The FBI is the lead federal agency for investigating cyber intrusions. Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to your local FBI Field Office Cyber Task Force.

Having an ongoing relationship with the local FBI prior to an incident is important. This helps your team plan and know who to call when you need to contact law enforcement. It also helps information sharing efforts that can help the whole community.

What to Expect When Working with the FBI

- Making FBI contacts prior to an incident can help an investigation move much quicker.
- The FBI will focus on the scope of the crime and seek evidence needed for prosecution.
- The FBI will not search for violations made by the victim company.
- The FBI will not share company information with regulatory bodies or the media, and in most instances, regulators will look favorably on reporting and working with law enforcement.
- The FBI will not seize victim company assets (For example, servers and computers) and will do our best to minimize interruptions to operations.
- As a victim, the FBI will treat you as a victim and has resources available to assist you.
- Be mindful that the FBI does not repair or restore network systems.
- The FBI will try to get information back to you as quickly as possible. The FBI will be diligently working on your case, but response time may vary depending on the circumstances.

What Information Should You Provide To The FBI

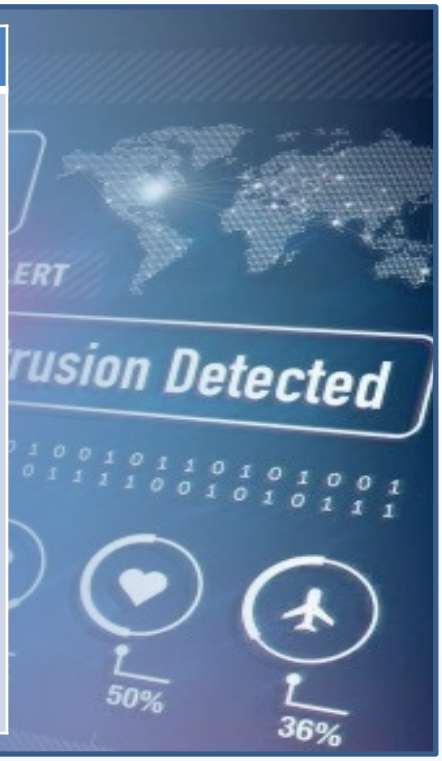
- Reporting Indicators of Compromise (IOCs) help everyone. Reporting IOCs to the FBI may help in other FBI investigations, even if the company does not intend to seek prosecution or has not suffered a loss.
- Facts Only – IP addresses of unauthorized access with date(s)/time(s) and context.
- DNS Logs/Netflow/Memory Capture.
- Report anything unusual and anything that could tie to attribution.
- Let the FBI know who you will contact for mitigation services. This is helpful so that the FBI can coordinate preservation of evidence that may be needed for investigation.
- Track your company's damages and losses.

Practice Your Incident Response Plan

- The victim company and the FBI should plan to have hypothetical discussions and conduct table-top exercises ahead of any incidents.
- We highly recommend that your team's playbooks and any tabletop exercises include all players if possible. For example, if your company's general counsel or others outside the cyber security team would be the decision makers during an incident, practice with all of them so during an incident there are no surprises on where to get the answers needed to engage with law enforcement.
- We recommend including the following company departments: Treasury/Risk; Internal Audit; Insurance Provider; Legal Representatives (Internal); External Counsel; Third Party Forensics Providers; Corporate Communications; Marketing and Public Relations departments.

When and Who to Call

- Email Scams with no loss report at IC3.gov; less than $5,000 report to IC3.gov and contact local police; greater than $5,000 call your FBI POC.
- Business Email Compromise (BEC) report to IC3.gov and call your FBI POC.
- Computer Intrusions, Espionage tips call your FBI POC.
- It is important to note that when filing a complaint with IC3, the information is reviewed by an analyst and forwarded to federal, state, local, or international law enforcement or regulatory agencies with jurisdiction, as appropriate. The IC3 does not conduct investigations and, therefore, is not able to provide the investigative status of a previously filed complaint. Investigation and prosecution are at the discretion of the receiving agencies. More information can be found at IC3.gov on the FAQs page.[1]



FBI Resources

Domestic Security Alliance Council (DSAC)	InfraGard	DOJ
A strategic partnership between the U.S. government and U.S. private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information between the federal government and the private sector. https://www.dsac.gov/about	A partnership between the FBI and members of the private sector for the protection of U.S. critical infrastructure. https://www.infragard.org/	The Department of Justice's Computer Crime & Intellectual Property Section (CCIPS) and National Security Division (NSD) are respectively responsible for implementing the Department's national strategies for combating criminal or nation-state sponsored computer and intellectual property crimes worldwide. More information about CCIPS and NSD, including press releases, indictments, and policy documents, can be found at their websites. https://www.justice.gov/criminal-ccips and https://www.justice.gov/nsd/external-engagement.
National Cyber Investigative Joint Task Force (NCIJTF) · CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@fbi.gov	**FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov**	
Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.	Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	

1 https://www.ic3.gov/faq/default.aspx#item2