Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Leah Schloss

Maury Riggan

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact Natalie.Clarke@lbresearch.com

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

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 978-1-83862-223-7

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

Acknowledgements

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

RICHARD DENATALE

HUNTON ANDREWS KURTH 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 third 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.

Contents

Part I

A 'Typical' Cyber Investigation

3

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

Benjamin A Powell, Leah Schloss and Jason C Chipman[1]

Incident response requires an immediate, coordinated effort to gather the facts and execute an incident response plan that enables a company reacting to a 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:

- conducting a forensic investigation to understand what has occurred, how it occurred and what, if any, damage was caused to the confidentiality, availability or integrity of company systems or data;
- preserving evidence;
- containing and remediating the incident;
- preparing for and complying with any notice requirements to regulators, consumers or other third parties;
- 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;
- preparing and monitoring for possible litigation, including preserving documents and monitoring dockets;
- briefing insurance carriers; and
- assuring auditors that IT controls remain sound.

The details of these specific 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

1 Benjamin A Powell and Jason C Chipman are partners and Leah Schloss is a counsel at Wilmer Cutler Pickering Hale and Dorr LLP.

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 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 and external vendors (e.g., law firms, forensic vendors) should form the core incident response team. Ideally, this should be addressed in the company's incident response policy (as discussed in Chapter 2) but some incident response teams may reasonably include some 'optional' members depending on the circumstances (such as the head of a particular affected business unit, 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 tasks. Each work stream should be assigned to designated in-house and external personnel, such as through a matrix identifying each 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 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. 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.

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.

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

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 to 15 (Aug 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf ('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', 1 (Sep 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf (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').

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]

While 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.

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 IT security staff. A court may determine that the business role of IT and IT 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

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.

6 While 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), https://www.proskauer.com/insights/download-pdf/4949.

legal privilege protects underlying investigative material, even if the in-house staff report their findings to counsel.

Several recent cases have affirmed the privilege protections applicable to third-party forensic consultants after a breach.

Genesco, Inc v. Visa USA, Inc

In this 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 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) a team 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 outside 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]

---

7 *Genesco, Inc. v. Visa U.S.A., Inc*., 302 FRD 168, 180 to 181 (MD Tenn 2014).

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 Oct 2015).

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

11 ibid.

12 ibid., at *3.

In re Experian Data Breach Litigation

Experian's external counsel retained the forensic 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 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] While 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]

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.

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 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]

While 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

13 *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *2 (CD Cal 18 May 2017).
14 ibid.
15 ibid.
16 ibid.
17 ibid.
18 ibid.
19 *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F Supp 3d at 1230 (D Or 2017).
20 ibid., at 1245.

later communications and underlying documents privileged or immune from discovery as work-product'.[21] Because Premera did not meet its burden to show that either (1) 'Mandiant changed the nature of its investigation at the instruction of outside 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"', it could not assert privilege over the reports.[22] However, specific documents or portions of documents could be withheld if they (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]

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 potentially even 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. Attorneys should be actively engaged in directing the investigator's work.

Premera also helps 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 drafted by counsel and incorporated edits from non-attorneys.[24] 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.[25]

The court found that only some of these documents were protected by attorney–client privilege.[26] 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.[27] Similarly, communications relating to these docu-

21 ibid.
22 ibid., at 1245 to 1246.
23 ibid., at 1246.
24 ibid., at 1240 to 1241.
25 ibid., at 1242.
26 ibid., at 1241.
27 ibid., at 1242.

ments 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.[28] However, drafts (and communications about them) in which Premera 'was required as a business 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].'[29] Because this includes documents the company 'would have prepared regardless of any concern about litigation, . . . [p]lacing them under the supervision of outside 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'.[30]

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.[31] United Shore's lawyers hired Navigant to assist them in an internal investigation. While 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'.[32] 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'.[33]

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 IT 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.

---

28 ibid., at 1244.

29 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 Feb 2019) and Jeffrey Schomig, 'Keeping PR Strategy Communications Privileged: Part 2', *Law360* (4 Feb 2019), https://www.wilmerhale.com/en/insights/publications/20190201-keeping-pr-strategy-communications-privileged-part-1 and https://www.wilmerhale.com/en/insights/publications/20190204-keeping-pr-strategy-communications-privileged-part-2.

30 *In re Premera*, 296 F Supp 3d at 1241 to 1242.

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

32 ibid., at *3.

33 *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)).

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, 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.

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.[34] In the reports, the PFI will describe whether and how 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.

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

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

such, PFI investigations are not protected by privilege. It is therefore important 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.

Coordinating with law enforcement

In the wake of a cyber incident, many companies share information with law enforcement, 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 (CISA) 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.[35] In rare circumstances, this can also arm law enforcement with information that is critical to bringing the perpetrator to justice. Cooperating with law enforcement is also typically viewed positively 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 law enforcement.

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. While the US Department of Justice (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.

35 See, e.g., Mark Eichorn, 'If the FTC comes to call', FTC Business Blog (20 May 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if -ftc-comes-call.

Logistics of sharing information

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

- Who. In the United States, cyber crimes are generally investigated by the Secret Service and the Federal Bureau of Investigations (FBI). The Secret Service is generally responsible for investigating financial crimes and fraud (such as those involving theft of payment card data)[36] while the FBI's authorities are broader. Companies should develop relationships with relevant law enforcement officials in advance of a breach. Both agencies maintain regional task forces throughout the country.[37] In addition to reporting to law enforcement, companies can also upload cyber threat indicators to the US Department of Homeland Security (DHS) online portal.[38]
- 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 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. 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 should be tracked and logged. Written communications should be marked to invoke all available protections (discussed below).

36 US Secret Service, 'The Investigative Mission', https://www.secretservice.gov/investigation/ (last visited 19 Mar 2019) ('Today the agency's investigative mission has evolved from enforcing counterfeiting laws to safeguarding the payment and financial systems of the United States from a wide range of financial and computer-based crimes.').

37 See Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, 'Best Practices for Victim Response and Reporting of Cyber Incidents', Version 2.0, Department of Justice [DOJ] (Sep 2018), https://www.justice.gov/criminal-ccips/file/1096971/download.

38 'DHS Cyber Threat Indicator and Defensive Measure Submission System', https://www.us-cert.gov/forms/share-indicators.

Cybersecurity Information Sharing Act

In 2015, the United States enacted CISA, which provides authorisation and liability protection for cybersecurity information-sharing.[39] Specifically, CISA authorises private entities to share 'cyber threat indicators'[40] and 'defensive measures'[41] with federal entities, for 'a cybersecurity purpose,'[42] as long as the information is shared in a manner consistent with CISA, including a variety of provisions intended to protect personal information.[43]

Pursuant to CISA, the DHS and DOJ have published guidance documents to help companies understand CISA and how to share properly.[44] CISA also required the DHS to establish an online portal for the US Federal Government to receive cyber threat indicators from the private sector.[45] However, the process created by the DHS does not limit or prohibit sharing information associated with known or suspected criminal activity or the sharing of cyber threat indicators with federal entities in support of law enforcement investigations.[46]

CISA 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.[47]

Liability protections are most clearly available when a non-federal entity shares cyber threat indicators and defensive measures with the DHS.[48] CISA 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)'.[49] In turn, Section 105(c)(1)(B) provides that sharing through the

---

39 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), includes authorisation and liability protections for cybersecurity monitoring, information-sharing and use of defensive measures. CISA has been codified in the US Code at 6 USC Sections 1501 to 1510.

40 CISA 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 USC Section 1501(6)(A) to (H).

41 ibid., Section 1501(7)(A).

42 ibid., Section 1501(4).

43 ibid., Sections 1503(c) and (d), 1504, 1505(b).

44 See, e.g., 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', 6 (15 Jun 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf [hereinafter, DHS/DOJ Guidance]; DHS and DOJ, 'Cybersecurity Information Sharing Act – Frequently Asked Questions', https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf [hereinafter, DHS/DOJ FAQ].

45 6 USC Section 1504(c).

46 ibid., Section 1504(c)(1)(e).

47 DHS/DOJ Guidance (see footnote 44), at 10 ('[CISA] 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 under [CISA], which is operated by DHS . . . . *The manner in which information is shared affects the protections private entities receive for sharing* cyber threat indicators and defensive measures.' (emphasis added)).

48 ibid. ('[S]haring receives liability protections under 106(b)(2) when conducted with the Federal Government through the DHS capability and process, or as otherwise permitted under section 105(c)(1)(B).')

49 CISA Section 106(b)(2) (codified at 6 USC Section 1505(b)(2)).

DHS-established portal 'shall . . . be the process by which the Federal Government receives cyber threat indicators and defensive measures'.[50]

Agency guidance acknowledges, however, that 'Sections 105(c)(1)(B)(i) and (ii) of CISA describe two additional means of liability-protected sharing'.[51] These Sections 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.'[52] As agency guidance explains:

> *[Section 105(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 105(c)(1)(B)(ii) discussed below, and then engages in communications with a federal entity regarding that previously shared indicator. . . .*
>
> *[S]ection 105(c)(1)(B)(ii) also permits communications between a regulated non-federal entity and its Federal regulatory authority regarding a cybersecurity threat.*[53]

Other than the three categories of sharing under CISA Section 105(c)(1)(B), sharing with the Federal Government is authorised but not protected from liability.[54] However, liability protection is only one of the protections under CISA and, arguably, it is limited in scope, particularly when it comes to sharing information with law enforcement.[55] CISA's numerous

---

50 ibid., at Section 105(c)(1)(B) (codified at 6 USC Section 1504(c)(1)(B)).

51 DHS/DOJ Guidance (see footnote 44), at 15. See also DHS/DOJ FAQ (see footnote 44), at 2 to 3.

52 CISA Section 105(c)(1)(B)(i) and (ii) (codified at 6 USC Section 1504(c)(1)(B)(i) and (ii)).

53 DHS/DOJ Guidance (see footnote 44), at 15. See also DHS/DOJ FAQ (see footnote 44), at 3 ('Section 105 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 [CISA] . . . So, [while] CISA 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').

54 DHS/DOJ Guidance (see footnote 44), at 10 ('In addition to sharing conducted as provided under section 105(c)(1)(B), section 104(c) also authorizes other sharing of cyber threat indicators and defensive measures with any federal entity, including sector-specific agencies; however, sharing that is not consistent with section 105(c)(1)(B) *will not receive liability protection under [CISA]*, even if a federal entity receiving the information shares it with DHS immediately upon receipt.' (emphasis added)).

55 See DHS/DOJ FAQ (see footnote 44), at 4 ('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 supplements—but does not supplant—other measures that already protect private entities that report crimes, including restrictions on disclosing investigative material.').

other protections, however, would be available regardless of the federal entity receiving the shared cyber threat indicators and defensive measures (as long as CISA's other requirements are met).[56] These include:

- No waiver of privilege. Sharing cyber threat indicators or defensive measures with the Federal Government under CISA 'shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection'.[57] This includes state or federal privileges and protections, notably including the attorney–client and work-product privileges.[58]
- Treated as proprietary. Shared information 'shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated'.[59] This provision triggers a variety of protections under federal law for the handling of sensitive business information.
- FOIA and CIIA protections. Information shared is protected from disclosure under the Freedom of Information Act and any state, tribal or local parallels.[60] Shared information will also be 'deemed voluntarily shared and exempt from disclosure' under the Critical Infrastructure Information Act.[61]
- Limitations on government use. Shared information may only be used for particular cybersecurity, law enforcement and defence purposes described in CISA.[62] Further, no government entity may use such information for regulatory action, including a regulatory enforcement action.[63]

56 DHS/DOJ Guidance (see footnote 44), at 10 to 11 ('Even though sharing conducted pursuant to section 104(c) but not consistent with section 105(c)(1)(B) does not receive liability protection (e.g., sharing with a federal entity that is not conducted through the DHS capability and process in section 105(c)), it still receives a variety of other protections that cover all sharing conducted pursuant to section 104(c).')

57 6 USC Section 1504(d)(1).

58 DHS/DOJ FAQ (see footnote 44), at 9.

59 6 USC Section 1504(d)(2).

60 ibid., Section 1504(d)(3)(B).

61 ibid., Section 1504(d)(3)(A).

62 ibid., Section 1504(d)(5)(A).

63 ibid., Section 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., Section 1504(d)(5)(D)(ii)(I). According to the DHS/DOJ Guidance, 'CISA'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 (see footnote 44), at 16.

Appendix 1

About the Authors

Benjamin A Powell
Wilmer Cutler Pickering Hale and Dorr LLP

Benjamin Powell is a partner at WilmerHale and co-chair of the firm's cybersecurity and privacy practice. He is widely recognised as one of the country's top authorities on handling cybersecurity, data breach and related investigation matters. He has advised companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy, including banking, investment management, software, retail, energy, defence and intelligence, media and entertainment, pharmaceutical, cloud services, government contracting, aerospace, information technology, manufacturing and travel.

Mr Powell was unanimously confirmed by the United States Senate as General Counsel to the Director of National Intelligence. His background includes serving as General Counsel to the first three Directors of National Intelligence, as Special Assistant to the President and associate White House Counsel and as a United States Air Force officer, and working at the Federal Bureau of Investigation, as corporate counsel at a software company in Silicon Valley and as part of the trial team that obtained the largest antitrust jury verdict in US history. He also is regularly asked to be lead counsel on major investigations and strategic counselling in a variety of sensitive regulatory matters for the world's most prominent companies.

Leah Schloss
Wilmer Cutler Pickering Hale and Dorr LLP

Leah Schloss is a counsel at WilmerHale. She advises clients on investigative, regulatory and compliance issues relating to cybersecurity.

Ms Schloss has extensive experience coordinating data breach investigations for clients in the retail, professional services, government contracts and technology industries. Her experience includes overseeing third-party forensic investigators; synthesising forensic fact development for briefings to client management, officers, boards and third parties; interfacing with various third parties, including payment card industry forensic investigators, payment card

brands, law enforcement and regulators, as well as breached entities' customers, insurance providers, auditors and vendors; assessing obligations under state and federal data breach notification laws; and drafting breach notification letters, media statements and securities disclosures.

Ms Schloss counsels clients ranging from financial services companies to clients in the healthcare, government contracts and defence sectors on cybersecurity legislative, compliance and governance matters, including legislative and regulatory developments, regulator investigations, state and federal data security guidelines and requirements (including sector-specific guidance such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act), and risk and governance assessments.

Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Jason Chipman is widely recognised as a national leader in handling complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States (CFIUS) and related export controls.

Mr Chipman has advised companies in nearly every sector of the economy on data security best practices and incident response, and because of his experience he is frequently asked to assist with corporate due diligence for transactions involving complex data security and privacy issues. He has helped companies large and small to navigate regulatory obligations associated with data security incidents in the United States, Europe and Asia. Mr Chipman is co-editor of *Getting the Deal Through: Cybersecurity*, a global cybersecurity guide, and he frequently speaks to groups about cyber preparedness and related issues.

Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue NW
Washington, DC 20006
United States
Tel: +1 202 663 6000
Fax: +1 202 663 6363
benjamin.powell@wilmerhale.com
leah.schloss@wilmerhale.com
jason.chipman@wilmerhale.com
www.wilmerhale.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

ISBN 978-1-83862-223-7