ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM OCTOBER 3, 2013

Cyber Investigations, Part 4: Hallmarks of Enterprise Impact Investigations

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

This article is the last 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" and 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" and 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. In Part 3, entitled "Conducting Enterprise Impact Investigations," we examined the need and underlying framework for conducting an "enterprise impact" investigation in appropriate circumstances. Part 3 was published in *Law360* on July 16, 2013.

Finally, this Part 4 will present hallmarks of an effective enterprise impact investigation from a forensic investigatory standpoint. As companies invest in people, processes and technology to prevent cyber attacks, attention must also be given to preparing for an incident. The reality in today's sophisticated threat environment is that even the best-defended perimeters will be breached by a determined attacker—or, even more likely, by an insider who uses legitimate network privileges to circumvent security controls. It is therefore critical for every organization to be prepared to respond effectively to an incident when—not if—it occurs. Part of that preparation involves ensuring that the response team has access to sufficient network information and log data to conduct an effective enterprise impact investigation.

Key Components of an Enterprise Impact Investigation

Any response to an advanced cyber attack or significant data breach should include development of risk-based strategies related to conducting the investigation, sensitive data access, containment and eradication/recovery of the event. In other words, decisions must be made at every step along the investigatory journey as to whether a particular investigatory step should be pursued and why (or more often, why not). The section below highlights areas of consideration for developing the strategies necessary to conduct an effective enterprise impact investigation.

Preservation of Digital Evidence. Following a compromise to its systems, a compromised entity must move rapidly to preserve any forensic evidence that might help elucidate (1) the vulnerability that allowed an attack to be carried out, (2) what method of attack was used to exploit the vulnerability, (3) how long the attack has been ongoing and (4) what systems and data may have been compromised as a result of the incident. This task includes imaging compromised or affected network devices, capturing volatile data from live memory, preserving log data that provides information on network traffic and system access, as well as capturing other network activity that may be related to the incident. As a general matter, compromised devices ripe for imaging include laptops, desktops, servers and other systems on which the attacker may have placed malware, accessed using stolen credentials or used in connection with accessing the network and/or exfiltrating data or other information. The type of log data that is most often helpful to incident investigators include firewall logs, intrusion detection and intrusion prevention (IDS/IPS) logs, event logs on Windows systems, system access logs, VPN logs, Anti-Virus logs, Domain Controller logs, router logs, database audit logs and application logs. Also, it is important not to neglect physical access logs, video monitoring systems and even telephone logs depending on the nature of the incident. While the compromised entity may not have these logs at all, or for the specific time period, it is important to cast a wide net in obtaining all possible sources of evidence.

Identification of the current IT enterprise landscape. A critical first step in an effective enterprise risk investigation is to gain an understanding of the current IT enterprise landscape. Network diagrams, or a corporate data map, if they exist and are accurate and complete, will often be a good starting point for understanding basic aspects of the environment and can be used to build out an accurate list of the servers, systems and workstations that may have been affected by a network intrusion incident. In addition to helping investigators understand how machines on a network communicate with each other, a good network diagram will also detail the types of data stored and/or processed on each device. This list or mapping of the landscape will allow the company to determine what level of risk attaches at each stage in the incident response, particularly in determining the risk associated with the scope and scale of the compromise and the extent the intrusion may be ongoing and/or contained.

Of course, arriving on-site and being handed a complete, up-to-date data map or network diagram is a rare occurrence. And, creating such a map or diagram in the immediate aftermath of a significant network intrusion would likely be a monumental task. The common pitfall to avoid here, however, is a reliance (let alone over-reliance) on whatever map or diagram exists as a basis for deriving the level of risk attached to the results of an ongoing forensic investigation. For example, if the forensic investigator presents to the organization that 70 percent of the systems scanned revealed no malware or compromise, but the investigator is working off an understanding of the network in which a key systems part of recent acquisition were not included on the diagram (and thus were not scanned), the company will have a false sense of security. Scenarios such as these can be common in responses to significant intrusions.

Understanding the nature of the compromise. The objective of the forensic investigation should be to provide the company with a clear understanding of how the intruders carried out the attack within the company's environment. Key points of focus should include the methods, tactics and techniques the criminals utilized to initially enter the network, move internally within the environment and exfiltrate data or information from the environment. Such a comprehensive understanding will support the company's ability to develop an appropriate containment approach. A critical part of any investigation is identifying the vulnerabilities that allowed the attackers to penetrate the environment. Multiple failures involving people, process and technology often contribute to a breach incident; it is important to identify all underlying causes so that the vulnerabilities can be remediated, and future similar attacks can be prevented.

Understanding the scope of the compromise. An obvious yet critical part of the forensic investigation is determining the extent of the compromise, including which systems were successfully compromised or accessed by the intruder and whether any sensitive information was actually exfiltrated during the attack. The investigative approach should seek to delineate the variety and types of systems that were potentially exposed (e.g., Windows, Linux, Mac and/or mainframe) and identify the types of data stored on each system (e.g., SQL databases, office files or email). The methodology should also define the areas of the business impacted by the compromise and the specific varieties of sensitive information stored on the affected systems (e.g., customer information, employee data, sensitive intellectual property). Too often, forensic investigators will stop short of assessing each environment, platform and/or line of business for indicators of compromise, focusing instead on the area where the criminal activity is most readily apparent or primarily centered. In addition, even if an investigator accurately identifies the scope of a breach from a system perspective, they do not always take the next step of working with counsel to create a record of sensitive information that, if compromised, would trigger contractual or regulatory legal obligations.

Developing an investigative strategy to accurately determine the scope of a compromise involves both the art and science of forensic investigation. The art component constitutes using deep experience in handling breach events and extensive knowledge of corporate IT environments to zero in on the best sources of evidence to determine what occurred. The science involves applying the appropriate tools and skills to analyze available evidence in a forensically sound manner in order to create a solid factual foundation upon which counsel can then base an evaluation of the true impact of an incident. Although there are many commonalities that arise time and again in breach incidents, every enterprise impact investigation is unique and investigators must be careful to select their techniques and tools to fit each scenario. Of equal importance, investigators must clearly document the steps taken, including any scanning that is performed and where it is performed. For example, scanning is usually performed by looking for known indicators of compromise, such as using a "blacklisting" approach to identify malware on compromised systems. However, in many circumstances, an investigator should also consider using a "whitelisting" approach, which can identify malicious code that is not yet detectable by traditional scanning tools. An investigator should not neglect to search volatile memory for traces of malware. Some of today's most sophisticated malware is designed to reside in active memory and to "re-install" itself even after a traditional scan has identified and eradicated the application.

Equally important is the delineation of what areas within a system were not scanned by the investigator (e.g., because the systems exist on a network diagram and could not be located, a decision was made not to conduct scanning on certain systems because of business risk, or the software scanning agent could not reach certain systems). As discussed above, without an understanding of the IT enterprise landscape, it will not be possible to fully understand what systems existed, but were left unscanned. At the end of the process, companies should understand not only what percent of the environment has been compromised by the criminal actor, but also what percent of the environment the company itself was not able to scan for indications of a breach. Again, a not uncommon scenario is that the forensic investigator presents that a small percentage of the environment was compromised but is unaware of (or does not inform the company of) a larger percentage of the environment where it is unknown whether compromise occurred.

Development of an intruder pathway. After developing an understanding of both the nature and scope of the investigation, those two steps should be combined to formulate an "intruder pathway." The ensuing diagram will show which systems were compromised, when, and for what purpose in the execution of the attack. Such a diagram will identify which systems were targeted in order to gain initial entry into the environment, which systems were accessed by the intruder as he traversed the network looking for valuable information to steal and what systems were compromised in order to exfiltrate data from the environment. Development of this pathway will also enable the company to identify systems that may have been accessed by the criminal actor for purposes of either network reconnaissance (i.e., learning the layout of the network by capturing user IDs and passwords) or business reconnaissance (i.e., understanding business processes to navigate to the targeted assets). This deeper understanding of the intruder activity will be instrumental in assessing enterprise risk from both a sensitive data and client intellectual property perspective, the importance of which is discussed below.

Understanding impact on compromised systems with sensitive data and client intellectual property. Regardless of the motive of the attacker in accessing or compromising a particular system, the type of data on the system and the level of access by the criminal to the system and/or to the data on the compromised system may trigger certain legal obligations. In order to determine what legal obligations may exist, companies should develop a risk-based approach to identify what sensitive data (i.e., personally identifiable information, customer data and other types of regulated data) may reside on systems accessed or compromised by the criminal actors. Often, scanning systems for particular data elements proves more reliable than merely relying on the relevant business owners' understanding of those systems. Absent specific forensic artifacts to directly prove or disprove a level of access, a broader understanding of where a particular system sits on the "intruder pathway" will be of particular value. There have been tremendous advancements in data analytics technology that can help an investigator identify sensitive information such as social security numbers, account numbers, protected health information and other personal information that may be widely scattered across a compromised network. Deployment of these tools should be carefully documented and the results properly recorded.

Understanding to what extent the incident is contained. Forensic investigators often rush to satisfy an increasingly nervous client in concluding that a particular incident is contained (i.e., any ongoing potential loss of data or information is stopped and further damage is prevented). Advanced criminal actors, however, might have spent days, months and sometimes years in a victim's environment prior to detection, potentially for the purpose of maintaining persistence, as discussed above. As a result, identifying their methods, tactics and techniques used in entering and reentering the environment in order to build out a containment approach often takes days, if not weeks or months. A deep and full understanding of the level of protection necessary to provide coverage against known attack vectors, methods and tactics with respect to all ingress points, egress points and malicious internal movement is necessary to fully understand any ongoing enterprise risk. Often, the worst thing a breached entity can do is rush to notify the public or regulators regarding the extent of a breach before the relevant facts are understood and documented. Such an approach can undermine the confidence of regulators, customers and employees if the company has to correct itself later after more facts are uncovered about the incident.

Full documentation of eradication and recovery of compromised systems. Finally, as part of an enterprise impact investigation, the company should develop a risk-based approach that is fully documented to ensure that malicious artifacts on compromised systems are removed and systems are properly restored or rebuilt prior to redeployment into normal operations.

Conclusion

As is the case with so many aspects of information technology risk management, the key to executing an effective enterprise impact investigation lies in the actions a company takes before an incident occurs. If a company does not maintain an updated and accurate data map or netflow diagram, an investigator will need to spend valuable time mapping the system once they are engaged, rather than collecting and imaging data immediately following a breach. It is critical for companies to regularly revisit their incident response protocols to ensure that investigators will have the information and resources needed to accurately reconstruct an incident and determine the true impact of an incident as easily and quickly as possible.

Depending on the scope and scale of an incident, the cost of a thorough forensic investigation can present a formidable challenge. Although not the norm, it is not uncommon for the cost of complex data breach response investigations to reach into the low- to mid-six-figure range for the investigators alone. Given that there is no apparent legal requirement to conduct an incident response in a particular way (and only vague guidance provided by HIPAA, as well as the PCI Data Security Standards, on how to conduct investigations), companies may be tempted to reduce the scope of the enterprise impact assessment to what they consider the bare minimum. This approach should be resisted for two important reasons: first, it may cause a company to misconstrue the true impact and depth of a breach, and second, a bare bones investigation will neither provide the company with enough information to take the steps necessary to prevent a similar breach from occurring in the future, nor will it plug other previously unknown security vulnerabilities unearthed during a thorough investigation. Complete, fully documented forensic investigations provide companies with the information needed to secure and update their systems to defend against future cyber attacks.

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

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