Establishing trusted partnerships with the FBI prior to a cyber event is essential in proactively protecting a company's network. The FBI can often provide information when an adversary is targeting certain companies or sectors. The FBI can also show the methodology behind their operations, the adversary's tactics and techniques, and can also frequently provide the motives behind the nefarious acts. The FBI may also provide indicators of adversary activity, all of which can be used to help defend your network against further attacks. Informing the FBI of intrusions provides an opportunity for the federal government to surge its capabilities in addressing the malicious activity. By opening lines of dialogue and encouraging information sharing, both private industry and government agencies demonstrate to the American public that there is a whole-of-nation approach in dealing with cyber threats.

Why Partner with the FBI

The FBI has a Cyber Task Force (CTF) in each of the 56 field offices and during an incident can deploy personnel such as the Computer Analysis Response Team (CART), the Cyber Action Team (CAT), and other investigative and analytical personnel with expertise on how to address cyber incidents that may affect a company network. Working with the FBI does not mean that collaboration will lead to an investigation. The FBI coordinates with each individual industry partner to determine the best course of action to address an incident. No matter what course of action is deemed appropriate, information provided by a victim or a potential victim is protected.

Preparation for Interaction with the FBI

The ability of a victim organization to effectively assist the FBI investigation into a cyber incident can at times be limited based on technical, legal, or corporate policy issues. Addressing these issues ahead of time will help save valuable time during an actual incident. The FBI frequently encounters victim organizations that do not have sufficient logging on their network to identify intrusion events or to be used after the fact in an investigation. It is important to make a concerted effort to understand what logging is required and to ensure it is in place. Having the appropriate personnel ready to assist in an investigation is also an enormous benefit. Network security personnel, computer incident response teams, network administrators, and corporate law teams are the front lines of defense for an organization and having those personnel available speeds along the assistance we can provide.

Many types of data can be shared with law enforcement based on content. However, there are limits on what corporate officers can consent to share based on the expectation of privacy of employees. Language in a legal banner or computer use agreement can make sharing information related to the intrusion much easier.

Technical Issues

The following logs are typically helpful, but each organization is unique. Tailor your logging toward your own organization, and try to preserve and/or heavily monitor ongoing malicious activity. In some cases it may be better to monitor the activity rather than try to take systems off-line.

- Firewall, Proxy, web-server, anti-virus, active directory, Network Address Translation (NAT), Window Event Logs, Intrusion Detection System (IDS), DNS, VPN, and various security appliance logs.

FBI Cyber Incident Response

Cyber incidents are typically motivated by criminals for financial gain, geo-political ideology, nation states trying to gain an intelligence advantage or cause disruptive or destructive activities to a corporate network. This usually revolves around the theft of intellectual property because the victim organization has something of value to the intruder, or the disruption of a network based on retaliation for perceived wrongs. Regardless of the underlying motives, the FBI can respond with a litany of services that can be used to protect networks from further attack or provide intelligence that can help you to build a resilient defense.

<table>
<thead>
<tr>
<th>Helping Industry</th>
<th>Engagement</th>
<th>FBI’s Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emphasis on the Victim</td>
<td>Single Point of Contact for the USG</td>
<td>Determining Attribution</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>Relationship &amp; Trust</td>
<td>Highly Skilled, Technical Assistance</td>
</tr>
<tr>
<td>Media &amp; Legal Coordination</td>
<td>Partnership</td>
<td>Strategic Analytics</td>
</tr>
</tbody>
</table>

For more information, contact your nearby FBI field office or visit [www.fbi.gov](http://www.fbi.gov).