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

**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-FBI
(1-800-225-5324)

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

# Partnering with the FBI

FEDERAL BUREAU of INVESTIGATION
935 Pennsylvania Avenue Washington, D.C. 20535

FBICYBER


FBICYBER

## What Should Be Reported?

*An array of technical data and incident information can prove helpful for investigators.*

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

## When Should my Organization Report a Cyber Incident?

The DOJ and FBI encourage companies to develop a relationship with their local FBI field office prior to an incident. Proactively building a relationship with the FBI provides companies with a dedicated FBI point-of-contact in the event of an incident and provides access to FBI cyber mitigation resources.

Electronic evidence dissipates over time, so speed is essential in a cyber intrusion investigation. Enlisting the FBI's help as soon as an incident is discovered enables quick investigative action and allows the preservation of evidence which increases the odds of a successful prosecution or other action to disrupt the perpetrators.

*...speed is essential in a cyber intrusion investigation.*

FBI CYBER

## Partnering with the FBI

*Together, we can get ahead of the threat and deter our cyber adversaires.*

The current cyber threat landscape highlights that cyber risk is business risk and cybersecurity is national security. The U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) play an essential role in detecting, deterring, and disrupting cyber threats by responding to cyberattacks every day across the country. Together, we can get ahead of the threat and deter our cyber adversaries.

The FBI leverages its unique, decentralized field office model to proactively develop relationships with companies and organizations in their geographic locations, putting the FBI in an ideal position to engage with potential victims of cyberattacks. The FBI encourages companies to develop a relationship with their local FBI field office prior to a cyber incident. Cyber-trained special agents, computer scientists, and intelligence analysts in FBI field offices provide local expertise available for deployment to victim sites immediately upon notice of an incident. These experts provide intelligence collection and analysis as well as technical assistance capabilities.

This handout describes the benefits of reporting incidents to the FBI, the steps the FBI will take to protect your organization's interests and information during an investigation, and the recommended timing and content of reports.

# What are the Benefits of Reporting a Cyber Incident to the FBI?

In response to a reported cyber incident, the FBI may be able to:

**Identify and stop the activity.**

- Information Sharing: FBI agents who are familiar with patterns of malicious cyber activity can work with your security and technical teams to help you quickly identify and understand the context of the incident.
- International Partnerships: The FBI has Cyber Assistant Legal Attachés around the world and can leverage the assistance of international law enforcement partners to locate stolen data or identify the perpetrator.
- Recovery Asset Team (RAT): Established in 2018, the FBI's RAT streamlines communication with financial institutions and assist in the recovery of funds for victim companies who made transfers to domestic accounts under fraudulent pretenses.
- Apprehend or impose costs on cyber actors: The DOJ and FBI can bring forth indictments and other deterrence actions to degrade cyber actors' capabilities.

**Seize or disrupt the actor's technical infrastructure.**

- The DOJ and FBI have a mounting record of successful court-authorized operations to disrupt cyberattacks and take down botnets that have hijacked millions of computers worldwide. These unique authorities allow actions to be taken against the cyber actor's technical infrastructure that private companies cannot legally take on their own.

*The benefits of reporting a cyber incident to the FBI are more evident today than ever before.*

**Share valuable insights from other investigations that may help mitigate damage and prevent future incidents.**

- Disclosing information about an intrusion to the FBI often enables investigators to make connections among related incidents.
- This enables FBI to share valuable insights and information with companies regarding the perpetrator's tactics, tools, and techniques. Such information may allow you to better protect your company's network and assist the FBI in identifying and warning you (and others) of future malicious activity.

**Support your organization's data breach response.**

- Under many state laws, law enforcement may be able to temporarily delay otherwise mandatory state data breach reporting when law enforcement determines doing so advances investigative goals.
- Proactive reporting to law enforcement may help your organization deal with government regulators, such as the Federal Trade Commission, which has declared that it will look more favorably on a company that has reported a cyber incident to law enforcement and cooperated with the investigation.
- If an incident becomes public, cooperation may strengthen your organization's position with shareholders, insurers, lawmakers, and the media.