ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JULY 17, 2013

Breach Investigations, Part 3: Conducting Enterprise Impact Investigations

By Kim Peretti, Alston & Bird LLP, and Jason Straight, Kroll Advisory Solutions

This article is the third in a four-part series describing some of the challenges to conducting breach investigations in response to increasingly sophisticated attacks. In Part 1, entitled "Right-Sizing the Data Breach Investigation," published in *Law360* on March 26, 2013, we provided an overview of the evolving advanced cyber threat landscape and the three common breach response scenarios (internal investigations to fix technical problems, investigation to assess payment card exposure and investigations to determine compliance with state data breach notification statutes). In Part 2, entitled "Understanding the Role of the PFI in Payment Card Breaches," published in *Law360* on April 19, 2013, we took a closer look at responses involving payment card breaches—both because of their unique nature and their potentially grave implications.

This Part 3 will discuss both the need, and the underlying framework, for conducting an "enterprise impact" investigation in appropriate circumstances. Finally, the fourth article will present hallmarks of an effective enterprise impact investigation from a forensic investigatory standpoint. The emphasis in Parts 3 and 4 will be on avoiding the pitfalls that trip up even those companies with significant experience in responding to data breach events. Too many companies fail to consider the less obvious, but potentially serious, consequences of a data security incident—especially when the investigation clearly identifies a data compromise that triggers a notification obligation of some sort (e.g., exposure of payment card data or personal information as defined by applicable state statutes). In such scenarios, many companies understandably tend to focus their response on clearly defining their notification obligation and neglect to explore the possibility that the attack had more wide-ranging effects, such as exposure of sensitive intellectual property or the creation of a resilient "backdoor" that may enable an attacker to return at a future date.

I. The Case for Conducting a Broader "Enterprise Impact" Investigation

Companies that fail to appropriately pursue a comprehensive investigatory approach to a security incident response may be exposed in two ways. First, from a practical standpoint, a broader investigation of a deep compromise to an entity's systems allows the company to understand the full scope and nature of the incident. With this understanding, the company is more likely to be able to identify all the pathways used by the attacker as various entry points to and exit points from the network. The more entry and exit points that are discovered, the more likely the organization can remove these methods of access by the criminal actors. This ensures not only that the current incident is contained, but that the organization is protected from a repeat offense from the same actors at

a later point. As one goal shared by sophisticated actors is to obtain and maintain deep and prolonged access to systems, such actors commonly attempt to re-compromise victims. Indeed, if the incident is detected, advanced threat actors usually wait for the company to perform some level of remediation following the detection, knowing that the company will be less prepared for a re-compromise because it believes its systems are more secure.

It is also important to realize that much of the advanced malware favored by attackers today is designed to evade detection and, even when detected, thwart efforts to eradicate it from a system by sitting in a computer's volatile memory and re-installing itself the next time the machine is booted. Moreover, even if the initial vulnerability that enabled the infection is remediated, a determined attacker may search for other weaknesses to exploit. Consequently, it is critical to fully understand the nature and scope of the compromise—in particular, the varying means of entry and exit to systems—and carefully assess all potential means of defense.

Second, from a legal standpoint, while there may be an absence of a direct legal obligation requiring a comprehensive review in the event of a security incident, there are a number of disclosure and notification obligations, and proactive regulator inquiries into cybersecurity practices and incidents, which are premised on a company's understanding of the full impact of a cyber event. One example of such disclosure obligation is the U.S. Securities and Exchange Commission's (SEC's) recently issued Guidance (CF Disclosure Guidance: Topic No. 2 Cybersecurity, October 13, 2011) on the topic of cyber risk and cyber incident disclosures. Among other items, the Guidance identifies a number of existing reporting requirements that may impose an obligation concerning cybersecurity risks and cyber incidents. With respect to a cyber incident, registrants are required to disclose an incident that has a material effect on the company's products, services, operations, or financial or legal condition.

While the Guidance does not identify the process that must be undertaken to determine if the breach is material, an accurate cyber incident disclosure would seem to be predicated upon an incident response that uncovers the true extent of the breach's impact on the organization. An internal investigation focused on IT risk or a response focused primarily on personal information or payment card data disclosure may not adequately focus on the broader organizational risk necessary for accurate cyber incident disclosure in some circumstances. For example, if in addition to compromising customer credit card data an attacker also stole product design documents or other valuable intellectual property, the resulting risk to the compromised organization may be dramatically greater than initially believed. Indeed, for some companies, the loss of critical intellectual property may represent an existential threat.

In addition to the SEC, other federal and state regulators similarly have an interest in understanding the broader organizational risks of cyber intrusions to their regulated institutions. On May 28, 2013, the New York State Department of Financial Services issued specific information requests (known as "308 Letters") to the largest insurance companies regarding, among other things, information on any cyber attacks the company has been subject to in the past three years and the cybersecurity safeguards the company has put in place. State and federal regulators enforcing consumer protection statutes have increasingly launched investigations in response to breaches disclosed by companies, which inquire, among other relevant questions, as to the completeness of the investigation undertaken by the company. Other regulators, such as the North American Electric Reliability Corporation (NERC) and the Federal Financial Institutions Examination Council (FFIEC), may similarly be interested in the responses undertaken by companies subject to advanced intrusions, as they are concerned with understanding any system risk and other industry-wide concerns to their regulated industries. This is often the case with companies in industries designated as critical infrastructure, such as energy and financial services.

Companies subject to regulatory inquiries concerning significant data breaches should expect probing into the breach response to understand any broader organizational risks.

II. The Framework for "Enterprise Impact" Investigations

Responding to advanced threat actors with an enterprise impact investigation requires three components: (1) oversight by counsel to establish and maintain attorney-client privilege protection over the investigation; (2) an effective corporate response; and (3) development of enterprise impact-based strategies related to the investigation, sensitive data access, containment and eradication/recovery of the event.

Role of Counsel and the Attorney-Client Privilege

Investigations of cyber intrusions and data breaches perpetrated by sophisticated threat actors are far-reaching, complex and technical, with an evolving set of facts that continue to surface for days, weeks and sometimes months. As discussed in Parts 1 and 2, until the investigation is over, the facts of how the compromise occurred, how many systems were compromised, what was on those systems and could potentially be exposed, whether and how much data was taken out of the environment, and whether the security incident is ongoing are likely to be under constant flux. This is particularly true in the case of an outside intruder who was able to traverse a network undetected for a period of months or an incident perpetrated by a trusted insider who exploited legitimate system privileges for nefarious purposes. While the attorney-client privilege does not protect the underlying facts of the investigation from ultimate disclosure, it will protect the "developing facts" and process used to arrive at those ultimate facts where counsel hires the investigator and directs the investigation.

To provide additional context, it is not uncommon for an investigation that initially appeared headed for a clear-cut determination to take an unexpected turn and lead to an unanticipated conclusion. Indeed, at the end of the investigation, while there may be some facts not in dispute, many are subject to interpretation and guided by assumptions (hopefully based on deep and broad experience) of the investigator of who the bad actors are, their motives and the potential consequences of the types of tactics, methods and techniques the particular bad actors often employ. In addition, seldom does an investigator have access to all the information needed to reach a definitive conclusion as to exactly what occurred. In most investigations, the role of the investigator is to create the most complete factual picture of the event so that counsel may apply legal judgment to define the full impact on the company. Certainly, because these investigations can be as much art as science, in any investigation with multiple investigators, there will likely be varying interpretations of key facts. It will fall to counsel to consider the various views and adopt the most defensible position for the company to take.

Given these complexities of forensic investigations, the importance of attaching privilege to cybercrime incidents—particularly those involving sensitive data—cannot be overstated. Lawsuits in the form of privacy-related class actions (under applicable statutory and common law theories), securities class actions and/or individual plaintiff actions can be expected for most breaches that involve personal information and/or payment card data. In addition to post-breach litigation, cyber intrusions and data breaches of any significance often result in regulatory inquiries and investigations, such as by state attorneys general (AGs), the Federal Trade Commission, the SEC, Financial Industry Regulatory Authority (FINRA), the Consumer Financial Protection Bureau, the FFIEC, and the Office of Civil Rights of the Department of Health and Human Services (OCR). And certainly, at the front of the helm are the ever-increasing congressional inquiries where consumer data is exposed or where national security

implications arise from a breach. Protecting the communications and documentation around the investigation through the attorney-client privilege when litigation or regulatory inquiries are anticipated can greatly assist the victim company in managing its litigation risk.

In addition to the benefits afforded by the privilege, counsel also serve an important role in the management of the investigation. As discussed below, responding to cyber intrusions and data breaches often involves a corporate response where any number of internal stakeholders and external third parties may need to be involved and any number of legal issues may surface. Managing this complex matrix of individuals and parties with varying, and often overlapping, roles and responsibilities while ensuring proper insight into potential legal issues produces the need for at least one person within the core corporate response team looking out for the legal issues that may surface.

Corporate Response Plan

Responding to security incidents is no longer solely within the domain of the information security department to respond with a technical fix for a technical problem. Effective responses to attacks from advanced threat actors require a corporate response. This is due in large part to the far-ranging scope of such compromises—which may have a significant impact on the enterprise's business operations—but also because of the visibility attached to even the smallest of breaches, leading to increased numbers of lawsuits and regulatory inquiries surrounding these events. It is also due to the fact that, as previously mentioned, as the details emerge in the investigation, the resulting risk to the compromised organization may prove dramatically greater than initially believed.

An effective corporate response has, among other hallmarks, a core set of leaders that provide balanced governance; a well-coordinated and orchestrated communication, notification and disclosure plan; the ability to quickly bring the right resources to bear; and effective management and coordination of the number of internal and external parties that may be part of the breach response.

Many companies understand that a response to a material breach may require the involvement of a core set of leaders within the organization, often labeled a "data breach response team," which may include the CFO, CIO and/or general counsel, as well as representatives from public communications/media, risk management, information technology/security, public information/communications, compliance, business operations and corporate insurance. All too often, however, the core team relies too heavily on the assurances of the individual from information security who is the de facto leader of the response, or the CIO to whom that individual often reports. While the information security leader and CIO may be well-intentioned, their information may naturally be filtered (their jobs may be on the line, after all!) and too overly optimistic on the scope of the breach or the state of the response.

The core response team needs to have one, and preferably two, adjacent leads to the response that are familiar enough with the complexities of these technical investigations to ask detailed and probing questions about these assurances. Only through a rigorous questioning of how the investigation is being conducted (as it is being conducted) will the company be able to ensure the investigation is properly addressing any enterprise impact to the organization. Individuals that could fill this role are outside forensic consultants, inside and outside counsel, and even the CFO. Mastering a balanced governance approach to investigations will avoid one of the most common pitfalls companies face in data breach response—overreliance on unverified, favorable facts.

Second, because of the far-reaching consequences of inconsistent and inaccurate disclosures, notifications and customer communications, companies need to ensure a well-coordinated and orchestrated media and communication plan is in place. Indeed, at the same time outside counsel and forensic investigations are brought to the table, companies often engage, and should engage, public relations services to assist with the development and deployment of a public relations and communications strategy.

Finally, companies should be aware of the different types of services and skillsets that may be needed in a breach response, and establish relationships with these service providers in advance of any security incident. Examples of such services include intelligence gathering, incident response support, forensic investigation, malware analysis, network traffic monitoring, data analysis and breach notification support. In the event the response needs to rely on one or more of these service providers or vendors, companies should plan for how to effectively manage and coordinate these internal and external parties well in advance of the crisis at hand.

Part 4 of this series will discuss the third component of an enterprise impact investigation—the development of enterprise impact-based strategies related to the investigation, sensitive data access, containment and eradication/recovery of the event.

This article was previously published by ***Law360***.

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com | alstondatabreach.com