NISOS
Webinar Brief

# Why Attribution Matters: A Legal Perspective


## Executive Summary

Identifying your adversary is critical for determining the parties from whom redress can be sought. While a John Doe defendant may get the discovery process rolling, there's likely not a litigator out there who would argue that failure to attach a real person or company to the other side of the matter is anything but significantly sub-optimal. At the most basic level, failure to name a defendant robs the plaintiff of the opportunity for redress and dramatically reduces the deterrence effect.

Less obvious to both in-house and outside counsel are the impacts within the victim organization and, in particular, their security team's efforts to prevent future incidents. Whether the threat actor's motivation is financial, political, or other, the attacker's motivations, tactics, techniques, and procedures tell security teams and lawyers how to contain damage, and from where to seek retribution. And that's where a lawyer and security practitioner's ability to rely on accurate attribution of a threat actor becomes important. Once an organization has those answers, damage control can begin, better technical controls can be implemented, future exposure can be minimized, and criminal or civil legal recourse can be undertaken.


## Attribution vs. Unmasking

The definition of attribution and/or unmasking is subject to ongoing debate.

- Attribution can be defined as the attempt to identify threat actors based on an understanding of their behavior, beliefs, and intentions - as shown through the footprint they leave behind, or their actions. Organizations that understand how the threat actor is taking advantage of an entity, their motivations, and how to address those factors can gain a foothold on stopping the ingress of threat actors through the level of understanding that attribution can bring.
- Unmasking, on the other hand, is generally defined as physically identifying the threat actor as an actual individual or group of individuals.

Attribution is also influenced and defined by the value of the potential universe of outcomes. If an organization is facing an ongoing and unresolved threat, immediate value can be gained by attributing or unmasking. Context around how and why attackers are perpetrating crimes against an organization is important to implement the proper technical controls. Law enforcement generally doesn't care when a certain organization is targeted for cyber-crime purposes. However, technical controls alone may not be enough. In cases of economic or business impact, stronger measures of attribution and unmasking may be necessary in order to pursue civil lawsuits or retribution against named individuals.

## Different Perspectives of Security Leaders: Define the Scope

Security executives often make decisions based upon resources and results. Security leaders generally fall into two categories:

- Leaders who are compliance, governance, and risk focused
- Those who are investigations, response, and intelligence focused

In many cases, security leaders do not care who is attacking them; they simply want to maintain confidentiality, integrity, and availability of information. And, of course, they want to stop the attack. Others want to build relationships with international law enforcement entities to ensure the perpetrators are identified and do not continue their attacks.

Regardless of the path, security leaders need to determine the scope of the investigation to achieve an appropriate outcome.

- If an organization has a business email compromise issue, the response may not warrant anything beyond the implementation of simple technical controls.
- If an organization has insiders or associates of insiders manipulating its stock price, the impact on brand reputation and the potential for lawsuits may warrant aggressive attribution and unmasking of the individuals responsible for the activity.

## Legal Leaders have a Different Perspective

In general, legal counsel will initially focus on the tactics and techniques of the perpetrators and the impact of the crime on the organization. Unmasking the attacker is not always a priority, but knowing how they operate is almost always relevant. The initial findings will influence how far to take the investigation. For example, if an organization has experienced a ransomware attack and the organization (or their insurance company) is inclined to pay the ransom, it's beneficial to have research to validate the attackers have a record of decrypting the victim's data upon payment.

Many incidents require notification of a security incident. During the notification phase, organizations often must inform customers, regulators, or suppliers. At this point, the tactics and techniques may matter less, and attribution may matter more. In these cases, lawyers generally are:

- Reviewing whether the stolen information was accessed or acquired, and
- Determining the extent of harm to those impacted.

By attributing the threat actor group responsible, all impacted parties can achieve better insight into the actor's intentions with the stolen data. Attribution can help create a defensible narrative. It can also help inform regulators, customers, or shareholders of the level of sophistication of the attack and whether the security measures that the attacker defeated to gain entry into its corporate perimeter were reasonable.

Further, sometimes attribution and unmasking are the strongest mechanisms for deterrence to get malicious activity to cease and desist. Some examples of this working effectively are:

- Contacting the perpetrator's family members or employer and ask them to stop
- Law enforcement conducting a "knock and talk" without prioritizing prosecution
- Rolling back anonymity by filing civil lawsuits and sending cease and desist letters
- Working with law enforcement to prioritize prosecution

## About Nisos

**Nisos** is the Managed Intelligence℠ company. Our services enable security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation and abuse of digital platforms. For more information visit: **www.nisos.com**

*This briefing is not legal advice and is provided for general informational purposes only.*