New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

Cybersecurity

An ALM Publication

WWW.NYLJ.COM

VOLUME 259—NO. 106

MONDAY, JUNE 4, 2018

When the FBI Can Help Companies Deal With a Cyber Event

BY AVI GESSER
AND JOSEPH KNIAZ

Companies that discover a potentially significant cyber incident usually turn to their trusted outside law firm and a cybersecurity firm for assistance. But many companies decide not to reach out to the FBI, which can be a mistake in certain circumstances. Considering the practical assistance that the FBI can provide to targets of a cyber attack, and its recent statements expressing a commitment to support corporate victims of data breaches, companies and their outside advisors should give serious thought to reaching out to the FBI as part of their incident responses.

Reasons for Reluctancy

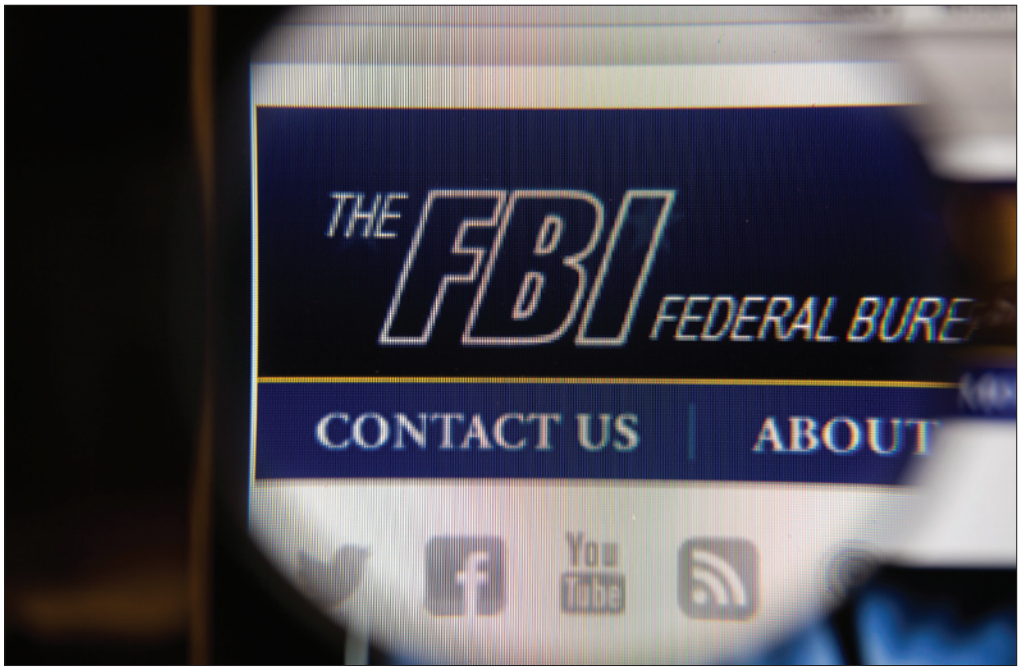
One reason that companies are reluctant to contact the FBI in the early stages of a cyber event is that they often know very little. In the first few days, details like how the attack was executed, what vulnerability was exploited, and which parts of the network were exposed, are illusive—or, as FBI Director Christopher Wray described it during Q&A at the 2018 Boston Conference on Cyber Security, they don't have the incident "wrapped up in a nice, neat bundle with a bow on top." Alison Noon, FBI Director Vows To Treat Hacked Companies

AVI GESSER *is a partner at Davis Polk & Wardwell.*
JOSEPH KNIAZ *is an associate at the firm.*

as 'Victims', Law360 (Mar. 7, 2018) ("Boston Q&A"). This hesitancy is understandable considering companies' experiences working with government agencies in other contexts, where it is expected that companies will have answers to the government's questions and will demonstrate an understanding of the relevant facts. But those rules generally don't apply in a cyber attack, and recent statements by the FBI underscore that the earlier the Bureau is notified, the more efficiently and effectively it can provide companies with assistance.

A second concern is that providing the FBI with information about a breach will somehow expose the company to criminal or regulatory liability by disclosing to the government that the company has a significant cybersecurity compliance shortcoming, like unpatched software. But the FBI has repeatedly emphasized that its priority is investigating the perpetrator of the breach, and that for the victim company, the FBI's focus is remediation. As Director Wray has stated, the Bureau does not "view it as our responsibility, when a company is sharing information with us, to then turn around and share that information with some of those other agencies…. We obviously have to comply with the lawful process if we encounter it, but I think we don't view it as our role to kind of rush out and share that information with those folks." Id.

Another fear companies have is that communicating with the FBI about the breach will waive privilege and expose sensitive materials to discovery in subsequent investigations or civil litigation. Care should be taken to establish and preserve privilege—but not by foregoing the FBI's potentially



SHUTTERSTOCK

invaluable assistance, especially in light of the statutory protections afforded by the Cybersecurity Information Sharing Act of 2015 (CISA), 6 U.S.C. §§1501–1510, which provides that the sharing of threat information and defensive measures with the FBI is not a waiver of any privilege.

How the FBI Can Help

The FBI can assist a company victimized by a cyber attack in a variety of ways. First, the Bureau may know exactly what they are dealing with and what measures may be effective to address it because they have seen it before, or they are currently helping another company facing the same threat actor. In such cases, the FBI can save companies days or weeks of time and effort by quickly helping to identify the most likely source of the attack, the technique used, and what remediation is needed. That's why involving the FBI early can mean the difference between a limited contained event and a much more serious one.

Involving the FBI early also provides the company with a concrete example of its proactive efforts to contain the breach and limit potential harm, should it face scrutiny of its mitigation efforts by regulators, insurers, auditors, investors, legislators or the media. By contrast, failing to do so, might, as Director Wray has noted, make it more difficult to explain to regulators "what you were really up to, especially when mitigation more and more is the name of the game." *Boston Q&A*.

The FBI can be particularly helpful in dealing with ransom and ransomware attacks, as well as wire transfer and business email compromise scams. For ransomware attacks, the FBI may assist in assessing options, including consideration of whether decryption is possible without paying and whether the particular attackers are likely to do what they promise if they are paid. In case of a fraudulent instruction to wire money, the FBI may be able to help the banks reverse the transfer.

The more companies that share information with the FBI on cyber threats, the more the FBI is able to help. As Richard Jacobs, an assistant special agent in FBI-New York's cyber branch, put it at the 2016 cyberSecure conference: "We would like a phone call…your breach might be connected to a dozen others and help us paint a picture of the criminals. The FBI's role is to get the bad guys out from behind the keyboard and into jail. If we don't neutralize those responsible, they will come back and attack again and again." Patricia L. Harman, *Should you call in the feds after a cyber breach?*, PropertyCasulty360.com (Sep. 30, 2016).

Establishing an FBI Contact

The FBI encourages companies to establish a relationship with law enforcement *before* a cybersecurity incident occurs. Already having a contact in one of the FBI's InfraGard chapters or the Cyber Task Force in a local field office can save critical time when a breach occurs, especially if through your contact with the agent, he or she has become familiar with the company's business, its potential vulnerabilities, and its security infrastructure. As CCIPS' Best Practices for Victim Response and Reporting of Cyber Incidents explains, advance contact with law enforcement can "help establish the trusted relationship that cultivates bi-directional information sharing that is beneficial both to potential victim organizations and to law enforcement." And even if the contact ultimately cannot provide assistance, he or she will likely appreciate being informed of the event, and may be able to refer the company to someone in government who can help. Again, the more companies share with the FBI, the more the FBI can help.

Preserving Privilege

Investigations of data breaches present unique challenges for maintaining privilege: the number of stakeholders, the different kinds of expertise required, and the overlapping demands of business, regulatory, and litigation obligations each create a risk of waiver. To encourage the sharing of cyber threats, Congress included a non-waiver provision in CISA that preserves privilege for information disclosed to the federal government, provided that the information meets the definition of a "cyber threat indicator" or "defensive measure" set forth in the statute and is shared for a "cybersecurity purpose." In addition, the company must take care to remove personal information pertaining to a specific individual that is "not directly related to a cybersecurity threat."

The CISA non-waiver provisions do not apply to disclosures made to state or local government entities. Moreover, CISA will not provide privilege protection if companies do not take proper steps to create and maintain privilege; CISA can protect a privilege, but it cannot create a privilege that did not exist in the first place. For example, although it did not involve disclosure to the FBI, in *In re Premera Blue Cross Customer Data Security Breach Litigation*, Case No. 3:15-md-2633-SI, 2017 WL 4857596 (D. Or. Oct. 27, 2017), a security consultant's review of the company's data management system was found not to be privileged because the original work was not done at the direction of counsel, and the court was not convinced that the later work was created "because of" anticipated litigation. By contrast, the court in *In re Experian Data Breach Litigation*, Case No. 8:15-cv-01592 (C.D. Cal. May 18, 2017), denied a motion to compel production of documents related to an investigation performed by a third-party data security consultant where, in the wake of the breach, Experian's outside counsel retained the consultant to conduct an expert report analysis to assist counsel in providing legal advice to Experian.

Companies wishing to avail themselves of CISA's non-waiver protections are careful to keep legal and business functions separate in cyber investigations, and ensure that work performed by third parties and other non-attorneys is done in support of a legal investigation and at the direction of counsel. These companies can reduce the risk of waiver when dealing with privileged materials by limiting the distribution of work product and by providing law enforcement with oral briefings—to the extent possible.