ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM MARCH 26, 2013

Breach Investigations, Part 1: Right-Sizing the Data Breach Investigation

By Kim Peretti

Introduction

In the age of targeted intrusions, sophisticated criminal and nation-state actors are often compromising hundreds of systems within a single company's environment. However, companies are often only seeing a small portion of the entire incident, as their response to such invasions can be, and often is, too narrowly shaped by state security breach notification requirements, industry rules governing payment card breaches and the absence of a direct legal obligation requiring a more comprehensive review.[1] If a company has a less-than-complete understanding of the nature and scope of the intrusion, it could be exposed when the criminals revisit the enterprise for further exploitation or when regulators and class-action plaintiffs begin probing into details of the company's response.

Generally, three common scenarios exist in data breach and cyber intrusion response, each of which approaches the response in pursuit of a narrowly defined purpose. These purposes include an internal investigation to fix a technical problem and get the team back to their day jobs, an investigation to assess payment card exposure, or an investigation to determine compliance with state data breach notification statutes.

In many instances, these responses are sufficient. In other critical instances, however—particularly when an advanced-threat actor is involved—these responses may be insufficient, in that they often do not involve a comprehensive review of the incident for purposes of determining the full impact to the organization. Was confidential information, intellectual property or other unregulated data potentially compromised? What was the extent of the compromise throughout the company's environment? Which business lines and platforms were impacted? What is the level of comfort in the containment approach for future attacks? What processes or systems failed that led to the incident in the first place? These are only a few questions left unanswered in overly myopic responses to advanced cyber intrusions and data breaches. This is not to say that such fault is universal or that no breach is properly scoped; many companies are quickly learning to appropriately tailor their response to the situation at hand. However, the concern is that companies with intentional or unintentional blinders on may never reveal the critical facts that truly define the breach, its causes and its logical results.

---

[1] The SEC 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 requires companies to disclose material breaches or cyber incidents, but does not identify the process that must be undertaken to determine if the breach is material.

This article is the first in a four-part series describing some of the challenges to conducting breach investigations in response to increasingly sophisticated attacks. In this Part 1, we provide an overview of the evolving advanced cyber threat landscape and the three common breach response scenarios outlined above. The second article will takes a closer look at responses involving payment card breaches—both because of their unique nature and their potentially grave implications. The third article will discuss both the need for, and requirements of, an "enterprise impact" investigation in appropriate circumstances. Finally, the fourth article will present hallmarks of an effective enterprise impact investigation.

Background – The Evolving Cyber Threat Landscape

Within a little over a decade, the cyber threat landscape has dramatically evolved. Ten years ago, the typical cybercrime case pursued by regulators and law enforcement involved a solo hacker gaining unauthorized access into one or a small number of systems for idle curiosity. The cases often involved one-time offenses and the stakes were small. By way of example, in 2003, the Department of Justice prosecuted one of its first phishers for sending an email to AOL subscribers asking for credit card information, which the criminal then used in a $47,000 scam to purchase goods off the Internet and have them shipped to a neighbor's home.[2] In contrast, today's "phishers" often work at the behest of well-funded, state-sponsored groups that use this tactic in an advanced and virtually undetectable form merely to gain access and maintain a broad level of persistence to the network.

Today's era of cybercrime has produced several threat groups and actors that are a world apart from that "lone phisher" scenario. These groups have the capability to conduct targeted, well-orchestrated, sophisticated, prolonged and repeat attacks on businesses, potentially inflicting significant damage to almost any target of their choosing. The three primary categories of actors most likely to cause damage, and which are responsible for a disproportionate number of the attacks that routinely occur, include "hacktivists," state-sponsored groups and global criminal hacking organizations. While historically (in the brief history of cybercrime) these actors had distinct methods, tactics and tradecraft, their distinction today lies primarily in their motive. Hacktivists, or loosely organized and affiliated groups of politically motivated hackers, aim for a "quick win" in either bringing down a website or publically disclosing confidential information to cause a company reputational harm and embarrassment. State-sponsored groups, or sophisticated and well-funded hacking groups sponsored by foreign governments, aim for a slow and stealthy win through a persistent pilfering of economic intelligence for a competitive advantage. Organized criminal hacking groups, on the other hand, steal sensitive or personal customer data and trade it in the criminal underground for financial gain.

The attacks perpetrated by these advanced actors often involve deep and prolonged access to systems and networks, where the actors can cause sustained damage over time. Perpetrators of sophisticated intrusions have a dual purpose in their mission, both of which are served well by obtaining broad access to the victim's environment. First, they attempt to obtain unauthorized access to the environment for purposes of targeting a specific asset(s), such as a piece of source code, research and development plans, an executive's email inbox or customer payment card account numbers. In the quest for the targeted asset, the intruders often conduct network reconnaissance to understand the network infrastructure, as well as business reconnaissance to understand where the asset(s) may be stored. In conducting network and business reconnaissance, intruders may rummage around on different platforms and in different business lines of operations within the environment—and, in doing so, they may (and

2 http://www.ftc.gov/os/caselist/0323102/0323102zkhill.shtm

often do) touch many systems in their pathway, sometimes in the hundreds. Second, the criminal actors will strive to maintain a persistent footprint in the environment. That is, they will strive to leave "backdoors" on as many systems as possible to ensure their ability to return at a later date, even if, and despite being, detected by the compromised victim entity. These dual purposes often ensure that the advanced threat actor compromises as large a number of systems as possible as part of their exploitation of the victim's environment. Moreover, it is this broad and deep level of access that can create an enterprise risk to the organization.

Three Common Breach Response Scenarios

Against the backdrop of this landscape, many companies responding to cyber intrusions and data breaches fall into one of three common responses: (1) an internal response in which IT staff or the incident response team focuses on a technical fix for a technical problem and strives to remediate the problem as quickly as possible; (2) a payment card data breach response in which a forensic investigator approved by, controlled by and reporting to external third parties focuses on potential payment card exposure; and (3) a personal information response that focuses on compliance with state data breach notification statutes.

a. Internal response or investigations directed by the CIO

Outside of breaches involving payment card or personal information, there is generally no requirement under state or federal law for a company to report a cyber intrusion or data breach, other than in accordance with SEC disclosure rules if the incident is a material event. As a result, when a company detects a compromise to its network (or is informed of its detection by a third party), an initial, and sometimes only, step a victim organization takes is to launch an internal investigation using the organization's IT operations or information security departments. Typically, this team tries to quickly determine the source of the attack (if possible), plug the hole with a technical fix and assure management that the problem is solved. Indeed, with a fear that their jobs may be on the line, there is little incentive for those within the department to share with those outside the department any system compromise or data breach. In addition, the IT or information security department may be aware of the system breach, but choose not to investigate it either further or fully. Both decisions can leave the company exposed.

Alternatively, the IT or information security staff may sense a more pernicious threat and escalate the incident to higher-level management, often through an inter-department information security council or data breach team. Because the information security director or chief information security officer often reports to the CIO, the CIO ultimately is given the authority and responsibility to run the investigation, which may be entirely internal or involve external forensic parties. While inside counsel may be involved, because of counsel's lack of familiarity or unfamiliarity with the technical side of the security incident, the CIO is the ultimate overseer of the investigation. The CIO—either alone or from pressure above—often views the investigation through the lens of "how quickly can I get my team back to their day jobs."

In either case, the company may rush to remediate the discovered problem (intentionally or unintentionally) without careful and thoughtful deliberation regarding the scope of the investigation to save time or resources, and often under the belief that what may in fact be a "band-aid" remediation has cured the problem. Moreover, in both situations, the company runs the danger of being left exposed, either because of a likely repeat offense or in terms of not fully appreciating the true enterprise risk.

In the other typical situation, the initial internal responders will escalate the incident to others in the organization because personal information or payment card information has been stolen or is at risk of disclosure. Many companies now have incident response decision trees that require some form of escalation when personal information or credit card data may be at risk of compromise or exposure. At this point, the breach is labeled as such and each classification brings with it its own limitations and challenges to conducting a fully scoped investigation, as described more comprehensively below.

b. Payment card breach response

Companies that experience breaches involving payment cards are subject to a set of industry rules formulated by a governing body comprised of the major payment card brands. These rules dictate the response that must be taken by the compromised entity. While there may be many positive aspects of this process, it should be noted that the intended purpose of these investigations is to minimize potential fraud losses to exposed cards; the responses may not necessarily include all of the activities necessary to assess and address more holistic risks for the enterprise. The role of the victim company in the response is limited, which among other things, may pose a formidable challenge in responding to a breach through an enterprise impact lens when necessary. This breach response will be covered in detail in the second article in this series.

c. State law driven data breach notification

The most direct legal obligations that surface in cyber intrusions and data breaches are the patchwork of state data breach notification statutes. As a general matter, these statutes require that any company in possession of certain personal information of covered individuals notify the individuals if there is a breach of this information. Key definitions in these statutes include "personal information" and "security breach." Generally, personal information includes a person's first name or initial and last name, plus one of the following data elements: Social Security number, driver's license number, or financial account or credit or debit card number. Most laws define security breach as an "unauthorized acquisition" of electronic data that compromises the security, confidentiality or integrity of personal information maintained by the business.

Most organizations have an employee who has some familiarity with and responsibility for these obligations, who is often in a privacy role within the general counsel's office. In a common personal information data breach scenario, the IT operations or information security department is made aware of an incident involving the disclosure of personal information and escalates the issue to the employee responsible for privacy compliance at the organization. Typical situations involve lost laptops with unencrypted names and Social Security numbers or a hacker compromising an e-commerce web server and stealing customer names and email addresses. The privacy employee proceeds to contact in-house or outside counsel, who then has conducted at their direction an in-depth analysis of whether the incident triggered the data breach notification statutes. In many cases, the legal analysis is straightforward after a complex data analytics exercise is performed (often by outside consultants) on the data that is presumed to have left the company's environment.

While it is certainly not the case with all companies or investigations, there is some risk that a company falls short in data breaches and cyber intrusions where personal information is not the targeted asset of the criminal actors or where a breach of personal information is not readily apparent. Given the broad and deep level of access that advanced criminal actors maintain in an environment, combined with the fact that unencrypted personal

information is often scattered on many systems in structured and unstructured formats within any company's environment, it is highly likely that sophisticated intruder activity will at the very least trigger a legal review under the state data breach notification statutes. This cannot be emphasized enough—companies should be reasonably comfortable that they know how broad and deep the breach/intrusion was, rather than just jump to the point where they've convinced themselves that payment card data and personal information are not involved.

In contrast to the more straightforward personal information breaches (e.g., lost laptops), however, these broader legal reviews are especially complex and technical. In-house or outside counsel will quickly find themselves swimming in a sea of technical terms in an attempt to apply the facts of the forensic investigation and the data analytics exercise to the law. Such terms, with respect to the systems or data impacted, may include "exposed," "exported", "accessed," "acquired," "touched," "harvested," "opened," "viewed," "exfiltrated," "captured," "collected" or "compromised," with each having the possibility to alter the legal obligation of the notification requirement. By way of example, if criminals left a backdoor on a system where personal information was present, and there was no evidence of access to the data, but evidence that other data on the system was exfiltrated, was there a "security breach" under a particular state data breach notification statute? What if the criminals sent commands from one database to another to traverse the environment where each database housed personal information? What if there is unauthorized access to systems and criminal-created user accounts on databases with personal information, but no evidence either way of whether the personal information files were viewed, downloaded or exfiltrated by the criminal actors? Determination of the precise forensic facts necessary to support the legal analysis is often further complicated by the fact that the evidence to prove or disprove a certain set of facts may be intentionally hidden or destroyed by the criminals, overwritten in the normal course of business or may never have existed in the first instance.

Granted, not every cyber incident or data breach results in a far-reaching compromise of systems or disclosure of personal, sensitive, confidential or regulated information. In every breach, however, companies should know how broad and deep the breach/intrusion was—not stop short once they identify certain payment card/personal information was compromised (and fail to examine other systems) or stop short by labeling it as a non-payment card/personal information breach (and failing to examine compromised systems for evidence of access to payment card/personal information). The cybercrime game has changed, and considering the sophistication and reach of the modern intruder, victims of a breach should not hesitate to be earnest in scoping their investigations; the price to pay down the road may otherwise prove unexpectedly steep.

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

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