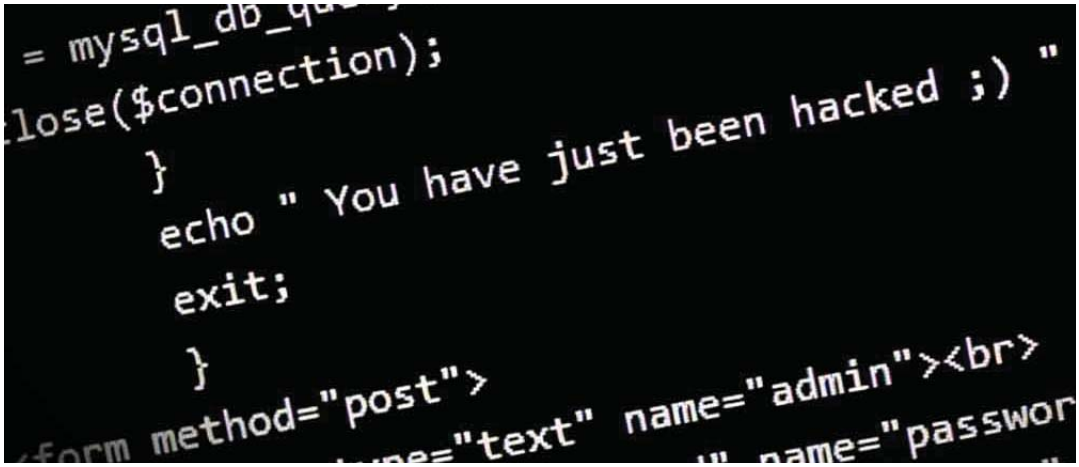
A CEO Blueprint: What to Do if Your Company Is Cyberattacked

By John E. Clabby and Joseph W. Swanson



Since the Target breach more than a year ago, we at Chief Executive *have gone to great lengths to make it clear to CEOs that cybersecurity is now their responsibility. We've emphasized that they need to be fully up to speed on their company's protective capabilities and emergency response plan, to ensure the systems are strong enough to keep hackers out and to ensure that they themselves can adequately answer all questions on the topic from board members, shareholders and the media, both during quiet times as well as after an attack. This article is a thorough blueprint that can help fulfill both those goals by fast-tracking CEOs' cybersecurity learning process.*

Picture this scenario: Hackers have penetrated your company's cyber defenses and made off with thousands of your customers' social security numbers, credit card numbers, or healthcare records. Or, perhaps a trusted, long-time employee has unexpectedly quit, and your information technology staff discovered that the employee used a thumb drive to download trade secrets, premerger documents, or patient records.

If your company finds itself confronted with such a scenario, there is much to do. Because you have prepared for this day, you activate your crisis response team. Select executives, IT staff and security personnel work alongside in-house lawyers, outside counsel, and HR staff to investigate, seal the breach, and, if news of the breach is public, manage the fallout. If consumer data was stolen, you prepare the appropriate data breach notifications, regulatory reporting, and media strategy. You communicate a single message, through your media relations staff, that minimizes the impact on the company's reputation, stock price, and relationships with key business partners.

If trade secrets were stolen but the news is not yet public, you assess the extent of the damage and then monitor your competitors. Amid all this activity, it's easy to forget that your company has been the victim of a crime. After all, someone broke into your computer systems, stole the company's crown jewels, and likely did it for profit. The following checklist identifies considerations to keep in mind when deciding if, when, and how to approach law enforcement for help in catching the bad guys.

Cont'd. on pg. 2

Are you required to notify law enforcement?

There is no single federal law establishing a uniform notification standard. But your company may be required to notify government officials depending on the nature of your business or the nature and size of the breach.

> "After a breach, communicate a single message through your media relations staff that minimizes the impact on the company's reputation, stock price, and relationships with key business partners."

For example, defense contractors must generally report the loss or theft of classified or export-controlled materials to the federal government. Healthcare providers must also report the loss of patient medical records to the appropriate federal and state authorities. In such specialized instances, the government will almost always commence a criminal investigation to identify and pursue the perpetrators.

Meanwhile, nearly all 50 states have enacted consumer-notification statutes for loss of consumer data affecting their residents. Some states, such as New Jersey and New York, require notifying the state attorney general or other state law enforcement agencies about a breach. Of course, such notification may result in criminal investigators seeking evidence from your company.

It is therefore critical for you to understand the regulatory environment in which your company operates and the states in which your company has customers. After a breach, investigate immediately to determine the nature and size of the incident, as well as the location of potentially affected individuals and entities, and then assess with counsel the applicability of any notification provisions.

If there hasn't been a criminal investigation, should you ask for one?

If your company is not subject to any of the aforementioned reporting provisions and law enforcement is not otherwise aware of the cyber attack, you need to weigh several competing considerations to determine whether to request a criminal investigation.

For instance, any of the following factors could militate against contacting the appropriate criminal authorities:

- **Possible liability –** Notifying law enforcement may ultimately lead to civil liability or worse for the company, depending on the firm's role in causing or failing to stop the breach. To make matters worse, facts bearing on the company's role may not be known to the company until weeks or months after the breach, and it may turn out that the breach was not the result of criminal activity. In other words, the company could notify law enforce ment unnecessarily and essentially call the police on itself. This is the most serious concern.
- **Disruption of your business –** The data breach is likely to disrupt your business; the presence of government agents or investigators on-site examining or imaging your servers and interviewing your employees will only add to that disruption.
- **Risk of increased publicity –** Although law enforcement likely will attempt to conduct their investigation without publicly exposing the intrusion or data breach (at least preliminarily), involving law enforcement may draw attention to the incident (both internally and externally) and could result in negative press. In the event of an arrest and trial of the perpetrator, the company's reputation could be damaged further if it turns out that lax controls at the company facilitated the crime.

> "Notifying law enforcement may ultimately lead to civil liability or worse for the company."

- **Confidentiality concerns –** Your company may be concerned about sharing with law enforce-

Cont'd. on pg. 3

ment confidential information, including trade secrets and privileged communications with counsel. An investigation carries with it the possibility of a prosecution, the exchange of discovery, and a trial, none of which is likely to be known in the immediate aftermath of the breach. The government, not the victim corporation, decides whether to bring charges.

Note that, at the outset of an investigation, you may be able to negotiate with the government a confidentiality agreement that specifies to whom the government may show the information. And if the investigation leads to an arrest and a trial, more robust confidentiality agreements and protective orders, often authorized by statute (depending on the nature of the information at issue), might provide greater protections to corporate secrets.

On the other hand, the following factors may warrant asking law enforcement to conduct an investigation:

- **When you are already notifying the government –** As noted above, your company may be obligated to notify non-law enforcement agencies, such as the U.S. Department of Health & Human Services in the event of a breach involving unsecured protected health information. In such a situation – given the possibility that the notified agency will refer the matter to law enforcement – it may make sense to reach out to law enforcement in the first instance to frame the issues, select the witnesses for interviews, and gain an initial impression as a good faith partner interested in cooperation.
- **Ability to manage the situation –** Being proactive and moving quickly in notifying law enforcement may help to influence the tone of the government's investigation, foster a cooperative relationship between your company and the investigators, and, most importantly, maximize the chances that the perpetrator will be caught and convicted.
- **Mitigation of liability –** Involving law enforcement early in the process may help the company to better position itself in dealing with any future regulatory actions stemming from the breach, as well as in responding to litigation from shareholders, consumers, and other entities.
- **Delayed public notification –** Notifying law enforcement may enable the company to postpone a disclosure of the breach to the public and regulators while the criminal investigation runs its course.
- **Deterrent effect –** By contacting law enforcement, your company may develop a reputation as being serious about data breaches and thus deter future intrusions. This is particularly true with respect to breaches of data that are considered trade secrets.

How should you notify law enforcement?

Which agency is appropriate? If your company decides to notify law enforcement, be sure to contact the appropriate agency. At the federal level, the Federal Bureau of Investigation ("FBI"), Homeland Security Investigations ("HSI"), and the Secret Service share primary responsibility for investigating cybercrimes, with significant overlap. The FBI is appropriate for most domestic cybercrime, including criminal hacking, theft of trade secrets, and identity theft. HSI investigates cross-border cybercrimes, including foreign-based hacks, while the Secret Service focuses on theft of payment card and other payment information. Finally, in the event of a smaller breach, it may be appropriate to reach out to state or local law enforcement agencies.

> "Being proactive may maximize the chances that the perpetrator will be caught and convicted."

How do I make contact?

To contact any of these agencies, work with your counsel to file a report with the local field office, headquarters, or via an online repository (e.g., the iGuardian portal shares intrusion information with the FBI). Your counsel may have contacts with the relevant agencies – particularly the local field offices – that could facilitate and help manage the company's initial interaction with law enforcement.

What other steps should you take to maximize the chances of catching the perpetrator?

- **Preserve the evidence –** Gather the evidence of the intrusion or, at a minimum, stop any automated systems from overriding it. Instruct your information technology staff to preserve IP logs and records of system log-ins and log-outs. Records of access and swipe cards, and closed-circuit camera logs, in particular, often have short re-record times, so be sure to preserve this evidence. Also, if the perpetrator was a

company insider, revoke his or her system credentials before taking any employment action, lest that person retaliate by seeking to destroy evidence.

- **Interview your staff** – Interview your IT staff and others with knowledge of the systems through which the intrusion or data theft occurred. No one knows your company's computer systems better than your staff does. Taking this step will help you identify the best witnesses to offer to the government to make your case effectively.
- **Put a bow on it** – Counsel can help you sort through the evidence of the breach and create a "prosecution memo" to share with law enforcement that is similar to what the prosecutor will ultimately have to create when seeking internal authorization for criminal charges. This document would lay out the evidence of the crime, connect that evidence to the suspect, and chart a pathway for successful prosecution, including by suggesting the particular statutes violated and anticipated punishments. Using outside counsel for your investigation also maximizes the protections of the attorney-client privilege, in the event that information is gathered as part of your internal investigation that you do not want disclosed to the government.
- **Create a single point of contact** – Have one person, either within the company or at outside counsel, who law enforcement can call to provide an update on the investigation or from whom law enforcement can request information. Empower that point of contact to interview and gather documents in response to the government's requests.

How should you plan for the next time?

Incorporate an analysis of if, when, and how to contact law enforcement into your company's overall data breach response plan. In doing so, identify the person or department within the company that will have the authority to make the decision to contact law enforcement and what the basis for that decision should be.

And in the event that law enforcement contacts your company before you have decided whether to call them, identify in your company's response plan who will have the authority to speak with them on such a call, along with what the initial steps will be to assist and respond to the inquiry.

Lastly, consider reaching out to law enforcement in non-crisis times. State, local, and federal agencies charged with preventing cybercrime often have industry liaisons whose jobs are to work with companies in a particular region or industry to educate employees on how to prevent and respond to cybercrime and to foster public-private cooperation. Corporate counsel, security staff, or experienced outside counsel may be able to arrange for such a meeting. ■

John E. Clabby

Joseph Swanson

John E. Clabby and Joseph W. Swanson are of counsel in Carlton Fields Jorden Burt's Tampa office, where they defend companies and officers in government investigations and securities and corporate governance litigation. Both are former criminal Assistant U.S. Attorneys and Computer Hacking and Intellectual Property ("CHIP") prosecutors, who specialized in gathering and assessing electronic evidence and investigating computer crimes. Clabby can be reached at jclabby@cfjblaw.com. Swanson can be reached a jswanson@cfjblaw.com.