# Guidelines for Working with Law Enforcement Agencies

*Campus security officers must balance privacy and security issues in dealing with law enforcement agencies as part of their institutions' legal obligations*

By **Michael Corn**

Many security professionals choose the career because of an interest in the technology of security. Few realize the degree to which a contemporary security office interacts with law enforcement agencies (LEAs) such as the FBI and state, local, and campus police. Those having had no interaction represent a shrinking minority, however. The past 10 years have seen a shift in malicious behavior from juvenile to professional; as often as not, the large botnets we target are used for identity theft or harvesting credit card numbers and may even involve national security.

As the field of information security has matured, the language of risk management is increasingly used to discuss the strategy and tactics of security. I view privacy concerns as primary in forming a cohesive and cogent philosophy of information security. Privacy is impossible to achieve without security; security without concern for privacy ignores the human dimension of the rich intellectual legacy that the modern university represents. A security incident has costs that, once accounted for, fade in memory; a privacy violation is a "read-once, write-many" condition.

Privacy as a prime motivator for security underscores the approach laid out in this article. Developing a solid working relationship with law enforcement, including having an established set of procedures and agreements, will enable you to

- fulfill your legal obligations as a representative of your university,
- ensure that you minimize the impact of requests for information from law enforcement, and
- protect the privacy of the individuals with whose data you have been entrusted.

## Your Obligations

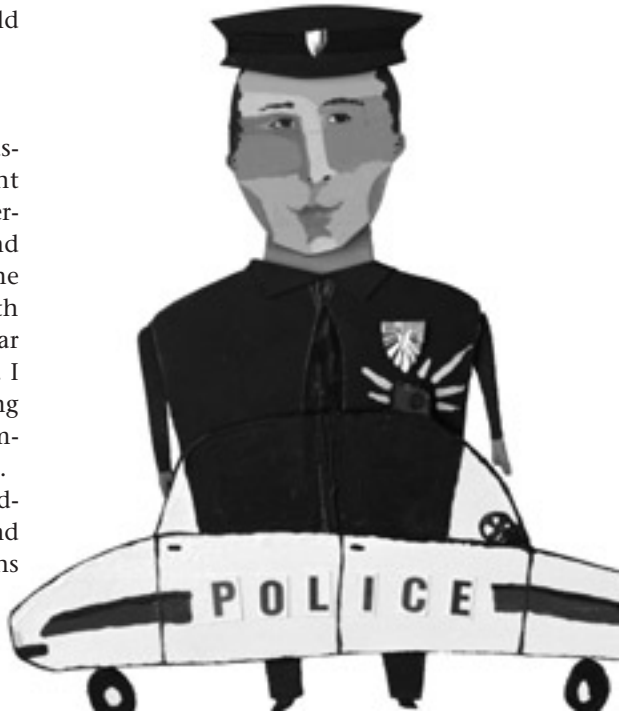
Your institution has the obligation to meet any valid legal request made by law enforcement. Typically that means finding the information requested as it exists within your environment; it does not require you to reengineer your environment. For example, if a request for network flow logs arrives in a search warrant and your routers cannot produce netflow data or if netflow data have not been collected, you are not obligated to modify your environment to meet the request. That is, you are not obligated to create data or build new systems to collect data that you would not otherwise gather.

## Form a Team

As security professionals, we can easily get drawn into law enforcement investigations beyond our formal expertise. Our role in these matters is—and should be—restricted to providing the information required to comply with a subpoena, search warrant, or similar document. To handle these requests, I recommend you form a team consisting of a security office representative, campus legal counsel, and campus police.

Campus police usually have standing relationships with various state and federal LEAs and can elevate questions or issues to the appropriate individuals. They can also vouch for the identity of the agents. Campus legal counsel can certify the accuracy and validity of any documentation, such as the actual search warrant or subpoena. Legal counsel can also interpret the precise details of the request, the deadlines, and its confidentiality. Their actions will protect you from foolish mistakes. The security representative handles collecting the actual information and advises on the existing technological abilities and limitations.

You need to remain flexible on how this team operates. Many, if not most, matters may not require involvement by campus police. If your campus lacks its own police department, seek the advice of your campus legal counsel before sharing information.



Collectively, this team can respond to almost any issue that arises during the course of responding to a request. Over time, the members of this team will learn to act for each other if necessary, ensuring professional handling of requests even in emergency situations where not all members are immediately available.

## Establish Campus Policy

It is essential to ensure that requests for information are valid legal instruments. Your campus should adopt a policy that formally identifies legal counsel as the arrival point for any LEA request. Doing so will minimize the number of requests that bypass your established procedures and ensure strict compliance with both the law and campus policies. This policy should be short and explicit, for example:

> If service of a subpoena, complaint, notice of class action, or other legal documents is attempted in person by a process server or other individual, the service should be politely declined and the individual referred to the Office of the General Counsel. If an officer or employee unknowingly or erroneously accepts personal service of such a document, he or she should immediately fax or hand-deliver the document to the Office of the General Counsel, indicating in a cover sheet his/her name and the date and time at which he/she accepted service.

or

> When you receive a legal document, prompt notification of the campus legal counsel office is essential. In some cases, delay in responding to legal documents can result in the loss of valuable rights. When you receive contact from a legal authority from outside the university, such as a non-university police officer or attorney not working for the university, you should contact the campus legal counsel office (and in some instances, the university police) before responding to information requests, etc.

Many schools already have such a policy, but they rarely publicize it. In particular, ensure that IT professionals who might be contacted by law enforcement are aware that they should not respond to requests for information without first bringing the matter to campus counsel. If you do not have in-house counsel, identify a single contact point for legal documents to coordinate getting these documents into the hands of your contracted counsel.

## Know Your Environment

Nothing will sour your relationship with law enforcement faster than demonstrating an unprofessional and inadequate understanding of your infrastructure. Be prepared by knowing the answers to questions such as:

- How long are networking logs (such as flow logs) retained?
- How long are backups of your services kept? Concentrate on e-mail and file storage.
- How long will it take your service managers to restore an individual account from back-up?
- Do any of your core services (instant messaging, e-mail) have "tapping" facilities?
- Which campus units run their own e-mail services?
- What is the process to acquire a SPAN[1] port on a switch?
- Who is responsible for IT within a department or building?

Additionally, be prepared to discuss with the agent in charge the information each log provides. Network flow logs, for example, appear to the uninitiated to be incredibly valuable. They say nothing about the content of any communication, however, only that a point-to-point connection occurred. They can also run to several gigabytes per hour. Similarly, e-mail logs, while potentially interesting, often contain information culled from the headers of an e-mail, which can be easily spoofed. It is a waste of both your and the agent's time to collect voluminous information of no value.

Although law enforcement agents are increasingly knowledgeable about IT data and systems, be prepared to share your expertise about your local environment. Doing so will minimize your and the agent's workloads and protect the privacy of your campus community.

## Confidentiality

Note that many of the documents discussed have strict confidentiality requirements; you should account for that in your standard practices for LEA interactions. It is not at all uncommon for even ordinary subpoenas to restrict your ability to discuss their content and in some cases their existence. National Security Letters and Foreign Intelligence Surveillance Court[2] requests are even more restrictive. The following is an excerpt from a National Security Letter:

> In accordance with 18 U.S.C. section 2709(c) (1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States...and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice...

When reviewing the documentation for validity and accuracy, your legal counsel should inform you of any confidentiality requirements specified. Confidentiality has two components: its specific impact on the collection of the requested information, and the general confidentiality of the investigation.

### *Confidentiality and the Collection of Information*

Because of confidentiality requirements, security staff charged with collecting the required information must work independently from the chain of command. The language in these documents does not permit you to casually discuss a request with your supervisor or senior administrators on campus. Consequently, I strongly recommend that those responsible for collecting information in response to an LEA request meet directly with the most senior administrative officers at the institution to discuss the general process to meet these requests. The CIO,

provost, and/or chancellor must have an opportunity to discuss these matters and what role, if any, they want to have. In general, I do not recommend that you encourage senior administrators to participate regularly and actively in these investigations, although they will want to be informed if the investigation in question appears to be going public (that is, developing a public relations component).

If a need develops to inform others of the investigation, be sure to discuss this with the law enforcement agent or officer responsible for the case before proceeding (this includes informing senior campus administrators). The responsible agent will either approve informing an individual or refuse the request to avoid the risk of compromising the investigation. Since the decision to bring others into the investigation is typically motivated by a sincere attempt to meet a request, the agent or officer in charge of a case will usually approve.

Commonly, technical staff or a unit head feels uncomfortable authorizing access to protected resources (such as a departmental mail server). In many cases the assurances of legal counsel and the security office will not give the unit head enough confidence to proceed. It might be necessary to facilitate a meeting with those handling the investigation, the unit head, and a senior administrator such as the provost. Should this prove necessary, having already reviewed the procedure with the provost will simplify this process considerably. Rely on your campus legal counsel to assist in mediating these situations; senior administrators are used to discussing confidential matters involving risk with counsel and may be more comfortable working with counsel than with you.

### *Confidentiality and the Investigation*

On most large campuses and many smaller institutions, the information requested by law enforcement might reside in a system controlled by a unit and not by the central IT organization. To comply with an LEA request might require disclosing the existence of the request to a departmental IT professional. As with any investigation, discuss this with the agent in charge and receive approval before going forward. Consider the context for the individual departmental IT professionals:

- Do they have a personal relationship with the target of the investigation?
- Do they have a reputation indicating they cannot be trusted to maintain appropriate confidentiality?
- Will they be able to comply without the support of their immediate superiors?
- Is the infrastructure in the unit such that other IT professionals will notice the data collection effort or mechanism?

Before approaching departmental IT professional staff, these matters should be discussed by the security representative handling the investigation with campus counsel and the agent(s) in charge of the investigation. Any risk to the investigation through collection of the requested information should be at the discretion of the agency making the request. An institution's duty is to meet the request to the degree possible and not to assume responsibility for the investigation itself.

With the approval of the supervising agent(s), a typical approach involves meeting with the department head first, and then (at their discretion) the appropriate departmental IT professional staff. If your institution has its own legal counsel, I strongly recommend that counsel participate in these conversations to ensure that (1) the individuals understand their legal obligations with regard to confidentiality and (2) the paperwork provided by the agency to the institution is complete and accurate.

You should also make sure that internal procedures for handling LEA investigations have exception mechanisms when dealing with exceptionally confidential material. Most security offices maintain issue tracking or ticketing systems. Typically, multiple members of the security office have access to these tickets and associated files. It might be necessary to handle these highly confidential incidents so that they are tracked in a more restrictive fashion, for example not tracking these activities electronically.

Documents marked or classified "Secret" often require special handling and have specific retention protocols. They should be stored in a secure safe with restricted access while in your possession. Discuss the life cycle of these documents with the responsible agents. As with all confidential documents, pay strict attention to the storage of paperwork. A safe in your operations center (usually manned at all times) is strongly encouraged.

## Narrowing the Scope of a Request

FBI and other law enforcement agents are busy people. Security staff are busy people. No one has the time to comb through terabytes of data for pieces related to a specific individual. A worst-case scenario is one where an agency requests all the traffic transmitted between a campus (or even a building) and the Internet. While such a request might be fairly simple to answer, doing so will inevitably compromise the privacy of individuals unrelated to the investigation that spawned the original request. This conflicts with the raison d'être of IT security—to protect the privacy of individuals within your institutional community.

For law enforcement, however, refining a request often requires an intimate understanding of the systems and infrastructure of your institution. Agents will frequently lack either the technical background or local details to formulate a precise request. When investigating an individual, for example, it could be very difficult (especially on large campuses) to respond to a request such as "provide e-mail headers for all e-mail associated with John Smith." Beyond the obvious issue of which John Smith is meant, determining how many e-mail accounts a specific John Smith has on campus might be impossible. He might have multiple departmental addresses, a centrally provided account, accounts associated with institutes or centers on campus, and individual local accounts. The odds of keeping an investigation con-

fidential while attempting to collect even the number of e-mail accounts could be very low.

On the other hand, if the agents understand that they can approach you ahead of time to discuss their purpose, it is often possible to end up with a request such as "e-mail headers associated with the account netid@yourschool.edu or netid@department.yourschool.edu." In these situations the two accounts listed might be under central control or accounts maintained by trusted individuals and thus satisfactory to the requesting agents.

Consider another example: A request arrives asking for the nightly backup of an account for the past six months. You currently have only the past 30 days online, with the remainder stored offsite in encrypted tape backups. Restoring the previous five months could be exceptionally disruptive to your operations. Working with the agents and ensuring that they understand that your working window is 30 days, it is possible they will provide you with a fresh preservation request every 30 days (or at least going forward from the last 30 days).

Some requests will entail significant work and could be highly disruptive. The agents you interact with are balancing an enormous workload with competing priorities. They will generally understand that requests that are highly disruptive to your operations could compromise either their investigation or your ability to react to requests. Consequently, it is in their interest to give you honest and accurate assessments of priority and timeliness.

## Prepare

Most institutions will never have to respond to LEA requests such as a National Security Letter or a wiretap. I do not recommend the anticipatory purchase of the equipment necessary to meet all and any requests. Still, it is prudent to engage in an annual tabletop exercise with key technical staff on how you would respond to various classes of requests.

- How and where would you collect traffic to and from specific IP addresses or ranges?
- How would you respond to a request for all e-mail traffic to and from an individual?
- How would you create a snapshot of a specific user's network file shares on an ongoing basis?

For every scenario you consider, remember the requirement that none of your techniques can be detectable by the subject of an investigation.

Also prepare a campus policy on data retention; that is, define how long different classes of data are retained. Having this included in policy may be a challenge, but a documented best-practices guide for data retention is a valuable resource.

## Local Awareness of Investigations

A final issue to consider is how to respond when asked about interactions with LEAs. Many individuals on campus, particularly among the faculty, will disapprove of campus representatives working with law enforcement. They might have a number of assumptions about the existence, or lack thereof, of LEA investigations. You should avoid discussing these matters and defer to legal counsel. Remember, to simply acknowledge the existence of certain classes of requests is itself a serious crime that could include any number of penalties.

## Conclusion

Law enforcement investigations tend to be disruptive and unsettling. A preservation request, for example, might require you to move immediately to preserve data that would otherwise "age out." Requests frequently arrive with a sense of urgency, either real or assumed. Being prepared in the fashion described in this article will give you a sense of control over the situation and confidence that you are responding as you should. Further, this sense of what can only be called professionalism will give law enforcement confidence as well. This confidence, both internal and external, is the foundation on which trust is built, and only with this trust can you fully engage LEAs in a manner that truly protects the privacy of the members of your campus community.

## Checklist

[ ] Create a policy to address the handling of all legal documents.

[ ] Form a team consisting of the security officer, legal counsel, and campus police.

[ ] Put campus legal counsel on your telephone speed-dial.

[ ] Meet with provost and/or chancellor to discuss law enforcement requests and investigations.

[ ] Review and document the salient features of your environment, including your institutional policies on data release and retention.

[ ] Understand your obligations with regard to confidentiality.

[ ] Discuss with the agent(s) in charge of an investigation whom you wish to inform of the investigation and why.

[ ] Work with the agent(s) in charge of an investigation to review what they are looking for and what will not be useful to them.

[ ] Develop internal procedures that control the materials and information of legally restricted information. Buy a safe for storing legal materials.

[ ] Work with law enforcement agents to better understand your environment and narrow the scope of information requests.

### Endnotes

1. On Cisco System switches, port mirroring generally refers to a switched port analyzer, or SPAN, port.
2. Also known as FISA requests, as the court was established by the 1978 Foreign Intelligence Surveillance Act, or FISA.

*Michael Corn (mcorn@uiuc.edu) is Director, Security Services and Information Privacy, Office of the CIO, University of Illinois Urbana-Champaign.*