New York Law Journal
INVESTIGATIONS
&
COMPUTER FORENSICS

Tuesday, May 29, 2007

ALM

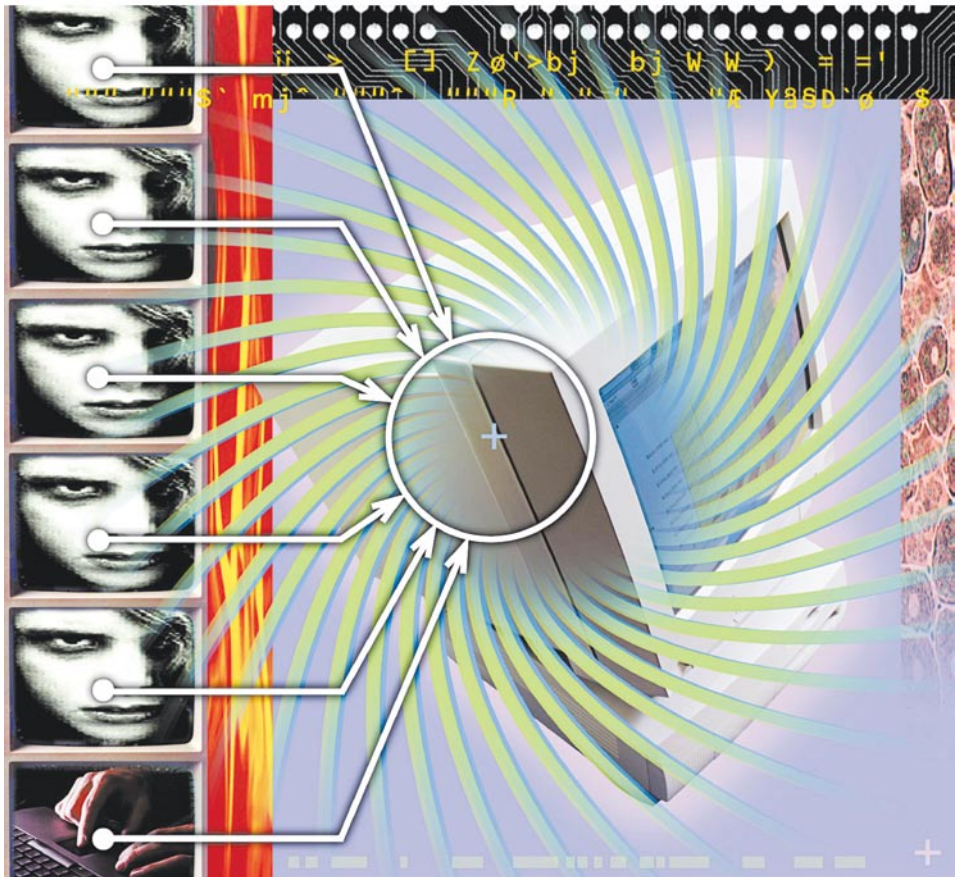
Data Breach!

Correct Response Crucial

**BY LISA J. SOTTO,
JOHN W. WOODS JR.
AND JOHN J. DELIONADO**

THE THREAT TO CORPORATE networks, and the information contained on those networks, has never been greater. While 15, or even five, years ago the compromise of computer data would likely have been the work of a lone hacker or disgruntled insider, there are increasing signs that these events are often the work of complex criminal organizations. The need for sophisticated professionals knowledgeable in the legal issues surrounding these events has increased.

Most individuals familiar with these events understand that a breach involving the compromise of personal data will trigger state laws requiring notification to affected individuals. For lawyers, however, these events pose a myriad of additional competing and important legal issues. Of critical importance is how a company handles a compromise event. The actions it takes in the first days after learning of an event can have a profound



ART BY NEWSCOM

Lisa J. Sotto *is a partner in the New York office of Hunton & Williams,* **John W. Woods, Jr.** *is a partner in the firm's Washington, D.C. and Richmond, Va. offices, and* **John J. Delionado** *is an associate in the firm's Miami office.*

The threat to corporate networks, and the information they contain, has never been greater.

effect, including the possibility of litigation, government scrutiny, negative public attention and the erosion of the organization's customer base.

Companies must recognize that a data breach requires actions that go well beyond simple compliance with state breach notification laws. Some of the issues about which a business may need legal advice are:

(1) conducting an investigation into the event;

(2) notifying auditors and the securities regulators;

(3) notifying law enforcement authorities;

(4) notifying contracting parties (such as payment card issuers);

(5) notifying regulatory agencies with oversight authority or consumer regulatory bodies; and

(6) notifying the public.

Investigating the Event

Given the issues that can arise, understanding the factual contours of the event are critically important. Most importantly, companies must recognize that upon discovery of an issue, the event should not be handled like just another problem for the Information Technology (IT) department.

Ignoring the threat is not an option, but it may be equally dangerous to engage the problem with inadequate resources. The most important step is for a company to retain a qualified network security consultant to conduct an investigation overseen by legal counsel. The structure of the engagement of outside experts in these events is critical, and these experts must be focused on conducting the investigation in a way that will best assist the company.

Many businesses have sophisticated counsel who are well versed in the litigation process and may have the ability to direct consultants and determine the source of the compromise. A word of caution, however.

Corporate counsel generally engage in a variety of functions within a company and often make or assist in its business decisions. This dual role of corporate counsel may serve to unravel what might have been a privileged internal investigation. Engaging and obtaining the advice of litigation counsel will best serve a company in such a situation since it provides to it the best chance to preserve available privileges. Legal privileges are hard to come by, and easy to lose.

Privilege extends to communications between a company and outside legal counsel. Courts also protect as "work product" any material prepared by a party or its attorneys or other representatives in anticipation of litigation.[1] Where an internal investigation is undertaken and experts are used, *United States v. Kovel*[2] provides the benchmark standard and must be considered by counsel. Courts have routinely applied the *Kovel* test to third party consultants ranging from accountants to patent consultants.[3] Where privilege has been properly protected, the work-product doctrine will extend to materials prepared for counsel by the consultants.[4]

A company must keep in mind that whatever is determined in the investigation, even where privilege is successfully protected, privilege "only protects disclosure of communications; [not] underlying facts[.]"[5] What will be protected by privilege in the event it is preserved are the judgments, strategy and recommendations by counsel and counsel's agent, the expert consultants.

Devoting proper attention to a breach event is a company's best chance to limit or, in some instances, avoid entirely any damage to itself. Taking all reasonably possible steps to preserve the privilege is fundamental when dealing with a breach, regardless of whether there was a compromise of personal information. How forensic experts are retained to go about the task at hand and who directs them can mean the difference between creating a valuable privileged engagement that can benefit a company versus a road map to would-be litigants and government regulators that documents a company's darkest hour.

After taking all prudent steps to best preserve privilege, the internal investigation must focus first on the nature of the compromise and how it occurred. Given that the response must begin immediately to determine the source and scope of the compromise, it is often necessary, or at least expedient, to have the outside consultant obtain information from a trusted internal IT professional within the company. As with any highly confidential and significant event, it is prudent to keep the circle of people circumscribed.

Inform Senior Management

The compromise of personal data has become a boardroom event.

The scope of the breach and the effect that it can have on a company may be an event that affects the corporate public profile and possibly its stock price in the event the company is publicly traded. Since a data compromise can have such a wide-ranging and significant impact, company management must be kept abreast of the information developed during the investigation, and particularly any significant revelations.

What the decision-makers in the organization must be informed of immediately is the security posture of the network and whether there has been compliance with relevant industry standards. In addition, a company needs to review whether it has followed its own information security policies and procedures.

Where an event is significant enough that the business' independent auditors must be informed, the auditors will undoubtedly seek answers to many hard questions. Auditors will focus on the findings resulting from the investigation as well as the methodology used in evaluating the event. They will also scrutinize the quality of the investigation and what it revealed.

For a publicly traded company, the decision-makers will need to evaluate whether a disclosure is warranted. Trusted securities counsel is essential to this process and should be engaged from the outset of the investigation to assist in making this critical determination.

Involving Law Enforcement

A compromise event is very often the work of criminals and not simply the result of negligence. Federal law enforcement has become increasing sophisticated and has developed the tools to identify and arrest those who commit criminal acts against a victim company.

The U.S. Secret Service has had great success with the Electronic Crimes Task Force that has been developed and flourished in many of the Service's large field offices and headquarters in Washington, D.C. This task force allies itself with state and local law enforcement as well to ensure that the best resources are brought to bear. Similarly, the Federal Bureau of Investigation has grown its crack Computer Analysis and Response Team and has had significant success combating computer crime.

Along with the Secret Service and the FBI, the U.S. Department of Justice (DOJ) now has a group of experienced and knowledgeable prosecutors to combat computer crime. At DOJ headquarters, there is now a group of trial attorneys in the Computer Crimes and Intellectual Property Section devoted to investigating and prosecuting computer crimes throughout the country. Further, many of the large U.S. Attorney's offices have sophisticated

Assistant U.S. Attorneys designated as computer and telecommunications coordinators experienced in investigating and litigating complex computer crimes.

The Computer Fraud and Abuse Act (CFAA) is the primary federal criminal statute that addresses computer crimes.[6] Potential criminal liability attaches when someone intentionally accesses a computer without authorization, typically known as an outside hack, or when someone exceeds authorized access.

In investigating crimes, law enforcement has the power and ability to go beyond the limitations of an internal investigation. Investigative techniques can include grand jury subpoenas, search warrants, Pen Registers (surveillance devices), Electronic Communications and Privacy Act warrants (which are essentially search warrants aimed at a user's account with an Internet service provider), and even Title III wire interceptions. Generally, any hope of catching the individual or group responsible for criminal conduct against a company depends on allowing law enforcement the time and ability to use the techniques available to it.

The state breach notification laws actually encourage companies to notify law enforcement by allowing a cooperating company to delay public notification in order to allow law enforcement to conduct a confidential investigation (assuming law enforcement agrees that a delay in notification would assist in its investigation). At least one state, New Jersey, has made notification to law enforcement a condition precedent to notifying affected individuals.

Notifying Contracting Parties

A company must evaluate whether it has contractual obligations to notify significant business partners of the compromise event.

Where payment cards are involved, the terms of the contract often require consultation with the card issuers in the event of a security breach. Where such obligation exists, the notification should be accomplished as soon as possible. Typically, a company will reveal the relevant facts discovered through its investigation, but not the privileged opinions of counsel or the experts.

Depending on the contract, the notice may need to take the form of a formal incident report filed with the card company. Further, card companies may require an independent audit by a data security firm conducted on their behalf and funded by the company that experienced the breach.

Contacting Regulators

Any company that is within a regulated industry will need to consult counsel about whether the entity regulating it must be informed.

There are strict guidelines, for instance, where a federally insured financial institution is involved since there is oversight by Federal Depository Insurance Company, the Office of the Comptroller of Currency, or the Federal Reserve. Compromise events, however, draw regulatory scrutiny even where a company is not federally regulated.

The Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act,[7] which prohibits unfair or deceptive trade practices. The FTC has demonstrated its commitment to investigate data breach events as it recently established a new division of Privacy and Identity Protection. The FTC looks to whether a company has failed to take appropriate action to protect personal information of individuals and, thus, constitutes an unfair or deceptive trade practice.

The FTC has focused its enforcement actions pursuant to Section 5 on security breaches. Notifying the FTC of the event and framing the circumstances can greatly assist a company in avoiding an enforcement action, rather than taking a more passive approach whereby the FTC may learn of the event through information in the public realm that may be rife with inaccuracies and hearsay.

Letting the Public Know

California was the first state to pass a law requiring organizations to notify affected citizens where their personal information was compromised.

As these compromise events came to light with some frequency in 2005 and garnered significant attention from the media and lawmakers, approximately 35 other states, plus New York City, Washington, D.C. and Puerto Rico, have enacted similar notification laws. At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that computerized sensitive personal information has been acquired or accessed by an unauthorized person in an accessible form.

State laws typically define "personal information" to include an individual's first name or first initial and last name, combined with one of the following: (a) a Social Security number; (b) a driver's license or state identification card number; or (c) a financial account, credit or debit card number, along with a required password or access code.

Where notification is required, it generally must be done in the most expedient time possible and without unreasonable delay. Companies are generally given time to investigate the event and, as discussed above, may be able to delay notification where they have notified law enforcement. In several states, however, including Florida, Ohio and Wisconsin, notification is required within 45 days of the date the incident was discovered.

Conclusion

Companies that are afflicted with a data breach cannot give such an event short shrift. As these events have become more widespread, public and government scrutiny over a company's handling of a breach event have increased. It is essential that victim companies take all prudent steps to prevent becoming further victimized in the legal courts or the courts of public opinion.

A company so afflicted must prepare to address the problem in a well-organized and meticulous manner, led by a team of sophisticated professionals able to recognize the myriad issues confronting the company. Recognizing that such a situation is front page news and not a back room event is the first step toward surviving the crisis and getting back to (successful) business as usual.

1. See generally *Hickman v. Taylor*, 329 U.S. 495 (1947).
2. *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
3. See, e.g., *In re Grand Jury Proceedings Under Seal*, 947 F. 2d 1188 (4th Cir. 1991) (finding privilege applied to communication with accountant where communication was "made for the purpose of facilitating the rendition of legal services covered by the privilege").
4. See *United States v. Nobles*, 422 U.S. 225, 239 (1975).
5. *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).
6. 18 U.S.C. §1030.
7. 15 U.S.C. §45.