Preparing for a Cyber Incident

Although every organization strives to never suffer from a cyber-attack, increasing use of the internet and expanding digital landscape makes it more likely that every organization will one day fall victim to a data breach, ransomware, or other cyber incident.

Preparation, which includes developing an incident response plan, is key to an effective response that minimizes harm and expedites recovery. One way to accomplish that is to establish a point-of-contact with your local FBI field office:

https://www.fbi.gov/contact-us/field-offices

Benefits of Working with the FBI:

- The FBI can respond with a range of investigative assets, all coordinated through the local FBI field office. These include Special Agents, Computer Scientists and Intelligence Analysts in every field office who specialize in computer intrusion investigations. They also include enhanced resources like the Cyber Action Team, a rapid response team of cyber investigation experts who can deploy nearly anywhere in the world to provide advanced digital forensics and incident response capabilities to identify, collect, and analyze the most relevant and immediately actionable evidence of a computer intrusion.

- We pursue investigations that can identify the source of the intrusion and provide context so you understand why you may have been targeted.

- We impose consequences for illicit acts. Consequences include indictment, prosecution, imposition of sanctions, and efforts to name and shame the responsible actors.

FBI Internet Crime Complaint Center (IC3):
https://www.ic3.gov

Report individual instances of cybercrime to the IC3, which accepts complaints from both victim and third parties.

National Cyber Investigative Joint Task Force (NCIJTF):

24/7 CyWatch Command Center (855) 292-3937 or
cywatch@fbi.gov

A relationship with the FBI can foster information sharing that proves beneficial both to potential victim organizations and law enforcement.

Responding to a Cyber Incident

Realities of Working with Law Enforcement:

- We treat victims as victims. Our role is to identify the responsible cyber actors and bring them to justice, not to interfere with your organization's efforts to respond, remediate, and restore operations. Victims are not named in court documents, and charges remain sealed until the responsible party is apprehended. Whenever practicable, protective orders are sought to reduce public disclosure of sensitive information, and exemptions are claimed to guard against any investigative or other sensitive information being released.

- We strive to minimize disruptions to your business operations. The FBI pursues investigative measures that avoid computer downtime, often seeking only log files and images of affected machines. We also do our best to schedule witness interviews in advance, and avoid displacing employees whenever possible.

- We seek only technical intrusion details, not sensitive internal communications evaluating your company's security. We work closely with incident response firms as permitted by a victim to obtain relevant information for investigative purposes. If evidence is commingled with customer data, we partner with your technical personnel to locate artifacts of the intrusion without sifting through sensitive third party data.

- We are law enforcement, not regulators. As a general rule, we don't share cyber incident information with regulators, and we refer regulators to the victim itself for further information. Indeed, the Federal Trade Commission and Securities & Exchange Commission have stated publicly that they view reporting favorably.