportedly forced to hand over millions of dollars to regain access to their data and systems.[16] Globally, another study shows that the average ransom paid by mid-sized organisations increased almost fivefold in 2021 compared with 2020.[17]

While the computer systems of firms, medical institutions and government agencies in the U.S. are targeted most frequently, the recent escalation in attacks is international. In the two-year period covering 2020 and 2021, around half of victims were located outside the U.S., mainly in developed countries, although Asia was relatively under-represented (Figure 3). Many of the attacked firms were small businesses, likely reflecting their limited resources devoted to cybersecurity defences compared with larger companies.

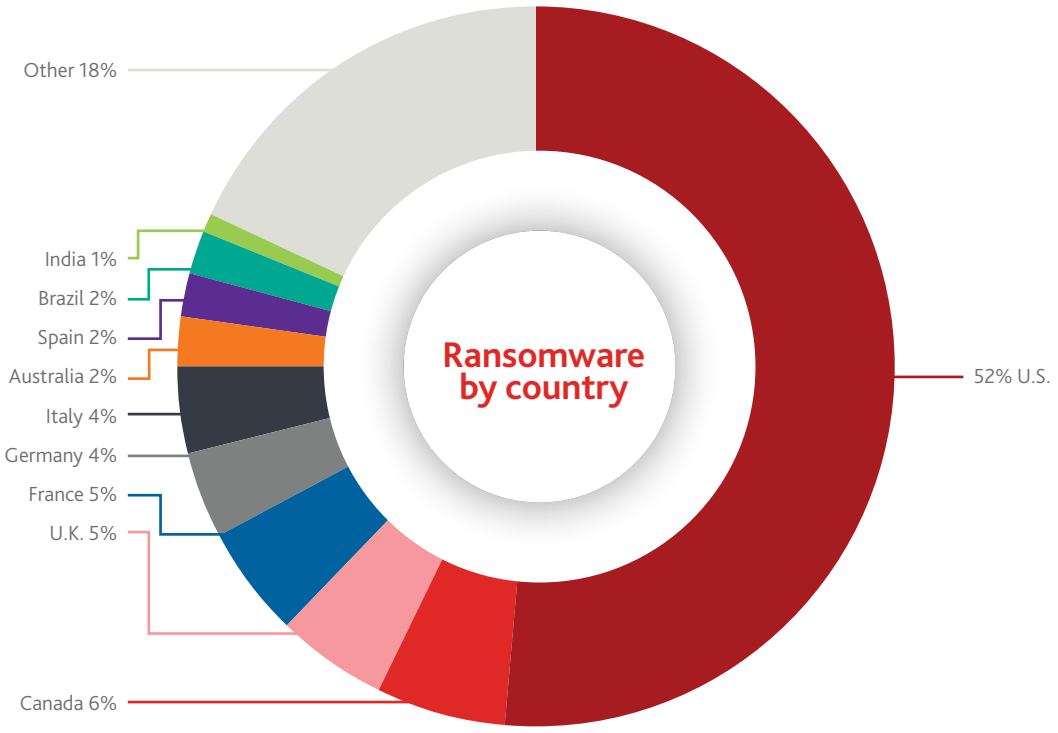
While the computer systems of firms in the U.S. are targeted most frequently, the recent escalation in attacks is international.

15 Coveware 2022.

16 For example, the U.S. insurer CNA Financial Corp. reportedly paid USD 40 million in March 2021 to regain control of its network after a ransomware attack. Similarly, JBS Foods, the world's largest meat supplier, revealed in June 2021 that it paid USD 11 million to ransomware hackers.

17 Sophos 2022.

Figure 3: Share of all ransomware victims in 2020 and 2021, by country



Source: Abnormal

Manufacturing companies are often in the crosshairs of ransomware criminals, accounting for around one in five victims.[18] Yet all industries are potential targets. Indeed, the subsector comprising computer and technical business solutions witnessed the largest number of ransomware attacks over the past year. One of the highest profile attacks was against Kaseya, a technology company that develops software to managed service providers (MSPs), in July 2021.[19] Retail businesses were also more frequently attacked than in earlier years. The broader scope of attacks could in part be linked to the COVID-19 pandemic, which has further expanded the attack surface given the increased reliance on remote network technology.

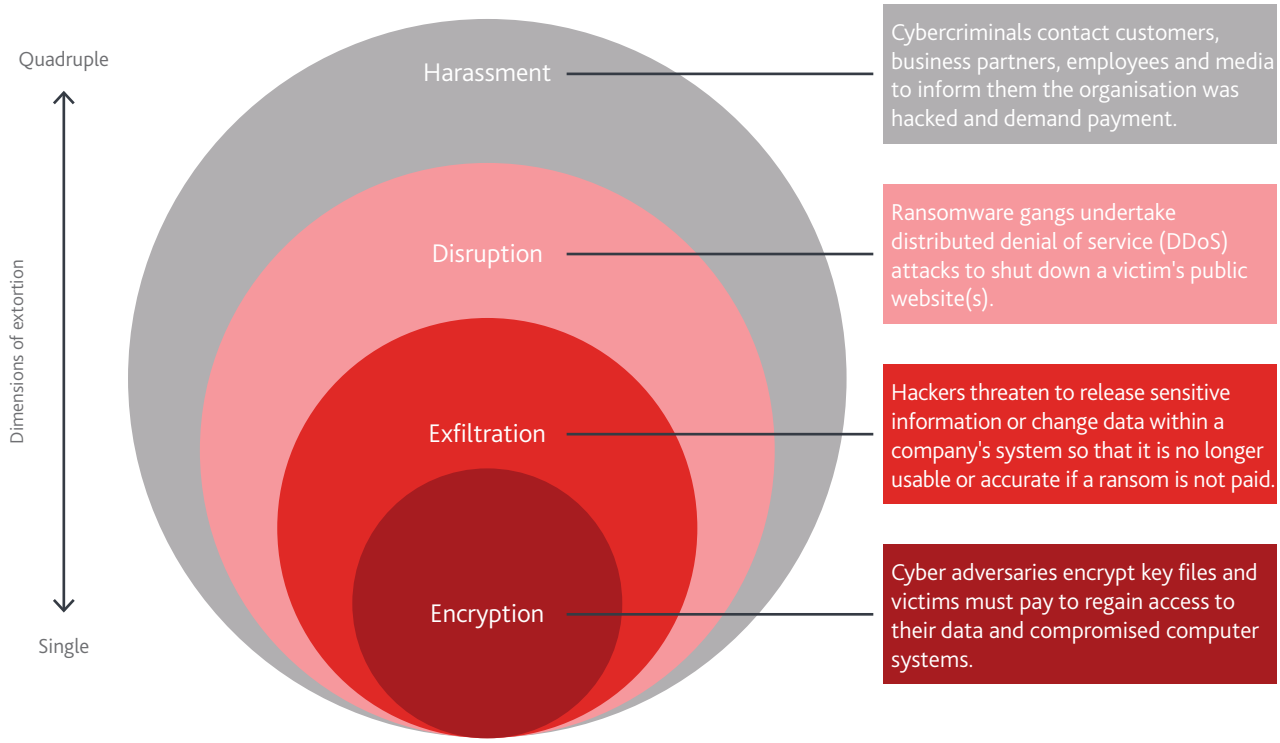
3.2 New extortion tactics, techniques and procedures

Early ransomware tended to be rudimentary and use basic data encryption techniques. Lately, cybercriminals have deployed increasingly sophisticated approaches. Ransomware operators now commonly use as many as four extortion techniques to pressure victims into paying (Figure 4). These can also be combined in different ways. For example, while many ransomware groups encrypt and steal a victim's data and demand a ransom to decrypt as well not leak the information, some groups may simply threaten to publicise exfiltrated data if their extortion demands are ignored.[20]

Alongside such double/triple/quadruple extortion methods, cybercriminals have shifted their tactics, techniques and procedures (TTPs). Rather than relying on 'spray and pray' phishing attacks, ransomware campaigns focus on leveraging network access footholds established by other malware infections or newly uncovered and/

18 Abnormal 2022.
19 Ibid.
20 Wired 2022.

Figure 4: Different extortion methods used by ransomware criminals



Source: The Geneva Association

or exploited software security flaws. This includes exploiting weak points and single points of failure in firms' physical and digital supply chains (including cloud-based applications) in order to deploy and spread malware via key software/IT service providers and/or disrupt critical infrastructure. They may even attack industrial control systems, such as those responsible for running power grids, manufacturing plants, oil refineries and sewage treatment plants, as a way of gaining access to their target's systems long before releasing the malware.

Recent increases in unique malware variants point to cybercriminals' growing maturity to diversify the tactics they use to attack organisations, their networks and their users. Attackers are also increasingly adept at reverse-engineering security patches to exploit vulnerabilities and orchestrating attacks at times when a firm's defences may be less robust; for example, on weekends and holidays, when there are fewer network defenders and IT support personnel at victim organisations.[21] The use of botnets to automate large-scale attacks only underscores the increased capabilities of ransomware threat actors. Likewise, intruders may 'live' undetected on a victim's system long after the initial incursion, collecting sensitive information and/or gaining sufficient access to compromise a target's backup systems, before deploying the ransomware.

More generally, cybercriminals continuously employ methods to create greater incentives for their victims to pay up and maximise the rewards from a particular intrusion. Instead of encrypting computers and servers, criminals may look to take operational control of all sorts of devices connected to the internet and demand payment for their release (a tactic often called 'jackware'). To date, such attacks have thankfully been rare. Ransomware operators also opportunistically vary their attack targets. Attracted by potentially large ransoms, they may sometimes go after high-value organisations and/or those providing crucial services (so-called 'big-game hunting'). This type of attack was especially prevalent in 2021, but following aggressive law enforcement last year, some threat actors redirected their ransomware efforts toward mid-sized corporate victims in a bid to reduce official scrutiny.

Ransomware threat actors also reportedly recruit 'insiders' to gain access to a firm's network. Any employee or a third-party vendor with trusted account privileges may be

21 CISA 2021.

able to instantly distribute ransomware on a network. This represents an especially serious threat to large enterprises with thousands of employees. According to a report from Hitachi ID Systems, 65% of surveyed IT and security employees received cybercriminal solicitations to assist in ransomware attacks in 2021.[22]

3.3 Evolving ransomware ecosystem

Although it is still possible for a lone hacker to create and distribute ransomware, this is no longer the norm. Instead, a whole ecosystem of actors has sprung up to facilitate 'ransomware-as-a-service' (RaaS): a distributed model enabling hackers to use off-the-shelf ransomware tools and services. Cybercriminals now adopt specialised roles, most of which may have nothing to do with the actual launch of an attack, including identifying unknown vulnerabilities, gaining initial access, developing malware, processing any ransoms paid and even handling the negotiations. They often interact via underground marketplaces and forums where intelligence, malware and associated services can be advertised and exchanged.[23] One example is WannaBuy, a platform on the dark web dedicated to the sale of compromised remote desktop protocol credentials, a key piece of software that enables users to establish sessions with remote devices over the internet.

> The 'ransomware-as-a-service' model enables hackers to use off-the-shelf ransomware tools and services

Many of these criminals operate as independent contractors, but some organisations are large enough to maintain a small cadre of 'employees' to undertake several of the specialist roles.[24] In addition to potentially carrying out attacks on their own behalf, such ransomware groups typically licence the use of their malware (often on a subscription basis) to affiliates that earn a percentage of each successful ransom payment. This allows less technical actors to deploy ransomware and expands the set of targets that can be hit, sometimes simultaneously, widening the footprint of attacks. In the same vein, ransomware groups may share resources and even join forces to form ransomware syndicates in order to maximise the return on their illicit activities.

The development of RaaS has been a major factor behind the recent escalation in ransomware. Cybercrime has become democratised, with almost anyone now able to launch sophisticated and often highly disruptive attacks. Bad actors no longer need to develop the tools to attack when they can just sign up for a subscription. Ransomware affiliates are often supported with onboarding documentation containing a step-by-step guide for launching ransomware attacks with the software. Some RaaS distributors even provide affiliates with a dashboard solution to help them monitor the status of each ransomware infection attempt.[25]

> An important facilitator of ransomware attacks are cryptocurrencies, such as Bitcoin.

As well as access to the malware itself, an important facilitator of ransomware attacks are cryptocurrencies, such as Bitcoin, which account for roughly 98% of ransomware payments and are often the key medium of exchange to acquire additional exploits traded in the dark web or some cybercrime-as-a-service.[26] Cybercriminals are able to exploit the anonymity associated with the use of many cryptocurrencies, especially if they take advantage of third-party services to obscure the trail back to the fund's original source, such as a 'tumbler service' to mix potentially identifiable or 'tainted' funds with others or a chain swap to exchange different cryptocurrencies. Over the past few years, stolen funds from ransomware strains have often been laundered through centralised cryptocurrency exchanges. According to blockchain data platform Chainalysis, 56% of funds sent from ransomware addresses since 2020 have wound up at one of six cryptocurrency businesses.[27]

22 Hitachi 2022.
23 According to cybersecurity firm Group-IB, the number of offers to sell access to compromised corporate networks nearly tripled in the year to June 2021, increasing from 362 to 1099. Group IB 2021.
24 Ransomware.org 2021.
25 Kost 2022.
26 Allianz Global Corporate & Specialty 2021.
27 Chainanalysis 2022.

4. Societal challenges posed by ransomware

The amount of money that the extorted firm is willing to pay reflects its assessment of the cost of non-compliance – for example, business interruption, reputational harm and expenses incurred to recover systems and data – relative to the size of the ransom. Before entering into any negotiations, victims need to assess both the effectiveness of the attack as well as the likelihood that the criminals will remove the malware and/or not disseminate data gathered from the intrusion. To the extent that companies have effective backup systems and can limit any operational and reputational damage associated with the loss of sensitive data, it is often optimal to rebuff any ransom demands, which is generally the advice from law enforcement agencies.

At the same time, the increased connectivity and storage of sensitive information in digital form has increased firms' vulnerability to attack and the potential for extortion. The development of RaaS has reduced barriers to entry for would-be cybercriminals, lowered the costs of malware production and improved the efficacy of attacks.[28] All these factors have materially shifted the balance of power in favour of criminals, meaning firms may see paying the ransom as the least costly course of action, especially if it reduces the duration of an incident, a key factor in the overall impact of a ransomware attack.[29] According to industry data collected by NetDiligence, the costs incurred by organisations that do not pay a ransom are on average three to four times larger in the case of business interruption and recovery expenses than those who accede to extortion.[30]

4.1 Economic externalities and moral hazards

Firms may see paying the ransom as the least costly course of action, but giving into extortion incentivises ransomware criminals and amplifies the risk of future attacks on everyone.

However, a ransomware attack is not a one-shot game. By paying ransoms, firms also potentially incentivise ransomware criminals, in the process amplifying the risk of future attacks on everyone, including themselves.[31] Paying outsized ransoms

28 Institute for Security and Technology 2021.
29 Checkpoint 2022.
30 NetDiligence 2021.
31 Dey and Lahiri 2021.

often becomes the benchmark for future attacks, fuelling ever larger extortion demands. The presence of such an economic externality means the social costs of ransomware payment may exceed the costs faced by any individual affected firm.

While this externality exists whether or not the victim of ransomware is insured, insurance could unintentionally make the situation worse, at least in theory.[32] Cyber-criminals may deliberately target companies that have cyber insurance, even hacking into computer systems to find out the terms and limits of coverage, and using that information to frame their extortion demands. Such intelligence may be gathered indirectly by attacking insurance carriers, brokers and other third parties for policyholders' details.[33]

Some researchers have dubbed this an example of the problem of 'third-party moral hazard', whereby the provision of insurance can create significant negative externalities through incentives for third parties (that is, parties other than the insured or insurers) to 'engage in antisocial, illegal and unethical activities into order to extract money from insureds or insurers'.[34] This potentially occurs in addition to the regular moral hazard that arises if policyholders fail to invest in adequate cybersecurity or take sufficient care of their information assets, relying instead on their insurance policy to cover all the costs of an attack, including any ransom.

4.2 Possible solutions and pitfalls

Policymakers in many countries are currently debating how far they should intervene to address this economic externality, although there are no easy solutions.

Policymakers in many countries are currently debating how far governments should intervene to address the economic externality. In theory, there are a number of ways in which states can seek to internalise externalities (i.e. alter incentives of those creating harm to others such that they incur the full costs of their actions), including laws, regulations and taxes. In practice, there are no easy solutions and measures often involve important trade-offs, not least because of the potential for unintended consequences.

4.2.1 Prohibit ransom payments

As explained in Box 1, paying a ransom or reimbursing victims of extortion is typically not illegal, although civil and/or criminal penalties apply if transactions contravene specific regulations related to sanctioned entities. One possible solution is therefore an outright ban on ransom payments. The reasoning 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), the hackers' incentive to demand a ransom in the first place would also be diminished.[35]

An outright ban on ransom payments could simply drive such transactions underground and/or encourage more destructive attacks.

No company wants to give in to extortion, not least because there is no guarantee that paying a ransom will unlock the affected system or ensure the firm is not hit by a repeat attack.[36] In addition, most firms want to comply with the law. Simply banning ransom payments (by companies or their insurers) is not likely to deter ransomware if the recovery and remediation costs of an attack are so great (relative to the extortion demand) that victims feel compelled to resort to illegal methods to pay hackers. Driving ransom payments underground will only make it more difficult for governments to track transactions and prosecute cybercriminals, rendering the underlying law ineffective. Outlawing ransoms may also motivate ransomware attackers to engage in a new form of extortion, such as blackmailing entities who make ransomware payments in violation of a ban.[37]

Many hackers deliberately target companies' IT backups to increase their leverage over victims. Cybercriminals may be tempted to escalate their tactics further to encourage illicit ransom payments. They may shift their focus from disruption to actual destruction of physical assets (including critical infrastructure) as well as bodily injury. This could

32 Dudley 2019.
33 For example, in February 2022 global insurance broker Aon revealed it is investigating a cyber incident impacting some of its systems, although the nature and extent of any data exfiltration is unknown. SecurityWeek 2022.
34 Parchomovsky and Siegelman 2020.
35 Logue and Shniderman 2021.
36 According to one study, on average organisations that paid the ransom got back just 65% of the encrypted files, leaving over one third of their data inaccessible. Sophos 2021.
37 U.S. Senate 2021.

lead to less frequent but more severe targeted attacks. In addition, such a ban on paying ransoms may undermine societal resilience if it discourages firms from taking out cyber insurance – in particular small businesses, which are often vulnerable to gaps in technology or have low awareness of the risk of attack by increasingly sophisticated criminal gangs.

Given the practical challenges of outlawing ransomware payments, no general ransom bans or restrictions on insurer reimbursements have been introduced to date. They continue to be discussed in certain jurisdictions, notably the U.S., the Netherlands and Australia, although there is no consensus on their adoption.[38, 39] Even the U.S. Federal Bureau of Investigation (FBI) advised against banning ransoms.[40] To the extent that legislation is passed, it may well be limited to prohibiting government agencies or public entities from paying ransoms. For instance, some U.S. states, including North Carolina, Pennsylvania and New York, have passed or are advancing legislation that would outlaw ransomware payments, at least by state and local governments, though a similar bill In Texas died at the committee stage.[41]

4.2.2 Compensate victims of an attack

An alternative to a complete ban could be for governments to provide advice and support to businesses responding to an incident, including financial backing to firms that refuse to pay a ransom. In principle, if the support is sufficient to boost victims' ability to withstand an attack, it increases the incentive to hold out against extortion. This could help deter ransomware by reducing the expected payoffs to cybercriminals. During the years of Northern Ireland's civil conflict, for example, insurers stopped insuring shops against the bombing of commercial premises, prompting the government to step in and set up a scheme to cover losses instead.[42]

Financial support from governments to businesses responding to an incident might help, although it should not undermine firms' incentives to invest in cybersecurity.

Box 1: Legality of ransom payments

In general, the payment of a ransom (whether direct or indirect through third parties) is not illegal. No major jurisdiction currently imposes an outright ban on cyber ransoms and most countries do not bar insurers from reimbursing victims. Even in Italy, where anti-kidnapping legislation introduced in the 1990s outlaws ransoms being paid to secure the release of hostages, the law does not currently prohibit the payment of ransoms to cybercriminals.

This does not, however, mean such ransom payments to cybercriminals never result in legal penalties. In many countries, payments to governments, individuals or entities that are subject to official sanctions (e.g. known terrorist organisations) are prohibited under various laws and regulations. These rules apply to more than the payments made by victims of an attack. Facilitators of such payments – such as financial institutions that process transactions, cyber insurers that reimburse ransoms and other companies involved in incident response and digital forensics – could also be liable.

Both victim and intermediary may be liable for civil penalties and even face criminal prosecution for knowingly violating regulations. For example, a recent advisory from the U.S. Department of the Treasury highlighted that ransomware payments to individuals or entities on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List (SDN List) are subject to civil enforcement and may incur criminal penalties if the initiator of the payment knew the recipient was on the SDN List or otherwise subject to embargo.[43]

Source: The Geneva Association

38 In the Netherlands, the Ministry of Justice and Security is currently investigating the feasibility of a ban for insurers to reimburse ransom payments, although so far no formal legislation has been proposed. See Government of The Netherlands 2021.
39 The Australian government intends to introduce new laws in 2022 (as part of its recently launched Ransomware Action Plan), but the extent to which this will include a ban on ransom payments is unclear. See Australian Department of Home Affairs 2021.
40 Miller 2021.
41 Bergal 2021.
42 Wheeler and Martin 2021.
43 Congressional Research Service 2021.

Apart from the fiscal cost, a challenge for such a policy would be to ensure firms invest in adequate cybersecurity. This means companies not only keeping up to date with the latest available software patches, and best practice in cyber hygiene protocol, but also not being dependent on government bailouts. Similarly, government support should not undermine firms' incentives to take out adequate insurance to protect their assets.

To address these problems, policymakers might impose preconditions on any financial support, for example that firms receive funding only once, and even then only if they invest a certain portion of the aid in improved recovery systems and better security education for employees, and that they take out cyber insurance.[44] This way, firms are incentivised not to agree to ransom demands while taking steps to enhance their cyber resilience, thereby reducing the externality they impose on others.

4.2.3 Tax ransom payments

Corporate bailout is not the only fiscal strategy. A policymaker could also look to tax ransom payments as a way of increasing the cost for firms that give in to extortion. Of course, implementing a tax can be problematic. Ransom payments are typically difficult for governments to track, especially if there are no related disclosure requirements.

An indirect route could be to remove tax relief associated with ransom payments. While many countries restrict tax deductibility for any amounts considered illegal or a criminal offence, this is not universally the case and uncertainty exists as to how far these rules apply to ransomware.[45] In jurisdictions like the U.S. for instance, companies may currently be able to write off ransomware payments as 'ordinary, necessary and reasonable' expenses on their profit and loss statements.[46] Tightening the rules and reducing such tax incentives could help shift the economics in favour of not paying ransoms.

4.2.4 Strengthen penalties for facilitating cybercrime

Tougher financial sanctions against those paying or arranging payment of ransoms might also serve to deter attacks. Stronger penalties for making payments to criminals or higher liability costs for harm caused to third parties may encourage victims to refuse to pay, in turn discouraging ransomware threat actors. These could complement stricter punishments for cybercriminals who carry out such attacks.

44 Wheeler and Martin 2021.
45 RSM 2022.
46 Suderman and Gordon 2021.

Tougher financial sanctions against those paying or arranging payment of ransoms might also serve to deter attacks.

Efforts to strengthen sanctions regimes to cope with ransomware, however, must also overcome practical hurdles. The real identity of the perpetrator of an attack is usually unknown and/or the link between ransomware groups and sanctioned entities is often unclear. Most ransomware strains come and go in waves, staying active for a short amount of time before becoming dormant.[47] When ransomware variants disappear, it is not at all clear if the underlying perpetrators have fully disbanded. Ransomware gangs often rebrand their malware, continue their operations under new names and/or their affiliates change, making it difficult for the authorities to keep any sanction list up to date.

Even if attribution for an attack could be established, in some jurisdictions a prosecutor would have to prove the payer knew the transaction involved a banned entity, which seems improbable. In addition, legal ambiguity remains over how courts interpret and apply possible defences for ransom payments that might otherwise constitute an offence. Payments in response to fears about imminent and physical harm are likely excusable on grounds of duress, which raises a question about how far that applies to other threats to data, information systems and economic well-being.

Tighter regulation to make it harder for criminals to convert cryptocurrencies into fiat currency may arguably be more effective in controlling ransomware. In particular, extending tax laws as well as anti-money laundering and counter-financing of terrorism (AML/CFT) regulations to cryptocurrency exchanges provide incentives to identify and verify users, rooting out suspicious activity in the crypto sector. However, in the face of increased regulatory scrutiny, cybercriminals are already demonstrating their innovation in how they seek to launder cryptocurrency. For example, the darknet market Hydra includes services that offer to hide large volumes of physical cash at a specified location, which can be retrieved by a customer once they deliver their Bitcoin.

However, cybercriminals are already demonstrating their innovation in how they launder cryptocurrency in order to evade detection.

4.3 Lessons from kidnap & ransom (K&R) insurance

The negative externality problem is not unique to ransomware. Similar issues arise in the context of kidnapping. Paying ransoms (whether directly by the victims' families or indirectly via reimbursements from their insurers) can encourage further extortion and boost ransom inflation. Yet market mechanisms have evolved to limit the scale of kidnapping without the need for overt government intervention. As explained in Box 2, re/insurers have developed solutions and market practices to encourage a standard approach to information exchange and resolution that works to stabilise ransoms. Effectively, the externality is internalised among a tight-knit group of re/insurers that offer K&R insurance.

Could comparable arrangements be developed for cyber insurance? It seems unlikely given the practical coordination challenges in managing ransomware incidents. The frequency of kidnapping thankfully remains low and relatively localised compared with ransomware attacks, which are becoming more prolific and widespread. Although the market for cyber insurance is concentrated – with a group of larger re/insurers accounting for the bulk of premiums globally – there are limited mechanisms to share intelligence about attacks, let alone impose sanctions on those re/insurers tempted to deviate from established ransom benchmarks.

Moreover, ransoms are negotiated under conditions of strict information asymmetry. Individuals covered by a policy most likely do not (and should not) know they are covered while kidnappers are kept in the dark in terms of who would pay the ransom (family, firm, insurer or government) and the financial position of these entities. By contrast, in modern ransomware attacks criminal gangs often covertly gather highly confidential information on their victim companies' vulnerabilities to improve their bargaining position. This undermines attempts to contain payout expectations and maintain ransom discipline across firms.

47 Chainalysis 2022.

Box 2: Kidnap and ransom insurance

Kidnap and ransom (K&R) insurance first developed in the 1930s though did not take off until the 1960s, following a series of kidnappings of businessmen and their families in Europe and Latin America.[48] Typically in such hostage situations, the K&R re/insurer will indemnify the policyholder for monies paid to kidnappers, the loss of ransom in transit and other expenses, such as fees for independent negotiators and crisis management responders. Over time, however, K&R cover has expanded considerably to include a wide range of extortion demands associated with industrial espionage, dirty tricks campaigns and, in some cases, threats to deploy malware.

The K&R insurance market is concentrated on the supply side. While a large number of insurance carriers, boutique insurers and brokers sell K&R insurance, ultimately the risk is usually borne by a small number of 'specialty risk' insurance companies at Lloyd's or is reinsured/retroceded through Lloyd's underwriters.[49] Many security and negotiation firms that specialise in kidnapping response are also located in and around the London Market.

Such market characteristics have important implications for how K&R insurance operates and the dynamics of kidnapping and extortion.

- **Information sharing:** Local underwriters regularly discuss the latest cases and ransoms paid, the duration of negotiations as well as the performance of crisis response consultants. This helps ensure that insurers are alert to new cases and the background/credibility of the criminals, which is important when framing negotiating strategies.

- **Ransom discipline:** Re/insurers have an incentive to keep extortion payments under control because of the potential sanctions they face from Lloyd's should they be tempted to simply agree to outlier ransom demands. In principle, the Lloyd's Corporation (which oversees and supports the Lloyd's market) can exclude and/or impose tougher underwriting standards on syndicates whose actions, while individually rational, might undermine or destabilise the market as a whole.

The market for K&R insurance functions as a de facto private governance regime to counteract the inherent externality associated with paying ransoms, i.e. the additional costs imposed on others by encouraging ever greater extortion demands. By providing a coordination mechanism through which insurance contracts are standardised and bargaining/resolution protocols are strictly maintained, the Lloyd's market (largely) prevents individual insurers from conferring externalities to the rest of the sector while still facilitating competition. Lloyd's underwriters also have a strong incentive to internalise externalities from uninsured cases to avoid inflating future ransoms, providing negotiation guidance, sometimes even on a pro bono basis.

Source: The Geneva Association, based on insights from Shortland 2016

48 Diebel 2019.
49 Shortland 2016.

5. Re/insurer perspectives on ransomware

The views of the insurance industry are not always prominent in the debate on ransomware. In order to provide a re/insurer perspective, we surveyed selected Geneva Association member companies that are active in cyber insurance.[50] This chapter summarises and synthesises the results of a short questionnaire and/or interviews with cyber experts at 15 re/insurers, which collectively account for a major share of the global cyber insurance market.

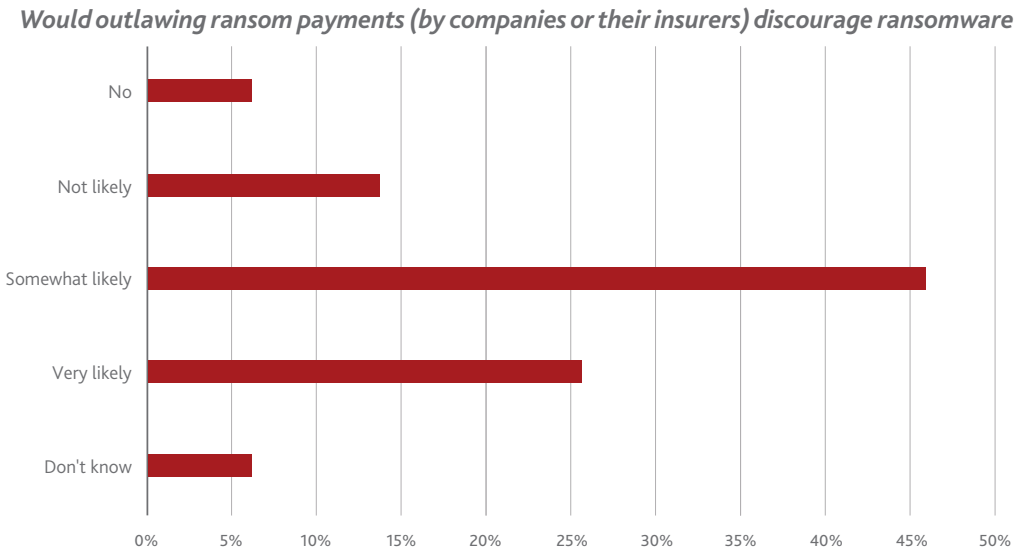
5.1 Banning ransom payments is a blunt, potentially ineffective instrument

Most re/insurers feel that banning ransom payments or prohibiting their reimbursement would probably discourage some ransomware but that it is a blunt policy response that may not always have the desired effect.

All respondents recognise the significant challenges posed by cybercrime and ransomware in particular. While there is no overall consensus, most feel that banning ransom payments by the targeted companies or prohibiting reimbursement by re/insurers would probably discourage ransomware attacks to some degree (Figure 5), at least against smaller firms with fewer resources. However, they also point out that 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.

50 The sample consisted of 15 re/insurance companies including most of the major global cyber re/insurers.

Figure 5: 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

Italy's experience with K&R 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.

5.2 Cyber insurance provides more than cover for ransoms

Insurance plays an important role in supporting companies to absorb ransomware-related losses, including privacy/data breaches, business interruption, recovery of data and systems, forensics and legal assistance.

While ransom payments often grab the headlines, the losses related to a ransomware attack go well beyond extortion demands. Insurance plays an important role in supporting companies to absorb a variety of first- and third-party losses resulting from ransomware. After an attack, cyber insurance can serve as 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.

Cast in that light, most re/insurers are not daunted by the prospect of a ban on ransom payments as the value proposition of cyber insurance would remain. In fact, cyber coverage could become even more valuable to the insured given the potentially higher recovery and remediation costs compared with paying a ransom. As well as any downtime, these costs could stem from the need to restore lost or corrupted data/information or manage any reputational fall-out and third-party liabilities from a data breach.

Adjusting the scope of cover offered will be easier in some markets than others. In the U.S., the most mature cyber insurance market, there could be initial pushback from customers who recognise that they operate in the most targeted country for ransomware attacks. According to the latest Zurich/Advisen survey of U.S. companies, 95% of respondents expect cyber extortion coverage to be included in their policies, on par with protection against data breaches.[51] Yet recent steps to restrict coverage – including increased participation in out-of-pocket expenses via co-insurance as well as reduced policy limits for ransoms – have been absorbed by the market, suggesting strong underlying demand for protection. Similarly, companies still derive value from their cyber insurance in markets where ransom payments are normally not covered, for example in Japan.

51 Zurich/Advisen 2021.

5.3 Involving experts leads to better outcomes for the insured

Most re/insurers believe involving independent experts in the response to ransomware attacks helps the affected organisations make informed decisions, especially in areas where they have little experience. Experts also bring in 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. Consistent with that, the ratio of average ransoms paid to initial ransom demands has reportedly declined, despite increased efforts by criminals to leverage data exfiltration and other methods to extort their victims.[52] The use of specialist intermediaries can also reduce operational frictions associated with a ransomware attack, such as ensuring the ransom recipient is not subject to criminal or anti-money laundering sanctions, reporting the incident to the relevant authorities and sourcing cryptocurrency to facilitate payment.[53]

Moreover, ransom brokers are almost always retained by the policyholders. Insurance companies may connect policyholders to intermediaries but only become involved when the negotiation and payment processes are largely complete. The brokers work in close cooperation with the insured's IT team to assess the best course of action, based on an assessment of costs and benefits to the victim, including the operations and data affected and the extent of any business interruption. While these paid advisors are negotiating with threat actors, additional work is typically undertaken in the background to liaise with law enforcement agencies. The goal is to assess if recoverability from backups is an option and how likely a ransomware gang will return any stolen data.

Ultimately, the victim company will decide how to respond to the extortion. At the same time, the intelligence provided by a ransom negotiator can convince the insured not to pay (for example, if the negotiator has prior experience of the threat actor not releasing effective decryption keys), even if that triggers an insurance payout for the costs of remediation. Indeed, while many insurance policies require the insurer's consent to pay a ransom, this is not the case when the decision is not to pay a ransom.

5.4 Insurance helps improve overall cyber hygiene standards

Apart from helping the insured cope with an attack, insurance can also play an important role in encouraging good cyber hygiene and risk prevention. Through premium discounts, co-insurance and retention arrangements as well as cover limits, insurance can incentivise

52 According to data from Corvus Insurance, the ratio of average ransoms paid to demands fell from 44% in Q3 2020 to 12% in Q3 2021. See Corvus Insurance 2021.

53 When the final amount is agreed upon by both parties, they involve a certified money services business (MSB) for the logistics of the payment. In the U.S., the MSB must confirm the group is not sanctioned by the Treasury Department's Office of Foreign Assets Control (OFAC), to secure cryptocurrency and complete the transaction.

organisations to adopt essential cybersecurity best practices (for example, investing in state-of-the-art backup systems, endpoint and anti-virus protection, implementing the latest software patches, and security awareness training for all employees).[54] These all should work to reduce rather than increase the chances of being hit by ransomware attacks. According to a recent survey by Marsh/Microsoft, the majority of corporate respondents said insurance is an important part of their cyber-risk management strategy, with 41% reporting that insurers' requirements influenced their decisions to augment existing controls or adopt new ones.[55]

Apart from helping the insured cope with an attack, insurance can also play an important role in encouraging good cyber hygiene and risk prevention.

The challenge for re/insurers is keeping track of the highly dynamic cyber risk landscape and adapting the availability and terms and conditions of cover as well as their services to better reflect the threats and vulnerabilities of the insureds. Early cyber underwriting practices relied heavily on simple questionnaires – often completed only once a year – to assess individual firms' cybersecurity, which provided basic metrics to support product and price differentiation. More recently, insurers have introduced more stringent requirements for coverage. Typical examples are multi-factor authentication on remote connections, endpoint detection, privileged access management tools and robust business-continuity planning such as regular backups. Some re/insurers have also proactively invested in new ways to assess insureds' cyber maturity and security controls. These include adoption of new technologies to scan clients' internal networks to identify policyholders' potential susceptibility to attack and prompting remedial action that improves a policyholder's security posture (see Box 3).

Box 3: How cyber insurance helps policyholders confront a ransomware attack

Insurers increasingly offer a variety of pre- and post-incident services that help their policyholders prevent, mitigate and respond to cyberattacks. These services augment the traditional loss indemnification role of cyber insurance in supporting ransomware victims, including absorbing the costs of restoring or decrypting data and compensating firms for lost income caused by business interruption/system outage.

Pre-incident guidance

As part of applying for cyber insurance, the underwriting process will often uncover weaknesses in an organisation's cybersecurity posture and provide guidance for strengthening its cyber resilience. Some carriers (directly or via partnerships with cybersecurity experts) are also able to monitor continuously observable information about their policyholders' and applicants' networks, alerting the insured to vulnerabilities that could also be found by attackers. In many cases, those issues can be addressed quickly, enabling companies to avoid or mitigate an attack.

Many insurers also offer products and services that can assist policyholders in preventing and/or preparing for a ransomware event – for example, employee training and testing, vulnerability scans, incident preparedness exercises, and consultation with legal counsel and loss prevention/security professionals. Such affiliated services are in fact increasingly demanded as part of cyber insurance solutions. A recent survey revealed that 62% of CEOs believe the provision of network security tools (e.g. firewalls) should be routinely included as part of cyber insurance.[56]

Post-incident support

Cyber insurance policies typically cover the fees charged by external experts (e.g. legal counsel, forensic investigators, ransomware negotiators) who are often brought in to respond to a ransomware attack. While insurers have established relationships with these specialists and can put the policyholder in touch with the right vendor immediately – very important during a crisis – the vendor will enter into a relationship with the policyholder, making the policyholder their client, not the insurer.

Source: The Geneva Association

54 Coveware 2018.
55 Marsh/Microsoft 2022.
56 Munich Re 2022.

Re/insurers have a way to go to in terms of upgrading cyber underwriting to better assess and price the risks. Some studies highlight how the positive effects of cyber insurance to incentivise stronger cybersecurity practices, particularly for small businesses, have yet to materialise fully.[57] While insurers can leverage their own claims data, they are often hampered by a lack of reported incidents (especially in unregulated industries and SMEs) and may have limited understanding of the root causes of incidents, cybercriminals' TTPs, etc. Sometimes it may not be easy to validate whether resilience measures have been appropriately implemented. Enhanced data capture and analysis – especially combining threat/vulnerability intelligence with actual loss experience – is coming on-stream to help identify important predictive (and possibly causal) factors behind particular claims and highlight the best means of risk mitigation.[58] This will enable more accurate risk-based pricing of cyber insurance and foster stronger incentives for enhanced cybersecurity.

5.5 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 the suggestions highlighted by re/insurers are mirrored in measures already announced by various governments to enhance cybersecurity in the wake of the recent ransomware epidemic (see Box 4). Most obviously,

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 • 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 (P2P) platforms to standards for due diligence in creating accounts and monitoring transactions, including additional know-your-customer (KYC) and traceability requirements • 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) • 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) • 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 • Set up government-sponsored agencies to support cybercrime victim organisations, especially small firms • Upgrade the technical knowledge and skills of public authorities and law enforcement to counter cybercrime

Source: The Geneva Association

57 MacColl et al. 2021.

58 For example, one analysis of publicly reported ransomware incidents between 2010 and 2020 revealed that the presence of certain threat and exposure signals, such as mentions on the dark web, compromised user passwords and spam activity, significantly increases the likelihood of a successful attack.

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 as well as guidance to victims on effective counter measures and decryptor tools to contain any spread of the malware.

Improved mechanisms to track, monitor and share information about ransomware strains should be beneficial.

Box 4: Recent government-led initiatives to counter ransomware

Rather than ban ransom payments altogether or amend existing sanctions regimes, which may simply create additional complexity, numerous governments instead seem to be coalescing around a combination of enhanced security measures to counter the rise in ransomware.

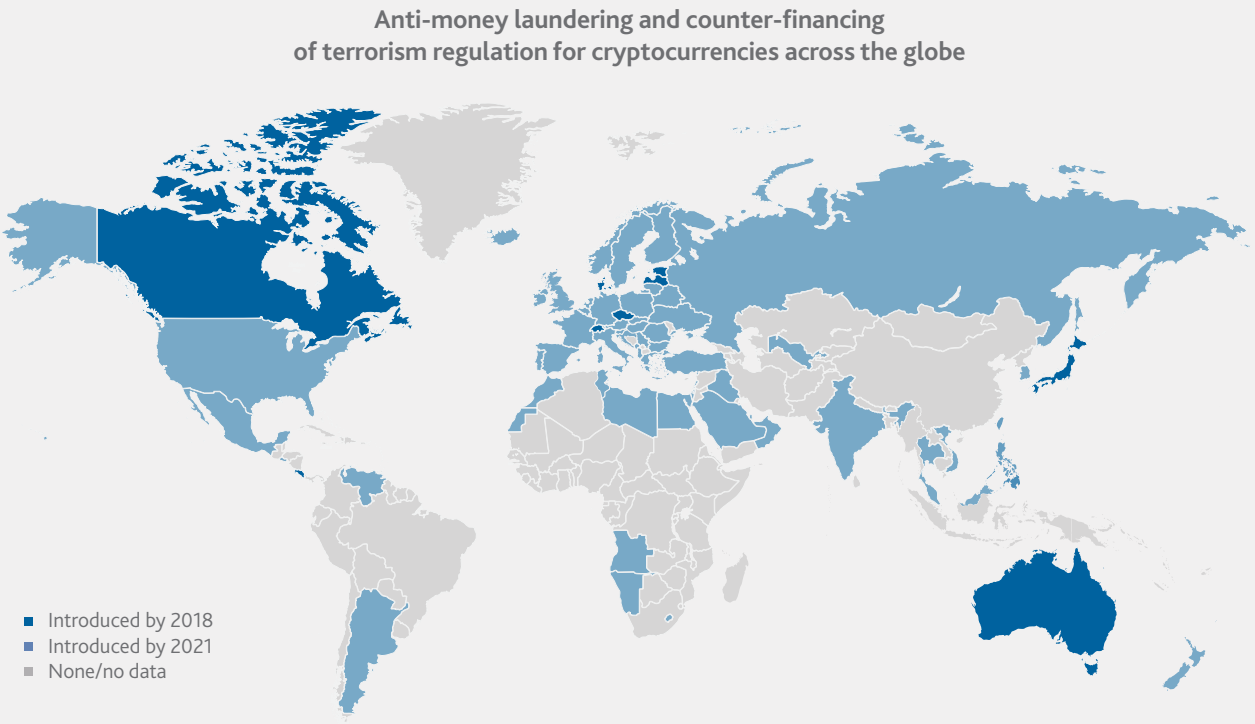
Enhanced disclosure regimes

A number of countries have set out proposals to strengthen the reporting of ransomware incidents, including the payment of ransoms. Especially noteworthy is the U.S. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which became law in March 2022. Updating disclosure laws should help increase understanding of the scope and scale of the crime, allow for better estimates of the societal impact of these payments and enable better targeting of disruption activities. In addition, requiring ransomware victims to report details about the incident prior to paying the ransom enables national governments to take action, for example issuing a freeze letter to cryptocurrency exchanges.

Regulation of cryptocurrencies

Many national authorities now impose restrictions on users and the infrastructure associated with virtual currencies and other crypto assets. In particular, most countries are rolling out tax laws and anti-money laundering (AML)/ combating the financing of terrorism (CFT) laws, or both, to organisations involved with cryptocurrencies, similar to those that apply to banks and other financial services. In November 2021, 103 jurisdictions subjected cryptocurrencies to these laws, with the majority applying both (Figure 6). This compares with the situation in 2018 when 33 jurisdictions regulated cryptocurrencies in these areas, with only five applying both tax and AML/CFT laws.[59]

Figure 6: Regulatory framework for cryptocurrencies (2018–2021)



Source: Library of Congress law library 2018, 2021

More effective incident response and international cooperation

Some countries have dedicated ransomware-response platforms, through which businesses and the general public are informed about the latest threats, as well as how to increase their resilience, report ransomware attacks and access a repository of decryption keys for specific types of ransomware. For example, the 'fight ransomware' campaign of the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) provides detailed guidance on incident handling.[60] Similarly, the Cybersecurity & Infrastructure Security Agency (CISA) in the U.S. provides resources, alerts and a reporting tool through a dedicated ransomware platform.[61]

Recognising the global security threat posed by ransomware, the recently established U.S.-led Counter Ransomware Initiative aims to enhance cooperation and coordination among the 30 participating countries to boost network resilience, tackle abuse of financial infrastructure for money laundering purposes and foster collaboration among law enforcement agencies.[62] In a similar vein, INTERPOL has urged a coordinated approach among police forces globally to counter ransomware, akin to their approaches to fight terrorism or disrupt organised crime groups.[63]

Cyber security governance and certification

Beyond regulations and law enforcement, most governments seek to foster enhanced cyber resilience by encouraging cybersecurity best practices. Some authorities are also taking steps to address vulnerabilities in software supply chains. For instance, ENISA, the EU agency for cybersecurity, recently launched cybersecurity certification schemes for IT products, cloud services and 5G networks, enabling users to assess whether products and services meet minimum cybersecurity standards. In May 2022, EU member states agreed on the Network and Information Security (NIS) 2 Directive, which mandates that a wider scope of critical sectors adopt cybersecurity measures, requires covered firms to assess the cybersecurity of their supply chains and holds executives accountable for cyber breaches.

Source: The Geneva Association

59 HKCERT 2022.
60 CISA 2022.
61 The White House 2021.
62 INTERPOL 2021.

However, moves towards mandatory reporting must be workable and flexible enough to avoid conditions that could aggravate the threat. An example would be publicly disclosing an intrusion before a patch or backup solution is in place, which could alert the bad actors and cause them to escalate any extortion. Equally, increased incident reporting needs to go hand-in-hand with smoother official procedures for collecting and acting upon information. In some of the high-profile U.S. ransomware cases in 2021, companies reportedly lacked clear initial points of contact with the federal government, leading to delays and coordination failures in formulating an official response to the attack.[63] To encourage compliance, the authorities could also do more to demonstrate the value to victim companies of disclosing information, which includes providing feedback on how it is helping to advance any criminal investigation.

Some of the cybersecurity vulnerabilities most commonly exploited by cybercriminals to distribute ransomware are years old.[64] Government intervention could also extend to create increased accountability for software and hardware vendors for intrinsic product failings. The current model of build, sell and patch flaws as they come to light fosters latent zero-day vulnerabilities – software weaknesses that can be exploited by attackers before the developer knows about them – which cybercriminals thrive upon. Tougher rules against distributing software with weak cybersecurity, potentially with enhanced liability regimes for harm caused by obvious security flaws, could incentivise more stringent testing and remediation of defects. However, authorities need to be mindful not to discourage innovation and increase software/hardware development costs.

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 be needed – especially to counter emerging trends such as the adoption of privacy-protecting coins and use of decentralised exchanges that make investigating online crimes and enforcing sanctions difficult.[65] 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.

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 be needed.

63 Congress of the United States 2021.

64 Cybersecurity researchers at Qualys examined the Common Vulnerabilities and Exposures (CVEs) most used in ransomware attacks in recent years. They found that some of these vulnerabilities have been known for almost a decade and had vendor patches available.

65 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. See Clark et al. 2022.

6. Concluding remarks

Ransomware attacks have become more significant in recent years, growing both in number and sophistication. Traditionally undertaken by organised crime gangs, the development of the RaaS ecosystem has opened up this part of the criminal world to a host of new threat actors. The COVID-19 pandemic has also created new avenues for cybercriminals to carry out various forms of online criminality, regardless of location.

A key policy challenge is the negative externality associated with the payment of ransoms. Those paying ransoms impose costs on others by potentially fostering more attacks and ratcheting up future extortion demands. To address that externality, legislators may be tempted to intervene by outlawing ransoms altogether and preventing insurers from reimbursing victims of an attack for ransom payments. While that might discourage some attacks, it is not clear that it will eliminate the problem, at least entirely. Such prohibitions may simply drive payments underground, especially if ransomware gangs resort to even more extreme measures to create potential harm and leverage their negotiating position.

Instead, efforts aimed at boosting firms' cybersecurity resilience, disrupting key infrastructure and partnerships within the ransomware ecosystem, and hunting down cyber adversaries are likely to be most productive. The initiatives pursued by various governments to extend existing regulation around anti-money laundering and terrorism financing to cryptocurrencies, as well as improve incident response, all move in that direction. Likewise, enhanced intelligence-led law enforcement to identify, track and prosecute cybercriminals across multiple jurisdictions, especially if executed as part of increased international coordination mechanisms, should help to upend the risk-reward ratio for hackers and deter ransomware attacks. But more can and must be done. This includes additional technical measures to boost cybersecurity defences and undermine RaaS as well as international diplomatic solutions to build a secure, trusted and interoperable cyberspace.

Alongside governments, private re/insurers have an important part to play in the battle against ransomware, both offensively and defensively. Re/insurers have an incentive to root out cybercrime that generates claims and hits their underwriting profits. Increased reporting of incidents and the swift exchange of actionable information will improve the authorities' abilities to accurately assess threats and effectively respond to them. There are already close connections between the industry and global law enforcement, with threat intelligence shared and data gathered, so ways to improve the efficiency of that exchange should be explored.

In addition to providing ransomware victims with the resources 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 hygiene 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. In short, it can boost society's overall cyber resilience to help ensure that the full network benefits of digitalisation can be realised – and are not undermined by the attendant increase in cyber hazards.

The cyber insurance market remains small and nascent. Premiums 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 insurance.[66] To foster further development, policymakers should steer clear of measures that could inadvertently stunt future expansion. Instead, policies that aim to safeguard cyberspace, promote cybersecurity and disrupt cybercriminals' operations will better counter the spread of cybercrime and increase re/insurers' appetite to absorb cyber risks from those less able to deal with them.

Cyber insurance can boost society's overall cyber resilience to help ensure that the full network benefits of digitalisation can be realised.

66 Aviva 2022.

References

Abnormal. 2022. The Evolution of Ransomware: Victims, Threat Actors, and What to Expect in 2022. February. https://abnormalsecurity.com/resources/ransomware-victims-threat-actors

Accenture. 2021. Global Cyber Intrusion Activity More than Doubled in First Half of 2021, According to Accenture's Cyber Incident Response Update. https://newsroom.accenture.com/news/global-cyber-intrusion-activity-more-than-doubled-in-first-half-of-2021-according-to-accentures-cyber-incident-response-update.htm

Allianz Global Corporate & Specialty. 2021. Ransomware Trends: Risks and resilience. https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

Aon. 2022. Cyber Insurance Market Insights: Q1 2022. April. https://aoninsights.com.au/wp-content/uploads/Cyber-Insurance-Market-Insights-Q1-22-FINAL.pdf

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

Aviva. 2022. SMEs Moving from Survival to Growth in 2022. https://connect.avivab2b.co.uk/broker/articles/news/smes-moving-from-survival-to-growth-in-2022/

Australian Department of Home Affairs. 2021. Ransomware Action Plan. https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

Australian Government. 2021. New Plan to Protect Australians Against Ransomware. https://minister.homeaffairs.gov.au/KarenAndrews/Pages/new-plan-to-protect-australians-against-ransomware.aspx

Bergal, J. 2021 States Consider Legislation to Ban Ransomware Payments. July. https://www.govtech.com/policy/states-consider-legislation-to-ban-ransomware-payments

Chainanalysis. 2022. As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

Chainanalysis. 2022. OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex. https://blog.chainalysis.com/reports/hydra-garantex-ofac-sanctions-russia/

Checkpoint. 2022. Behind the Curtains of the Ransomware Economy – The Victims and the Cybercriminals. April. https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

CIAB 2021. Commercial Property/Casualty Market Index: Q4 2021.

CISA. 2022. Stop Ransomware. https://www.cisa.gov/stopransomware

CISA. 2022. 2021 Trends Show Increased Globalized Threat of Ransomware. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

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/

Comply Advantage. 2022. Cryptocurrency Regulations Around the World. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

Congressional Research Service. 2021. https://crsreports.congress.gov/product/pdf/R/R46932

Corvus Insurance. 2021. Corvus Risk Insights Index, Q4 2021, Cyber & Technology E&O. https://info.corvusinsurance.com/hubfs/Risk%20Insights%20Index/CRII%20Q4%202021.pdf

Coveware. 2018. Corporate Ransomware Response & Protection Best Practices. 19 December. https://www.coveware.com/blog/2018/12/19/definitive-guide-to-corporate-ransomware-response-amp-protection-best-practices

Coveware. 2022. Law Enforcement Pressure Forces Ransomware Groups to Refine Tactics in Q4 2021. https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

Diebel. A. 2019. How the Kidnapping of Executives Made the Insurance Industry Boom. https://www.afr.com/companies/financial-services/how-the-kidnapping-of-executives-has-made-the-insurance-industry-boom-20190423-p51gbv

Dey. D. and A. Lahiri. 2021. Should We Outlaw Ransomware Payments? Proceedings of the 54th Hawaii International Conference on System Sciences.

R. Dudley. 2019. The Extortion Economy: How insurance companies are fueling a rise in ransomware attacks. PROPUBLICA. August. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

Gallagher Re. 2022. CY–FI. The Future of Cyber (Re) insurance. February. https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf

Group IB. 2021 - https://www.group-ib.com/media/gib-2021-2022-report/

Hitatchi. 2022. *The Rising Insider Threat.* https://www.hitachi-id.com/resources/graphics/malware-employees-approached-by-pulse-0-0

Hong Kong Computer Emergency Response Team Coordination Centre – HKCERT. 2022. Fight Ransomware. Retrieved, 4 April 2022 from: https://www.hkcert.org/publications/fight-ransomware

Institute for Security and Technology. 2021. Combating Ransomware: A Comprehensive Framework for Action – Key recommendations from the Ransomware Task Force.

INTERPOL. 2021. Immediate action required to avoid Ransomware pandemic. https://www.interpol.int/en/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL

Johansmeyer. T. 2022. The Cyber Insurance Market Needs More Money. Harvard Business Review. March. https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money

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

Kost, E. 2022. What is Ransomware as a Service (RaaS)? The dangerous threat to world security. https://www.upguard.com/blog/what-is-ransomware-as-a-service

McAfee. 2020. New MCAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion. https://www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629

J. MacColl, J. Nurse and J Sullivan. 2021. Cyber Insurance and the Cyber Security Challenge. RUSI Occasional Paper. June.

Marsh. 2022. Global Insurance Market Index Q1 2022. https://www.marsh.com/us/services/international-placement-services/insights/global_insurance_market_index.html

Marsh/Microsoft. 2022. The State of Cyber Resilience. May. https://www.guycarp.com/insights/2022/06/marsh-microsoft-cyber-risk-survey-addresses-key-trends.html

Miller, M. 2021. Top FBI Official Advises Congress Against Banning Ransomware Payments. https://thehill.com/policy/cybersecurity/565110-top-fbi-official-advises-congress-against-banning-ransomware-payments/

Munich Re. 2022. Global Cyber Risk and Insurance Survey. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

NetDiligence. 2021. Ransomware 2021 Spotlight Report. https://netdiligence.com/wp-content/uploads/2021/01/NetD_2021_Ransomware-Spotlight-1.pdf

Office of the Government Chief Information Officer (no date). Information and Cyber Security in the Wider Community. https://www.ogcio.gov.hk/en/our_work/information_cyber_security/community/

Paderborn. 2022. Ransom Payments in Ransomware Attacks: Scientists call on German politicians to act in an open letter. https://www.uni-paderborn.de/en/news-item/98221

Parchomovsky, G. and P. Siegelman. 2020. The Paradox of Insurance Faculty Scholarship at Penn Law. 2158. https://scholarship.law.upenn.edu/faculty_scholarship/2158

Ransomware.org. 2021. Money Launderers. https://ransomware.org/what-is-ransomware/the-importance-of-cryptocurrency-raas-and-the-extortion-ecosystem/#money-launderer

RSM. 2022. Cybercrime Victims Face Tax Deduction Difficulties. https://www.rsmuk.com/blog/cybercrime-victims-face-tax-deduction-difficulties

SecurityWeek. 2022. https://www.securityweek.com/insurance-broker-aon-investigating-cyber-incident

Shortland, A. 2016. Governing Kidnap for Ransom: Lloyd's as a 'private regime'. Wiley Periodicals.

SonicWall. 2022 SonicWall Cyber Threat Report. https://www.sonicwall.com/2022-cyber-threat-report/

Sophos. 2021. The State of Ransomware 2021. https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

Sophos. 2022. The State of Ransomware 2022. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

Suderman, A. and M. Gordon. 2021. Hit by a Ransomware Attack? Your payment may be deductible. https://apnews.com/article/technology-business-government-and-politics-d8c1e9958ad1e89eab83f44e6ca70a94

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

The White House. 2021. Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

Thompson, C. 2021. Ransomware Could Soon be About More Than Just Money – Ransomware has the potential to be a powerful bargaining tool. https://www.codastory.com/disinformation/ransomware-coersion/

U.S. Department of the Treasury. 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

U.S. Senate. 2021. America Under Cyber Siege: Preventing and Responding to Ransomware Attacks. Testimony of Bryan Vorndran, Hearing before the Senate Committee on the Judiciary, 117th Congress. 27 July 2021. https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks

Wheeler, T. and C. Martin. 2021. Should Ransomware Payments be Banned? https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/

Willis Towers Watson. 2021. Cyber Loss Trends 2021. https://www.wtwco.com/-/media/WTW/Insights/2021/07/cyber-loss-trends-2021.pdf?modified=20210728183147

Wired. 2022. https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/

Zdnet. 2022. https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/

Zurich/Advisen. 2021. Information Security and Cyber Risk Management. October.

The frequency of ransomware attacks is increasing, along with the size of ransom demands. While cyber insurance provides vital financial protection and operational support in the event of attack, ransomware has contributed to the recent deterioration in cyber insurers' underwriting performance. Enriched by re/insurer insights and learnings, this report identifies the challenges and economic externalities of ransomware, highlighting that cyber insurance and policy can work together to boost cybersecurity and, more broadly, socio-economic resilience.

The Geneva Association

International Association for the Study of Insurance Economics
Talstrasse 70, Zurich, Switzerland
Tel: +41 44 200 49 00

www.genevaassociation.org