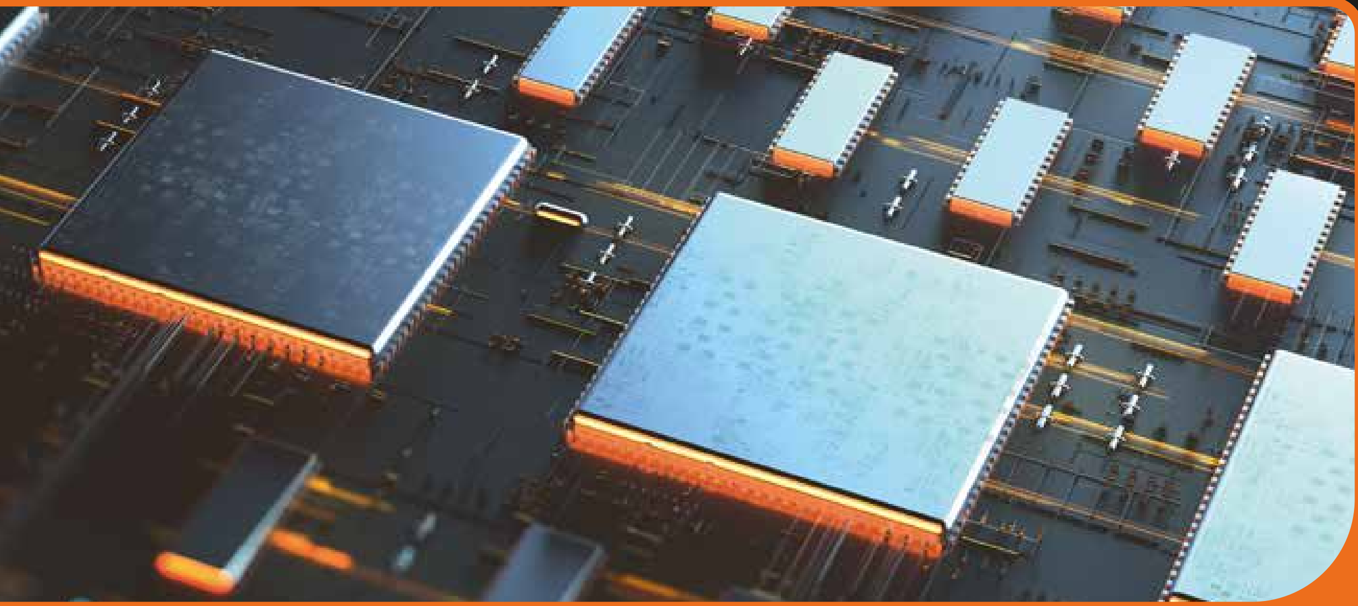
International
Comparative
Legal Guides



Practical cross-border insights into cybersecurity

Cybersecurity
2022

Fifth Edition

Contributing Editor:

Nigel Parker
Allen & Overy LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Infiltrate, Extort, Repeat – The Ransomware Pandemic

Nigel Parker

Nathan Charnock

Daniel Ruben

Allen & Overy LLP

Introduction

The last two years have seen a pandemic of epic proportions sweep across the globe, wreaking havoc in its wake and doing untold damage to the lives of billions. As organisations have adapted to deal with unprecedented challenges posed by COVID-19, hackers have taken advantage of a febrile environment, resulting in a spike in so-called "ransomware" attacks. These have had a sometimes-crippling effect on countless organisations, large and small. Often, victims must decide between paying a ransom, to restore systems and recover data, or refusing and facing potentially significant costs and catastrophic business interruption.

In this chapter we explore some of the strategies that can be implemented to prepare for, and minimise the impact of, a ransomware attack. We also consider the merits, legality and practicalities of paying a ransom.

Ransomware on the Rise

Ransomware is a form of malware that, once infecting a computer or system, encrypts data and files to render them inaccessible and unusable. Attackers will then typically send a ransom note demanding payment in return for the decryption keys required to restore access, and may threaten to publicly release sensitive data that they have obtained during the attack as a form of "double extortion".

Ransomware attacks pose a growing risk as they become more lucrative and easier to carry out. The emergence of groups offering so-called "Ransomware-as-a-Service" (RaaS), such as REvil and DarkSide, combined with the ready availability of on-demand malware kits, has made the process simpler than ever for would-be attackers. In addition, hackers typically demand payment in anonymous cryptocurrency that is difficult to trace, further reducing the risk of repercussions.

The COVID-19 pandemic fundamentally changed the way many access their online systems, with remote access systems such as remote desktop protocol (RDP) servers and virtual private networks (VPNs) becoming fundamental to the operation of businesses worldwide, as people logged on from home. This extension of networks gave rise to new vulnerabilities for exploitation by hackers using a combination of weak passwords, credentials gained through phishing attacks, the absence of multi-factor authentication and software deficiencies. The result – an estimated 300 million ransomware attacks were carried out in 2020, a rise of more than 150% on the prior year.[1]

In 2021, business costs associated with ransomware were expected to hit $20 billion, while cyber insurers have reported a fourfold jump in claims from 2019 through 2020.[2] This rise in costs is being driven in part by the "big game hunting" tactic that is being adopted by many attackers. Larger companies have been targeted with the aim of extracting larger ransoms, driven by the knowledge that many will not be able to endure the damage resulting from the average 15 business days of downtime caused by ransomware attacks.[3] In March 2021, we saw US insurance giant CNA Financial pay $40 million to regain control of its network;[4] in the same month, Acer received what is thought to be the largest ransom demand to date when REvil offered a "discounted rate" of $50 million while using stolen corporate data from the electronics manufacturer as leverage.[5] According to Palo Alto Networks, the average ransomware payment increased by 171% to $312,493 in 2020.

Fortify Your Defences and Equip Your Team

As with all forms of cyber-attack, it is a huge challenge to prevent ransomware attacks from occurring. The continuous nature of technological change, software development, and support and maintenance, combined with growing sophistication and frequency of attacks, means that even the most proficient of information security teams can struggle to stay one step ahead of the attackers. What businesses can do is ensure they invest in information security as a key priority and have robust programmes and procedures in place to ensure they are well prepared in the event that they become a target of attackers. The UK's National Cyber Security Centre recommends adopting a "defence-in-depth" approach, constructing multiple layers of defences with mitigations at each layer to best improve the opportunity to identify potential ransomware attacks and address them before they are able to cause damage.[6]

As a minimum, businesses should ensure they have:

1. **A well-resourced security programme**: A comprehensive information security programme is perhaps the most effective way businesses can reduce the risk that they fall victim to a ransomware attack. The scope of these programmes can be vast depending on the size and complexity of technology

stacks. However, a baseline programme for all medium-large businesses should include the implementation of appropriate antivirus and anti-malware software, regular and proactive network monitoring (on a 24/7/365 basis), regular patching and software updates, robust access controls including the use of multi-factor authentication and other human verification systems (for all remote access points) and use of other network-based bot management tools to detect illegitimate traffic.

2. **Appropriate internal training**: Many attacks are caused by human error or inaction. It is imperative that all staff receive regular training so they are aware of the risks associated with cyber-attacks and understand their own role in preventing and responding to them. Phishing was the second most common cause of ransomware attacks identified by Group-IB,[7] and providing simple tips to help employees recognise malicious emails can help reduce the risk of a successful attack.
3. **Incident response plans and procedures**: Organisations should ensure that they have detailed incident response procedures in place and should conduct regular table-top exercises to test these procedures and ensure relevant personnel (including senior personnel) understand their roles. The response procedures should include a predefined list of critical systems of which recovery is to be prioritised.
4. **Business continuity plan and disaster recovery**: In addition to general business continuity and disaster recovery plans, organisations should design a strategy for recovering in the event of a ransomware attack to minimise disruption and allow for continued operation of key business functions while remedying any attack suffered. Incident response procedures should be tested under disaster recovery conditions to ensure that they are workable in such scenarios. Often ransomware attacks can restrict the use of email and business mobile phones; therefore having a plan that enables core teams to work without these functions is imperative.
5. **Maintain regular back-ups**: Regularly backing up data and ensuring that these back-ups are secured is vital to preparing for any potential ransomware attacks. Having access to back-ups of important files, stored in multiple locations both locally and on cloud-based services, which are separate from and not connected to the network, will allow access to these files to be maintained in the event of an attack. Sophos found that 56% of victims of ransomware attacks in 2020 were able to use back-ups to retrieve their data, rather than paying a ransom.[8]
6. **Internal expertise**: A well-resourced team of information security specialists is essential to enable a business to maintain its day-to-day operations, to manage and implement its security programme and to react in the event of an incident.
7. **Access to external resource and expertise**: When an attack occurs, a business will likely want to engage external support from external specialists, including those with expertise in incident response, dark web monitoring, system rebuild, cyber forensics and PR management as well as external legal counsel who can assist with regulatory notifications, complaints, enforcement against third parties and advising on the payment of ransoms. Establishing these relationships (and putting in place engagement terms) before an attack has occurred will save a huge amount of time in the vital hours immediately following an incident.
8. **Accountability and risk monitoring**: The appointment of a Chief Information Security Officer or another senior executive officer with responsibility and accountability for information security (as well as appropriate incentives) will drive good performance and ensure that senior executives are alive to and aware of the risks associated with ransomware attacks.

React, Respond and Remediate

Each ransomware attack will present a unique set of circumstances, but as part of your incident response process you should ensure you:

1. **Triage** – conduct an initial triage of the incident as quickly as possible so you can establish the facts and better understand the scope and impact of the attacks and assess its severity.
2. **Instigate incident management procedures** – involve key stakeholders such as representatives from the information security, IT and legal teams as well as communications and customer service representatives where relevant. It is important to keep detailed incident logs to record decisions and to use out-of-band modes of communication such as telephone calls to avoid tipping off the attackers or any other malicious surveillance.
3. **Implement initial remediation steps as soon as possible** to try to stop the attack or at least prevent further spread of the malware across multiple systems and servers. Implement disaster recovery and business continuity plans and look to contain the incident and evaluate whether there is a risk of the attackers moving across other servers that are yet to be affected, whether locally or globally. This may involve quickly isolating or disconnecting affected systems and resetting credentials and passwords (including compromised admin credentials). Following the initial response, work will likely need to begin to clean the infected devices and reinstall the operating system (prioritising key systems first). The team must then ensure that both the cleaned devices/systems and the back-ups are free from any ransomware before restoring data from the back-up and reconnecting systems to a clean network. Of course, if a ransom is paid and data is released, the business may be able to avoid a full-scale rebuild.
4. **Brief senior executives** of events to ensure they are up to speed and able to take important decisions quickly (including whether to pay a ransom and dealing with any media interest).
5. **Deploy third-party advisors** to assist with your response. As noted above, these could range from specialists in incident response, dark web monitoring, system rebuild, cyber forensics and PR management as well as external legal counsel who can assist with the regulatory response. These specialists may also be able to help you to contact and negotiate with the attackers.
6. **Work with other interested third parties** who may have had corporate or other sensitive data compromised or accessed during the attack. Consider liaising with financial service providers to help prevent fraudulent activity if customer information has been accessed.
7. **Consider involving law enforcement** who may be able to assist with the investigation and help facilitate any ransom payments. You will want to take local legal advice here depending on the jurisdiction involved.
8. **Make regulatory and contractual notifications** where required, including to data protection authorities or other industry or government regulators. These often need to be made within a very short period of time. The business may also have contractual obligations to notify third parties of the breach.

9. **Complete a detailed incident review** to analyse how the ransomware attack was able to succeed, how the organisation responded and what lessons could be learned. Set a deadline and ensure accountability for implementation of any identified remediation measures.

The Hostage Dilemma – Should You Pay the Ransom?

A ransomware attack has spread across your key business systems and the attackers have access to huge volumes of sensitive customer, commercial and employee data. Thankfully you have good back-ups in place but rebuilding and restoring your systems will take weeks and the attackers are threatening to release that sensitive information on the dark web, unless you pay them $5 million in Bitcoin. What do you do?

This question raises a number of issues for businesses, including ethical dilemmas, practical and operational difficulties, legal complications, financial challenges and public relations headaches. In all cases, the decision to pay a ransom needs to be taken carefully, with a very small group of senior stakeholders and the input of external advisors where appropriate.

The initial answer is usually: "No – we will not negotiate with the attackers." However, many businesses do often decide that ransoms are a price worth paying when faced with the alternative of an unknown period of business disruption, potentially combined with the prospect of sensitive data either being leaked or irretrievably lost.

Richard Hanlon of Aon Cyber Solutions thinks that "paying the ransom is the tip of the iceberg" and that "whatever the business, it's better to understand ransomware losses in the context of business interruption, because that's the single biggest threat from a ransomware attack". The UK's National Health Service incurred £92 million of costs to restore its services in the months following the 2017 WannaCry attack. It is also important to note that losses can extend well beyond remediation expenses, as victims may find themselves exposed to long-term impacts such as loss of business, third-party claims and reputational damage. Research by Sophos estimated that, last year, the average cost of rectifying a ransomware attack, when considering downtime and the costs associated with recovery, sat at $1.85 million with 26% of victims choosing to pay ransoms.[9] In the first part of 2021, this figure had risen to 32%.[10]

Whilst the payment of a ransom may ultimately be a commercial decision, there are a number of other considerations that a business will want to take into account when choosing whether or not to pay:

- **Attacker credibility/reliability**: If cyber specialists are able to identify the likely attacker, it will be helpful for your business to understand whether that particular attacker/group has a reputation for ceasing an attack and returning stolen data when they receive a ransom payment.
- **Governmental and societal pressures**: Depending on the nature of the business and the jurisdictions impacted, victims may want to consider what view government bodies may take of paying a ransom. Experts within the cybersecurity industry remain deeply divided on whether victims should pay ransoms. The Ransomware Task Force, a global coalition of cyber experts, has made nearly 50 recommendations to governments across the world to help curb the burgeoning illicit industry but were unable to come to an agreement on whether countries should ban ransom payments. In the United States, the FBI does not advocate the paying of ransoms, in part because it does not guarantee that access will be regained, while in the last year the US Department of the Treasury's Office of Foreign Assets Control has looked to impose financial penalties on organisations that make ransomware payments and in doing so "may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims".
- **Legal restrictions**: It will also be important to consider if there are any legal restrictions that prevent or restrict the payment of ransoms in the affected jurisdictions. For example, in the UK, whilst the payment of ransoms is not illegal in most situations, there is a risk that making such a payment could be considered a criminal offence under the Terrorism Act 2000 if it is known or there is reasonable cause to expect that the person receiving the payment will or may use it for the purposes of funding terrorism.
- **Ethical stance**: Many businesses will also want to consider their own moral stance on paying a ransom. These payments typically involving the funding of a criminal enterprise that is likely to repeat the offence elsewhere and funnel the funds into further illegal activities. This reality will have to be weighed against the costs of any potential harm that may arise from the attack continuing, such as the release of huge amounts of sensitive data. Increasingly, organisations are implementing policies that set out their position on the payment of ransoms in different circumstances.
- **Reputational risk**: Whilst many businesses will try to keep details of any ransom payment confined to a small number of senior individuals, there remains a risk of a leak. Therefore, careful consideration of the public relations impact will need to be considered and a communications plan implemented.
- **Financial impact**: Businesses should take a holistic view of the financial impact of paying a ransom, considering not just the payment itself but also the cost of the attack continuing and the impact of the attack of revenues generally (whether or not a ransom is paid).
- **Practicalities**: Importantly, if a business does decide to make a ransom payment, there are a number of practicalities to consider. In particular, access to cryptocurrency will be needed in short order and an organisation will need to decide who will need to sign off on and make the relevant payment. In addition, depending on the jurisdiction, businesses may also want to inform law enforcement of an intention to make the payment to ensure transparency and to enable them to provide any assistance.

Conclusion

The COVID-19 pandemic provided a breeding ground for cyber criminals to infiltrate organisations on a scale not seen before, with ransomware the malware of choice for many seeking to cause maximum disruption to businesses during already challenging times. The ethics of paying a ransom still divide opinion across the world but the devastating effects of not doing so means businesses face a very real dilemma when making this tough decision. The most effective way to address the threat of these attacks is to invest in strong defences and experienced personnel whilst implementing robust processes and procedures so that a business stands ready to react, respond and remediate any incidents that occur.

Endnotes

1. *Help Net Security*, "Number of ransomware attacks grew by more than 150%", 8 March 2021.
2. *The One Brief*, "It's Time to Forget These 5 Ransomware Myths", 14 July 2021.
3. *Health IT Security*, "Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111k", 4 May 2020.
4. *Bloomberg*, "CNA Financial Paid $40 Million in Ransom After March Cyberattack", 20 May 2021.
5. *Forbes*, "Acer Faced With Ransom Up To $100 Million After Hackers Breach Network", 21 March 2021.
6. *National Cyber Security Centre*, "Mitigating malware and ransomware attacks", 9 September 2021.
7. *Ibid*., endnote 1.
8. *Sophos*, "The State of Ransomware 2021" A Sophos Whitepaper, April 2021.
9. *Ibid*., endnote 8.
10. *Ibid*., endnote 8.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.

Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and IT law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sectors, including IP licensing, outsourcing and service provision arrangements.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

Daniel Ruben is a trainee solicitor in the commercial team at Allen & Overy.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.

We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group