FBI CYBER QuickBytes

When Should I Contact the FBI?

Before a Cyber Incident.

Developing a relationship with your local FBI field office gives a company a dedicated contact prior to any cyber event and provides access to FBI cyber mitigation resources.

During a Cyber Incident.

Speed is essential in a cyber intrusion investigation. Electronic evidence dissipates over time and quick investigative action by the FBI helps disrupt the perpetrators efforts and increases the odds of a successful prosecution.

How Do I Contact the FBI to Report a Cyber Incident?

FBI Field Offices
(local or international)
www.fbi.gov/contact-us

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

Online Tips and Leads Form
tips.fbi.gov

FBI Tip Line
1-800-CALL-FBI3
(1-800-225-5324)

CyWatch 24/7 Cyber Center
1-855-292-3937 or
cywatch@fbi.gov

Benefits of Reporting a Cyber Incident to the FBI

- Identify and stop the activity. FBI Cyber can work with your security and technical teams to help you quickly identify and respond to an incident.
- Unique FBI authorities allow us take action and seize/disrupt a cyber actor's technical infrastructure, something private entities cannot legally do on their own.
- Support your organization's data breach response. If an incident becomes public, cooperation can strengthen your organization's position with shareholders, insurers, lawmakers, and the media.

How Will the FBI Protect Our Interests and Information?

- The FBI's efforts are directed towards the intruder and their actions on the system/network and not on the victim's defenses.
- The FBI works closely with a victim company's legal counsel to address concerns.
- The FBI is mindful of the reputational harm that a cyber incident can cause.
- Often, the FBI requires only technical details to advance investigations, not privileged communications or unrelated documents.
- FBI investigations are carefully coordinated with your company to minimize disruption to normal business operations.

What Should Be Reported to the FBI?

- The identity of the victim
- The nature of the incident
- When the incident was initially detected
- How the incident was initially detected
- A timeline of events
- Logs for the affected machines
- The actions that have already been taken
- Who has been notified of the incident
- The identity of whoever reported the incident