United States
Secret Service
Cybercrime
Investigations

PREPARING FOR A CYBER INCIDENT

Contacting Law Enforcement: *What You Need to Know*

If there is suspicion that the cyber incident is a result of criminal activity, contact law enforcement as predetermined in your Incident Response (IR) Plan. The U.S. Secret Service developed a *Preparing for a Cyber Incident - Introductory Guide*, which describes what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations.

The ability of law enforcement to respond in an effective manner depends on law enforcement's ability to access crucial information. Law enforcement should be contacted at the earliest opportunity, even if you are unsure about the actual cause of the intrusion. The amount of time that passes between an incident and when law enforcement is engaged is the biggest factor in the potential availability of valuable evidence, either from within the victim's network environment and/or from external entities (i.e. ISPs, phone companies, telecoms). The following is a non-exhaustive list of information that your organization should be prepared to provide to law enforcement to assist in the investigation.

WHAT TO PROVIDE DURING AN INCIDENT:

- ✓Logs considered to be very significant: Firewall, Event logs, Active Directory
- ✓Logs considered to be significant: DNS, Web Proxy, Remote Access Authentication, DHCP lease, router, IDS/IPS alerts, endpoint security (Antivirus, Antimalware), VPN, two-factor authentication, SNMP, SIEM
- ✓Live forensic image of RAM and virtualized RAM (if available, also a back-up copy for Delta Analysis) on compromised client or servers
- ✓Live image of breached servers (not storage pools), to include remote, third-party and cloud servers, either as a full export or a back-up copy of the server in its current state
- ✓Timeline of events
- ✓Physical and virtual network topology
- ✓Copy of malware or tools used by suspected offenders
- ✓Copies of emails suspected to be malicious with full headers and attachments
- ✓Copies of links suspected of causing the breach
- ✓Names of organizations and individuals outside your organization who were already notified of the incident
- ✓Access to real-time IR firm analysis (an IR firm's final report is ineffective for an investigative function)
- ✓Contact information for your organization's IR Team and/or third-party IR Firm
- ✓Contact information for your organization's external counsel, if applicable
- ✓Contact information for the PCI Forensic Investigator you have engaged, if applicable
- ✓Visibility of any internal and/or external communications issued by your organization to your workforce, customers, and/or the public

United States
Secret Service
Cybercrime
Investigations

PREPARING FOR A CYBER INCIDENT

Contacting the U.S. Secret Service: *What You Need to Know*

When you contact the Secret Service, **WE WILL:**

- **Work directly with your organization's IR Team and/or third-party IR Firm.**
- **Compare the indicators of compromise (IOCs) - signs that an incident may have occurred/may be occurring now - with other cases.**
  - **The Secret Service will compare the IOCs with other cases (known IPs, malware, tools, methods, etc.), which can then be shared with your organization.**
- **Work with domestic and international law enforcement partners to identify, locate and apprehend the suspected offenders.**
- **Work with prosecutors (United States Attorney's Office, District Attorney, etc.).**
- **Facilitate communication with other agencies that could potentially minimize incident damage.**
- **Remain in contact with your organization while the investigation progresses.**
- **Assist you with preparing to issue communications to your workforce, customers, and the public.**
  - **Law enforcement agencies will ask your organization to refrain from issuing public communications for up to 48 hours, to enable securing evidentiary material.**

When you contact the Secret Service, **WE WILL NOT:**

- **Provide services an Incident Response firm would such as mitigation of the infection on your network(s), removal of malware, etc.**
- **Contact the press or issue public communication.**
  - **The Secret Service will not issue information or comment on any active investigation.**
- **Provide complete mitigation and remediation support.**

Contact the local U.S. Secret Service
Cyber Fraud Task Force Network Intrusion Team