FBICYBER
GLOBAL CYBER EXPERTS IN YOUR LOCAL COMMUNITY

CYBER THREAT RESPONSE
OUR ROLE INCLUDES...

- Investigating, attributing, and disrupting malicious cyber activity.
- Providing cyber threat information, experts, and capabilities to inform your cyber intrusion response efforts.
- Notifying entities who may be unaware they have been compromised.

FBI CYBER
ASSISTANCE

- Investigate cybercriminals to seek justice and prevent crime.
- Employ a global network of cyber threat experts.

- Share cyber threat information to inform response actions.
- Introduce targeted entities to decryption capabilities or other known mitigation tools, if available.
- Assist in freezing, seizing, and returning stolen and extorted funds, when possible.

FBI CYBER FACT
VS. FICTION

- The FBI provides information to help you respond to cyber intrusions. *We do not restore systems or data.*
- The FBI works with your IT team to collect evidence about cybercrime, with your consent. *We do not search for unrelated activity when investigating a cyber intrusion.*
- The FBI coordinates with your attorneys. *We do not give legal or regulatory advice.*

- The FBI works with your press team upon request. *We do not publicize your cyber intrusion.*
- The FBI seeks data about cybercriminals and shares this information with federal partners who have a need-to-know, like CISA. *We do not seek information for regulatory purposes.*

PRE-INTRUSION TIPS

CONNECT. Determine who to contact before a cyber intrusion occurs.

FBI Field Office: **Learn who from your local field office to include in your cyber incident response plan, when to contact them, and explore opportunities for the FBI to join your table top exercises.**

Private Incident Response Firms: **These firms offer remediation services that the FBI does not. The FBI can share information with the firm you choose.**

STAY INFORMED. Read the latest federal cyber alerts and implement their recommendations. Find them at IC3.gov, StopRansomware.gov, and CISA.gov.

POST-INTRUSION TIPS

REPORT. Notify the FBI with relevant cyber intrusion details.

PRESERVE. Collect indicators of compromise (malware samples, logs, and other relevant intrusion data).

COMMUNICATE. After reporting an intrusion, keep lines of communication open between your team and the FBI.

SHARE. The FBI relies on targeted entities sharing data so the FBI can investigate and disrupt perpetrators.

HOW TO CONTACT
FBICYBER

Local or International FBI Field Offices **www.fbi.gov/contact-us**

FBI Internet Crime Complaint Center (iC3) **www.ic3.gov**