ORRICK

CORPORATE COUNSEL

Is It a 'Cyberattack' or a 'Data-Breach Incident'?

Section: From the Experts
July 25, 2014
By Mark Mermelstein, Antony Kim and Robert Uriarte

While it is said that in war history is written by the victors, in the context of a highly publicized cyberattack it's worth considering whether history can be written by the victims. The public thirst for information (and sensationalism) that typically results from announcement of a cyberattack involving data theft provides an important opportunity for shaping the narrative surrounding the incident. But seizing on this opportunity requires a delicate balancing act. By providing too much information too soon, a victim may make damaging misstatements and thereby incur legal liability. But by providing too little too late, a company can significantly impair its public goodwill and incur the wrath of regulators—to say nothing of the plaintiffs' bar.

This article goes beyond the nuts and bolts of how to respond to a data-breach incident, and offers some lessons learned from the frontlines of the cybersecurity war to help companies successfully navigate the legal and public-relations minefield that ensues.

Responding to a cyberattack such as one that results in consumer personally identifiable information (PII) being accessed and even exfiltrated through a vulnerability in the company's computer system can feel like fighting a multiheaded hydra. The various stakeholders involved—company management, members of the board, regulators, outside auditors, shareholders, affected consumers, customers and potential customers, vendors and suppliers, banks and credit card brand companies, state and federal regulators, class action lawyers, and even Congress—are all evaluating their options.

The victim company may want to approach law enforcement officials to encourage them to investigate and criminally prosecute the perpetrators. Regulators such as the state attorneys general and the Federal Trade Commission will want to ensure that the company's statutory notification obligations have been fulfilled, and may consider bringing claims against the company for failing to maintain adequate security measures around the information in the first place. Consumers whose PII was compromised may have similar claims against the company for the damages they've incurred. Banks will want to recoup from the company any costs they've incurred as a result of having to issue new credit cards or indemnifying consumers for fraudulent transactions charged to their cards. Auditors will need to determine if the company's controls were and are sufficiently robust, and whether the attack affects the business or operations in any material way. The board will need to determine that company management has responded appropriately to the incident, that mitigation strategies were put in place and that a remediation plan to "fix" the vulnerability is in place and on pace. Shareholders will evaluate the confidence they have in the company in which they've invested and whether to consider derivative claims against management. Certainly, if management has made a false statement to the market in the immediate aftermath of the breach, such as downplaying the number

of affected consumers, and as a result the company's stock price falls, securities fraud claims are not beyond imagination.

On the flip side, companies that muzzle their spokespersons in favor of waiting for "perfect information" about the nature and extent of the breach and the remediation plan before making any public statements may lose credibility in the marketplace. They may also invite claims by injured parties who argue that they would have taken steps to protect themselves if only they'd known about the breach sooner. And of course, potential customers will need to assess whether they have sufficient confidence in the company's cybersecurity going forward that they will entrust it with their PII.

How, then, should management (typically with the help of outside counsel) administer the often competing agendas of these various stakeholders? It can be instructive to view a company's response to a cyberattack through the prism of how it will play out in front of a jury in the not-so-distant future (whether the "jury" is composed of the public, a regulator or the board). In more traditional litigation, litigators are brought in long after the relevant facts are established, after the incident giving rise to the litigation has occurred and after the conclusion of the post-incident remediation efforts the company has taken. In the context of a cyberattack, attorneys who can both counsel a company through incident response and address claims of all sorts that arise from the breach are typically on the scene hours after the breach is detected. Having litigators on the scene early creates a unique opportunity to shape the facts that will be central to any future effort to protect the company, including facts surrounding the company's investigation, remediation and notification efforts.

Rather than counsel being presented with a written script to present at a trial, litigators can help author the script. How does this play out in practice? In most breaches, all eyes are on the company, on how it was penetrated, on its cybersecurity (often, a lack thereof) and on its response to the breach. This focus can overshadow the fact that really well-organized (sometimes well-funded) criminal actors were engaged in sophisticated reconnaissance, penetration and exploitation, and often broke in and exfiltrated data without setting off any alarms.

In the home-invasion context, no one blames the homeowner who diligently locks his door and sets his burglar alarm when he nonetheless gets burglarized in the middle of the night. It's like measuring the effectiveness of a baseball pitcher after he's given up the game-winning home run. It would seem to be a losing proposition. The focus needs to be shifted—the company should be portrayed as the victim of a sophisticated cyberpredator.

Here are some lessons from the frontlines that can help move the narrative from the strength (or lack) of a company's cybersecurity to a story about the bad guys who perpetrated a sophisticated criminal attack.

- **Lesson No. 1:** It all starts with the way the incident is described. Words affect perception. Consider whether the incident should be referred to not as a "data-breach incident" but rather a "cyberattack," thereby subtly shifting the focus from the company (and that fact that it has been penetrated) to the perpetrator who has broken in.

- **Lesson No. 2:** We should expect breach victims to behave like crime victims. Crime victims report crime to law enforcement, report it quickly, and seek to investigate and prosecute the perpetrators.

Breach victims ought to consider that too and work with the assistance of counsel to cooperate with law enforcement by providing technical information and other support. While it is certainly difficult to recover lost data and to bring the attackers to justice, the effort is worth it even given the small chance of success.

- **Lesson No. 3:** Forensic consultants should be considered a partner in building the company-as-victim narrative. Consultants are often engaged simply to look for indicators of compromise, the attackers' method of intrusion and evidence of what was taken. But they should be directed to also look for evidence regarding the relative sophistication of the attackers. For example, they should consider whether the attackers exploited a vulnerability that could or should have been anticipated or one that was a so-called "zero day vulnerability" (i.e., a vulnerability that was not reasonably known by anybody until it was exploited by the attacker). In the latter case, the company is hardly a negligent actor; it was a victim of a sophisticated attack through an attack vector that *nobody* knew existed. They should also consider how many IT and security "hoops" the attackers had to jump through to access the company's crown jewels—again establishing the company's diligence and the attacker's technical expertise. And they should consider whether any methods or tools of subterfuge were deployed to explain why the attackers went undetected while in the company's system.

- **Lesson No. 4:** Think carefully before offering compensation. In a commercial burglary context, a company wouldn't immediately offer compensation to all of the customers who happened to be standing in the store at the time of burglary, whether or not they were injured. So, too, in the data-breach context, it may not necessarily make sense for the company to offer up free credit monitoring to all affected consumers, whether or not there is evidence that consumers have suffered any tangible losses. Offering up compensation early may send a message that the company is more culpable than it actually is. There are, of course, reputational and damage-mitigation reasons for offering credit monitoring, but these considerations should be carefully weighed against their potential costs

- **Lesson No. 5:** Plan carefully before deciding whether—and when—to go public with information. Recent incidents demonstrate the fine line between prompt and premature disclosure. In one recent incident, a company was sued for waiting too long to disclose a data breach when it reported the incident to the public a full four days after it detected the intrusion. But in another recent incident, a company was sued for making an inaccurate statement about the scope of data that was compromised. Cyberattack victims often find themselves between a rock and a hard place. Frequently there is a need to make at least some limited disclosure before an investigation is complete—perhaps because of a statutory notice period, a press leak, an attacker's public boasts (Twitter is a popular mechanism used by some malicious actors to claim bragging rights), or to provide an opportunity to the affected consumers or credit card brands to protect themselves such as by cancelling and reissuing new cards. On the other hand, the fact that a statement was made in haste or based on insufficient inquiry is rarely a justification for a misleading statement to the market about the nature and extent of breach, particularly if a company's share price falls as a result of the statement. The timing and scope of public disclosure is tricky. Best to learn the facts as quickly as possible. Forensic investigators retained under counsel's attorney-client privilege can investigate and provide preliminary results that arm the company to make accurate public statements.

- **Lesson No. 6:** Companies should be mindful of the attorney-client and work-product privileges and their critical interplay with parallel proceedings. Companies taking heed of lesson No. 2 above (cooperating with law enforcement) may be encouraged to share forensic information quickly, and often under the theory that the more information law enforcement is provided, the greater the chance they will proactively go after the bad guys. However, companies must realize that information gained during the course of an attorney-client privileged internal investigation, such as one conducted in the immediate aftermath of a data-breach incident, may lose its privileged status once that information is turned over to the authorities. The law in most jurisdictions is pretty clear that once privilege is waived over a certain document, it is waived for all purposes. This prohibition on "selective waiver" means that a company cannot provide information to law enforcement to aid in the prosecution of the perpetrators and then refuse to give that same information over to regulators or class action plaintiffs under the theory that it is shielded from disclosure under the attorney-client privilege. The same holds true for documents provided to outside auditors. As a result, extreme care needs to be given to what documents are created and to whom they are disseminated, lest a company be later prosecuted by the very reports it commissioned.

Finally, we suggest that companies also keep these tips in mind:

- Establish collaboration and trust with relevant law enforcement agencies before problems arise.

- To the extent that the company has come to the conclusion that regulator investigations appear likely, consider being proactive and forthcoming with them, as opposed to waiting for them to find you. Start developing the proper narrative, and begin shifting the focus to the criminal actors and away from the victim company.

- When responding to a data-breach incident, there are many moving parts. Different interests within the company will prioritize different facets of the response. Further complicating matters, an action that makes sense to the company's IT department may be harmful to the company's public-relations or legal interests. It's important for the company to have someone in charge. Data-breach responses require a quarterback, a well-organized response with adequate leadership—preferably by someone who is battle-tested.

Mark Mermelstein and Antony Kim are partners in Orrick, Herrington and Sutcliffe's Los Angeles and Washington, D.C., offices, respectively, and serve as co-heads of Orrick's privacy, data security and Internet safety group. Robert Uriarte is an intellectual property managing associate in Orrick's Silicon Valley office.