The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 22 November 2, 2016

INFORMATION SHARING

FBI Veteran Discusses Using Law Enforcement's Cyber Resources to Improve Security and Obtain Board Buy-In

By Rebecca Hughes Parker

One key to smooth relations with law enforcement after a breach is establishing a connection before there is any trouble, John Riggi, now a managing director at BDO and the former Chief of the FBI's Cyber Division Outreach Section, told The Cybersecurity Law Report. One way to develop that relationship is to invite the FBI to give a threat brief to the board of directors, he said. Riggi is a 30-year FBI veteran who worked on the government's partnerships with the private sector for the investigation and exchange of information related to national security and criminal cyber threats. In our interview, he addressed how the FBI views its relationship with the private sector, the various ways companies of different sizes can take advantage of the FBI's resources, the concerns companies may have when working with the FBI and the government's role in the Yahoo breach. See also "*Law Enforcement on Cybersecurity Matters: Corporate Friend or Foe?": Part One* (Jun. 22, 2016); *Part Two* (Jul. 6, 2016).

CSLR: What are some of the primary steps companies should take to establish a relationship with the FBI on cyber issues?

Riggi: The first thing I would always advise a company to do is to try to establish a relationship with its local FBI cyber task force, ideally before an incident occurs. The company should understand who the relevant supervisor is at the FBI, and who the individuals in that task force are. The company also has to ensure that the task force knows who the company is, the nature of the business, and the type of data the company holds, especially the higher risk data that might be subject to cyber attack – the data that may become a target for cyber adversaries.

For instance, if you are a defense contractor, nation states like Russia or China or others may be coming after your trade secrets. If you hold intellectual property on some very specialized, unique manufacturing process or technology, then, yes, nation states might still be coming after you, but criminal organizations might be coming after you as well to steal that intellectual property and monetize it.

CSLR: How does the FBI view information sharing with the private sector?

Riggi: The section of the FBI I ran was specifically designed to work with the private sector. The FBI, and the government in general, realized it cannot effectively combat the cyber threat without the assistance of private sector. And there are some real practical reasons for that.

Much of the evidence and intelligence relating to cyber threats lies on private networks that the government doesn't have access to. Contrary to popular belief, the government does not see it all. And I say this when I speak publicly – the government does not see all network traffic. The government does have intelligence, perhaps classified intelligence, and evidence collected from investigations that are like pieces of the puzzle. The private sector has lots of pieces of the puzzle as well that are related to the activities that occurred on their networks.

Unless both the private sector and the government put those pieces together, neither party can develop a clear picture of the adversaries, what their intentions are and what their capabilities are.

[See also "*In a Candid Conversation, FBI Director James Comey Talks About the 'Evil Layer Cake' of Cybersecurity Threats*" (Jun. 3, 2015); and "*Comey Discusses Cooperation Among Domestic and International Cybersecurity Law Enforcement Communities*" (Jun. 17, 2015).]

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 22 November 2, 2016

CSLR: What is your advice for mid-size or smaller companies that may have a lower level of cyber risk, but still want to be in the loop about cyber threats?

Riggi: The FBI has limited resources so they are not going to be able to have an ongoing relationship with every business in their territory. But if your company could be a significant target of cyber adversaries, or if you face an elevated cyber risk, you should proactively establish that relationship.

Other companies with lower levels of cyber risk can take advantage of an organization called InfraGard. It is basically open to any individual who is a U.S. citizen and does not have a criminal record. The organization is sponsored jointly by the local businesses in the area and the local FBI office. There is an InfraGard chapter in every FBI field office. InfraGard can be one way to share in the collective knowledge of other businesses in the community and establish a relationship with the FBI office, locally.

CSLR: What are some of the other ways that companies can take advantage of the cyber resources the FBI has?

Riggi: Companies can benefit indirectly from what the FBI is doing in terms of cyber investigations and threats. The FBI routinely publishes what are known as FLASH, which are information reports that detail technical indicators of compromise, or IOCs, associated with malware and cyber threats.

The FBI, in conjunction with private sector information and other government agencies, often issues private industry notifications as well. They can be either industry-specific or they could be broad-based. If there is a threat that is generalized, such as the compromise of business emails, a notification will go out universally across sectors. These notifications tend to take on a more narrative tone than the FLASH reports. They may describe the type of threat and talk about tactics, techniques, or procedures that are being used by a cyber adversary to attack individual businesses, and may discuss steps companies take to mitigate that threat.

CSLR: We have heard before that one way to increase the buy-in from the board of directors is to have the FBI speak directly to them. Is that something companies are doing?

Riggi: It is. Part of the FBI's mission is to work with the private sector, and one effective way the FBI can do that is by giving a threat brief to the board directly.

One of the most effective weapons against the cyber threat is for an organization to establish a culture of information security, internalized and prioritized by every employee, especially in organizations wherein the loss of intellectual property or loss of confidence due to a cyber incident could represent an existential threat. In my view, that information security culture must be a top-down approach, beginning at the board level. In addition, boards are coming under increased scrutiny by the regulators, the press and the public as to their sufficient engagement in cybersecurity issues.

[See also *"How In-House Counsel, Management and the Board Can Collaborate to Manage Cyber Risks and Liability": Part One* (Jan. 20, 2016); *Part Two* (Feb. 3, 2016).]

CSLR: What are some of the challenges the private sector may see with sharing information with the government and working alongside it after a breach? How do you respond to those concerns?

Riggi: I understand the private sector's concerns about contacting the FBI if there has been a cyber breach. If the company decides to contact the FBI, it has to consider when to do it and how to do it, and it has to understand what the FBI response is going to look like. Many times companies are uncertain what assurances they can receive from the government that their confidentiality will be protected and that the government would be sensitive to treating a victim of breach as a victim of crime.

I'm happy to report that a lot of the initiatives that I helped lead before leaving the FBI and the government focused on treating victim companies of breaches

as victims of crime. And some of that philosophy has actually been codified into Presidential Policy Directive 41, (PPD-41) which was just issued at the end of July. The Directive discusses treating the victim corporation as a victim of crime and states that the government response should be sensitive to preserving the company's proprietary information, preserving its confidentiality – basically treating the victim corporation as any victim of crime should be.

The Directive also helps delineate responsibilities within government, designating the FBI as the lead investigative agency for major cyber incidents and the Department of Homeland Security as the lead for asset response and asset recovery. In other words, it is DHS's role to help the victim organization mitigate the effects of the breach and recover from the breach. It also stressed that the government should have a unified response to any major cyber incidents. So, it imposes upon the government the requirement to coordinate with each other in responding to a major cyber incident.

CSLR: How much has lack of coordination between government agencies been a problem?

Riggi: It has been a problem in the past because the jurisdictional "lanes" were not clearly delineated. Any coordination has relied more on goodwill and personalities than on rules and institutionalization of coordination. But the new Presidential Policy Directive, number 41, (PPD-41) I previously discussed and for which I and BDO served as official private sector validators, will go a long way in helping define the "lanes."

CSLR: One reason some companies are wary to report a breach the government is a fear that their own measures were not up to standard. Some of the recent actions involving the Safeguards Rule by the SEC may make companies even more reticent.

Riggi: Yes. The FBI, though, is an investigative agency, a criminal investigative agency, and a national security agency. And its role is not to find fault or lay regulatory blame on a victim corporation that comes in, nor is its role to necessarily contact the regulator.

I used to tell victim companies directly, "We are going to leave that decision to you. You and your general counsel decide what your regulatory reporting obligation is." Now, the Presidential Policy Directive doesn't address that directly. It just says the responding agencies should be sensitive to the victim corporation's confidentiality.

However, legislation that went into law in December 2015, called the Cyber Information Sharing Act, or CISA, actually does provide a measure of regulatory liability protection for companies that voluntarily share cyber threat information with the government. [See "*Opportunities and Challenges of the Long-Awaited Cybersecurity Act of 2015*" (Jan. 6, 2016).]

CSLR: Attributing (and understanding) cyber attacks can be difficult and uncertainty as to who caused the breach and how far it reaches may also be a bar to a company's willingness to report.

Riggi: My advice is to let the FBI determine that. If you are the victim of a major cyber intrusion, you should report it to your local FBI office and let the FBI determine attribution. Determining attribution is one of the FBI's primary objectives during a cyber investigation. The FBI has advanced technical capability, human talent and access to highly sensitive classified and unclassified investigative information and intelligence, which would assist in identifying the perpetrator of the cyber attack and their motivations.

CSLR: Are there any mistakes you see companies making when they work with the government? Is there other advice you would give them to better work with the FBI, from the perspective of both your current and former roles?

Riggi: First of all, don't wait until you have a cyber incident to reach out to your local FBI task force. You should try to meet them or establish some type of pre-existing trusted relationship prior to having an incident. It is very difficult to make friends in the middle of a crisis. An old expression is that you don't want to "patch the roof during a hurricane."

This way, there will be a comfort level established and the company can better understand what the FBI's response would be. Some of these parameters can actually be worked out ahead of time. Many of the potential legal issues and the concerns that the general counsel might have working with government also can be addressed at that time.

The FBI, when I was there, was very happy to work with outside counsel. The FBI was also amenable to working with consulting firms, like BDO, who may have already been on scene. In the old days the FBI would say, "Well, if anyone outside of law enforcement has touched the computer, we're not going to be able to work with the information contained on the device. The evidence has been contaminated." The FBI has learned in recent years how to work very effectively with managed cybersecurity firms and consulting firms that may have been on scene first.

CSLR: It seems like the government has had to quickly increase its cyber capacity.

Riggi: The government's knowledge of cybersecurity is increasing quickly and, fortunately and unfortunately, the FBI has had a lot of experience in the last couple years with cyber incidents. I started in the cyber division in 2014 and that was just prior to a string of major breaches – Target, JP Morgan, Anthem, OPM, Community Health Service, Sony, U.S. Postal Service, White House, State Department, just to name a few. These were all in a very compressed period so that we became very good at incident response. We were collecting lots of intelligence very quickly and correlating it and assimilating it. And we learned very quickly how to integrate intelligence and the evidence derived from the investigation of these breaches, with information held by the broader government and intelligence community, and to determine attribution and motivation.

So, in a very short timeframe, the FBI and the government in general developed a wide knowledge base because, quite frankly, there are so many networks under attack.

CSLR: A major breach that was recently discovered was at Yahoo. The announcement came during M&A transaction negotiations with Verizon. What are some of the lessons from that? What would the FBI's role be in that breach?

Riggi: Well, before a company eyes another company it needs to assess the cybersecurity posture. It's just like buying a house without a home inspection. People need to understand what the cybersecurity infrastructure looks like in that organization. There should be an independent inspection of their cybersecurity capabilities of the target of that merger or acquisition. BDO routinely performs cybersecurity risk assessments as a method to identify existing vulnerabilities in an organization's information security and information technology infrastructure and make recommendations on remediation.

So, for instance, if the merger target is a health care organization provider, and it subsequently determined there's malware resident on the system or the organization is not HIPAA compliant, it could cost millions of dollars to bring it up to regulatory compliance. That's a big issue for organizations and could be as devastating as buying a house and later discovering it's infested with termites.

[See also "*Essential Cyber Due Diligence Considerations in M&A Deals Raised by Yahoo Breach*" (Oct. 5, 2016).]

CSLR: Would Yahoo would be considered the victim in this scenario by the FBI? Would the FBI be working at all with the acquirer?

Riggi: With any breach of that size, the FBI would be working hand in hand with the victim corporation, in this case Yahoo, and the FBI would strive to preserve confidentiality for the victim.

In this case, Verizon, which is also an internet service provider, may be able to provide independent intelligence to the FBI, such as information of value to the investigation outside of this merger concerning the malware that may have transited the internet or Yahoo's networks.