CRS INSIGHT

Justice Department's Role in Cyber Incident Response

November 15, 2016 (IN10609)

|

Related Author

- Kristin Finklea

|

Kristin Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

Criminals and other malicious actors increasingly rely on the Internet and rapidly evolving technology to further their operations. They exploit cyberspace, where they can mask their identities and motivations. In this context, criminals can compromise financial assets, hactivists can flood websites with traffic—effectively shutting them down, and spies can steal intellectual property and government secrets.

When such cyber incidents occur, a number of issues arise, including how the government will react and which agencies will respond. These issues have been raised following a number of high profile breaches such as those against the U.S. Office of Personnel Management. Federal law enforcement has the principal role in investigating and attributing these incidents to specific perpetrators, and this responsibility has been codified within the broader framework of federal cyber incident response.

Presidential Policy Directive (PPD) on U.S. Cyber Incident Coordination

The Obama Administration, through PPD-41, outlined how the government responds to significant cyber incidents—those that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." Responding to cyber incidents involves threat response, asset response, and intelligence support. The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead on *threat response*. Asset response and intelligence support responsibilities are led by other federal agencies.

The concept of threat response, as outlined by PPD-41, involves "conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response."

FBI Cyber Investigations

The FBI pursues cybercrime cases ranging from computer hacking and intellectual property rights violations to child exploitation, fraud, and identity theft. Its top priorities involve combating computer and network intrusions and

investigating ransomware. The FBI's Cyber Division focuses on "high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets." One key challenge, acknowledged by Administration officials and others, involves moving away from reacting to malicious cyber events and toward preventing them.

Indeed, cyber attack prevention is one of the main tenets of the FBI's Next Generation Cyber (NGC) initiative. Established in 2012, NGC has focused FBI resources on enhancing cyber capabilities. It has aimed to do this through (1) strengthening the NCIJTF, (2) bolstering the FBI's cyber workforce, (3) expanding Cyber Task Forces (CTFs) in all 56 field offices and focusing their efforts on computer/network intrusion investigations, and (4) increasing information sharing and coordination with the private sector.

Task Forces and Partnerships

The NCIJTF was established by National Security Presidential Directive-54/Homeland Security Presidential Directive-23 in January 2008. As established, the NCIJTF's mission is to "serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations." Led by the FBI, the NCIJTF coordinates over 20 U.S. agencies from law enforcement, intelligence, and the military. It also collaborates with the private sector and international partners. Early, there had been concerns that "the NCIJTF was not always sharing information about cyber threats among the partner agencies." There were also criticisms that the NCIJTF was perceived as an extension of the FBI's Cyber Division instead of as a multi-agency effort. DOJ's Inspector General more recently noted that these issues have improved.

The FBI leads several other task forces and partnerships focused on cyber threat response. For instance, there is a CTF at each field office. These CTFs focus on local cybersecurity threats, respond to incidents, and maintain relationships with companies and institutions. The CTFs also support the national effort to combat cybercrime by participating in national virtual teams on certain cyber issues and providing cyber subject matter experts or surge capability outside of their territories, when needed. Additionally, the FBI has established and maintained Cyber Action Teams of agents and computer scientists that can be rapidly deployed around the world to assist in computer intrusion investigations. In addition to domestic field offices pursuing international leads in investigations, the FBI has positioned cyber assistant legal attachés (ALATs) in some foreign countries. These ALATs work with law enforcement in host countries to share information, collaborate on investigations, and enhance relationships with partner agencies. The ALATs focus on "identifying, disrupting, and dismantling cyber threat actors and organizations."

Going Forward: Communication and Technology

Federal law enforcement responds to cyber intrusions in both public and private sector networks. One challenge investigators face is that a majority of private sector partners do not automatically engage federal investigators when they experience a breach and instead turn to private firms for attribution and remediation. For instance, the Democratic National Committee retained a firm named CrowdStrike to secure its network when it discovered a breach—attributed to the Russian government—in the spring of 2016. The FBI has been encouraging private companies to reach out directly to law enforcement to help investigate, attribute, and mitigate breaches.

In addition to working with law enforcement and private sector partners, FBI investigators seek to bolster their internal investigative capabilities to avoid being outpaced by technology, a phenomenon that the FBI has called 'Going Dark.' Notably, law enforcement supports strong encryption to protect networks, devices, and information. However, they note that malicious actors also exploit the widespread use of end-to-end, or what investigators have called 'warrant proof' encryption, locking out investigators. Experts have recommended that the FBI invest resources to strengthen its investigative toolbox—rather than asking technology companies to build in exploitable weaknesses or "backdoors" to their products—so that it can best respond to cyber threats.