Ensuring best practices in the investigation of an incident

Every company must be prepared to investigate and remediate security incidents effectively, including with respect to managing the legal risks that may arise from such incidents. David Fagan, Ashden Fein, and David Bender of Covington & Burling detail ten recommended actions for companies conducting cyber security investigations to ensure that an investigation is carried out effectively as well as how to remain compliant with evolving legal standards and preserve applicable privileges, in the event of a regulatory inquiry or litigation.

Perfect data and cyber security does not exist. With the advancement of cyber threats outpacing defensive technologies, no company is immune to cyber security incidents; even companies with best-in-class security practices suffer from cyber intrusions and insider threats. This reality demands that companies be prepared to investigate and remediate incidents effectively, including with respect to managing the legal risks that may arise from such incidents.

For many companies, the investigation and remediation of cyber security incidents has fallen principally, if not exclusively, into the domain of their information technology ('IT') or information security specialists. Complex incidents, however, often require additional resources, including the engagement of third party experts, such as forensic investigation firms, and implicate various legal considerations. This article provides a list of recommended actions for companies conducting cyber security investigations.

1. Maintain appropriate definitions and triggers for an incident response team

One of the principal challenges for many organisations is determining when incidents should trigger a broader response team. In this regard, it is crucial to maintain an incident response plan that properly defines the triggers for mobilising an incident response team. The mere fact of an attempted cyber attack is generally not enough to trigger a full incident response team; indeed, many large enterprises will face dozens, if not hundreds, of threats from malware or other attempted attacks every day. However, the IT resources and others in the organisation must be able to identify attacks that create broader risks to the organisation, including, for example, attacks that have resulted in unauthorised access to systems in a manner that could result in the loss, disclosure, modification, destruction or misuse of information or other impacts that could create legal obligations. Such incidents often impact multiple functions within an organisation, and the incident response team should ensure coordination across each relevant function.

2. Preserve legal privilege

As the incident response team moves into action and coordinates across the organisation, it is equally crucial that the response occurs at the direction of legal counsel in a manner that preserves applicable privileges. In turn, all stakeholders within a company should remain cognisant of legal privilege considerations - including management, affected business units, technical resources responding to the incident, and other functions that may be impacted (such as, depending on the incident, HR, finance/internal controls, communications, etc). This will ensure, to the extent possible, that investigative records, digital forensic reports, expert consultants' recommendations, and the legal advice that leads to key business decisions remain shielded from unwanted disclosure in subsequent litigation or regulatory action.

3. Ensure engagements with forensic resources are appropriately structured

As noted, complex cyber security incidents often require the assistance of outside digital forensic experts. There are two important aspects of an effective engagement with a forensic firm. First, organisations should evaluate vendors up front to ensure that they have the appropriate expertise for a particular attack vector and, most importantly, can apply the resources with that expertise to the particular incident. Too often in our experience, we have seen clients secure engagements from forensic firms with strong credentials, but those firms are spread thin and do not apply the resources with the most direct experience to the incident. In sum, the brand name on the forensic firm is not the only factor that matters; the experience of the particular resources who will work on the incident is equally, if not more, important.

Second, it is imperative that the engagement terms with the forensic firm are appropriately crafted to ensure the work occurs, to the fullest extent possible, pursuant to the protection of the applicable legal privileges. In particular, the engagement terms should clearly delineate and identify whether a given vendor has an investigatory as opposed to a technical remediation role.

Two recent court cases highlight the importance of separating an

investigation from remediation efforts and engaging forensic experts through counsel for the purposes of protecting applicable privileges. In an order relating to the class action litigation brought by banks against Target (arising from Target's 2013 data breach), the Court distinguished between remediation reports, which were not privileged, and investigation reports, which were privileged[1]. The Court did not consider the remediation reports privileged because they merely updated Target's board of directors on business issues relating to the breach, and did not contain any legal advice or communications with counsel. However, the investigative reports, which were directed by counsel for providing legal advice relating to the breach, were protected by the attorney-client privilege. In another case, a court only shielded those materials prepared by a third-party forensic firm that were 'addressed directly' to the company's counsel under the attorney-client privilege[2]. Of course, these privilege principles apply more broadly than the company's engagement of forensic services firms, and underscore the importance of engaging counsel to direct the course of the investigation to aid in preparing legal advice.

4. Preservation of evidence and mitigation steps

There is a necessary corollary to ensuring that investigations of cyber security incidents occur in a manner that preserves applicable legal privileges, including in structuring the engagement with forensic firms: pursuant to the investigation, the company should put in place appropriate protocols to preserve evidence of the attack and its investigation. This may include preserving audit logs and other sources for indicators of compromise, as well as retention of correspondence from key custodians related to the breach. The preservation should be sufficient to enable the company to produce, to the extent possible, a record of both the incident and the steps taken to respond and remediate. All preservation requests should occur at the direction of counsel with the intent to aid in the investigation and to document the response.

In carrying out an incident response plan, it is imperative to understand that the plan is not an exact script that mandates a particular response

5. Move with deliberate speed

In responding to cyber security incidents, a company must balance the need to move expeditiously to curtail exposure from the incident and, as necessary, provide notifications to impacted parties with the need to make judgments about remediation and notification based on a full understanding of the facts. This is particularly important because complicated cyber attacks tend to have a 'fog of war' element to them in the initial hours and days after they are discovered; the true extent of the compromise generally is not knowable upfront, and facts can shift as the investigation unfolds. Rushing to conclusions in such circumstances creates a risk that actions that may seem sound at the present are, in fact, incorrect or could create greater risk, such as taking particular servers offline prematurely and tipping off the adversary. Likewise, notifying impacted parties before the facts are fully understood could result in the disclosure inadvertently containing wrong or incomplete information. Indeed, the greatest legal risk from cyber security breaches tends to arise in one of two ways: failing to notify promptly enough, or, conversely, notifying too quickly with incomplete information that then must be corrected. Thus, the best approach to a complex cyber security breach is one that pursues the investigation with 'deliberate speed' - i.e. expeditiously investigating while also allowing the facts to unfold, to the extent possible, before reaching conclusions.

6. Maintain flexibility

In carrying out an incident response plan, it is imperative to understand that the plan is not an exact script that mandates a particular response. Rather, the plan should be a guide to ensure appropriate coordination and escalation within a firm, and appropriate planning for an incident should include testing and updating the plan. When an incident occurs, however, it very likely will present facts that cannot be foreseen or 'gamed' in advance. The ability, therefore, to maintain flexibility in the application of the plan and apply judgments based on the facts as presented, rather than pursuant to a script, is an important element of an effective response. Such flexibility may include also determining to augment resources as circumstances develop that might require particular expertise - such as augmenting forensic resources with dark web investigators to search for evidence of data extraction or sources of malware.

7. Understand when to escalate

It is best practice to develop internal notification requirements that identify when certain events or triggers merit reporting to management or boards of directors. Such reporting can be particularly important to stave off later litigation, such as shareholder suits. For example, in dismissing a shareholder derivative suit arising from cyber attacks against Wyndham Hotels[3], the Court found that the board had a "firm

grasp" of the incidents and deserved deference under the business judgment rule, citing the following facts: the board discussed the attacks at 14 meetings, the board's audit committee reviewed the attacks during at least 16 meetings, and the board understood the subject matter of the incident. While the board need not be apprised of every development over the course of the investigation, a company should carefully consider, in consultation with counsel, when an incident or development warrants such escalation.

8. Evaluate engagement with law enforcement

One critical question that often arises for victims of cyber attacks is whether and when to engage law enforcement. On the one hand, engagement of law enforcement may provide legal benefits: engaging officials who are responsible for investigating cyber crime can help build the record that the victim is acting responsibly in responding to the attack; there are legal safe harbors under state laws for delaying notification to individuals if law enforcement requests such delay, potentially providing more time to investigate incidents, and certain other regulators - particularly in foreign jurisdictions - may defer to US laws if they understand US law enforcement officials are engaged. In addition, the Federal Trade Commission has indicated that it will take a more favourable view of companies that cooperate with law enforcement in the wake of a breach than those that do not[4]. On the other hand, any engagement of an independent third party, including law enforcement, must be undertaken carefully given that information shared with the third party may not be privileged. Thus, when contemplating engagement with law enforcement, organisations who have been victim to cyber attacks should understand upfront what information they are comfortable sharing, and the format in which they would provide the information. For example, it is not uncommon for law enforcement officials to request copies of forensic reports that outside forensic experts have produced. It is important to understand that such reports need not be disclosed to law enforcement; however, in the absence of legal process compelling disclosure, it is possible to arrange for sharing certain conclusions of the forensic investigation with law enforcement, while other conclusions and the forensic steps can be preserved as confidential.

9. Assess regulatory and notification obligations

As an investigation unfolds, a company must evaluate whether the nature of the incident requires any notification to affected individuals, regulators, or business partners. For example, in the US, 47 states have enacted data breach notification laws, which generally require notification to state residents of incidents involving unauthorised acquisition of certain types of personal identifying information and may require notification to state regulators in certain circumstances. Federal laws in the banking, healthcare and defence sectors also may trigger notification obligations, and the Federal Communications Commission likewise has been applying its authorities to incidents involving personal identifying information or other account information known as customer proprietary network information. Other jurisdictions outside the US - especially, but not limited to, certain EU Member States, Canada, Japan and Korea - also may have notification obligations either to affected individuals or regulators for breaches that impact their citizens. And there may be contractual obligations to notify business partners if a cyber security incident impacts their information. If notifications are required, an organisation that has incurred a cyber breach should do so in a manner that comports with legal requirements to act expeditiously while (consistent with recommendation 5 above) not acting rashly and providing notice prematurely.

10. Remediate and learn

Finally, once the investigation is complete, a company should take steps to remediate both the systems that were involved in the incident and any company policies and procedures that did not work efficiently or effectively during the incident response. This should include an assessment of the lessons learned from the incident and incorporation of those lessons into policies and procedures. Regulators invariably look to past incidents at a company, and whether the company implemented further safeguards as a result of those incidents.

David Fagan Partner
Ashden Fein Associate
David Bender Associate
Covington & Burling, Washington DC
dfagan@cov.com

1. See Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384, at *1–3 (D. Minn. 23 Oct 2015) (order granting-in-part and denying-in-part plaintiffs' motion to compel).
2. See Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 193–94 (M.D. Tenn. 2014).
3. Palkon v. Holmes, No. 2:14-CV-01234 (SRC), 2014 WL 5341880, at *5–6 (D. N.J. 20 Oct 2014).
4. https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call