The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 10 May 17, 2017

TECH MEETS LEGAL

Investigative Realities: Working Effectively With Forensic Firms (Part Two of Two)

By Stephen Surdu and Jennifer Martin
Covington & Burling LLP

Lawyers and forensic investigators must work together when investigating breaches, but the differences in their outlook and approach can sometimes make that difficult. This article addresses how to work with forensic teams when documenting and otherwise communicating findings, and during the remediation process. The first installment of the series addressed investigative realities and how attorneys and forensic investigators can gain an understanding of each other's perspectives and preemptively discuss any potential issues to be in the best position to address them efficiently during an investigation.

See also The FCPA Report's three-part series on forensic firms: "*Understanding and Leveraging Their Expertise From the Start*" (Feb. 22, 2017); "*Key Contract Considerations and Terms*" (Mar. 8, 2017); and "*Effective Vetting and Collaboration*" (Mar. 22, 2017).

Perspectives on Communications and Written Deliverables

One area where forensic investigators and lawyers differ significantly is in communications. Investigators are charged with identifying relevant systems, gathering logs and other evidence, and deploying forensic tools as quickly and efficiently as possible. During this problem-solving exercise, communications and information sharing between technologists often results in significant back-and-forth and the number of people involved in troubleshooting can quickly escalate.

Counsel, on the other hand, is primarily concerned with and quelling public or leaked speculation and preventing unnecessary disclosures of problems in the environment and oversharing of information. Most importantly, counsel has the responsibility to maximize the likelihood that formal attorney-client privilege and work-product doctrines will attach to protect the communications and work product associated with the investigation, thereby protecting clients from regulatory and litigation risks in the future.

Moreover, attorneys are expected to aggressively manage their clients' risks and present the facts of the situation in a way that is as favorable to their clients as possible, consistent with legal and ethical responsibilities. Investigators are expected to serve their clients including, as appropriate, by preparing reports that are objective and fact-based and mitigating any security risks to the environment. Although both parties have a risk-management objective, investigators are not as inclined to consider a client's broader risk profile.

Both parties should recognize the need to record the forensic methodologies and factual findings to establish the reasonableness of the investigation, and the credibility of the conclusions. However, they may differ on the best way to protect that information and what type of content is important to document.

Final Reports

Lawyers are very sensitive to how documents may be used in litigation proceedings and by regulators. Forensic reports may contain sensitive work product and security information, and can be used, sometimes unfairly and out of context, to pick holes in the analyses and undermine the forensic work. Similarly, discussions of strategic options, differences in opinion, and other work product created during the course of an investigation can also be used to weaken a client's position. For those reasons, lawyers are very

careful as to how they frame the content of reports. Typically, anything other than precise factual conclusions supported by evidence and unassailable logic will be questioned and omitted.

Forensic investigators recognize that their reporting may be evaluated by other law firms, regulators, law enforcement and even their competitors – sometimes years after the investigation. The long-term concern about the reputational impact of this scrutiny may influence their willingness to accept edits from counsel, including suggestions to omit findings, assumptions, reasoning, or final conclusions that may disfavor their client. This occasionally leads to tension in the discussions when reports are being finalized.

Often, counsel determines that it would rather not prepare a final report at all. Such a decision should not be confused with a failure to keep accurate notes of methodologies and findings, or the failure to prepare a technical forensic report. Rather, counsel may determine that the risk of discovery of potential evolving or seemingly inconsistent findings or conclusions outweighs the need for regular written interim reports, or a final summary report of the incident.

Interim Reports

Investigators generally have a strong preference to produce both interim and final reports. For investigators, a benefit of producing interim status reports is that it allows the investigators to organize their work so they can better articulate status, plans and issues. As noted previously, in complex situations consisting of multiple system analyses, it can be very difficult to keep track of the status of the investigation as a whole or what analysis should be prioritized without a well-organized and written summary.

Focusing on How to Document

To investigators, ambiguous guidance regarding what can be written and what cannot makes it much more difficult for them to solve complex problems. If they are not confident they can produce documentation that they use to control their activities and ensure quality, their analysis will suffer. Without a record, it is harder to review processes and determine where mistakes have been made.

Thus, decisions on record creation should reflect a balance of competing needs: the importance of keeping track of investigative analyses and the need to communicate those findings at all levels of the organization while limiting the risk of unnecessary disclosures. The justification for maintaining work product and a case-management record needs to be understood in the context of long-term discoverability and communications discipline. It may be more important for lawyers and investigators to discuss best practices on how to document the investigative work in terms of necessity, tone, accuracy and precision, and audience, than whether to document the work. Proper management of communication will serve to increase efficiency and effectiveness throughout the investigation.

Again, investigators and counsel alike ultimately share the goals of discovering the truth so as to best position the client, and maintaining professional and ethical integrity and reputations. An understanding as to why information is, or is not, important in a written form is critical for achieving these objectives.

Law Enforcement Communication

Related to the issue of communication and risk of disclosure are the questions of whether and how to involve law enforcement in a cybersecurity incident. Many forensic investigators have law-enforcement backgrounds, and at times see collaboration with law enforcement as a natural part of incident response and information sharing. Legal counsel must view such communications in the light of their professional obligations to serve the interests of, most commonly, private organizations. This often requires weighing the competing costs and benefits of referring a matter

to law enforcement, including whether the incident is already in the public realm, international in scope, and/or presents a broader threat to public safety.

Given that this calculus is highly dependent on the circumstances of the particular incident, investigators generally should not reach out to law enforcement – or provide requested materials to law enforcement – without first involving legal counsel, and without a broader discussion among stakeholders. (There can be exigent circumstances, however, that might require immediate reporting to law enforcement.)

When cooperation with law enforcement is deemed prudent, the mechanisms for safeguarding the confidentiality of information and communications must still be determined. In some instances, asking law enforcement for a warrant or subpoena to compel disclosure may be appropriate, while in other cases consent may be the best approach to maintaining control over information flows. Law enforcement agencies are accustomed to working with victimized companies to assist with these nuanced legal concerns.

Similarly, it is not uncommon to enter into non-disclosure agreements with law enforcement, or seek other assurances to protect the confidentiality of shared information, to the extent possible within our legal systems.

See "*Law Enforcement on Cybersecurity Matters: Corporate Friend or Foe? (Part One of Two)*" (Jun. 22, 2016); *Part Two* (Jul. 6, 2016).

Remediation Timing and Approach

The steps that must be taken to resolve, recover from and remediate a particular incident can range from an immediate and simple restoration of a single device, to months of staging and planning activities that can impact the entire enterprise. The scope of recovery and remediation activity depends on the nature of the attackers, their objectives, the scope/extent of the incident, the defensive posture of the victim organization and the ongoing monitoring and alerting capabilities of the victim organization.

To best work with forensic teams, counsel should be familiar with how the various factors impact remediation planning and execution. These factors affect not only what steps will be taken, but also the timing of those activities.

Incident Complexity

The less complex the situation is, the easier and faster remediation tends to be. Ideally, remediation is performed as soon as the scope of the incident has been determined and any relevant evidence has been preserved. However, that may not be appropriate when the attacker has the motivation and means to counterattack. Nation states and some advanced criminal organizations fall into this category. Dealing with these advanced attackers is like a chess game: remediation strategies must be thoughtful, tactics coordinated, and solutions implemented in such a way that activities do not alert the attacker of defensive measures applied to the environment.

The remediation phase in complex cases requires significant planning and coordination. Rushing leads to mistakes and can result in the attacker undermining temporary remedial measures, retaking the network, stealing more information, and destroying important evidence. If the attacker counterattacks and changes his tactics it can require the victim to restart the entire investigation. Once this breed of attacker knows it has been detected, it often escalates to using more advanced and stealthy tactics.

This occurs more frequently than many victims realize. Over the years, many victim organizations believe they have successfully removed the attacker from their environment but the attacker came back. Sometimes this is, in fact, the case, but often, the victim lost the trail of a hiding intruder while remediation steps were being undertaken. The attacker simply abandoned his current tools and began using different techniques,

malware, IP addresses and accounts, which remained undetected. When this happens, the entire incident response must begin anew.

The Scope/Extent of Incident

The second factor that affects remediation is the scope or extent of the compromise. The more limited the scope of the incident, the less time the investigation should take and the more limited the remediation activities typically are. Regardless of the sophistication of the attacker, the more systems that are compromised, the more account credentials that are stolen, and the more vulnerabilities that an attacker has leveraged, the more involved the remediation will be. Large enterprise-wide breaches that involve hundreds or thousands of systems in large networks spanning dozens of data centers often require months of remediation planning, quiet implementation of improved defenses, and a high degree of coordination to ensure the environment is free of the attacker.

The Victim's Defensive Posture and Monitoring Capabilities

Lastly, even a well-planned remediation strategy will not succeed if the victim does not have the ability to recognize and defend against counterattacks. Oftentimes, those very limitations allowed the victim to be compromised in the first place. Consequently, victims of advanced attack groups must improve their defensive posture and monitoring capabilities concurrent with conducting their investigation if they are to reduce the likelihood of another compromise subsequent to their remediation. Examples of interim remediation steps that can be initiated concurrent with the investigation are:

- improving logging by activating more logging sources, making the logging more detailed or extending log-retention periods;
- improving device-hardening practices and implementing those practices for new system deployments;
- implementing commercial software such as multi-factor authentication that address known weaknesses in the security posture;
- upgrading unsupported operating systems;
- instituting more robust network segmentation - especially for enclaves housing sensitive data; and
- implementing a formal security information and event management (SIEM) platform.

It is prudent to carry out these improvement activities without raising the attacker's suspicions that he has been discovered. The victim organization should undertake general security-improvement steps that could be viewed as usual and customary, but it should avoid targeting the specific vulnerabilities being used by the attacker.

An example of an appropriate interim remediation step would be instituting a stronger password policy and implementing it in applications and operating systems across the enterprise. However, implementing a forced enterprise-wide password reset for all employees is an inappropriate interim remediation step if it signals to the attacker that he has been discovered. Forced password resets are typically reserved for remediation when the objective is to force him from the network.

Timing

Although remediation planning, preparation, and staging often occurs over a period of time, there are other instances where it occurs almost immediately. In the case of a DDoS attack, mitigation and remediation activities commence as soon as the attack is identified. Likewise, a website defacement is likely to be addressed in very short order. However, removing an advanced attacker from a very large network is a much more nuanced process.

In advanced threat situations, it is important to understand the extent of compromise as completely as possible before attempting to remediate. At the same time, the best chance of success exists early in the process when the attacker is unaware

they have been discovered. To paraphrase Albert Einstein, remediation should occur as soon as possible, but no sooner.

Once remediation preparation steps have been completed, the best criterion for deciding when to remove an advanced attacker from an environment is when all of the attacker's actions are being captured in both host-based and network-based evidence in near-real time. When investigators have achieved that degree of visibility and immediacy they are in the best position possible to take back their network.

If the victim organization cannot allow that kind of ongoing activity due to risks or business disruption, then a decision needs to be made about when to force the attacker out of the environment and how. That decision requires a balancing of risks, including the potential loss in visibility and evidence gathering, by all of the stakeholders.

The timing of the remediation event can be subjective in many cases but the better the decision-makers understand each of these factors, the more likely the remediation will be appropriately timed and successful.

See also "*Key Strategies to Manage the First 72 Hours Following an Incident*" (Feb. 8, 2017).

Three Further Steps to Avoid Pitfalls

The concepts described in this article provide a solid foundation for improving the working relationship between counsel and forensic investigators. Further steps that lawyers should take to enhance their effectiveness in investigations include:

1) Deepen Technical Understanding to Fulfill Fundamental Legal Responsibilities

Technical education and experience are great foundations to have when involved in cyber-incident investigations, but many lawyers learn the same way most forensic examiners do: they gain experience one engagement at a time, ask questions of their colleagues, and refine their approaches.

Lawyers need not know how to image a drive or perform memory forensics to add insight and value into managing risk. By gaining some knowledge of security and technical fundamentals, and the types of digital evidence that may exist, lawyers bring a new perspective, can test the strength of forensic analyses and conclusions, and develop legal strategies based on a clear understanding of the facts as supported by the evidence. The early and continuous involvement of knowledgeable legal counsel in an investigation is part and parcel of successful incident-response work, and an essential requirement of the legal team.

2) Identify the Best Individuals

Skills and capabilities can vary significantly from one forensic investigator to another. They all have different strengths or capabilities. No single firm is equally strong at litigation support, white collar crime, commodity threats and advanced threat investigations. No single firm addresses all geographies equally well. The largest organizations do not always have the best capabilities. Identify the individuals, not firms, who have the most desirable skills and constantly evaluate their capabilities. The capabilities of firms tend to ebb and flow with the comings and goings of individuals who are experts in these areas.

3) Remain Current on the Major Trends

Cyber threats evolve over time, but many of the same factors that allowed attackers to be successful 10 years ago allow them to be successful today. Users continue to make mistakes. Malicious insiders create upheaval for organizations. Attackers penetrate victim networks using social engineering, known vulnerabilities, and stolen credentials.

That being said, significant changes in technology have changed how investigations are performed. The network perimeter has dissolved as mobile devices and cloud computing have become more prevalent. Ransomware is now highly automated. Attackers target major data-aggregation points rather than individual targets. Security operational support is being outsourced more frequently.

Organizations are still battling people with the same malicious motives. Traditional common-sense investigative skills and experience remain essential for both attorneys and forensic experts. The different perspectives and insights both groups bring to investigations should not be seen as obstacles. Instead, they should be viewed as assets that enable them to meet shared objectives.

See also "*Eight Attributes In-House Counsel Look For in Outside Cybersecurity Counsel*" (Jun. 8, 2016).

Steve Surdu has more than 30 years of experience in information technology consulting, working with clients in many industries - playing senior executive roles at security consulting firms such as Foundstone and Mandiant. As senior advisor at Covington, he assists clients in a variety of computer security areas such as strategic planning, defensive posture development and incident response. He supports clients so they can improve their internal security capabilities, mitigate risk associated with mergers/acquisitions, resolve cybersecurity incidents and more effectively deliver their own security products and services to the market. Mr. Surdu's extensive experience in responding to large-scale computer security breaches, through which he developed a thorough understanding of various threats, includes investigating site defacements, personally identifiable information thefts, ACH account fraud, payment card thefts, ATM cash drawdowns and intellectual property thefts.

Jennifer Martin has worked at the intersection of law and cybersecurity for over 18 years, currently as of counsel at Covington. Her expertise in this area has been uniquely honed through her experience managing cyber risks and responding to threats from a variety of perspectives: as the director of cyber incident response and operations, as lead in-house internal investigations counsel at Symantec; as a managing director of a top cybersecurity and forensics consulting firm; and as a federal and local cybercrime prosecutor and policymaker. She has supervised countless cyber incident response matters, including data breaches, insider thefts of trade secrets, and intrusions, from initial detection through containment, notification, recovery and remediation. She is recognized for her skill in building effective cross-functional teams comprised of critical stakeholders — impacted business units, and legal, technical, and communications departments. In addition, she has advised executive leadership on programmatic strategies for mitigating cyber risk, and on evolving legal, regulatory and ethical expectations and requirements.