NORTON ROSE FULBRIGHT

How To Navigate Advanced Persistent Threat (APT) Intrusions

This article provides an overview of concepts counsel must account for when navigating an APT intrusion or any sophisticated attack.

By **Chris Cwalina**, **Steven Roosa** and **Tristan Coughlin** | February 28, 2020 at 02:30 PM

Advanced Persistent Threat (APT) intrusions are sophisticated cyber-attacks carried out by well-funded and organized cyber-criminals, nation state actors or, more recently, a combination of both. The attacks are designed to establish persistence using various tactics, techniques and procedures (TTPs) that are intended to avoid detection and mimic authorized activity in the environment, known as "living off the land." APTs' goals may include the acquisition of intellectual property, personal data and financial information or the compromise of infrastructure or specialized data. APT intrusions often result in the unauthorized actor achieving part or all of their objective and can lead to serious reputation and financial damage to a company.

Below is an overview of concepts counsel must account for when navigating an APT intrusion or any sophisticated attack.

Directing the Investigation; Establishing Privilege

As soon as a potential APT intrusion is detected, it is critical to engage attorneys to direct the investigation and establish attorney-client privilege. APT intrusions may involve significant "dwell" time, which means evidence may not be available or definitive. Indeed, APT activities often relate to preexisting vulnerabilities in an environment—even ones that may have been identified by the client. Further, decisions made after the discovery of an incident with regard to containment, remediation, forensics and evidence collection may impact a company's liability down the line. Therefore, it is important to establish privilege at the outset of an investigation.

External counsel should retain third-party assistance, such as forensic investigators, for the purposes of providing legal advice. When external counsel directs third-party forensic investigations and appropriate privilege protocols are in place, courts have generally held forensic investigator's records, reports, communications and other materials related to the investigation are privileged and thus do not need to be disclosed during litigation or regulatory proceedings.

Privilege is never absolute, but clients can take steps to strengthen their position. At least one court has held that documentation related to the forensic investigation of an incident by a third party was not privileged because the third party was already engaged to assist with other ongoing work streams when the third party discovered the incident and the amended statement work did not change the scope or purpose of the third party's work other than to have the third party report to counsel after the incident was discovered. Companies can better establish privilege if counsel engages the third party for the purposes of providing evidence that enable counsel to provide legal advice. In addition, this work stream should be outside of any previous work stream and in anticipation of litigation or regulatory action.

Other Investigation Issues

APT investigations can be time-consuming and depend on how deeply immersed a threat actor is in an environment and whether the company has good visibility into its environment. Completing a thorough investigation is critical, and understanding the motives and TTPs deployed by an APT group can help streamline and focus an investigation on potential legal implications.

One of the first challenges of an APT intrusion is identifying the threat actor. Forensic teams can use TTPs to identify a threat actor, and if the actor is identified, lawyers can better understand and assess the motivation and risk of the attack. Identification will also enable IT teams to better implement containment and remediation measures. The legal team should partner with forensic teams and internal IT to stress test any findings and ensure all relevant evidence is appropriately collected and analyzed. The forensic teams and internal IT teams' findings will also assist the legal team in determining legal notification requirements based on the evidence available.

Law enforcement interaction can also be beneficial during an investigation and may be necessary depending on the APT and subject matter involved. Assistance is often a valuable resource and can provide known indicators of compromise (IOCs) from other cases, which can be instrumental in determining motive of the attacker. Law enforcement may also provide guidance on how to remediate and investigate a particular threat actor group. For a variety of reasons, including evidentiary and potential liability concerns, the legal team is the likely appropriate client team to interact with law enforcement.

Legal Issues

Whenever a cyber intrusion occurs, determining notification requirements is a priority. Whether to disclose an APT intrusion to another company, law enforcement, regulatory body, the government, or impacted individuals will depend on: (1) the type of company and data potentially affected; (2) the risk associated with such access; and (3) whether any personal data involved triggers data breach notification laws. This analysis is rarely straightforward and requires deliberation on a number of legal implications and potential outcomes because it is both difficult to identify an APT group and, depending on the APT's skill level, only a limited amount of evidence may be available.

Recently, cyber incidents have prompted increased litigation and scrutiny from regulators both in the United States and internationally. Accordingly, decisions to disclose must be made carefully and with a firm understanding of the investigation and the state of the network when the incident occurred. Lawyers are in a better position to present their client's case to regulators when they are familiar with a company's technical and administrative controls and are fluent in applicable legal requirements. Importantly, lawyers steeped in the realities of a company's environment are best-positioned to explain that reasonable security measures were in place despite the intrusion.

With regard to litigation, fully understanding the actions and motives of the threat actor will inform legal strategy. Certain APT groups are known to steal personal data for immediate monetary gain, whereas other APT groups may steal data for monitoring and surveillance. Motive is important because there is currently a circuit split on when class action plaintiffs have standing. Courts agree that alleging actual monetary damages satisfies the "injury in fact" requirement of standing, but courts are split on whether "substantial" risk of future or unknown harm is enough to satisfy standing requirements.

Best Practices and Lessons Learned

Many companies have been compromised, are compromised or will be compromised. Regardless, there are things a company should do now to prepare. An APT intrusion will place an exponential drag on a company's productivity—evidence of a breach will bring scrutiny to any decisions made about security. Companies should expect to explain and defend how cybersecurity was prioritized and handled.

Before an APT intrusion occurs, in-house counsel should help determine whether the client has a defensible cybersecurity program in place. If a company is not sure, consider a compromise assessment overseen by legal or outside counsel. And a company should make sure legal and information security teams have a collaborative relationship—and that they don't get to know each other during a breach. In practice, this means that they work together on everyday cybersecurity incidents, test an incident response plan, work together on a governance program, and meet outside counsel and third parties before they need them.

Below are best practices to consider during an intrusion:

- Engage outside counsel to lead the investigation. If not already selected, ensure experienced outside counsel is brought in to lead the investigation before any third party, including any forensic vendor, is substantively engaged.
- Establish protocols. At a minimum, protocols should state: (1)

the investigation is being led by legal counsel who will instruct all external advisors, (2) the objective of the investigation (e.g., to inform legal analysis of obligations, liability, risks, and/or in contemplation of anticipated legal or regulatory proceedings); (3) key work streams; (4) investigation team composition; (5) communication/ reporting lines; (6) steps taken to preserve evidence including the issuing of legal holds; and (7) communications protocols.

- Identify key people involved in the incident response team (IRT). Often we have found that even when an IRP does exist, the team composition is too large and roles and responsibilities are unclear, especially with respect to material decisions that need to be made quickly. A company's IRP should make clear the governance structure, decision-making authority, and the team structure.
- Establish communications protocol. Communication protocols are critical to protecting attorney-client privilege and controlling the incident narrative both internally and externally. Only those necessary should receive internal communications. External communications should be tightly controlled and limited to a need-to-know basis. No communications should be released without prior approval of legal. Failure to control internal and external communications can lead to leaks and result in statements harmful to future litigation or regulatory defenses. Statements may also cause reputational harm or lend themselves to misinterpretations that make the company look like they were hiding something or purposefully misleading consumers.

Legal teams are a key component of any successful cyber incident investigation, even more so when the incident involves an APT. We continue to see the same mistakes being made. The information in this article provides a snapshot of some of main issues we regularly see.

Chris Cwalina is Norton Rose Fulbright's global co-head of data protection, privacy and cybersecurity. Steven Roosa is the global law firm's US Head of NRF digital analytics and technology assessment platform. Tristan Coughlin is a senior associate in the data protection, privacy and cybersecurity practice.