



THE CYBER INVESTIGATIONS GUIDE

THIRD EDITION

Editors

Benjamin Powell and Shannon Togawa Mercer

The Cyber Investigations Guide

Third Edition

Editors

Benjamin A Powell

Shannon Togawa Mercer

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK
© 2023 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

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 was accurate as at May 2023, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-253-6

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

Acknowledgements

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

Anderson Mōri & Tomotsune

BCL Solicitors LLP

Clifford Chance US LLP

Cravath, Swaine & Moore LLP

Jones Day

K&L Gates LLP

Nyman Gibson Miralis

Ropes & Gray LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

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

It aims to fill a gap in the literature by providing 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 seventh 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 Cyber Investigations Guide 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 Cyber Investigations Guide* as the close-up.

The Cyber Investigations Guide 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.

David Samuels

Publisher

May 2023

CHAPTER 1

The ‘Art’ of Investigating: Responding and Investigating at the Same Time and Overseeing a Privileged Forensic Investigation

Benjamin A Powell, Jason C Chipman and Shannon Togawa Mercer¹

Incident response requires an immediate, coordinated effort to gather the facts and execute an incident response plan that enables a company reacting to a cyber-security incident or data breach to address multiple work streams simultaneously. All at once, the company will need to manage, and be prepared to tackle, various work streams, including, but not limited to:

- containing and remediating the incident;
- conducting a forensic investigation to understand what has occurred, how it occurred and what damage, if any, was caused to the confidentiality, availability or integrity of company systems or data;
- preserving evidence;
- preparing for and complying with any notice requirements to regulators, consumers or other third parties (such as business customers);
- preparing for and responding to formal and informal regulatory or legislative enquiries;
- coordinating with law enforcement;
- developing and, where necessary, deploying contingency planning, messaging strategies and communications to in-house and external audiences;

¹ Benjamin A Powell and Jason C Chipman are partners and Shannon Togawa Mercer is a senior associate at Wilmer Cutler Pickering Hale and Dorr LLP.

- preparing and monitoring for possible litigation, including preserving documents and monitoring dockets;
- briefing insurance carriers; and
- assuring auditors that information technology (IT) controls remain sound.

The specifics of these work streams, and considerations for each, are detailed later in this chapter and in subsequent chapters of this book. In this chapter, we begin by highlighting some of the tactical processes, deliverables and tools that should be launched immediately, as they facilitate an effective, strategic and forward-leaning incident response, rather than a reactive and chaotic one. We then discuss two work streams in which companies can be particularly proactive: managing the forensic investigation and coordinating with law enforcement.

Launching an incident response

An effective incident response requires an organised process, regular communication, a single consolidated understanding of the facts, and a system for tracking key communications and events. Specifically, the following steps and documents should be initiated immediately and regularly updated or reassessed, as appropriate, throughout the incident response:

- *Assembling the team:* The first step is identifying which in-house personnel, including who leads and manages the incident response team, and external vendors (e.g., law firms, forensic vendors, communications firms and ransomware responders) should form the core incident response team. Ideally, this should be addressed in the company's incident response plan or policy, but some incident response teams may reasonably include 'optional' members depending on the circumstances (such as the head of a particular affected business unit, the chief privacy officer or data protection officer if personal data may be compromised, or the head of human resources if the breach has affected a large number of employees). Companies should quickly identify which incident response team members are relevant for a particular incident and continue to reassess whether additional members should be engaged.
- *Assigning responsibilities and tracking tasks:* Each work stream should be assigned to designated in-house and external personnel, such as through a matrix identifying each responsibility, work stream, point of contact, action item, status and expected completion date. This should include work streams for incident response, forensics, communications with key in-house and external audiences, and legal and regulatory analysis and coordination.

- *Scheduling calls and meetings:* The incident response team should meet regularly to ensure that messaging, goals and developments remain coordinated across work streams. For example, those developing communications documents will need to be aware of new forensic developments, and those coordinating regulatory communications will need to be aware of any developments in messaging strategy. Regular communication will also ensure that company priorities potentially affecting or affected by the incident response (e.g., regularly scheduled filings to the US Securities and Exchange Commission) can be synchronised with the incident response efforts. Typically, we recommend at least two daily calls or meetings: (1) a strategy and update meeting with the incident response team leadership (including external counsel) to review the current status, recent developments and next steps, and to open questions for each work stream; and (2) a technical update with the forensic team, internal IT or information security, and external counsel to discuss forensic developments, resolve technical challenges and prioritise tasks.
- *Maintain a detailed chronology:* All key events and communications should be tracked in a centralised, detailed chronology, preferably prepared and maintained by external counsel. The chronology should include minute details in a straightforward factual manner, including key in-house and external communications (e.g., board briefings, updates to insurance carriers, productions to law enforcement), investigation and remediation updates, and key forensic details. This will allow the company to cross-correlate events from different work streams and respond in the future to specific detailed questions regarding the incident, the investigation or the company's response.
- *Draft a centralised narrative:* Information known about the incident, when it was identified and what key questions remain should be drafted in a centralised narrative, again preferably prepared and maintained by external counsel with input from relevant experts responding to the incident. To the extent known, it should describe the initial point of entry and how it was leveraged, key instances of lateral movement and potential data compromise. The narrative should be high level and clear about outstanding strategic considerations. This document should be used as a starting point for all external communications to ensure consistency and accuracy in messaging.

While these processes and documents are under way, the forensic work will begin in earnest, proceeding with four primary objectives: (1) preserving potentially relevant evidence in a forensically sound manner; (2) investigating what happened; (3) containing the incident to prevent further exposure and remove the threat actor; and (4) remediating identified vulnerabilities.

Many companies understandably prioritise containment and remediation. However, to successfully mitigate the incident and prevent potential further exposure, evidence preservation and a preliminary investigation must often be completed first. Before an incident can be safely contained, the company must have a sufficiently complete understanding of the vulnerabilities leveraged by the threat actor; otherwise, containment efforts may miss potential areas of exposure or back doors installed by the hacker, allowing the hacker to maintain a low profile and continue its attack. Appropriate evidence preservation is also key to fully understanding an attack's life cycle. Although the dynamics of specific types of attacks, such as ransomware attacks, may accelerate or shift the way a company is thinking about prioritising containment and remediation or allocating resources, a good incident response process will engage in balancing urgent and important needs.

Managing a third-party forensic investigation

Most companies engage third-party forensic investigators to assist in responding to a breach. In virtually all significant incidents that may involve regulatory enquiries, customer concerns or other significant issues, having a third-party expert perform the forensic analysis provides necessary resources,² gives assurance to regulators and customers that an incident has been examined by an independent party,³ and brings in additional expertise to examine a problem, including where experts may have experience with prolific or known threat actors.

-
- 2 See, e.g., Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, US Department of Commerce, National Institute of Standards and Technology, Special Publication 800-61 Revision 2, 'Computer Security Incident Handling Guide', 14–15 (August 2012) (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [last accessed 5 April 2023]) ('Incident response work is very stressful, as are the on-call responsibilities of most team members. This combination makes it easy for incident response team members to become overly stressed. Many organizations will also struggle to find willing, available, experienced, and properly skilled people to participate, particularly in 24-hour support. Segregating roles, particularly reducing the amount of administrative work that team members are responsible for performing, can be a significant boost to morale.').
- 3 See, e.g., Federal Trade Commission (FTC), 'Data Breach Response: A Guide for Business' (February 2021), 1 (https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf [last accessed 5 April 2023]) (encouraging companies to '[c]onsider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps').

In addition to these advantages, using a third-party forensic investigator, and particularly one engaged by external counsel, can be critical to maximising privilege protections for forensic analysis, work-product and working papers. In the event of a cyber incident, the breached company may face a variety of legal risks, as discussed elsewhere in this book. In such situations, customers, regulators or class action plaintiffs would undoubtedly seek discovery of written materials relating to a forensic investigation. Materials created at the direction of legal counsel to enable external counsel to advise the company may be protected under privilege and help to ensure the company is given effective legal advice.

The best way to mitigate these risks – and the path pursued in virtually every significant cybersecurity incident to date – is to ensure the forensic investigation is conducted under legal privilege. In this section, we describe key considerations for conducting the investigation in a manner that maximises privilege protection. We then briefly discuss other considerations in overseeing an investigation being conducted by an external firm, including ensuring appropriate and efficient coordination between external forensic vendors and in-house IT staff, reviewing deliverables from the forensic vendors and, in the case of a payment card breach for which a payment card industry (PCI) forensic investigator (PFI) is engaged, navigating that investigation alongside the privileged investigation.

Protecting privilege over forensic work

In the United States, the attorney-client privilege protects confidential communications between clients (including employees and former employees of corporate clients) and their lawyers relating to the provision of legal advice. This privilege also applies to consultants retained by attorneys to help provide legal advice.⁴ Separately, the work-product doctrine protects documents and working papers prepared by lawyers, clients and their consultants and experts in anticipation of litigation.⁵

Although the forensic facts of an incident alone may not be privileged, and may ultimately need to be disclosed to third parties, maintaining attorney-client and work-product privilege protections over the underlying investigatory documents would allow a breached company to proceed in a manner that minimises its legal exposure.

⁴ *United States v. Kovel*, 296 F.2d 918, 921 (2d Cir 1961).

⁵ Privilege law may vary from jurisdiction to jurisdiction. We encourage those conducting breach response investigations outside the United States to further assess how applicable privileges may apply in this context in other jurisdictions.

A key enquiry into whether communications or work-product are privileged is determining whether the communication occurred or the work-product was generated for the purpose of providing legal advice or in anticipation of litigation – rather than in the ordinary course of business. Generally, this is a far more straightforward enquiry in the case of an independent forensic investigator (particularly one engaged and supervised by external counsel)⁶ than in the case of in-house IT and information security staff. A court may determine that the business role of IT and information security staff is to investigate cybersecurity incidents for the sake of the business (e.g., to remediate the breach), irrespective of legal or litigation considerations, such that no legal privilege protects underlying investigative material, even if the in-house staff report their findings to counsel.

Although several cases have affirmed the privilege protections applicable to third-party forensic consultants after a breach, there is a small but more recent body of case law suggesting that courts will not assume, by default, that the work-product and communications of a third-party forensic investigator in incident response is protected by the attorney-client privilege or work-product privilege.

Genesco, Inc v. Visa USA, Inc

In this 2014 case, the court found that the attorney-client privilege and work-product doctrine protected communications between Genesco's general counsel and Genesco's third-party forensic investigator, Stroz Friedberg, because the retainer agreement, an affidavit and other documents showed that the general counsel engaged Stroz Friedberg in anticipation of litigation to assist him in providing legal advice.⁷ Specifically, the general counsel's affidavit explained that he retained Stroz Friedberg after (1) the PFI had identified evidence of an intrusion, (2) he had conversations with external counsel regarding the legal ramifications of the intrusion (including the likelihood of litigation), (3) the company determined that he should conduct an investigation into the incident 'separate and apart from

6 Although some organisations rely on in-house counsel to run breach responses and engage or oversee forensic investigations, the argument that privilege applies in those cases can be more complicated than in the case of external counsel. This is because in-house lawyers may have a dual business and legal role, such that a company 'may face more difficulty showing that in-house counsel communications deserve privilege protection than showing that communications of outside lawyers who predominantly provide legal advice deserve protection'. Margaret A Dale and Yasmin M Emrani with Practical Law Institute Intellectual Property & Technology, 'Data Breaches: The Attorney-Client Privilege and the Work Product Doctrine', 3, Thomson Reuters [2017] [www.proskauer.com/insights/download-pdf/4949 (last accessed 5 April 2023)].

7 *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 FRD 168, 180–81 (MD Tenn 2014).

the investigation already being conducted by [the PFI] on behalf of [the card brands] for the purpose of providing legal advice to Genesco regarding the intrusion and in anticipation of litigation', and (4) counsel identified the need to retain a computer security consultant to assist in this investigation.⁸

In re Target Corporation Customer Data Security Breach Litigation

Target engaged two teams from Verizon to conduct forensic investigations: (1) one to advise the data breach task force, which was established at the direction of in-house and external counsel after a public announcement of the breach and after several class action lawsuits had been filed against Target, to 'educate Target's attorneys about aspects of the breach' so that counsel 'could provide Target with informed legal advice'; and (2) a team of investigators engaged in a PFI role.⁹ Target limited its privilege claims to the first team, which, per the engagement letter between external counsel and Verizon, was engaged to 'enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries'.¹⁰ The plaintiffs had argued that communications and documents prepared by Verizon were not privileged because 'Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued sales, discover its vulnerabilities and protect itself against future breaches'.¹¹ The court agreed with Target, finding that the data breach task force 'was focused not on remediation of the breach . . . but on informing Target's in-house and external counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in [pending and reasonably anticipated] litigation'.¹²

In re Experian Data Breach Litigation

Experian's external counsel retained the forensic consulting firm Mandiant.¹³ Experian said that 'the only purpose of [Mandiant's] report [wa]s to help [external counsel] provide legal advice to Experian regarding the attack'.¹⁴ The Mandiant report, which was finalised after Experian publicly announced the breach and

⁸ ibid., at 180.

⁹ *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522, 2015 WL 6777384, at *1 (D Minn 23 October 2015).

¹⁰ ibid., at *1 (internal citations omitted).

¹¹ id.

¹² ibid., at *3.

¹³ *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *2 (CD Cal 18 May 2017).

¹⁴ id.

the first claims against Experian had been filed, was provided by Mandiant to Experian's external counsel, who then provided it to in-house counsel.¹⁵ The plaintiffs argued that the report was not protected by the work-product doctrine because 'Experian had independent business duties to investigate any data breaches and it hired Mandiant to do exactly that after realizing its own experts lacked sufficient resources'.¹⁶ Although the court agreed Experian had those obligations, it found that the 'record . . . makes it clear that Mandiant conducted the investigation and prepared its report for [external counsel] in anticipation of litigation, even if that wasn't Mandiant's only purpose'.¹⁷ The court emphasised that the full report was not given to Experian's in-house incident response team, that external counsel instructed Mandiant to conduct the investigation and that the report would not have been prepared in substantially the same form or with the same content but for the anticipated litigation.¹⁸

Where privilege likely applies

In each of the above cases, the court found that privilege protections applied for reasons that would generally not be applicable to an in-house forensics team – because (1) the scope or purpose of work in the engagement letter emphasised that the work was being conducted to provide legal advice, (2) the forensic investigator reported to counsel, and (3) the work was performed not as part of the ordinary course of business investigation but to provide legal advice.

In re Premera Blue Cross Customer Data Security Breach Litigation

The holding in *In re Premera Blue Cross Customer Data Security Breach Litigation* was generally consistent with these principles, but reached the opposite conclusion. The company asserted attorney-client or work-product privilege over several categories of documents, including reports issued by a forensic investigator under the supervision of Premera's external counsel.¹⁹ Mandiant had been hired by Premera, prior to the discovery of the breach, to review the company's systems. During this investigation, Mandiant discovered malware. Premera then hired

15 id.

16 id.

17 id.

18 id.

19 *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F Supp 3d at 1230 (D Or 2017).

external counsel and, subsequently, Premera and Mandiant amended the statement of work (SOW) to shift supervision of Mandiant's work to external counsel but without changing the description of Mandiant's scope of work.²⁰

Although Premera argued that the situation changed after discovery of the breach, the court found that the unchanged scope of work in the SOW did not support the assertion. The court found that 'change of supervision, by itself, is not sufficient to render all the later communications and underlying documents privileged or immune from discovery as work-product'.²¹ Premera could not assert privilege over the reports, because it did not meet its burden to show that either (1) 'Mandiant changed the nature of its investigation at the instruction of external counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation' or (2) 'all of the underlying documents relating to the Mandiant reports were created because of anticipated litigation and "would not have been created in substantially similar form but for the prospect of litigation"'.²² However, specific documents or portions of documents could be withheld if those documents or portions of documents (1) were prepared to communicate with an attorney for the provision of legal advice, (2) contained counsel's own impressions in anticipation of litigation, (3) communicated factual information to counsel to prepare for litigation, or (4) involved a factual investigation done solely at the behest of counsel for the purpose of litigation and not under the original work scope.²³

In Re: Capital One Consumer Data Security Breach Litigation

A Virginia court reached a similar conclusion in *In Re: Capital One Consumer Data Security Breach Litigation*.²⁴ In that case, a magistrate judge held that a forensic report drafted by Mandiant – retained by Capital One's counsel – was not protected under the work-product doctrine.²⁵ In assessing whether the work-product privilege applied, the judge examined whether *Capital One* would have prepared the Mandiant report in question in a similar form but for the litigation. The court concluded the report did not meet the 'but for' test because Capital One had a pre-existing relationship with Mandiant through which Mandiant conducted

20 ibid., at 1245.

21 id.

22 ibid., at 1245–46.

23 ibid., at 1246.

24 MDL No. 1:19md2915 [AJT/JFA](ED VA) [*Capital One*].

25 The only issue in the *Capital One* case was whether the report was protected under the work product doctrine.

substantially similar work for Capital One business units. The magistrate judge declined to address whether Capital One waived any privilege by providing the Mandiant report to regulators (i.e., Office of the Comptroller of the Currency, Consumer Financial Protection Bureau).

Wengui v. Clark Hill PLC and In re Rutter's Data Security Breach Litigation

Some parties have attempted to avoid the outcome from *Capital One* by creating a dual-track approach to incident response investigations. This approach calls for an organisation's internal cybersecurity team to conduct its own investigation of an incident, with a forensic vendor engaged to support the business while a legally privileged investigation is pursued with an external vendor engaged by counsel. In practice, it remains unclear whether such an approach strengthens a litigant's privilege claim. In *Wengui v. Clark Hill PLC*,²⁶ the US District Court for the District of Columbia concluded that a forensic report commissioned by external counsel was not privileged, and not subject to the work-product doctrine, because it would have been commissioned by the business in any event. The defendant in *Wengui* argued that the business had a separate forensic vendor engaged, although the Court noted that the factual record showed that the business unit actually relied on the work commissioned by external counsel.

Whether litigation is indeed identifiable or impending has also affected a court's decision about whether work-product doctrine applied to forensic analysis. The US District Court for the Middle District of Pennsylvania found that a forensic report commissioned by external counsel was not protected by the work-product doctrine because, at the time of the investigation, the company did not know whether unauthorised activity had actually resulted in a data breach. In *In re Rutter's Data Security Breach Litigation*,²⁷ a company that had received alerts suggesting unauthorised activity hired external counsel who, in turn, contracted with Kroll Cyber Security, LLC (Kroll) to determine the character and scope of the incident. The Court found that Kroll's resulting report was not covered by the work-product doctrine because the company did not have a 'unilateral belief that litigation would result at the time it requested the Kroll Report'; it was merely investigating whether a breach had actually occurred. The Court looked at the scope of work in the contract with Kroll, the delivery of the report to the company

²⁶ No. 19-3195 (DDC, 12 January 2021).

²⁷ Civ. A. No. 1:20-CV-382 (M.D. Pa. 22 July 2021).

and not counsel, and testimony from company individuals to conclude that it could not be said that the 'primary motivating factor' behind the Kroll report was to aid in 'identifiable or impending litigation'.²⁸

The rulings in *Capital One, Clark Hill* and *Rutter's* emphasise the need for carefully approaching privilege issues to ensure the protected status of investigation work-product and communications.

Other documents

Premera helps to shed some light on how courts may view the privilege status of other documents, beyond forensic investigators' reports and working papers, created in the course of a privileged breach response. Premera asserted privilege over a number of documents, including (1) drafts of documents written or edited by counsel, and (2) documents drafted by non-legal personnel at the request of counsel but not created by or sent to counsel. The first category included documents that were drafted by and sent to or from non-attorneys but included edits from counsel, or were drafted by counsel and incorporated edits from non-attorneys.²⁹ For some, Premera asserted privilege only over the drafts. The second category included documents with information relating to 'technical aspects of the breach and its mitigation, company policies, public relations and media matters, and remediation activities' and were prepared either by Premera personnel or third-party vendors retained by external counsel.³⁰

The court found that only some of these documents were protected by the attorney-client privilege.³¹ For example, documents containing edits by an attorney communicating legal advice would be protected attorney-client communications, as long as the edit was not done solely with a business purpose in mind.³² Similarly, communications relating to these documents sent to or from counsel seeking or providing actual legal advice, such as about possible legal consequences of proposed text or a contemplated action, would be privileged.³³ However, drafts (and communications about them) in which Premera 'was required as a business

28 The court in this case also considered whether the materials were protected under the attorney-client privilege, but found that the report and communications between Kroll and the company were either factual or, where advice and tactics were involved, did not include legal input.

29 *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, op. cit. note 19, at 1240–41.

30 *ibid.*, at 1242.

31 *ibid.*, at 1241.

32 *ibid.*, at 1242.

33 *ibid.*, at 1244.

to prepare [the document] in response to the data breach' (e.g., press releases and breach notice letters) were not automatically privileged by virtue of '[t]he fact that Premera planned eventually to have an attorney review those documents or that attorneys may have provided initial guidance as to how Premera should draft [them]'.³⁴ Because this includes documents the company 'would have prepared regardless of any concern about litigation, . . . [p]lacing them under the supervision of external counsel and then labelling all communications relating to them as privileged does not properly establish an attorney-client privilege'; instead, '[t]he focus of the privilege must be the purpose for which a document was created'.³⁵

Companies must also take care in the aftermath of an investigation to ensure that the privilege remains protected. In *Leibovic v. United Shore Financial Services, LLC*, the court found that United Shore had waived privilege for an investigation by disclosing 'the details' of the results in an interrogatory response.³⁶ United Shore's lawyers hired Navigant (a management consultancy firm) to assist them in an internal investigation. Although the court did not specify what United Shore disclosed in the interrogatory response, it found that the response 'went beyond providing factual information regarding the existence of the investigation and retention of Navigant[, . . . but] included details regarding Navigant's conclusions'.³⁷ The court placed significant emphasis on the fact that United Shore had disclosed the details of Navigant's conclusions during and in support of litigation. This is consistent with the overall principles that litigants cannot use privilege as 'a shield and a sword'.³⁸

34 ibid., at 1241. While maintaining privilege over public relations vendors and efforts is beyond the scope of this chapter, it can be key in breach response work. For further guidance on maintaining privilege over public relations documents generally, see Jeffrey Schomig, 'Keeping PR Strategy Communications Privileged: Part 1', Law360 (1 February 2019) and Jeffrey Schomig, 'Keeping PR Strategy Communications Privileged: Part 2', Law360 (4 February 2019) (www.wilmerhale.com/en/insights/publications/20190201-keeping-pr-strategy-communications-privileged-part-1 and www.wilmerhale.com/en/insights/publications/20190204-keeping-pr-strategy-communications-privileged-part-2 (last accessed 5 April 2023)).

35 *In re Premera*, 296 F Supp 3d at 1241–42.

36 *Leibovic v. United Shore Fin. Servs.*, LLC, No. 15-12639, 2017 WL 3704376 (ED Mich 28 August 2017), mandamus denied by *In re: United Shore Fin. Servs.*, LLC, No. 17-2290, 2018 WL 2283893 (6th Cir 3 January 2018).

37 ibid., at *3.

38 *In re: United Shore*, No. 17-2290 2018 WL 2283893, at *2 (quoting *United States v. Bilzerian*, 926 F 2d at 1295, 1292 (2d Cir 1991)).

As exhibited by these cases, entities investigating a breach should take appropriate steps both in the engagement phase and during an investigation to maximise the likelihood that communications and forensic vendor work-product will be protected by privilege. Third-party forensic experts generally should be engaged by external counsel. The contract, and the SOW, should expressly make it clear whether the forensic work is being performed to assist counsel in providing legal advice in anticipation of potential litigation or regulatory enquiries, or both. During the course of the investigation, attorneys generally should be included in emails and, where practical, in correspondence between the company and the forensic investigators. All communications, working papers and deliverables should be labelled as privileged and, ideally, any reports coming from third-party providers should be delivered to external counsel. Attorneys should be actively engaged in directing the investigator's work.

Coordinating internal IT and external forensic teams

The main concern companies often express about using third-party investigators is that the investigation will be slower and more cumbersome than an investigation conducted by in-house teams. IT and information security personnel are often particularly concerned about vendors' lack of knowledge of the relevant systems and people, as well as delays in the early days of an investigation that may occur as vendors deploy their people and tools.

These concerns can be mitigated by engaging a forensic vendor prior to an incident occurring. Having this relationship in place, with contracts already negotiated and designated points of contact, allows forensic investigators to 'hit the ground running' when they receive notice of a breach. The more fully this relationship is developed before a breach (e.g., through discussions about the overall system architecture, advanced deployment of tools and developing a rapport), the quicker the external team can begin its incident response following a breach and the more streamlined the process will be as it progresses. Often, these pre-negotiated arrangements are made between external counsel, the forensic vendor and the company (in the form of a three-party agreement), with the knowledge that the services will be activated when an incident occurs for the purposes of assisting external counsel in the provision of legal advice to the company.

In addition to preparations in advance, forensic investigators have the most success in launching their investigation in an expeditious manner when they can work with the in-house team. By leveraging their knowledge of systems, networks and people, the vendor team can deploy its tools and obtain the artefacts and data it needs quickly.

Reporting considerations

Many companies assume, as standard, that they want the results of an investigation to be documented in a formal written report. However, this may not be necessary or otherwise desirable in all situations. Companies should consider the necessity for such a report prior to deciding whether to commission a formal report, including considering the possibility that a report may not be shielded, in whole or in part, by privilege.

A company should consider whether external counsel should direct the report, and perform any reviews of it, before providing it to the company. External counsel should ensure the accuracy of the underlying descriptions of the incident as part of providing legal advice to the company. The goal should be to ensure that the report is straightforward and factual, without unnecessarily loaded terms or graphics. To the extent that the company has taken containment and remediation steps, these steps should be validated by the forensic investigator and included in the report. Once the report is finalised, its circulation should be limited. For example, the company should consider whether only certain parts of the report should be shared with the in-house IT team.

Parallel investigations by PCI forensic investigators

In the event of a suspected compromise of payment card information, one or more payment card brands may direct the breached entity to engage a PFI to conduct an investigation and report its findings to the card brands. PFIs must issue reports using card brand-approved templates.³⁹ In the reports, the PFI will describe whether and how the PCI was compromised, confirm the date of containment, recommend further security enhancements, and identify specific areas of security non-compliance and whether that non-compliance caused or contributed to the breach.

³⁹ 'Payment Card Industry (PCI) Data Security Standard: PFI Preliminary Incident Response Report – Template for PFI Preliminary Incident Response Report', Version 2.2 (August 2017) (https://www.pcisecuritystandards.org/documents/PFI_Preliminary_Incident_Response_Report_v2.2.pdf?agreement=true&time=1552267715716 [last accessed 5 April 2023]); 'Payment Card Industry (PCI) Data Security Standard: Final PFI Report – Template for Final PFI Report', Version 2.1 (August 2017) (https://www.pcisecuritystandards.org/documents/Final_PFI_Report_v2.1.pdf?agreement=true&time=1552267715728 [last accessed 5 April 2023]).

This report will be provided to the card brands and will form the basis of any card brand fines. The card brands will also typically seek regular telephonic updates from the PFI. As such, PFI investigations are not protected by privilege. It is important, therefore, to navigate the relationship between the company and the PFI strategically and effectively. This requires:

- working throughout the investigation to establish goodwill between the company (and its counsel) and the PFI;
- having the company's privileged investigator collect the same evidence and follow similar forensic leads as the PFI so that the company can understand the technical facts underlying the PFI's findings; and
- managing and segregating the PFI's investigation (as well as communications with the PFI and the card brands) from the company's privileged investigation so as to avoid potentially compromising the privilege.

Ransomware considerations

Ransomware attacks have become prevalent in recent years. Although ransomware incident response follows a similar arc to general incident response, there are a few unique considerations, including threat actor communication and the 'pay, no-pay' decision. Companies facing a ransomware or extortion event will need to take special incident response coordination steps, particularly if there is a potential business need to acquiesce to a payment demand. These types of attacks often prompt victim organisations to engage third-party experts to assist with interacting with a threat actor, evaluating threat actor demands, and potentially facilitating payment. Although the official position of federal law enforcement on ransomware attacks is to report the incident and refrain from paying a ransom, the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) have also asserted that the decision to pay a ransom is a business issue that companies must evaluate in light of the overall risks associated with an incident. US Government guidance states that '[a]ny entity infected with ransomware should contact law enforcement immediately', that 'there are serious risks to consider before paying the ransom' and that the government 'does not encourage paying a ransom to criminal actors'.⁴⁰

⁴⁰ See US Government, 'How to Protect Your Networks from Ransomware', at 5 (www.justice.gov/criminal-ccips/file/872771/download [last accessed 5 April 2023]); see, also, Federal Bureau of Investigation, 'Incidents of Ransomware on the Rise: Protect Yourself and Your Organization' [29 April 2016] (www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise [last accessed 5 April 2023]).

Where a payment is contemplated, it is important to engage with in-house and external counsel, to report the incident to law enforcement in advance, and to seek assistance from external counsel to evaluate regulatory risks. Ransomware and extortion payments present special regulatory concerns that must be carefully evaluated. In September 2021, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory addressing risks associated with facilitating ransomware payments: the Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The Advisory identifies regulatory risks associated with OFAC's strict liability regime:

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC.⁴¹

The OFAC guidance suggests that risk associated with payment may be mitigated by, among other things, cooperation with law enforcement. The guidance states that:

OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response. OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.⁴²

41 The Department of the Treasury, Office of Foreign Assets Control [OFAC], 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (21 September 2021) ('Updated OFAC Ransomware Advisory'), at 4 (<https://ofac.treasury.gov/media/912981/download?inline>) [last accessed 5 April 2023]).

42 *ibid.*, at 5.

Although explicit regulatory guidance on ransom payment is limited, given the prevalence of ransomware attacks, other regulators and government bodies have issued ransomware guidance, including the Federal Trade Commission⁴³ and the New York Department of Financial Services.⁴⁴ As ransomware attacks increase in frequency and breadth, we expect regulators (both within and outside law enforcement) will continue to pay close attention to how companies respond to such attacks.

Coordinating with law enforcement

In the wake of a cyber incident, many companies share information with law enforcement agencies, often publicly touting this coordination in public statements about the incident. In this section, we describe both the advantages and limitations of sharing with law enforcement. Next, we describe some of the logistical considerations in providing information to law enforcement. Finally, we describe some of the protections available to companies sharing information under the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and how to maximise available protections when sharing with law enforcement.

Advantages and limitations to sharing with law enforcement

Sharing information with law enforcement offers a number of advantages. Regulators typically look favourably on this form of information-sharing, and coordination with law enforcement may be particularly important when responding to a ransomware event for reasons noted above.⁴⁵ In some circumstances, this can also arm law enforcement agencies with information that is critical to bringing the perpetrator to justice. In recent ransomware incidents, law enforcement has been able to partner with victim companies to trace ransomware payments and,

43 See FTC, Cybersecurity for Small Business, 'Ransomware' (<https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last accessed 5 April 2023)).

44 See New York State, Department of Financial Services, Industry Guidance, 'Ransomware Guidance' (30 June 2021) (https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance (last accessed 5 April 2023)).

45 See, e.g., 'Updated OFAC Ransomware Advisory', op. cit. note 41; and U.S. Treasury, Financial Crimes Enforcement Network, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments', FIN-2020-A006 (1 October 2020) (<https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf> (last accessed 5 April 2023)).

in some cases, claw back payments.⁴⁶ Cooperating with law enforcement agencies is also typically viewed positively, both by customers and as a reputational matter. In certain limited circumstances, notifying law enforcement can also provide companies with an opportunity to delay notice to consumers if notification could impede a law enforcement investigation. In such circumstances, the company should obtain a written request from the relevant law enforcement agency.

That said, in deciding whether and how to share information with law enforcement, it is important to maintain realistic expectations. For example, except in exceedingly rare circumstances, law enforcement will not perform a forensic investigation for the breached company. It is also rare for law enforcement to provide the reporting company with information about a suspected perpetrator of the breach, or to immediately take legal action against a suspected perpetrator. Although the DOJ is increasingly bringing charges against major cyber criminals and nation-state actors, these charges often come years after the fact, and frequently are the culmination of investigations into multiple incidents committed by the same or related actors. In these cases, law enforcement typically does its best to anonymise the victim companies.

Logistics of sharing information

Once a company has decided to engage with law enforcement, a number of practical considerations come into play. These include the following:

- *Who:* In the United States, cyber crimes are generally investigated by the Secret Service and the FBI. The Secret Service is generally responsible for investigating financial crimes and fraud (such as those involving theft of payment card data and, increasingly, incidents in which ransomware payments are made)⁴⁷ while the FBI's authorities are broader. Companies should develop

46 See, e.g., U.S. Department of Justice (DOJ), News Release, 'Justice Department Seizes and Forfeits Approximately \$500,000 from North Korean Ransomware Actors and their Conspirators' (19 July 2022) (<https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors> (last accessed 5 April 2023)); see, also, DOJ, News Release, 'Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside' (7 June 2021) (<https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside> (last accessed 5 April 2023)).

47 See, e.g., US Secret Service, 'Our Investigative Mission' (<https://www.secretservice.gov/investigation/> (last accessed 5 April 2023)); see, also, US Secret Service, 'Secret Service Announces the Creation of the Cyber Fraud Task Force' (9 July 2020), sixth paragraph (<https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force> (last accessed 5 April 2023)).

relationships with relevant law enforcement officials in advance of a breach. Both agencies maintain regional task forces throughout the country.⁴⁸ In addition to reporting to law enforcement, companies can also upload cyber threat indicators to the US Department of Homeland Security (DHS) online portal.⁴⁹

- *When:* Companies should contact law enforcement as soon as possible, if appropriate.
- *What:* Law enforcement is typically interested in hackers' tactics, techniques and procedures. Companies should share this information, to the extent that it is available, including 'indicators of compromise' (i.e., lists of suspicious internet protocol (IP) addresses, domains or accounts; malware hashes, signatures and files; and attacker tools). Law enforcement may also seek copies of compromised systems or raw log data; companies should consult their legal counsel before sharing such data.
- *How:* Typically, data is shared either digitally or in hard copy. Often the FBI will request that the company, or the company's external counsel, submit a report via the Internet Crime Complaint Center (IC3). Sometimes, law enforcement may request a briefing, possibly with the forensic investigator. In those circumstances, companies should work with legal counsel to ensure appropriate steps are taken to preserve privilege. All communications with law enforcement agencies should be tracked and logged. Written communications should be marked to invoke all available protections (discussed below).

⁴⁸ See DOJ, Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, 'Best Practices for Victim Response and Reporting of Cyber Incidents', Version 2.0 (September 2018) (www.justice.gov/criminal-ccips/file/1096971/download [last accessed 5 April 2023]).

⁴⁹ Cybersecurity & Infrastructure Security Agency (CISA), 'CISA Cyber Threat Indicator and Defensive Measure Submission System' (www.us-cert.gov/forms/share-indicators [last accessed 5 April 2023]).

Cybersecurity Information Sharing Act

In 2015, the United States enacted CISA 2015, which provides authorisation and liability protection for cybersecurity information-sharing.⁵⁰ Specifically, the Act authorises private entities to share 'cyber threat indicators'⁵¹ and 'defensive measures'⁵² with federal entities, for 'a cybersecurity purpose,'⁵³ as long as the information is shared in a manner consistent with the Act, including a variety of provisions intended to protect personal information.⁵⁴

Pursuant to CISA 2015, the DHS and DOJ have published guidance documents to help companies understand the Act and how to share properly.⁵⁵ CISA 2015 also required the DHS to establish an online portal for the US Government to receive cyber threat indicators from the private sector.⁵⁶ However, the process created by the DHS does not limit or prohibit the sharing of information associated with known or suspected criminal activity or of cyber threat indicators with federal entities in support of law enforcement investigations.⁵⁷

-
- 50 The Cybersecurity Act of 2015 was enacted as Division N in the Fiscal Year 2016 omnibus spending bill. Title I of the Act, commonly referred to as the Cybersecurity Information Sharing Act (CISA 2015), includes authorisation and liability protections for cybersecurity monitoring, information-sharing and use of defensive measures. CISA 2015 has been codified in the US Code at 6 U.S.C. §§1501 to 1510.
- 51 CISA 2015 defines a 'cyber threat indicator' broadly, to include, among other things, 'information that is necessary to describe or identify' malicious reconnaissance, a security vulnerability, a method of defeating a security control or exploitation of a security vulnerability, malicious cyber command and control, or the actual or potential harm caused by an incident. See 6 U.S.C. §1501(6)(A) to (H).
- 52 ibid., §1501(7)(A).
- 53 ibid., §1501(4).
- 54 ibid., §§1503(c) and (d), 1504, 1505(b).
- 55 See, e.g., The Department of Homeland Security (DHS) and DOJ, 'Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015' (Oct 2020) [DHS/DOJ Guidance] (https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf [last accessed 5 April 2023]); see, also, DHS/DOJ Guidance, 'Annex 2: Cybersecurity Information Sharing Act of 2015 – Frequently Asked Questions' (DHS/DOJ FAQ).
- 56 6 U.S.C. §1504(c).
- 57 ibid., §1504(c)(1)(e).

CISA 2015 does not include requirements to share with any particular agency. Rather, it authorises sharing with any federal entity. However, which mechanism is chosen for sharing might affect the availability of liability protections.⁵⁸

Liability protections are most clearly available when a non-federal entity shares cyber threat indicators and defensive measures with the DHS.⁵⁹ CISA 2015 provides liability protection against suits for certain sharing of cyber threat indicators and defensive measures with the federal government if the information 'is shared in a manner that is consistent with section 105(c)(1)(B)'.⁶⁰ In turn, Section 105(c)(1)(B) provides that sharing through the DHS-established portal 'shall . . . be the process by which the Federal Government receives cyber threat indicators and defensive measures'.⁶¹

Agency guidance acknowledges, however, that Paragraphs (i) and (ii) of Section 1504(c)(1)(B) of CISA 2015 describe two additional means of liability-protected sharing.⁶² These paragraphs provide two exceptions to the requirement that the DHS portal 'shall be the process' for sharing with the federal government. These include:

- (i) . . . communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and*
- (ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.*⁶³

58 DHS/DOJ Guidance [op. cit. note 55], at 11 ('The [Cybersecurity Information Sharing] Act authorizes non-federal entities to share cyber threat indicators and defensive measures with Federal entities . . . specifically . . . through the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, which is operated by DHS . . . *How a non-Federal entity shares cyber threat indicators and defensive measures with the Federal Government affects the types of protections the non-Federal entity receives under CISA 2015.*' [emphasis added]).

59 id. ('when such sharing is conducted with the Federal government through the DHS capability and process, or as otherwise provided for by section 1504(c)(1)(B), it also receives additional liability protection under section 1505(b)(2)').

60 CISA 2015, Section 106(b)(2) [codified at 6 U.S.C. §1505(b)(2)].

61 ibid., at Section 105(c)(1)(B) [codified at 6 U.S.C. §1504(c)(1)(B)].

62 DHS/DOJ Guidance [op. cit. note 55], at 16.

63 CISA 2015, Section 105(c)(1)(B)(i) and (ii) [codified at 6 U.S.C. §1504(c)(1)(B)(i) and (ii)].

As agency guidance explains:

[Section 1504(c)(1)(B)(i)] would apply when a non-Federal entity first shares a cyber threat indicator with the DHS capability and process or a regulator as permitted by section 1504(c)(1)(B)(ii) discussed below, and then engages in communications with a Federal entity regarding that previously shared indicator. . . .

[S]ection 1504(c)(1)(B)(ii) also permits communications between a regulated non-Federal entity and its federal regulatory authority regarding a cybersecurity threat.⁶⁴

Other than the three categories of sharing under Section 105(c)(1)(B), sharing with the federal government is authorised but not protected from liability.⁶⁵ However, liability protection is only one of the protections under CISA 2015 and, arguably, it is limited in scope, particularly when it comes to sharing information

-
- 64 DHS/DOJ Guidance (op. cit. note 55), at 16. See, also, DHS/DOJ FAQ (op. cit. note 55), at 28 ('Section 1504 contains two exceptions that authorize sharing cyber threat indicators or defensive measures with Federal agencies other than through the DHS capability and process. Liability protection is available for private entities that share information directly with other Federal agencies under those provisions. The first exception . . . provides for sharing . . . "regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator." Sharing such information can therefore receive liability protection so long as the sharing is consistent with the other requirements in section 1505 . . . So, [while] CISA 2015 is not primarily designed to address sharing cyber threat information with law enforcement[. . . it] does provide liability protection for sharing cyber threat indicators or defensive measures with law enforcement, if the indicator or defensive measure is shared with law enforcement as part of a communication regarding a cyber threat indicator that was previously shared by the private entity through the DHS capability and process').
- 65 DHS/DOJ Guidance (op. cit. note 55), at 16 ('In addition to the liability protections . . . , the Act provides other protection to sharing entities and protects information shared in accordance with the Act. Sharing with the Federal government other than in a manner consistent with section 1504(c)(1)(B) does not receive section 1505(b)'s liability protection; however, such sharing is eligible for all of the other protections furnished by the Act, just the same as sharing conducted with DHS under section 1504(c), so long as the sharing otherwise adheres to CISA 2015's requirements (e.g., removal of certain personal information pursuant to section 1503(d)(2), sharing cyber threat indicators or a defensive measure, and sharing for a cybersecurity purpose).').

with law enforcement agencies.⁶⁶ CISA 2015's numerous other protections, however, would be available regardless of the federal entity receiving the shared cyber threat indicators and defensive measures (as long as the other requirements under CISA 2015 are met).⁶⁷ These include:

- *No waiver of privilege*: Sharing cyber threat indicators or defensive measures with the federal government under CISA 2015 'shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection'.⁶⁸ This includes state or federal privileges and protections, notably including the attorney-client and work-product privileges.⁶⁹
- *Treated as proprietary*: Shared information 'shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated'.⁷⁰ This provision triggers a variety of protections under federal law for the handling of sensitive business information.
- *Protections under the Freedom of Information Act (FOIA) and the Critical Infrastructure Information Act (CIIA)*: Information shared is protected from disclosure under the FOIA and any state, tribal or local parallels.⁷¹ Shared information will also be 'deemed voluntarily shared and exempt from disclosure' under the CIIA.⁷²

66 See DHS/DOJ FAQ (op. cit. note 55), at 30 ('Sharing cyber threat information with law enforcement generally does not raise liability issues, particularly in the context of reporting an actual or attempted crime . . . In short, CISA 2015 supplements—but does not supplant—other measures that already protect private entities that report crimes, including restrictions on disclosing investigative material.').

67 DHS/DOJ Guidance (op. cit. note 55), at 16 ('such sharing is eligible for all of the other protections furnished by the Act, just the same as sharing conducted with DHS under section 1504(c), so long as the sharing otherwise adheres to CISA 2015's requirements (e.g., removal of certain personal information pursuant to section 1503(d)(2), sharing cyber threat indicators or a defensive measure, and sharing for a cybersecurity purpose').

68 6 U.S.C. §1504(d)(1).

69 DHS/DOJ FAQ (op. cit. note 55), at 9.

70 6 U.S.C. §1504(d)(2).

71 ibid., §1504(d)(3)(B).

72 ibid., §1504(d)(3)(A).

- *Limitations on government use:* Shared information may only be used for the particular cybersecurity, law enforcement and defence purposes described in CISA 2015.⁷³ Further, no government entity may use such information for regulatory action, including a regulatory enforcement action.⁷⁴

73 ibid., §1504(d)(5)(A).

74 ibid., §1504(d)(5)(D)(i). However, this information may, consistent with regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems. ibid., §1504(d)(5)(D)(ii)(I). According to the DHS/DOJ Guidance, 'CISA 2015's legislative history states that congressional drafters viewed this as a narrow exception to ensure that government agencies with regulatory authority understand the current landscape of cyber threats and those facing the particular regulatory sector over which they have cognizance' (DHS/DOJ Guidance (op. cit. note 55), at 18).