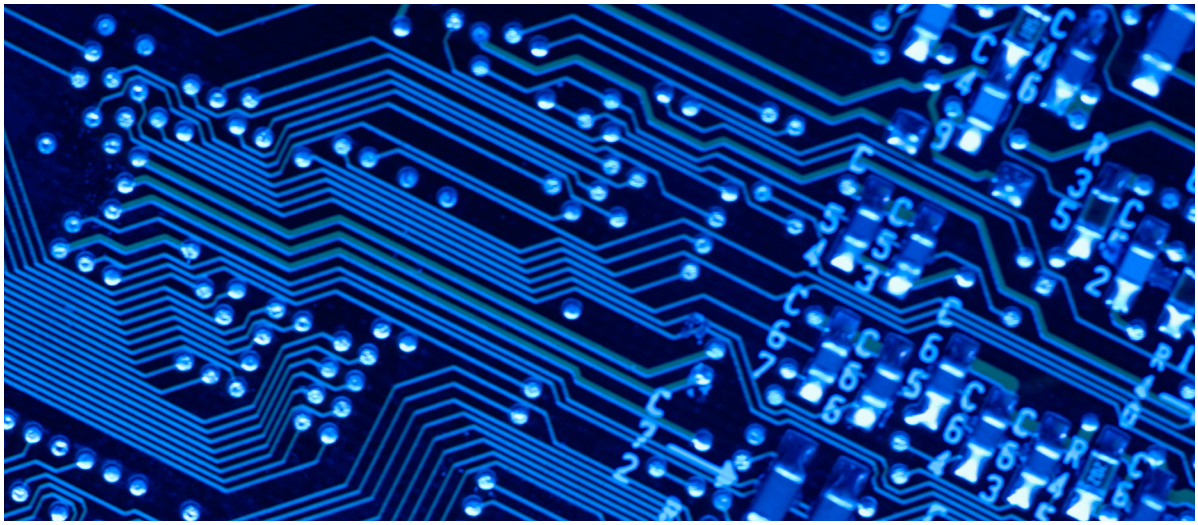
ELECTRONIC CRIMES TASK FORCE



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.

Do you have a response team as part of your response plan? Does it involve in-house legal counsel, human resources personnel, corporate security, IT security, technical professionals and someone from your communications group to coordinate messaging? The response team must not only act as liaison within its own company but also must coordinate and communicate with law enforcement, third-party forensic responders, outside legal counsel, media, and various state notification procedures. Synchronizing an effective incident response sometimes involves bringing in third-party entities. A well-organized and practiced response plan will have pre-established contacts for law enforcement and any needed third-party technical and legal support.

- Hiring outside legal counsel: Companies sometimes hire outside legal counsel to assist with risk and remediation procedures such as: compliance requirements, data breach disclosure laws, industry standards, regulations and federal and state laws. Attorney-client privilege can be invoked between the victim company's outside legal counsel and hired third-party forensic firms that perform a review of the system during a breach. Invoked privilege allows the forensic company to report breach results directly to the law firm. Coordination is needed to ensure that the law enforcement agency investigating the case has access to that flow of information.

- Hiring a third-party forensic company: Third-party forensic firms can assist in containing the breach and collecting sensitive electronic data (evidence) in a forensically sound manner. These companies are there for mitigation, remediation and assistance in investigating the internal workings of your network. Your federal or local law enforcement agency investigating the case will work directly with the firm to obtain any actionable leads infiltrating or exfiltrating your network. Law enforcement agencies investigate the breach but do not mitigate damages to your system.

Step #2. Containing the problem while investigating the incident

After it is determined that there is a breach the containment phase begins. Companies look to contain, repair, and secure the problem so their organization may move forward. While containing the problem, the immediate notification to law enforcement is also very important. Although common trends in breaches can be seen across the threat landscape, intrusions or incidents are always different because each victim company is unique. Companies have their own proprietary physical networks and the logical flow of data that migrates through their system is almost never the same. Although law enforcement notification procedures may vary amongst Federal and State agencies, all notifications involving the United States Secret Service should be made by telephone or direct contact. There should be direct contact with the Secret Service so that the following facts can be established:

- 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.

ELECTRONIC CRIMES TASK FORCE

References and resources:

http://www.secretservice.gov
http://www.us-cert.gov/government-users/reporting-requirements

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/Incident-Response-Guide.pdf

http://cias.utsa.edu/docs/TakeHome/Supplemental%20Materials/DHS%20US-CERT.pdf

http://www.dhs.gov/office-cybersecurity-and-communications

http://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf

http://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821

http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm.

http://www.trustwave.com

http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf

http://www.securityinfowatch.com/article/10537067/the-risks-of-outsourcing- information-security

http://www.businessforum.com/woj01.html

http://www.listcrime.com