CARLTON FIELDS

Catching Corporate Hackers In Fla.: Tips For In-House Counsel

May 09, 2016

In the aftermath of a hack, a general counsel's office should work with its information security staff to investigate the breach, issue notifications under Florida law, help with any media strategy, and coordinate with the C-suite to explain the incident to the board and investors. Counsel's role in catching the bad guys is often overlooked in this frenzy of activity. The following four steps offer guidance to in-house counsel who find themselves in this position. **1. Initial Investigation and Required Reporting in Florida** To determine the extent of the breach and the identity and location of the affected individuals, the company must gather and analyze the evidence of the intrusion. This initial investigation can yield important clues as to how the crime took place and who committed it. Counsel should therefore put in place a "litigation hold" that will prevent the inadvertent erasure of a hacker's tracks. This initial investigation should also identify the information security or information technology employees with knowledge of the systems through which the hack occurred. These key personnel can best explain the crime to law enforcement. Florida law requires individual notice when a company learns of unauthorized access to Florida residents' "personal information," such as a name and Social Security number or an email and password. If the breach involves more than 500 Florida residents, the company must also notify the attorney general within 30 days. Individual notice to Florida residents must be made within 30 days, unless a law enforcement agency determines that it would interfere with a criminal investigation. Such an authorized delay in reporting the breach would allow the company more time to plan its notifications and to put in place remedial measures. **2. Deciding to**

Push for a Criminal Investigation If reporting requirements have not led to a criminal investigation, counsel should next determine whether one is in the company's best interests. There are several factors to consider. On one hand, a criminal investigation might raise the company's risk profile for civil liability, depending on the company's role in failing to prevent the breach or detect it in a timely manner. On the other hand, enlisting law enforcement to investigate the crime alongside a company' s information security staff may help corporate counsel determine and understand what happened. Law enforcement has at its disposal grand jury subpoenas, search warrants, specialized databases, and relationships with other agencies, including abroad. Any information gained from such sources, if shared by the government, gives the company an advantage in responding to litigation from shareholders, consumers, and other entities, and allows for better, earlier remediation. Further, there is a growing expectation among shareholders and regulators that companies will engage with law enforcement in the wake of a breach. Corporate counsel should also determine whether they are comfortable with the level of business disruption that will result from government agents being onsite and the need to make witnesses available during the course of any investigation and prosecution. In addition, a prolonged investigation may keep the company in the news cycle beyond the story's natural life. If the hacker is arrested and goes to trial, the company's reputation could be damaged further by repetition of its failure to safeguard its data. Alternatively, if the company is a bank, insurance company, health care company, or other target likely to face repeat hacking, having a reputation for prosecution may deter future hacks. Complete, early and publicized cooperation with law enforcement regarding hacks is akin to the "shoplifters will be prosecuted" sign in convenience stores. And criminal prosecution results in far more deterrence than a company-filed civil lawsuit against the hacker. Finally, the company should consider what use law enforcement will make of any confidential corporate materials it gathers. An investigation carries with it the possibility of an arrest, the exchange of pretrial discovery, and a trial. Early on, the company should ask law enforcement about plans to protect trade secrets, embarrassing or sensitive materials, and other proprietary and competitive information. Generally, law enforcement agencies are sensitive to these concerns from companies and will work to address them. A confidentiality order offers one specific solution if the investigation results in a prosecution or other litigation. **3. Cooperating with Law Enforcement** Once counsel has decided to contact law enforcement, there are many things the company can do to increase the chances of a conviction. The first contact is critical. Depending on the size of the breach, counsel might start with a federal government agency such as the FBI or the Secret Service. Federal investigators typically have greater resources and can ensure greater punishment for hackers. In the event of a smaller breach, it may be appropriate to reach out to state or local law enforcement agencies directly, or through corporate security staff or outside counsel. Miami, Tampa and Orlando each have an Electronic Crimes Task Force (ECTF), a working group between federal, state, and local law enforcement and the private sector, organized by the U.S. Department of Homeland Security. This collaboration between law enforcement officers make it more likely the call will be directed to the appropriate agency. In addition to reporting cybercrimes through the local ECTF, a company may also notify authorities through other means, such as the FBI's Internet Crime Complaint Center. At the initial meeting with law enforcement following the breach, the company

should provide a single point of contact for future communications. This person should have sufficient authority to respond to law enforcement questions about the investigation and help agents access documents and witnesses. This person should also have sufficient knowledge of the company's information technology environment to interact meaningfully with a knowledgeable law enforcement professional regarding the breach. The odds of a successful prosecution increase if counsel drafts a "prosecution memo." This document is similar to what a prosecutor will ultimately create when seeking internal authorization to bring criminal charges. The memorandum from counsel should identify the statutes that were violated, the elements of each, and the evidence against the suspect on those charges. The memorandum should also explain why the government should accept the case for prosecution. Factors to highlight here are severity of the hack, the size of the loss, the disruption to the business and its customers, the estimated imprisonment for the perpetrators, and the need for deterrence. Although providing such a memo may waive the attorney-client privilege as to some aspects of the company's investigation, participation by counsel throughout the investigation maximizes the protections of the privilege and work product doctrine over any portions of the internal investigation that are not disclosed to the government. **4. Preparing for the Next Hack** Counsel should consider developing a relationship with law enforcement in noncrisis times. Depending on their industry, corporate counsel, corporate security or external counsel may have longstanding relationships with local, state, or federal agencies. The company's usual law enforcement contacts can make introductions to their cybersecurity experts. Finally, written planning around the first three steps, well before a breach, will contribute to better decisions when counsel inevitably find themselves in the crisis mode of an active breach. Republished with permission by Law360 (subscription required).

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology
White Collar Crime & Government Investigations

Related Industries

Technology