March 2, 2015

Weil

Alert
Cybersecurity, Data Privacy & Information Management

The Key Players in Cybersecurity Investigations

By Robert F. Carangelo and Paul A. Ferrillo

Following detection of a cybersecurity breach or discovery of potential indicators of one, a company will face numerous challenges that must be addressed quickly. The situation can rapidly deteriorate, particularly because at that point in time, it is likely that the hackers have had access to the company's network for months, if not longer. Additional data exfiltration could occur, surfacing previously undisclosed thefts of customer information or key intellectual property. Depending upon the intrusion, malware or wiperware could further damage both the network and physical infrastructure of a company. These are but a few of the ways that a cyber-breach can evolve from the point of detection, but they highlight the importance of a rapid response and investigation.

Companies need to consider this potential scenario, and the planned response, well in advance of an actual cyber-attack. Key to an effective response are three important actors: an experienced outside lawyer, a skilled cybersecurity forensic investigator, and the general counsel.

In previous articles we have emphasized the need for an incident response plan (IRP) that can be implemented and executed on short notice.[1] Here, we explore the interplay between the roles and responsibilities of a cyber forensic investigator, outside counsel, and the general counsel of the company during the investigation portion of an IRP following a breach. It can be crucial for a company to execute such an investigation in a coordinated and efficient manner, as it and the information it generates will be important when responding to various inquiries, as well as to potential lawsuits.

Role of Outside Counsel

Large companies typically have capable in-house legal staffs that can handle many stages of the investigative process after a cyber-breach is confirmed by the IT department. However, one of the most important reasons why a company should work with an outside lawyer in the event of a cyber-breach is it needs to ensure that it maintains attorney-client privilege and attorney work product protections. Doing so will help minimize issues regarding the capacity in which the in-house lawyers are acting, and will offer the best argument for protecting communications about the results of the data breach investigation, and related communications between the forensic investigators and the company.

Though scenarios will vary based upon the severity of the breach, there are many communications, actions, and potential disclosures that should be considered and coordinated between the company, the forensic investigator, and third-parties.

1. If criminal conduct is a possibility (especially if the cyber-attack is suspected to have been perpetrated by either a nation-state or cyber-terrorist organization), it may be necessary to quickly contact the FBI and/or the U.S. Secret Service to assist with the investigation. Each has different investigative tools at its disposal to pursue cybercriminals, and one or both may have had experience with the same actor with respect to different targets. The government may have useful information that can assist in not only identifying the full nature of the breach, but also potentially in remediation efforts.[2]
2. If insiders are suspected of the theft of important information or funds, it may be necessary for outside counsel to conduct an internal investigation so that the facts of the potential insider theft can be determined.
3. As is critical in most investigations, the outside lawyer and the forensic investigators must work together to forensically copy network servers and hard drives, secure all evidence necessary to assist with containment and remediation, and help all involved constituencies (law enforcement, regulators, and the public) understand the full extent of the breach.
4. If personally identifiable information (PII) was stolen, data breach notifications to customers or patients may be necessary under federal and state law. Depending upon the industry, communications may be necessary with one or more regulatory authorities. If confidential personal employee information was hacked, disclosure and communications between the company, its HR department, and its employees likely will be necessary, as well.
5. Finally, if the breach is substantial enough as to be deemed material under federal securities laws, public disclosure to investors is likely necessary.[3] Outside counsel may also be helpful in drafting the appropriate disclosures and in responding to inquiries from the SEC and other regulators.

The Role of the Cyber Forensic Investigator

There are scores of cyber forensic investigators in the marketplace for both large and small companies, and many companies have pre-existing relationships with cybersecurity vendors. There are also a number of ways that an investigation should be tailored based upon the initial indicators of compromise that are detected internally, and based upon the size of the company. Below are factors to consider when selecting a cyber forensic investigator:

1. **Experience:** There is nothing more important than experience. Today's major breaches are carried out by sophisticated cybercriminals focused on the wholesale destruction or theft of millions of pieces of customer or patient data. The malware tools used are complex and have likely been masked throughout the breach process. The time-lag before discovery on the network gives hackers a huge head start. The forensic investigator should have major breach experience and also be able to identify and understand the various threat vectors and signatures that could have been used based upon other attacks. While each incident is different, and the choice of a forensic investigator will often depend on the magnitude of the breach, a more expensive (but experienced) vendor may be able to shorten the investigation, remediation, and recovery time necessary to fix the breach.[4] As noted by one IT commentator, being able to apply analytics sets good cyber forensic investigators apart:

   > Analytics is about the ability to extract meaning, sort through masses of data, and in patterns and unexpected correlations. It's not about knowing everything − it's about finding what is relevant and getting closer to the right elements with the right people. To do that, you need to maintain a level of objectivity; set aside your personal and professional influences and biases and focus on the data. Forensics professionals cannot solely rely on technology to solve problems — they must build analytical skills that are learned and refined by thinking through trial-and-error.[5]

2. **Responsiveness:** Building relationships with forensic investigators before a cyber-attack occurs will help

achieve two main goals. It will increase the chances that the vendor will be available when needed on short notice, and the chances that it will be able to act faster.

3. **Credibility:** Given the technical nature of a cyber-attack, it is necessary to rely heavily on the forensic investigator. It follows, therefore, that vendors with experience and strong references are a safer choice. Additionally, the forensic investigator likely will need to interact with regulators and possibly courts, so finding one with stature is imperative.
4. **User Friendly:** Similar to using experts in other complex areas, one of the most important attributes of a good forensic investigator is to be able to translate complicated technical topics into plain English. Often, people who lack technical expertise will be making decisions and taking actions based on information provided by the forensic investigator, so the easier it is to understand the expert, the more informed the decision-makers will be.
5. **Retain the Right Team:** When a company is the target of a large-scale cyber-attack, it needs the best forensic investigator possible. However, there are different levels of expertise within a forensic investigation firm, so it is important to ensure that the team that attends the initial meeting with the board and/or general counsel is the same team that will run the investigation. Pay particular attention to the number two person on the team because she likely will be the one carrying the laboring oar.

The Role of the Company's General Counsel

The company's general counsel or designated in-house lawyer will manage communications and disclosures that likely will be necessary in the event of a material breach. It is critical that the general counsel is one of the first individuals contacted by IT after there is a confirmed cyber-breach. Working hand-in-hand with the outside counsel, the following responsibilities should be promptly considered by the general counsel:

1. Managing board and/or audit committee involvement and expectations.
2. Determining what information was stolen, and if it was customers' PII, consider disclosure obligations to customers, federal and state regulators, and law enforcement. If employees' PII was compromised, internal communications to employees and others may be necessary.[6]
3. Overseeing an internal fact investigation by outside counsel and forensic investigators, particularly if it is suspected that an employee or former employee may be involved in the alleged breach.
4. Working with a crisis management/public relations firm to draft appropriate disclosures aimed at reassuring customers and investors that the company has a firm grip on the problem and is resolving it as quickly as possible – especially given the potential for a cyber-attack to damage the company's reputation with consumers, investors, and other constituencies.
5. Working with outside counsel on SEC disclosures in the event that the cyber-attack is considered material under the federal securities laws.

Prepare In Advance

Many of the tasks and goals described above should be part of a company's cyber IRP. By practicing and testing the IRP with all parties involved, real-life execution will run much more smoothly. The better the preparation, the better the response will be.

---

1. *See* "The Importance of a Battle-Tested Incident Response Plan," available at http://blogs.law.harvard.edu/corpgov/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/.
2. *See* Mandia, et al., "Incident Response and Computer Forensics," (McGraw Hill, 2014), at 115.
3. *See* "CF Disclosure Guidance: Topic No. 2 (Cybersecurity)," Oct. 13, 2011, available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
4. *See* "FireEye is 'First in the Door' on Big Cyberattacks," available at http://www.dailyherald.com/article/20150214/business/150219416/.
5. *See* "Tech Insight: What You Need To Know To Be A Cyber Forensics Pro," available at http://www.darkreading.com/tech-insight-what-you-need-to-know-to-be-a-cyber-forensics-pro/d/d-id/1139922?.
6. *See* "M-Trends 2015: A View from the Front Lines," at 5 (discussing rise in data breach disclosures), available at https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

Cybersecurity, Data Privacy, and Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy, and Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Robert Carangelo	Bio Page	robert.carangelo@weil.com	+1 212 310 8499
Paul Ferrillo	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372