Articles + Publications | August 26, 2022

The Do's and Dont's of Cybersecurity Forensic Investigations

SPEAKERS

Ronald Raether, Jr. | Sadia Mirza | Kamran Salour

Published in Law360 on August 26, 2022.

According to the Verizon Wireless 2022 Data Breach Investigations Report, there are four prominent paths that threat actors use to gain unauthorized access into an organization's network:

1. Stolen or compromised credentials;
2. Phishing;
3. Exploiting vulnerabilities; and
4. Botnets.

Threat actors have exploited these four attack vectors to unlawfully access thousands of businesses, including those that are security-forward, forcing those business to respond to often costly cybersecurity incidents.

For example, according to IBM's 2022 Cost of Data Breach Report, breaches caused by stolen or compromised credentials had an average cost of $4.5 million. These costs include both the direct and indirect expenses.

Direct expenses include "engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services." Indirect costs include in-house investigations and communications.

Luckily for businesses, not all cybersecurity incidents require the same response or lead to the same costly outcomes. Not every potential phishing scam or exploited vulnerability will trigger the need to conduct a forensic investigation or to prepare a forensic report.

For many organizations, there may be dozens, hundreds or even thousands of security alerts triggered daily.

So when do businesses need to retain forensic experts to assist with potential or actual security incidents? As with many legal questions, the answer is that it depends.

What Is a Forensic Investigation?

A forensic investigation is an investigation performed by an independent third party, often under the cloak of legal

privilege. The investigation's purpose is to understand the nature, size and scope of the incident and to ensure that it is contained.

Consistent with its purpose, forensic investigators usually look to answer:

- Whether the network has been accessed by a threat actor;
- How the threat actor gained access to the network, i.e., root cause;
- What the threat actor did while in the network, e.g., lateral movement or access/exfiltration of data; and
- If the incident has been contained or eradicated.

After the investigation, investigators usually issue a forensic report — or a functionally equivalent document — detailing the nature of the investigation and their findings.

Why Is a Forensic Investigation Needed?

From a cybersecurity perspective, a forensic investigation may be needed to ensure the incident is contained and the threat fully eradicated.

Unfortunately, organizations often overlook forensics when an incident causes significant business interruption, e.g., in a ransomware attack, or when funds have been lost, e.g., in a wire transfer scam.

The focus, instead, is often on the recovery process, which may include restoring systems from clean backups, attempting to recoup lost funds, rebuilding systems from scratch, etc. Businesses must be careful, however, as returning to normal operations when the incident has not been contained may only lead to further damage.

For example, in a ransomware attack, restoring systems from clean backups when the threat actor still has a foothold in the system may prove fruitless if the threat actor can later encrypt the clean backups or execute a different exploit — e.g., exfiltration of trade secrets or sensitive consumer data.

Likewise, in a wire transfer scam, focusing only on the recovery of lost funds would be detrimental if a threat actor is still able to monitor the organization's emails, which may allow for subsequent attacks.

Conducting a forensic investigation is therefore critical to ensure that the incident is contained and eradicated and there are no hidden exploits or back doors into the network left behind.

So does every incident require a forensic investigation? No, of course not. Whether a forensic investigation is needed is likely a matter of judgment, and may require engaging different teams — e.g., information security, legal, information technology, product, etc. — to assist with the decision-making process.

This is one reason why cyberinsurance is beneficial as it provides businesses with access to readily available experts — such as outside counsel and forensic firms — who have substantial experience with these types of matters and can provide guidance in connection with the same.

Why Can the Business Not Conduct the Investigation Itself?

Businesses may shy away from third-party forensic investigations for one simple reason — they cost money. This is especially true when the business believes, often in good faith, that its security team can perform the same investigation without incurring any additional costs.

While there may be situations when engaging a third-party forensic firm is not needed, businesses must be mindful of the legal implications of doing so.

Typically, third-party forensic firms are retained by outside counsel on behalf of the victim-business for the purpose of seeking or obtaining legal advice and/or in anticipation of litigation. This, in turn, allows businesses to claim privilege and work-product protection over the investigation and related communications.

While recent judicial decisions have reaffirmed that establishing these protections involves a highly fact-sensitive inquiry, businesses may have a difficult time arguing that protections apply to investigations conducted internally, which are likely to be viewed as serving a business — and not a legal — purpose.[1]

Because privilege is meant to permit candid and open communications without fear of them being used against the company, conducting a privileged forensic investigation that is intended, in part, to stop a criminal from further harming the company is likely in every organization's best interest.

Businesses may also want to engage a third-party firm to perform the investigation for optics. Indeed, being able to relay to regulators and affected individuals that a specialized third-party forensic firm was engaged to determine the nature and scope of the incident may not only be helpful when communicating about the incident but may also be expected — e.g., when reporting a data security incident to regulators, several of them require businesses to indicate whether a forensic investigation was performed.

Failing to do so may lead to further questions about the investigation itself and whether it was thorough and complete.

Lastly, engaging a third-party firm to perform the investigation may remove the appearance of bias. While certain in-house security professionals may actually be in the best position to investigate the cause and scope of a cybersecurity incident given their familiarity with the network, this could create obstacles — from an optics perspective — that could otherwise be avoided if a third party is used.

Do's and Dont's of Forensic Reporting

Investigators usually issue a forensic report at the end of the investigation detailing the nature of their investigation and findings. While these reports should be privileged when the relationship is set up properly through counsel, a good rule of thumb when it comes to forensic reporting is to assume that it will be part of litigation later on.

To this end, businesses, law firms and even forensic firms must take caution when drafting forensic reports.

Below are a few steps all involved parties can take to minimize the chance of creating bad documents.

Clearly Describe the Objectives of the Investigation

Often, businesses may engage a third-party forensic firm to conduct only certain aspects of the investigation. Thus, it is important for forensic reports to clearly describe the objectives of the investigation — i.e., what was the forensic firm tasked with — and the results of the investigation.

If a report does not discuss certain aspects of an investigation, and the investigation objectives are not delineated, one may assume that the report, and consequently the investigation, were incomplete.

Is a Forensic Report Even Needed?

Before tasking a forensic firm with drafting a forensic report, it is important for counsel to advise the risks and benefits of obtaining a report given the affected businesses' intended use of the report.

If the business wants a report to share the investigation findings with customers and clients, for example, then a forensic report may not be useful.

Forensic Reports Are Nonfiction Writings

Forensic reports should be purely factual. There is no room for imagination, opinions or speculations.

Rather, everything documented in a forensic report should be based on facts and supported by forensic findings.

Put Conclusions Upfront

This is a forensic report — there is no need for a plot twist.

Let the reader know upfront, perhaps in an executive summary, whether there was any unauthorized access or exfiltration of data or files. This point is critical as it determines whether the incident qualifies as a data breach under applicable laws.

No unauthorized access or exfiltration of data? State that clearly upfront as well.

Avoid Arbitrary Gradings, Scales or Severity Scores

Everyone involved in the drafting process needs to be mindful that forensic reports are often used against companies during litigation and regulatory investigations.

Assigning arbitrary grading scales or severity scores to the incident, or even components of the incident, are not likely to be useful to the business and will likely be used against the business should the document become discoverable.

Omit General Security Recommendations

While it may be tempting to include security recommendations in a forensic report, recent case law suggests that doing so may hurt the business's position that the document was created for legal purposes.

Thus, it is recommended to omit security recommendations from the report altogether, and have that discussion verbally, if needed.

For this same reasons, forensic firms should also avoid using forensic reports as a means to sell other products or services.

Mark it Privileged and Confidential

If the forensic report is intended to be protected, be sure to mark it as such.

While failing to do so will not likely compromise the protections, it will likely create unnecessary obstacles that could have been avoided if the proper markings were included.

---

[1] For additional information about privilege in the context of incident response, see Troutman Pepper's article, "Focusing on the Primary Purpose: Protecting the Attorney–Client Privilege and Work Product Doctrine in Incident Response," *Cyber Security: A Peer-Reviewed Journal*, July 11, 2022.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber