Global Information Assurance Certification Paper

Creating and Maintaining Policies for Working with Law Enforcement

GLEG Gold Certification

Author: Tim Proffitt, tim@timproffitt.com

Adviser: Jeff Turner

Accepted:

Outline

Myths and Misunderstandings

Industry surveys show a wide variety of reasons why companies are reluctant to report computer incidents to law enforcement. The perception on the part of some entities is that there is little upside to reporting network intrusions. The perceived rationale for not reporting an intrusion includes the following[1]:

- The victim company does not know which law enforcement entity to call. Surely, the victim reasons, the local or state police will not be able to comprehend the crime and the FBI and Secret Service would have no interest in my system.
- If the victim company does report the intrusion to an appropriate agency, law enforcement will not act. Instead, the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions.
- If law enforcement does act on the report and conducts an investigation, law enforcement will not find the intruder. In the process, however, the company will lose control of the investigation. Law enforcement agents will seize critical data, and perhaps entire computers, damage equipment and files, compromise private information belonging to customers and vendors, and seriously jeopardize the normal operations of the company.
- If law enforcement finds the intruder, the intruder likely will be a juvenile, reside in a foreign country, or both, and the prosecutor will decline or be unable to pursue the case.
- If the intruder is not a minor, the prosecutor will conclude that the amount of damage inflicted by the intruder is too small to justify prosecution.
- If law enforcement successfully prosecutes the intruder, the intruder will receive probation or at most

insignificant jail time, only to use his or her hacker experience to find fame and a lucrative job in network security.

As formidable as this list may appear, each of these can be overcome by better-informed management and technology security teams. Further, the risk presented by failing to report intrusions is tremendous. The Internet is continuing to get more complex, more interconnected and thus more vulnerable to intrusions. Connected information systems are gaining more importance to our private lives as personally identifiable information is prevalent in today's economy.

The Mindset of Law Enforcement

The mindset of law enforcement is an important factor to consider in situations involving a technology security incident where you may wish to bring in external parties. Law enforcement's mission is to identify the perpetrators and to build a prosecutable case. Typically, the larger the damages are, the better the case will be. On the other hand, the security professional may be more concerned with protecting information and ensuring the business continuity of the enterprise systems. Both objectives are valid but not always mutually attainable. Understanding how both objectives can be accomplished is the intent of this paper.

Law enforcement continues to evolve with the demands of the Information Age. Depending on the type of fraud, abuse or crime, you will work with differing authorities.[2]

- The Secret Service investigates matters ranging from espionage to computer intrusions.

- The United States Attorney's Office supports investigations and prosecutes if the elements of a federal violation can be substantiated.
- The FBI will investigate fraud and related activity via computers, possession of access devices, trade secret incidents and espionage.
- The ATF will investigate bomb threats and trafficking of weapons via the Internet.
- The US Postal Inspection Service will investigate fraud with a mail focus.
- The Federal Trade Commission will investigate Internet fraud and SPAM.
- Local law enforcement will deal with child pornography and sex crimes via the Internet. In recent years, many police agencies have undergone extensive training on investigating these crimes. Local units do investigate system intrusions and cases involving computer viruses or sabotage.
- Local law enforcement will address theft of money, the theft of commodities, or the exploitation of children
- U.S. Immigration and Customs Enforcement can investigate intellectual property crimes and software piracy.

Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

Security teams can anticipate that in the crimes listed above, the law enforcement agency will be calling the shots. The

security team's role will typically be one of a subject matter expert on the systems being investigated and will be tasked with providing evidence. The security team should always be cooperative, work to meet their organizations goals and the outcome of the law enforcement agency they are cooperating with.

The Search Warrant

Civil, criminal or other investigations by a government agency can lead to seizure of technology assets under a court order. In the case of trade secrets, private companies have even obtained court orders for the seizure of a competitors system by law enforcement.[3] A lawful search warrant permits the government to enter corporate premises and physically seize computers, data and other evidence. Agents can seize computers, printers, faxes, backup tapes, electronic storage devices and traditional paper documents. Critical business information can be seized by agents even if this information is vital to the daily operations of the company. Agents may approach and interview employees, many of which may not be prepared to answer the questions posed or approved to sign documents on behalf of your corporate council.

Preparation for a seizure minimizes disruption and lessens mistakes. Organizations should develop policies for employees to follow when presented with a search warrant.

- Copy and read the warrant carefully to find out what they want to search or seize.
- Obtain identifying information of all agents and prosecutors

- Notify upper management and the legal department about the warrant immediately.
- Notify employees that may be impacted by the investigation that they are under no obligation to sign any statements or answer any questions without legal council. Additionally, employees should be careful not to do anything that might appear to be obstruction of justice.
- Designate a response team leader or CSIRT to be the point on contact with law enforcement and the business during the search.
- Negotiate the ground rules for the search.
- If the authorities want to search local machines, the impact on the organization may be minimal. Get the appropriate manager to evaluate the impact and to assist the officers. In some cases, such as child pornography, the police may need to take the entire computer.
- If servers are a target, see if a good backup can be made. Involve your server and network administrators with police in bringing down the server in an orderly fashion. The CSIRT should also be tasked with bringing online the replacement server.
- Rarely will an entire network have to be taken down. Have your CSIRT work with the police on orderly access to parts of the network described in the search warrant.
- After the search and seizure, the team will leave you “an Officer’s Return” on what property was seized. Retain this document for review by your legal staff. Make arrangements with law enforcement to follow up with them on the status of your equipment. Offer whatever technical assistance to law enforcement that your legal department deems advisable.

- Meet with your management, legal counsel, and technical staff after law enforcement leaves to assess the impact of the seizures on your operations.
- Consider designating an employee to document the entire process as it unfolds. Some experts recommend video taping the entire process if applicable.

When cooperating with an investigation, your team needs to be aware of the boundaries that exist. Collection of evidence should always be conducted as if the efforts will be used in a court of law. An agent or person acting on behalf of a governmental authority is prohibited from engaging in a pattern or practice of conduct by law enforcement officers that deprive any person of rights, privileges, or immunities secured or protected by state or federal law. Your team, when at trail, could be labeled as an agent of law enforcement by the defense attorneys in an effort to discard the evidence collected. Know what evidence you can legally collect without breaking the rights of the targeted individuals.

What Evidence is Good Evidence?

If your organization is deciding whether or not to contact law enforcement about a crime, it is necessary to have some evidence. There are several questions the security team should be asking:

- Can the evidence be documented?
- Do you have audit trails that expose the incident?
- Can your team identify individual users, physical locations or IP addresses?

- Can you rule out an error produced by your deployment process pushing out poorly written code or other types of false positives produced by your environment?

Normally your Computer Security Incident Response Team (CSIRT[4]) is in the best position to rule out non-criminal causes for what has happened. Your organization should have clear details before calling in external parties. Law enforcement wants to investigate computer crimes, not accidents.

The CSIRT first response should include:

- Ruling out a normal hardware or a software failure.
- Documenting the timetable of what happened.
- Produce audit trails for unusual activity during the timetable.
- Identifying any users or services involved.
- Try to determine the motive.
- Document any damages caused by the incident
- Initiate chain of custody procedures.

One of the things to consider prior to getting law enforcement involved in an incident is whether the case even justifies law enforcement involvement. If you do not involve law enforcement, what risk is assumed? Obviously, there are legal and ethical issues to consider here. If you discover a repository of child pornography in a peer to peer application running in your environment, you will want to report the incident to the police immediately. However, other lesser incidents may not be worth law enforcement's full investigative efforts. An outbreak of the Storm worm on your sales force workstations may not be a prime

candidate for contacting law enforcement. In some cases, it could be better to deal with the incident internally.

At a minimum, your CSIRT should report everything they know to be a crime at least to the CERT, the national computer incident center or the Internet Crime Complaint Center (IC3). The CERT will report incidents to law enforcement if you authorize the release of such information. Felonies should rank an immediate notification to the authorities.

In most scenarios, the security team will contact the authorities on incidents that are perceived to have a serious impact on the organization. The definition of what serious impact represents will require definition by the management and should be adequately stated in the organization's security policy. Additionally, this should be defined in the incident response policy. (See the create policy section for more details)

The Scene of the Crime

Once the decision has been made to call in law enforcement, what does the security team need to do before they arrive? What should be done with the evidence? What logs and records should be secured? Should computer equipment should be turned off or disconnected from the network? Should you begin forensic analysis? If physical evidence forms a part of the crime, what steps should you take to preserve it? Do you take photographs and rope off the scene? Do you begin to interrogate all employees in the building?

The security team can best assist law enforcement by carefully preserving a crime scene. The scene could stretch across your WAN or even to workstations in other countries. Your main objective will be to not alter the state of computer-based evidence. The security team should allocate all relevant logs and files, source code, hard drives, mass media, etc. The same applies to electronic communications such as email or instant messaging and any electronic documents stored in networked repositories. Local machines suspected of containing evidence need to be left untouched in their original state. Normal business retention rules should be immediately suspended for electronic or paper records involved in the incident until the police have a chance to examine the evidence. If you are utilizing backup tapes for the systems being investigated, it is recommended to set aside those backup tapes to remove them from your company's normal tape cycle. You would not want to inadvertently overwrite valid evidence that could help your investigation.

If possible, do not perform any security activities on the system(s) in question. In trying to conduct forensic analysis, security personnel (unless they are qualified experts), may create serious chain of custody and evidentiary problems for law enforcement. Not knowing how to inspect the computer properly can cause the deletion or alteration of key evidence. If your team has not had extensive training, leave things alone.

The CERT[5] publishes an outline on what to preserve at a computer crime scene.

- Preserve the state of the computer at the time of the incident by making a backup copy of logs, damaged or altered files, and files left by the intruder.
- If the incident is in progress, activate auditing software and consider implementing a keystroke monitoring program. Be sure your legal warning banner precedes logon activities.
- Report the incident to the CERT/CC using the incident reporting form. Consider authorizing them to release the incident information to law enforcement.
- Document the losses suffered by your organization as a result of the incident. These could include :
  - Estimated number of hours spent in response and recovery. (Multiply the number of participating staff by their hourly rates.)
  - Cost of temporary help
  - Cost of damaged equipment
  - Value of data lost
  - Amount of credit given to customers because of the inconvenience
  - Loss of revenue
  - Value of any trade secrets

Business Continuity During an Investigation

Any investigation involving an external presence requires time and resources. It is important to anticipate such an occurrence and to plan how to cooperate with law enforcement without shutting down critical functions of your organization. For the most part, specialists can generate drive images, data dumps, copy files, and create logs without confiscating the

organization's computers. Your management should have a plan in place to allow the investigation's targets to be taken in a manner that will at least minimize the disruptions in the organization's operations. The following is a list of suggestions that will help to minimize the disruption caused by an on-site investigation:

- Schedule a kickoff meeting with key employees to educate them on what needs to be done for the investigation.
- If parts of the network need to come down, arrange for this outage to take place during the most opportune time without delaying the investigation.
- Narrow down which logs and audit reports will be needed by law enforcement as this will minimize the amount of time to retrieve them.
- Keep the investigation compartmentalized, on a need-to-know basis. This action will reduce the amount of staff involved and protect the investigation.
- Keep the lines of communication open with law enforcement. Your team generally understanding what law enforcement is investigating will aide in retrieval of records and logs.
- Notify the team that with any data identified for investigation, they should confirm that a backup exists.
- Encourage onsite copying of memory and hard drives. In most cases, the removal of equipment to a forensics lab is not necessary. Negotiate with law enforcement to schedule these procedures during non-peak hours and keep your equipment on the premises and in service.

As the technology world exists today, many organizations are already deploying or strongly considering placing their systems in a high availability mode. Load balancing, active-passive systems, failovers and redundancy are all becoming mainstream concepts. These technologies will greatly aide your ability to provide data and systems to external parties without seriously impacting your organization. Your management team should continually be considering what damage would be caused if a section of your information systems is the target of a seizure.

Video Surveillance and Paper Records

Paper records and video surveillance tapes can play a major role in investigating technology incidents. Industry experts believe up to 85 percent of computer crimes are thought to be committed by insiders. Auditable paper and video documentation becomes important evidence in investigating an organization's employees.

If your organization has deployed video cameras to monitor the entrances to your exterior doors, data centers or laboratories, the video will produce concrete evidence of who entered and exited at a given time. If entrances use electronic access cards, the reports from your card system will contain the logs of employee traffic into sensitive areas 24 hours a day.

Paper documents such as personnel records, project documentation, sign-in sign-out logs, meeting notes, and job assignment records all tell a story. When you want to know who worked on what or who had access to which project, paper records generally provide the needed history. Law enforcement will be interested this evidence.

When examining paper records or videotape, have your assigned documentation employee maintain a record of what has been examined and any cross-references against other records. If you supply paper records to law enforcement, make an entry of those documents in the records. Such a record will prove to be an invaluable resource in quickly locating information later in the investigation.

Building Cooperative Relationships

Law enforcement may be reluctant to share information with your team. Building a relationship with them before you have a crisis can be very important. Get to know the leadership of your local police department's computer crimes unit. If you belong to a local technology association or computer security organization, contact the public affairs office of the police, and arrange to have a speaker come to your group. Get involved in networking through your local chapters.

- American Society for Industrial Security, asisonline.org
- High Technology Crime Investigation Association, htcia.org
- Infragard (FBI public private partnership), infragard.net
- Information Systems Security Association, issa.org
- Information Technology Association of America, itaa.org
- Internet Security Alliance, isalliance.org

It is recommended that your CSIRT attend conventions and seminars on computer security. Here you meet law enforcement and get to know them outside of a potentially stressful investigation. Most importantly, if law enforcement calls for

help on a case, try to give them a helping hand. Cooperation is always a two-way street.

Contacting Law Enforcement

To initiate an investigation you can contact your local FBI office or another appropriate federal, state, or local law enforcement agency. They can best process your complaint if they receive accurate and complete information from you. Therefore, you will want to provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your primary telephone and secondary numbers
- Information about the individual or organization you believe committed the crime.
- Specific details on how, why, and when you believe the crime was committed.
- Any other relevant information you believe is necessary to support your complaint.

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (i.e. hacking)	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Password trafficking	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Counterfeiting of currency	• U.S. Secret Service

Child Pornography or Exploitation	• FBI local office • U.S. Immigration and Customs Enforcement • Internet Crime Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	• U.S. Postal Inspection Service • Internet Crime Complaint Center
Internet fraud and SPAM	• FBI local office • U.S. Secret Service (Financial Crimes Division) • Federal Trade Commission (online complaint) • Securities and Exchange Commission (online complaint) • The Internet Crime Complaint Center
Internet harassment	• FBI local office
Internet bomb threats	• FBI local office • ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	• FBI local office • ATF local office

The Internet Crime Complaint Center (IC3) is an interesting way to file a criminal report with law enforcement. The IC3 will submit your report to several agencies on the federal and local levels. After the IC3 routes your report to the proper agency, that organization will initiate an investigation if they feel it meets their requirements. Your team will receive case information via email, requiring username and password, once the process is initiated.

Federal Laws You Should Know

When building your policy or standards there are several legislative works that impact how technologists can conduct business and/or investigations.

- Electronic Communications Privacy Act
- Privacy Protection Act
- The Fourth Amendment
- Department of Justice Guidelines on Search & Seizure of Computers
- Computer Fraud and Abuse Act
- Patriot Act

Although this is not a complete list of applicable laws or guidelines, you can build a solid policy from reviewing the works above. Understanding your business processes and understanding the applicable laws will greatly aide your team in cooperating with a law enforcement agency.

Create a Law Enforcement Policy

Your organization should work in conjunction with management and with law enforcement guidelines to develop your policy.
The policy should

- Define the methods your CSIRT will interact with law enforcement
- Responsibilities of employees involved with the investigation
- Management of your technology resources
- Continuity of the organizations operations
- Documentation
- Communication

It is important to have the policy promoted by your management team. Having the complete backing of the management team will

aide in completing the objectives of the policy during the investigation. Being presented with a seizure or a search warrant can be a very stressful and chaotic time. Department supervisors may not want to corporate, provide evidence, allocate people resources or allow computing infrastructure to be taken offline. The formalized policy will greatly aide in conducting a reasonable investigation with the cooperation of your organization. A sample ***Law Enforcement Investigation Policy*** can be found in Appendix A.

Educate your user base on the policy. It is important that your employees know how to handle an investigation, prior to law enforcement arriving at your front door. Yearly education about your organization's security policies is considered a normal business practice. Most organizations are conducting annual security and awareness training along with sexual harassment or workplace violence classes. Work with the business unit that is responsible for the training to insert information regarding your law enforcement policy.

As technology changes, so will your policy. Law enforcement agencies will evolve, contacts will change and new computer crimes will reveal themselves. These changes should be reflected in your policy and standards.

Appendix A

1) **<company> Law Enforcement Investigation Policy**

   a) **Purpose**: The purpose of this policy is to cover the efforts of working with a law enforcement agency during an investigation. This policy applies to all employees, vendors, and agents operating on behalf of <company>.
   b) **Policy Standards**
      i) **Contacting Law Enforcement**
         (1) A law enforcement agency will not be contacted without notifying <company> legal council first.
         (2) Law enforcement will be contacted when a criminal activity is discovered that has a serious impact to <company> or State / Federal laws have been broken.
      ii) **Interaction with Law Enforcement**
         (1) A point of contact will be appointed to coordinate efforts with the law enforcement agency. CSIRT team leads are typically assigned this role.
      iii) **Employee Interaction**
         (1) Employees are encouraged to be truthful and forthcoming with investigators.
         (2) Employees will not act in a manner that can be interpreted as obstruction. Shredding, deleting, or removing information during an investigation is prohibited.
         (3) Employees are not required to answers questions or sign papers without legal council present.
      iv) **Resource Allocation**
         (1) Systems, data, paper records, etc. will be provided when requested. The POC is responsible for coordinating activities to backup, restore, schedule downtime, and make copies where applicable.
      v) **Communication**
         (1) Legal council will be contacted immediately upon notification of an investigation.
         (2) Employees that will be involved in the investigation will be notified of their responsibilities (and limits) to the investigation.
      vi) **Documentation**
         (1) An employee will be designated to document the entire process of the investigation by law enforcement.
         (2) A receipt of what systems, data, paper, etc. that is taken offsite by law enforcement is required,

c) **Failure to Comply**

i) Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary action up to and including termination. Legal action also may be taken for violations of applicable regulations and laws.

References

[1] *Richard P. Salgado,* Working with Victims of Computer Network Hacks
[2] DOJ, Reporting Computer, Internet-Related, or Intellectual Property Crime
[3] Mark Freeman, Forum on Risks to the Public in Computers and Related Systems,
[4] Tim Proffitt, Creating and Managing an Incident Response Team for a Large Company
[5] Carnegie Mellon University, How the FBI Investigates Computer Crime

Last Updated: May 23rd, 2017

Upcoming Training

SANS Minneapolis 2017	**Minneapolis, MN**	**Jun 19, 2017 - Jun 24, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, IL**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
SANS vLive - LEG523: Law of Data Security and Investigations	**LEG523 - 201710,**	**Oct 09, 2017 - Nov 08, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**