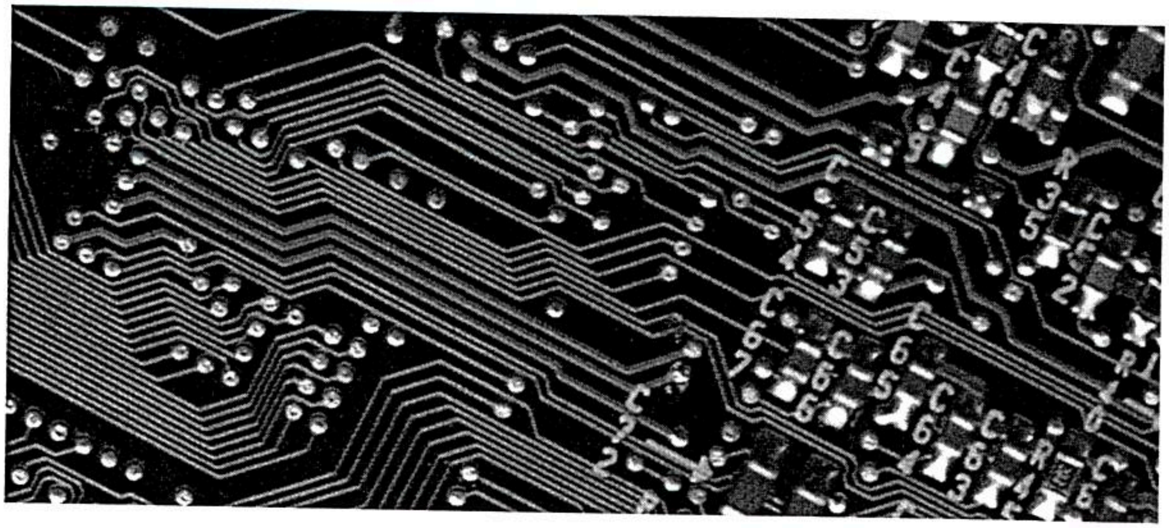
ELECTRONIC CRIMES TASK FORCE



Incident Response and Planning Strategies When Notifying Law Enforcement

Introduction

As cyber incidents rapidly spread across the nation's financial and critical infrastructure an effective response requires close coordination from multiple stakeholders affected by the incident. The purpose of this document is to provide insight from the United States Secret Service Electronic Crimes Task Force on law enforcement's response as a stakeholder investigating cyber intrusions. Although there are a number of previously published incident response resources (articles, brochures, manuals and other printed materials, etc.) readily available, we are simply providing steps to consider when notifying law enforcement. A well-defined and organized response to a cyber incident requires a team effort. Getting the right people involved is essential to properly responding, coordinating, mitigating, and investigating your incident. Although law enforcement is just one of several stakeholders needed for a response strategy, our objective is to assist with the prevention, detection, and aggressive investigation of attacks on our nation's financial and critical infrastructures.

The following three steps are intended to guide organizations when notifying law enforcement.

Step #1. Knowing who to involve in your initial response

Getting the right people involved and coordinating your efforts is key to any successful response. A company must identify a central point of contact or leadership team that not only has the responsibility, but also have the authority to act. The leadership role must be established to perform the day-to-day analysis of the situation and make key decisions. A central point of contact should be established and be at the highest level in executive management or have the backing of executive management.

- A determination of the nature of the incident (what happened)
- Is the attack ongoing or is it hours/days old
- Network topology – provide a current and functional understanding of the organization's network and flow of data
- Security setup and configuration (IDS, log servers, router configurations, etc.)
- Brief overview of inventory of computer systems and network components
- Access control – who has access to systems and by what means

A data breach contains three (3) basic components

1. How did they get in?
2. How did they move through your network and what did they take or alter?
3. How did they exit your system?

Step #3. Collecting and reporting the facts.

A cybercrime case is no different than any other criminal case when it comes to prosecution. You must have evidence of the crime. The investigation will only go as far as the victim company can take it. In order to capture and prosecute criminals, trace evidence of the crime must be located, captured, and documented in a forensically sound manner. Having a sound log management system in place is key to stopping criminals from infiltrating your system, restricting their access within your system, and preventing them from exfiltrating data out of your system. Most importantly, proper log management provides trace evidence if a crime occurred. In the world of computer security, controlling the flow of data in and out of your network includes the authorization, authentication, and auditing of your system. Firewalls, data-loss prevention systems, intrusion detection systems and access control lists all work great if they are configured and managed properly. Logs must be preserved so that any actionable investigative leads or trace evidence can be found and documented.

The response team must:

- Control physical access to computers and network components
- Log and report the sequence of events or incidents
- Preserve all evidence and maintain a chain-of-custody

Cyber crime is borderless yet cyber criminals routinely hide behind borders. Businesses today are faced with the unique challenge of competing in a global society while having to secure global access. Today, businesses and corporations fmust define their level of acceptable risk. The recommendations in this document were designed to enable all response partners to prepare for and provide a unified response to cyber incidents. These steps were developed according to the principles outlined in the President's Comprehensive National Cyber Security Initiative (CNCI), reinforcing its major goals designed to help secure the United States in cyberspace.