Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at May 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

9

Ransomware Attacks and Responses

Ryan Fayhee and Tyler Grove[1]

Ransomware attacks have become a daily occurrence across a wide spectrum of businesses, healthcare facilities and educational institutions. This trend has only been exacerbated by the covid-19 pandemic, as many businesses have transitioned to fully remote work.[2] Victims of ransomware attacks risk the loss of essential data, operational delays and significant reputational damage. Often, victims are forced to respond to ransom demands within a limited time frame. Many are reasonably tempted to simply pay the requested sum when that monetary price is balanced against devastating enterprise risk.

However, there is also considerable risk to making such payments if the attackers are subject to sanctions or are a terrorist organisation, exposing in particular insurers and response vendors acting as third-party payors, cyber-risk vendors and other private responders in the absence of some reasonable diligence in the midst of an attack. The two primary US government agencies responsible for enforcing these rules – the Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN), both housed within the US Department of the Treasury – recently released advisories that signal an intention to strictly apply these laws, even against victims of cybercrime.[3] It is therefore critical that victims of ransomware attacks understand the risks involved and best practices in responding before taking any action and carefully plan in advance for an attack.

---

1 Ryan Fayhee is a partner and Tyler Grove is an associate at Hughes Hubbard & Reed.

2 See, e.g., '*COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%*', Sec. Mag. (Jul. 22, 2020), https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50.

3 See *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. Dep't of the Treasury (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf ('OFAC Advisory'); Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, FIN-2020-A006, U.S. Dep't of the Treasury (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf ('FinCEN Advisory').

This chapter first provides an overview of the common forms of known ransomware and developing trends. It then summarises some of the key legal risks if ransom is to be paid, particularly those arising under sanctions, terrorist financing, and anti-money laundering laws.[4] Finally, it recommends best practices to consider in response to an attack.

Ransomware attacks and trends

Ransomware is malicious software that blocks access to a computer system or data as a means to extort monetary payments from victims in exchange for restoring access. Ransomware often works by encrypting the targeted files, and attackers may additionally threaten to sell or make public sensitive or embarrassing data if the payments are not made.

While ransomware attacks can affect businesses of any size and sophistication, increasingly ransomware attackers are targeting larger enterprises and extorting more significant payouts, often referred to as 'big game hunting.'[5] These attacks may also involve a correspondingly higher investment by the attacker in studying the target to identify potential vulnerabilities and developing advanced infiltration strategies.[6]

On the other hand, some attackers may seek to extort the same targets repeatedly.[7] Rather than seeking one larger payout, these attackers may demand comparatively low ransoms that incentivise the victim to pay without making substantial improvements to their cybersecurity or to otherwise address the vulnerability. These attackers hope that, in the aggregate, multiple 'nuisance' ransoms would exceed the amount that could be obtained through a single attack.

As commercial enterprises become savvier about preventing and detecting ransomware, ransomware developers have adapted and have, in fact, built an economy around their malign activities. Some ransomware attackers target sensitive or embarrassing information on their victims' networks. In addition to encrypting the data on the victim's networks, these attackers may make a copy of the data and demand two payments: one to encrypt the data on the victim's system, and one to prevent the attacker from selling or releasing the data.[8] The attackers may also simply sell the data, without regard to whether the ransom is ultimately paid by the victim.

One developing typology is the franchising of ransomware, known as ransomware-as-a-service (RaaS), and other forms of resource-sharing among attackers. RaaS allows malicious

4 There is no federal statute that comprehensively governs payments made in response to ransomware attacks. There may be additional legal risks and reporting requirements depending on, among other things, the jurisdictions affected and the organisation of the targeted business.

5 See *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, Alert No. I-100219-PSA, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002.

6 See, e.g., Lyle Adriano, *Ransomware 'big game hunting' has insurers on the ropes*, Insurance Business Mag. (Oct. 28, 2019), https://www.insurancebusinessmag.com/us/news/cyber/ransomware-big-game-hunting-has-insurers-on-the-ropes-189771.aspx.

7 See, e.g., Alexander Culafi, *Repeat ransomware attacks: Why organizations fall victim*, TechTarget (Jun. 16, 2020), https://searchsecurity.techtarget.com/news/252484720/Repeat-ransomware-attacks-Why-organizations-fall-victim#:~:text=Repeat%20ransomware%20attacks%20have%20become,hit%20with%20ransomware%20multiple%20times.

8 See, e.g., Alex Scroxton, *Double extortion ransomware will be a big theme in 2021*, Computer Weekly (Dec. 2, 2020), https://www.computerweekly.com/news/252493002/Double-extortion-ransomware-will-be-a-big-theme-in-2021.

actors to essentially license out their malware to less technically sophisticated criminal partners, either through a fixed fee or on a profit-sharing basis.[9]

Another emerging technique is the use of 'fileless' ransomware. In fileless ransomware, malicious code is inserted directly into a programs script or is written into its memory, so that there is no standalone malware file on the machine.[10] Fileless ransomware is, accordingly, significantly more challenging to detect.

Legal risks

Despite the increasing prevalence of ransomware attacks and the growing number of victims, responding to a ransom demand is fraught with many pitfalls. Businesses and their counsel should understand the basic legal frameworks that underlie these risks before deciding on how to respond to a ransom demand. Some of the most common legal risks if ransom is paid include those from transacting with a party subject to sanctions, making a payment to a terrorist organisation, as well as failing to make required Suspicious Activity Reports (SARs). Each risk is discussed in turn below.

Sanctions risks

There are a number of authorities that allow OFAC to sanction known cybercriminal organisations, such as those engaging in systemic ransomware attacks. In particular, on 1 April 2015, President Obama issued Executive Order 13694,[11] which was subsequently amended on 28 December 2016 by Executive Order 13757.[12] Those orders authorise OFAC to add individuals and entities to the Specially Designated Nationals (SDN) list who are determined to engage in certain malicious cyber activities. These activities include, inter alia, 'causing a significant disruption to the availability of a computer or network of computers' or 'causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain.'

OFAC has designated a number of established cybercrime organisations and associated individuals under these authorities, which, as detailed in the OFAC Advisory, include the following:

- Evgeniy Mikhailovich Bogachev, the developer of Cryptolocker, which has infected an estimated 234,000 computers since 2013;
- Ali Khorashadizadeh and Mohammad Ghorbaniyan, two Iranian nationals who helped exchange digital currency (Bitcoin) ransom payments into Iranian rials on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims in 2015; and
- Evil Corp, a Russian cybercrime organisation, and its leader, Maksim Yakubets, for developing and using the program Didrex to steal more than US$100 million since 2015.[13]

9 See, e.g., *Ransomware as a Service (RaaS) Explained*, CrowdStrike (Jan. 28, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

10 See, e.g., *How Fileless Ransomware Works,* CrowdStrike, https://www.crowdstrike.com/resources/infographics/how-fileless-ransomware-works/.

11 See Executive Order 13694 (Apr. 1, 2015), https://home.treasury.gov/system/files/126/cyber_eo.pdf.

12 See Executive Order 13757 (Dec. 28, 2016), https://home.treasury.gov/system/files/126/cyber2_eo.pdf.

13 See OFAC Advisory at 2.

Additionally, a number of US sanctions programmes apply to governments of countries viewed by the US government as adversaries, and extend to entities and organisations owned or controlled by those governments. For example, Executive Order 13772 blocks all property and interest in property of the government of North Korea, which is defined to include the government's 'agencies, instrumentalities, and controlled entities'.[14] Cybercrime groups under the control of the government of North Korea are therefore subject to sanctions, even if they are not explicitly identified on a US sanctions list, and on 13 September 2019, OFAC affirmed that three well-known North Korean hacking groups – Lazarus Group, Bluenoroff and Andariel, who used the ransomware program WannaCry 2.0 to infect approximately 300,000 computers in May 2017 – were, in fact, controlled by the government of North Korea.[15]

US persons – including US nationals, permanent residents, individuals physically present in the United States, and entities organised under US law – are prohibited from engaging in virtually all transactions involving these or other SDNs, or entities owned 50 per cent or more by an SDN, whether directly or indirectly. This prohibition extends to actions and activities that would 'facilitate' a transaction by a non-US person that would be prohibited if done by a US person. The concept of 'facilitation' is broad, and may include, for example, approving or directing payments by non-US persons, changing policies or procedures to remove US persons from the transaction, and even strategising about potential transactions with prohibited parties.

In addition, US persons are broadly prohibited from engaging in transactions with or involving citizens and permanent residents of comprehensively embargoed territories who are ordinarily resident in those territories, which include the Crimea region of Ukraine, Cuba, Iran, North Korea and Syria. This restriction applies regardless of whether the national of the embargoed territory is an SDN or otherwise identified on a sanctions list.

Non-US persons should also take heed of these prohibitions. If a US person or US dollars are involved in a transaction, non-US persons could face scrutiny for 'causing' the US person to violate sanctions. This risk also arises when converting US dollars (which generally are processed by a US correspondent bank) or using a US-based bank account or cryptocurrency exchange to make a ransom payment to a sanctioned party. Even if a US person or US dollars are not involved, Executive Order 13694 authorises OFAC to designate as subject to sanctions (i.e., include on the SDN list) any person determined 'to have materially assisted' or 'provided financial, material, or technological support for' persons sanctions under the order, and it is possible that ransom payments to sanctioned groups could be viewed as 'material assistance' by OFAC.

Significantly, civil violations of US sanctions are assessed under a strict liability standard, meaning that intent is not considered and even inadvertent transactions may, and often do, constitute violations. This renders payments to ransomware attackers extremely risky because often very little is known about the attacker that could allow the victim to gauge whether the attacker is an SDN or a national of a comprehensively embargoed country. If, after a payment, it is later discovered that the attacker was, in fact, subject to sanctions, the payor

14 See Executive Order 13772 (Mar. 15, 2016), https://home.treasury.gov/system/files/126/nk_eo_20160316.pdf.

15 See Press Release, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups, U.S. Dep't of the Treas. (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774; *see also* OFAC Advisory at 2.

could be liable if OFAC discovers the transaction and brings an enforcement action. Civil violations may result in a monetary penalty of up to US$311,562 (as periodically adjusted for inflation) or twice the value of the transaction, whichever is higher.

If a person or entity violates sanctions 'wilfully,' or even 'wilfully blind', it could be subject to criminal liability. The standard for 'wilful' intent is set forth in *Bryan v. United States*, 524 US 184 (1998). Under *Bryan*, an act is wilful if done with the knowledge that it is illegal. The government, however, is not required to show the defendant was aware of the specific law, rule, or regulation that its conduct may have violated. Criminal violations may result in fines of up to US$1 million and forfeiture of any property involved in the violations, as well as up to 20 years in prison for individuals convicted of criminal sanctions violations.

Terrorist financing

Section 2339B of Title 18 of the United States Code provides:

> *Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.*

Notably, to face liability under this section, the violator 'must have knowledge that the organisation is a designated terrorist organization . . . , that the organization has engaged or engages in terrorist activity . . . , or that the organization has engaged or engages in terrorism.' Significantly, Section 2339B has broad extraterritorial application.

In scenarios where the ransomware attacker is known to be a foreign terrorist organisation, payment of the ransom could therefore constitute a violation of §2339B. It is worth noting that, in policy guidance regarding US citizens taken as hostages abroad, the US Department of Justice (DOJ) emphasised that it 'has never used the material support statute to prosecute a hostage's family or friends for paying a ransom for the safe return of their loved one'.[16] However, it is not clear if DOJ would extend this policy to payments of commercial ransoms where human life was not at risk. Considering the emphasis in the OFAC Advisory and FinCEN Advisory on compliance with sanctions and anti-money laundering requirements even for victims of ransomware attacks, §2339B should also be viewed as a potential risk when considering payments in response to ransomware attacks

Anti-money laundering reporting obligations

Certain businesses that qualify as a 'financial institution'[17] under the Bank Secrecy Act (BSA) – including 'money services businesses' that include certain currency exchanges and money transmitters – are required to file SARs. A financial institution is required to file a SAR if it:

- knows, suspects or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to US$5,000 (or, with one

16 See Press Release, No. 15-790, *Department of Justice Statement on U.S. Citizens Taken Hostage Abroad*, U.S. Dep't of Jus. (Jun. 24, 2015), https://www.justice.gov/opa/pr/department-justice-statement-us-citizens-taken-hostage-abroad.

17 See 31 U.S.C. § 5312(a)(2) and (c)(1).

exception, US$2,000 for money services businesses) or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity;
- is designed to evade BSA regulations;
- lacks a business or apparent lawful purpose; or
  involves the use of the financial institution to facilitate criminal activity.[18]

Thus, qualifying 'financial institutions' must report extortive demands for a ransom payment to FinCEN through a SAR. Generally, SARs must be filed within 30 days of the detection of the suspicious activity. The wilful failure to timely file a SAR could carry a civil monetary penalty not to exceed the greater of the amount involved in each transaction (capped at US$233,313, as adjusted for inflation) or US$58,328, as adjusted for inflation.[19] Negligent violations are subject to a penalty of US$1,180, as adjusted for inflation.[20] Notably, each day that the violation continues is considered a separate violation.[21]

Even victims of ransomware attacks that are not 'financial institutions' subject to the BSA, and therefore not required to file a SAR, should be aware of the filing requirement, as third parties involved in the payment of a ransom could be required to submit a report. This risk could arise, for example, if the victim attempts to convert fiat currency into cryptocurrency, which is often a condition demanded by attackers in making a ransomware payment. Financial institutions that submit SARs are required to keep them confidential, and the subject of the SAR would not be informed that a report had been filed.

Response best practices

Companies should consider the following best practices when responding to an attack. It is highly recommended that at-risk companies consider these steps and how they might be tailored to the company's specific business before a ransomware attack occurs.

Create a plan and response team

Even before a ransomware attack occurs, it is critical that at-risk businesses develop a formal response plan, designate internal and external personnel who will form the response team, and clearly identify the responsibility of each team member. Among other things, the response plan should identify a reporting hierarchy to streamline decision making, as ransom payments are often demanded under intense time pressure. The response team should include key internal personnel, including, as appropriate, the company's chief legal officer, chief information security officer, chief information technology officer and chief operating officer. The response team should also include external resources, including external counsel specialising in compliance and data privacy issues, a cybersecurity firm, a digital forensics or investigations firm, media relations specialists, and other third parties as necessary. Once the response plan is formulated, it should be distributed to relevant employees, and regular training should be conducted to educate employees on how to identify and escalate potential issues.

18 See FinCEN Advisory at 6-7.

19 See 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f).

20 See 31 U.S.C. § 5321(a)(6)(A).

21 See 31 U.S.C. § 5321(a)(1).

Gather information and conduct screening

As soon as a ransomware attack is discovered, the response team should gather all relevant information to enable decisions on how to respond. Depending on the time allotted for a response, this information should include, among other things, identifying which data or systems are compromised and evaluating whether the form and characteristics of the attack or malware used are similar to any prior known ransomware attacks. The OFAC advisory identifies several categories of key information to be evaluated, including:

> *relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications.*[22]

However, ransomware victims should be aware that some groups attempt to mask their identity by using similar techniques as rival cybercriminal organisations. Further, given the rise of RaaS, the nature of the malware used may not always be indicative of the identity of the attacker.

The company should then conduct screening of the attacker using whatever information may be available. If a company, with the assistance of external resources, is able to determine that the attack is similar to other known prior attacks, the company should screen the name of the known or suspected perpetrators of the prior attacks against sanctions lists and assess whether they are affiliated with government actors that may be subject to sanctions. The payment information for the ransom should also be screened, as OFAC includes on its sanctions lists the digital wallet addresses of some well-known ransomware attackers.

Consider notifying law enforcement and relevant agencies

Contemporaneously with gathering information and screening, a ransomware victim should consider notifying law enforcement and OFAC of the attack. Among other benefits, law enforcement, who will have access to non-public information, may be able to assist with identifying the likely perpetrators of the attack, which will in turn be able to better inform the victim of whether a payment is prohibited. Timely notice to law enforcement is also viewed favourably by OFAC in making enforcement decisions, in the event a ransom is paid and it is later discovered that the attackers are subject to sanctions. The OFAC Advisory, for example, states:

> *OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law*

22 See *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, No. FIN-2020-A006, U.S. Dep't of the Treas., at 7 (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

> *enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.*[23]

Separately and apart from the involvement of law enforcement, if a payment is made to a ransomware attacker, and a company is unable to determine that the attacker is sanctioned, the victim could consider filing a protective voluntary self-disclosure with OFAC. As a matter of policy, OFAC will reduce the maximum civil penalties applicable to a violation by half, and voluntary self-disclosures often result in no penalties, especially for companies with no prior violations in the past five years. The self-disclosure could then provide the relevant details regarding the nature and characteristic of the attack, the information available to the victim, and the screening and diligence results based on that information. The self-disclosure could further describe the victim's ransomware response plan procedures and actual response to the attack, including whether any specialised law firms or cybersecurity firms were used. To be considered 'voluntary', a self-disclosure must be submitted before OFAC opens its own investigation into a transaction. For this reason, a victim planning to make a self-disclosure may wish to do so prior to or at the same time as notifying other law enforcement.

Government investigations

Whether or not a payment is made in response to a ransom, there is a risk of subsequent government investigations. This could be the result of the victim notifying law enforcement (as discussed above), of a SAR being filed by a third party, or of other non-public intelligence available to law enforcement. Inquiries could range from informal requests for information to formal subpoenas or search warrants. Ransomware victims should therefore consider procedures for handling requests from law enforcement and other government agencies. Among other things, employees should be instructed to refer all requests to the appropriate corporate officers, such as the in-house legal department. It is also strongly recommended that victims receiving a request for information from law enforcement, whether formal or informal, consider the involvement of specialised external legal counsel to allow for the application of the attorney–client privilege.

Investigate and address vulnerabilities

Once an initial response has been made, whether or not it involves the payment of a ransom, a victim of an attack should conduct a full investigation into the root causes of the attack and take mitigating steps to avoid future similar attacks. Among other things, it is possible that malware could remain on infected systems and the point of entry for the attackers into the systems could remain open. Considering the rise of repeat attacks, these vulnerabilities should be identified and remediated as soon as possible. A sophisticated cybersecurity firm and digital forensics firms should be able to assist with this exercise.

In addition to identifying the root causes of the attack, the follow-on investigation should include confirmation of whether any compromised data was actually disclosed. Even if a ransom was paid, it is possible that attackers could still seek to sell a victim's data. A third-party cybersecurity firm can assist with conducting scans of the dark web and other

23 OFAC Advisory at 4.

common repositories of stolen data to identify whether any of the compromised data is present (and if so, whether that data can be linked back to the ransomware attack, or may be the result of a separate security breach). Depending on the data and the jurisdictions involved, there may be a legal obligation to make notifications of the breach to the data owners or government authorities.

Conclusion

Ransomware attacks are unfortunately a growing commercial reality that will continue for the foreseeable future. US sanctions, terrorist financing and anti-money laundering laws make no distinction between transactions conducted by victims of a crime or otherwise, and ransomware victims who choose to pay demanded sums to their attackers face a myriad of legal risks. Through understanding the common forms of ransomware attacks, the legal framework regulating the payments and the best practices in responding, victims can better judge their specific risks and navigate the complex regulatory backdrop to avoid government penalties on top of the potentially significant financial and reputational harm brought by an attack.

Appendix 1

About the Authors

Ryan Fayhee
Hughes Hubbard & Reed

Ryan Fayhee leads the sanctions, export controls and anti-money laundering practice group at Hughes Hubbard. Prior to private practice, Ryan served for 11 years in the DOJ, where he was a leading prosecutor handling complex investigations and prosecutions affecting the national security and foreign policy of the United States. He also previously served as the National Export Control Coordinator, the principal DOJ attorney overseeing sanctions and export control prosecutions nationally. Ryan represents companies, boards of directors, audit committees and senior executives in internal and government-facing cross-border investigations and advises clients on compliance and acquisition due diligence with a focus on sanctions, export controls, anti-money laundering, anti-corruption and cybersecurity. Ryan has significant experience assisting multinational companies facing crises and other high-profile reputational risks. Ryan is also an experienced trial lawyer and regularly represents clients in federal court and before the DOJ, federal law enforcement authorities, and trade regulators at the Office of Foreign Assets Control, the Bureau of Industry and Security and the Directorate of Defense Trade Controls.

Tyler Grove
Hughes Hubbard & Reed

Tyler Grove is an associate in the Washington, DC office of Hughes Hubbard & Reed. As a member of the firm's sanctions, export controls and anti-money laundering group, Tyler advises domestic and international clients on all facets of compliance and enforcement, including cybersecurity and ransomware best practices. Tyler also advises on economic trade sanctions, export controls and anti-money laundering matters; filings with the Committee on Foreign Investment in the United States; and investigating and drafting complex voluntary disclosures submitted to the Commerce, State, and Treasury departments. Tyler also has experience representing clients in complex litigation, fact investigation and discovery in

various government-facing matters, including those involving professional liability, securities, antitrust and trade issues.

Hughes Hubbard & Reed
1775 I Street, NW
Washington, DC 20006-2401
Tel: +1 202 721 4600
Fax: +1 202 721 4646
ryan.fayhee@hugheshubbard.com
tyler.grove@hugheshubbard.com
www.hugheshubbard.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5