THE INVESTIGATIONS REVIEW OF THE AMERICAS 2017

Published by Global Investigations Review in association with:

Baker Botts LLP
Demarest Advogados
D'Empaire Reyna Abogados
EY
Fasken Martineau DuMoulin LLP
FeldensMadruga
Freshfields Bruckhaus Deringer US LLP
Herbert Smith Freehills
Hogan Lovells
Miller & Chevalier Chartered
Sidley Austin LLP
Urquiza, Pimentel e Fonti Advogados
Von Wobeser y Sierra SC
Weil, Gotshal & Manges LLP
Wilmer Cutler Pickering Hale and Dorr LLP

GIR
Global Investigations Review

www.globalinvestigationsreview.com

Cross-border overview: mitigating and investigating a cybersecurity incident

Stephanie Yonekura, Allison Bender and Laura Groen
Hogan Lovells

Introduction

Cybersecurity incidents are steadily rising to the top of the list of major risks facing companies in every industry around the globe. Expending resources to prevent and prepare for a breach of data security is no longer a luxury; it is a necessary priority for corporate leaders and companies worldwide. The importance of thorough preparation for such an incident, and thoughtful planning to mitigate the risk of breach, cannot be overstated.

Mitigation first requires a high-level understanding of all systems and arenas that could potentially be impacted in a breach with an eye for vulnerabilities. Once the scope of the potential effect of an incident is understood, you can begin the process of careful task delegation. All planning for an incident should be conducted with an acute awareness of protecting the attorney-client privilege while allowing the business to run. Counsel should consider themselves a critical gatekeeper and watchdog over the privilege in the drafting of the investigative report, complying with notification and reporting requirements, and disclosing the breach to the public or to law enforcement.

This article aims to outline the priority considerations for mitigating risks, conducting and handling investigations, complying with reporting requirements, and evaluating cross-border implications in light of recent trends and case law developments.

Mitigation

Planning

Mitigation requires quickly and thoroughly understanding the scope and impact of a suspected or confirmed cybersecurity incident, particularly with respect to harm to customers, business partners and the company. Mitigation begins with planning and cybersecurity preparedness. Regardless of industry, the following core principles apply:

- Know your data. Know the third parties who also have your data. Know what obligations you may have to third parties for any data of theirs that you hold. Ensure appropriate protections for all such data.
- Have an incident response plan. Clearly define roles for your incident response team. Practise applying the incident response plan through periodic cybersecurity exercises.
- Regularly review and address cybersecurity vulnerabilities, threats and risks.
- Make cybersecurity a habit for every individual, at every level, in every department of your company. Cultivate awareness. Adapt training and preparedness activities to match the dynamic cyberthreat landscape. Document training, compliance and audit activities.

While these core principles will not prevent every potential cybersecurity incident, adherence will likely prevent at least some, and it will accelerate the response to others. Once a suspected or confirmed incident has been identified, the advice of legal counsel should be quickly engaged, both internal to the company and external, to best manage legal risks arising out of or related to the incident. A key first step is protecting privilege. The failure to timely and properly do so could lead to costly disclosure and exposure of information that would have rightfully received protection had the privilege been a core consideration from the beginning.

Protecting privilege

Protecting attorney-client privilege and preventing waiver should be at the forefront of the mind of anyone shaping an organisation's cybersecurity incident response. The 'purpose' of an internal investigation is generally multi-faceted, and without a thoughtful approach you could be left attempting to justify the protection of the privilege over communications and documents whose legal purpose may not be immediately apparent.

US courts in the past several years have increasingly provided guidance for how and when privilege is maintained in the course of an investigation. In recent decisions, courts resist pressure from plaintiffs to delineate clear categories of corporate actions in internal investigations that will be considered privileged from those that will not. Instead, the approach is much more fact-sensitive. The privilege takeaways from these cases can be summarised as follows:

- Legal advice need only be a 'significant purpose.' Courts recognise that internal investigations are rarely pursued solely for business reasons or exclusively for legal guidance; the pursuit of legal advice need only be a 'significant purpose' for the attorney-privilege to apply.[1] Use of outside counsel strengthens privilege claims. As discussed below, US courts have considered the use of outside counsel as a persuasive factor in considering whether actions were taken in the pursuit of legal advice and guidance. A company need not demonstrate that outside counsel was retained exclusively for legal purposes for the privilege to apply.[2] You should consider each country's specific attorney-client privilege rules in conducting any internal investigations. For example, in Russia, the attorney-client privilege does not extend to communications with in-house lawyers.
- Privilege extends to non-lawyers. Regarding witness interviews, the protections of the privilege extend to non-lawyers, such as computer forensics experts, conducting interviews at the direction of counsel.[3]
- Documents can serve a dual purpose and remain privileged. Documents created in anticipation of litigation with the dual purpose of assisting in business decisions still fall within the scope of the work product doctrine.[4] Further, the public release of a memorandum of findings in an internal investigation does not necessarily waive attorney-client privilege as to the underlying communications and documents relied on in its creation.[5]

The trend by courts to adopt a fact-sensitive evaluation of the privilege, as opposed to establishing bright-line rules, may serve to ease concerns that any minor misstep in the course of an investigation will trigger surrender of the privilege. However, the lack of a distinct

divide between privileged and unprivileged could tempt the unprepared to discover (and fall over) the unseen edge.

A wise response is to instead utilise recent case law as a guide to best practices that will demonstrate a clear assertion of the privilege from the outset of the investigation, for cybersecurity incidents likely to lead to litigation or regulatory enforcement action. A recent case, *In re: Target Corporation Customer Data Security Breach Litigation*,[6] outlines a thoughtful approach implemented by Target in the wake of a major data security breach. At the direction of in-house counsel, Target established a Data Breach Task Force and retained outside counsel to provide legal advice. Target asked a vendor hired to assist with the investigation to provide two teams that would handle two separate tracks of the investigation: one that would act at the direction of outside counsel for the purpose of providing legal advice, and one to conduct a non-privileged investigation to enable Target and its affiliates to respond quickly and appropriately to the breach.[7] The two teams were walled-off from one another to prevent the sharing of any privileged material handled by the 'legal' investigatory team. The clarity of this approach enabled Target to better demonstrate to the court precisely how the privilege had been maintained over documents created in the 'legal' track of the investigation.

Not every cybersecurity incident brings a high risk of litigation or regulatory enforcement. For example, a denial of service attack on an informational website or your Twitter customer-service support tool hopefully will result in only brief disruption, as company IT resources quickly respond. Still, effective mitigation requires laying the groundwork for your response in advance. It will rarely be clear in the first 24 four hours of identifying a suspected or confirmed cybersecurity incident what the full arc of the investigation may require.

In light of the above, the following are suggested 'best practices' for assuring the privilege is maintained in the course of an internal investigation following a cybersecurity incident:

- As part of planning for any cybersecurity incident, engage outside counsel. Although the privilege applies equally to outside and in-house counsel in most countries, US courts have noted that the utilisation of 'outside counsel strengthens the claim of privilege.'[8] Engaging outside counsel to lead an investigation demonstrates the intent to receive legal advice and guidance in the course of the investigation. To rely solely on in-house counsel heightens the risk that you will be required after the fact to attempt to distinguish actions with a significant legal purpose from those that serve a sole business purpose.
- Plan for outside counsel to directly engage cybersecurity forensic investigators and other investigative services. Most companies do not maintain specialised forensic investigative expertise in-house and will usually require support from vendors to respond to a cybersecurity incident. If vendors will be engaged to support the response to any cybersecurity incident, outside counsel can play a role in preserving privilege by retaining, on behalf of the company, cybersecurity forensic investigators and other investigative services, for example, specialty cybersecurity services, such as deep web or dark net searches for compromised data. Privilege need not apply to the retention of and services provided by a credit monitoring service, mailing house, call centre, or crisis communications and public relations firm, for example. In-house counsel frequently elect to engage these other vendors directly.
- When a suspected or cybersecurity incident is identified, consider the two-track approach. A two-track approach to an internal investigation, with distinct teams that are barred from cross-communications, will help you structure your investigation in a way that is privilege-conscious from the start and more likely to hold up under scrutiny. As soon as it is reasonably likely that significant litigation or regulatory enforcement action will follow, this two-track approach should be invoked for the investigation, typically within the first few hours if practical. Prior to a crisis and as part of your planning, determine what types of tasks would be handled by each team. At a minimum, outside counsel should direct the 'legal track' of the investigation and all interview records, documents and communications should designate their purpose as providing legal guidance and advice to the company.

Investigations

Understanding a cybersecurity incident typically requires a close look at both internal and external aspects.[9] Internal aspects of the investigation are likely to include reviews of personnel who may have contributed to the incident (eg, individuals who may have clicked on a phishing link, fallen for a business email compromise scam, or downloaded malicious programs), personnel responding to the incident (eg, first reports and activities of the incident response team), and potentially those personnel affected by the incident (eg, employees whose personal information may have been compromised). External aspects of the investigation are likely to include review of data compromised or exfiltrated; tactics, techniques and practices of the adversary; adversary infrastructure; indicators of attack and compromise; etc. Both the internal and external aspects of the investigation require particular considerations.

Internal investigation and Upjohn warnings

Upjohn warnings should be clearly presented at the start of any interview conducted in an internal investigation. The best practice is to document these warnings, read them out loud, and have them signed by the interviewee.[10] Although courts have clarified that there are no 'magic words' to preserve privilege,[11] the warnings should explain in plain language that:

- the interview is being conducted at the direction of the corporation's legal department for the purpose of obtaining legal advice;
- the interview is subject to the attorney–client privilege;
- the interviewer is acting on behalf of and solely in representation of the corporation;
- the corporation is the holder of the privilege and the only one who can waive privilege; and
- the information obtained in the interview may be shared by the corporation with management, the board of directors, and possibly third parties, including government authorities.

These warnings serve the dual purpose of informing the employee interviewee that they are not represented as an individual by corporate counsel (in accordance with the principles of *Upjohn*)[12] and affirmatively asserting the privilege over the interview. In the context of internal investigations, courts have considered express declarations made before the interview stating that the interview is being held at the direction of counsel and subject to the privilege a persuasive factor in determining whether the interview was conducted for the 'significant purpose' of aiding the company in obtaining legal advice and guidance.[13]

External investigation and forensic reports

Despite the technical rigour inherent in cybersecurity forensics, counsel plays a critical role in the finalisation of the draft investigative report. Each technical conclusion must be supported by facts rather than assumptions. Recommendations for action that are not relevant to underlying root causes have the potential to distract rather than

clarify and strengthen. Understanding that the report will likely be discoverable in litigation following a breach, counsel plays a role in asking these fundamental and necessary questions, 'Why does the report say this? How do you know?'

Reporting, notifications and other disclosures

While reporting, notifications and other disclosures will not be the primary focus of investigative counsel, significant consideration must be given. The timeline for notifications will aggressively press the investigative schedule, and notification timelines will vary based on the laws of the jurisdiction, type of data affected, industry practice, and persuasive government and non-governmental guidance. Law enforcement engagement has the potential to complicate counsel's own investigation; however, the fact that the victim company has contacted law enforcement is typically included in consumer and regulatory notifications, and it is viewed favourably by US courts in subsequent litigation. Sharing cyberthreat indicators and defensive measures may not mitigate client liability during an incident, but such sharing may serve other valuable client ends by combating cyber criminals together and acting as the canary in the coalmine for the good of the global economic community as a whole. Throughout all such reporting, notifications and disclosures, counsel must anticipate enforcement inquiry and litigation discovery.

Timeline for notifications

In the United States, 47 states, the District of Columbia, Guam and Puerto Rico have data breach notification laws. Data security laws are becoming more common at the state level. Certain industries also may have data breach and data security requirements applied through regulations at the federal or state level, such as the healthcare and financial institution industries. Other notification requirements may be applied to companies by contract. Internationally, these requirements are proliferating as well. For example, Norway has a broad notification requirement that a company must report a breach to the Data Protection Authority if a breach has resulted in the unauthorised disclosure of confidential personal data. The trigger, threshold, timing and contents of a notification will vary depending on applicable law, and the conduct of a company's investigation must be sensitive to these requirements. In most cases, the timeliness of your response (date the incident was discovered, date the incident was confirmed, and date of the notification) will have an impact on whether the response is perceived as reasonable. In addition, notifications require a company to indicate whether law enforcement was contacted. In some cases, the timing of the notification may be delayed by reasonable investigation or at the direction of law enforcement. The investigation should be conducted with deliberate speed, taking into account the various requirements that may apply to notifications.

Reporting to law enforcement

A cybersecurity incident is almost always related to some type of criminal act, for example, in the unauthorised access to information or in fraud after acquisition of that information. If the incident is identified and reported to law enforcement during the active commission of a crime, harm to the company and other victims may be blunted by an effective investigation, for example, engaging law enforcement to track down and recover a fraudulent wire transfer discovered within hours. On the other hand, most cybersecurity incidents are discovered after the fact, and at this point, a robust law enforcement investigation may bring additional risk and complication to the company, particularly if the company is no longer able to effectively organise and direct its own investigation. Whether and when to report will therefore be key considerations. In addition, who the company reports to may be a consideration. Reporting a crime online through a webform with the Internet Crimes Complaint Center or Federal Trade Commission is likely to result in a different level of engagement than calling the local field office of the Federal Bureau of Investigation.

Cross-border considerations

With multi-jurisdiction cybersecurity incidents, cross-border considerations arise in the investigation as part of reporting, notifications and other disclosures, and as part of managing litigation and other enforcement actions. If European Union personal data is involved, the investigation approach must consider who may receive such data and whether additional measures are necessary to support cross-border transfer for forensics and the broader investigative response. Decrypting employee communications to support the forensic investigation may require notice and in some cases, consent, prior to review. Law enforcement response across jurisdictions must also be considered. Notifications often will be made voluntarily in certain jurisdictions, because another jurisdiction requires a broader disclosure, even if the likelihood of a subsequent enforcement action or litigation in that jurisdiction may be lower. Interpretations of local law should be informed by local counsel, as interpretations of what may be considered 'significant potential for harm,' for example, may vary widely across borders. A centralised approach to conducting the investigation will aid the company in applying holistic risk considerations across jurisdictions.

Conclusion

Awareness of these fundamental considerations, together with a deliberate and tested approach to incident response, will enable your organisation to avoid the pitfalls that have endangered those that have not had the benefit of hindsight. Aim for the goal of being well-versed in these topics long before a data-security threat is at your door. No one becomes an expert in the heat of a crisis – a 'learn as you go' approach will certainly lead to costly mistakes like the loss of privilege and the unnecessary disclosure of sensitive information. Thus, there is no time like the present to engage in optimal preparation for the next attack.

Notes

1 *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 759 (D.C. Cir. 2014).
2 *In re General Motors LLC Ignition Switch Litigation*, 80 F.Supp.3d 521, 529–31 (S.D.N.Y. 2015).
3 Kellogg, 756 F.3d at 758.
4 *General Motors*, 80 F.Supp.3d.at 532.
5 Id. 3d at 528–29.
6 *In re Target Corporation Customer Data Security Breach Litigation*, 2015 WL 6777384 *1–2 (D. Minn. Oct. 23, 2015).
7 Id. at *2.
8 *General Motors*, 80 F.Supp.3d at 528.
9 With the exception of purely insider threats.
10 See *United States v Ruehle*, 583 F.3d 600, 605–06 (9th Cir. Cal. 2009).
11 *Kellogg*, 756 F.3d at 758.
12 *Upjohn Co. v United States*, 449 U.S. 383, 394 (1981).
13 See id.; *General Motors*, 80 F.Supp.3d at 532.

Stephanie Yonekura
Hogan Lovells

Stephanie brings a unique perspective to any internal investigation. Having served as the Acting US Attorney in Los Angeles, she knows the hot-button issues that are considered in every stage of any government investigation.

As the Acting US Attorney of the largest office outside of Washington, DC, Stephanie was an active participant in the larger Department of Justice community, serving on nationwide committees on white-collar fraud, cybercrime and intellectual property. Stephanie interacted with corporations when they were under investigation as well as when they were victims of crimes.

Stephanie worked with the FBI, SEC, IRS, CFTC and various inspectors general as a prosecutor for more than 14 years, on issues including financial institution fraud, government fraud, securities fraud and cybercrime. She developed a strong reputation with the court, defence counsel and investigating agencies for digging into the facts and collaborating with law enforcement agencies and victims. She was also known for her ability to streamline investigations and make fair and equitable charging and sentencing decisions. In the courtroom, Stephanie exudes confidence, knowledge and integrity.

In private practice, Stephanie uses her extensive experience in the trenches, in the courtroom and as the chief law enforcement officer in Los Angeles to help clients understand the key issues and investigate matters strategically.

Some of Stephanie's experience includes:

- overseeing the investigation of the hacking of one of the world's largest entertainment companies reportedly by a foreign government; and
- supervising a residential mortgage-backed securities investigation into a major financial institution.

Hogan Lovells

1999 Avenue of the Stars
Suite 1400
Los Angeles CA 90067
United States

Stephanie Yonekura
Tel: +1 310 785 4668
stephanie.yonekura@
hoganlovells.com

Allison Bender
Tel: +1 202 637 5721
allison.bender@
hoganlovells.com

Laura Groen
Tel: +1 310 785 4758
laura.groen@
hoganlovells.com

www.hoganlovells.com

Hogan Lovells is a global law firm. Our 2,500 lawyers on six continents provide practical legal solutions wherever our clients' work takes us.

Change is happening faster than ever, and to stay ahead, our clients need to anticipate what's next. Legal challenges come from all directions. We understand and work together with our clients to solve the toughest legal issues in major industries and commercial centers around the world. Whether they're expanding into new markets, considering capital from new sources, or dealing with increasingly complex regulation or disputes, we can help.

A fast-changing and interconnected world requires fresh thinking combined with proven experience. That's what we provide. Progress starts with ideas. And while imagination helps at every level, our legal solutions are aligned with our client's business strategy. Our experience in cross-border and emerging economies gives us the market perspective to be a global partner. We believe that when knowledge travels, opportunities arise.

About our investigations, white-collar and fraud practice
Regulatory investigations. Allegations of fraud, bribery and corruption. Sanctions and money laundering. Whistleblower complaints. Dawn raids. Multinational corporations and their executives face a growing range of threats to their business and reputations. If you get hit, you're going to need a strong investigative team. We work with our clients to manage the issues and limit the impact on their business.

Our strength lies in managing the overall impact – often with a multi-jurisdictional element. Our award-winning team handles asset recovery and issues relating to enforcement, whistleblowing, bribery and corruption investigations, criminal liability, regulatory violations and tax investigations. We are adept at pursuing claims against a company's executive board, and we can implement internal policies and compliance programmes.

Local matters often give rise to international legal risk and investigations. Our team is experienced in handling cross-border work, including offshore jurisdictions. We know what is required to handle such issues, having worked in China, Russia, Europe, the Americas, Africa, and the Middle East, freezing assets, or managing the interplay between foreign corruption and local jurisdictions. Our team has been there.

Allison Bender
Hogan Lovells

Allison Bender joined Hogan Lovells' privacy and cybersecurity practice in the Washington office as a senior associate in October 2015, where she focuses on cybersecurity counselling, incident response including engagement with law enforcement, and public policy. Prior to joining Hogan Lovells, Allison served as a senior cybersecurity attorney in the Office of the General Counsel at the Department of Homeland Security (DHS), where her experience includes, for example, serving as the primary operational legal counsel for the federal response to Heartbleed and a major security clearance contractor as well as providing key legal and policy leadership for a number of cybersecurity information sharing initiatives.

Allison brings key experience in incident response as well as cybersecurity policy, information sharing, liability and incentives. She was primary operational legal counsel for the federal response to the Heartbleed vulnerability, a major security clearance contractor breach, and the Healthcare.gov data breach. She served as Chair of the Automated Indicator Sharing Privacy & Compliance Working Group, provided primary legal advice for the implementation of Executive Order 13691 regarding information sharing and analysis organisations (ISAOs) and private sector clearances, advised the DHS Cyber Information Sharing and Collaboration Program (CISCP); and advised the Interagency Task Force implementing Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity,' Presidential Policy Directive 21, 'Critical Infrastructure Security and Resilience,' focusing on the 'NIST Cybersecurity Framework,' information sharing, liability and incentives. Allison was also principally involved in DHS policy efforts related to cybersecurity export controls, particularly Wassenaar implementation.

Laura Groen
Hogan Lovells

Laura Groen applies a unique combination of creative thinking and critical problem-solving when undertaking complex legal analysis for her civil litigation clients. As a former clerk for the Ninth Circuit Court of Appeals, Laura gained invaluable insight into effective writing for the court and honed her pointed legal writing style and oral advocacy skills. Laura embraces the challenge of finding or creating new solutions for old problems. She eagerly pursues innovative advocacy in both state and federal court for clients who span a broad spectrum of industries.

Laura graduated magna cum laude, Order of the Coif, from Loyola Law School in 2013. After law school, Laura worked for another large international firm in complex civil litigation before accepting a Ninth Circuit clerkship in the chambers of the Honourable Ferdinand F Fernandez.

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

THE QUEEN'S AWARDS
FOR ENTERPRISE:
2012

ISSN 2056-6980