Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Art of Enforcement

In the computer age, actions that take seconds to complete may take years to be defined, and even longer to become regulated by law. The use of Computer Code to automate transactions and transmissions has catapulted the application of Law into the 21st Century, often with almost comical results. A delicate balance of powers between the Public Agencies charged with enforcing the law, and the private corporations attempting to defend themselves with it, must be achieved for the common good of both. Those charged with def...

Copyright SANS Institute
Author Retains Full Rights

AD

SANS GSEC Practical Paper V1.2F

SANS Security Essentials GSEC

Jeff Neithercutt

September 28, 2001

The Art of Enforcement

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Art of Enforcement

In the computer age, actions that take seconds to complete may take years to be defined, and even longer to become regulated by law. The use of Computer Code to automate transactions and transmissions has catapulted the application of Law into the 21st Century, often with almost comical results. A delicate balance of powers between the Public Agencies charged with enforcing the law, and the private corporations attempting to defend themselves with it, must be achieved for the common good of both. Those charged with defending either public or private entities against these types of cutting edge attacks are sometimes forced to call upon their own discretion and ingenuity in responding to these incidents. Combining the roles of the Corporate Security Investigator, the Corporate Incident Response Team, and the powers of the Public Agency Prosecutor can be incredibly beneficial to all, but can lead to pitfalls as well. This paper will attempt to address the differences between the powers of the People, the powers of the Public Agency, and the needs of the Corporation in today's information technology intensive world.

Historically, the main problem with our judicial system has been its inability to keep up with the current trends in civil and criminal behavior. It seems that the system is constantly playing catch-up with the brightest devious minds in our world. We consistently find situations where an evil genius, or your average bored teenager, concocts a plan that has either a new twist, or a completely new approach to an issue that has either been ill-defined, or not yet broached by those in our system who are charged with writing the laws of the land. When these unique situations occur, we have what the system calls a "precedent setting" case. These cases will slowly wind their way through the system, and eventually, sometimes years, sometimes decades later, the legislature will either decide to pass regulations guiding or banning the activity presented in the case, or do nothing.

One of the most interesting aspects to the new "information age" is the transfer of investigative techniques from paper to plastic. That said, the modern day computer crime occurs in the "ether" jurisdiction. This creates serious issues with the Public Agencies created to combat these types of crimes, as they are often allocated their funding based solely on the number of investigations conducted in their assigned jurisdiction. Finding a Public Agency willing to help a private entity investigate the multi-national ether-based crime is a real challenge. The enterprising private Computer Crimes Investigator must diligently pursue the case in the manner necessary both to protect the interest of his charge, and to meet the needs of the public agencies he is requesting assistance from. Additionally, in a Corporate Response Action, the corporation must determine how many resources and how much money it wishes to spend in order to reach the goal of the investigation. There will be times when the cost does not justify the result, especially in Civil Procedures. It is vital the investigator have the guidance of their employer in determining the extent to which they should carry the investigation using that employer's resources. This is particularly important when the investigation may result in the suspension or termination of an employee for Corporate Policy, Procedure, or Agreement violations, as a wrongful termination suit is more likely to be brought when dealing with these issues than with those of a criminal nature.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

With the advent of the computer as an integral part of the Corporate workplace, we are faced for the first time in our history, with individuals and Corporations, on a massive scale, looking for ways to defend themselves against unseen attackers, and often, thousands of them. Our Criminal Justice System was designed in a manner consistent with the prosecution of the known or suspected perpetrator of a crime, hence the right that a suspect has to face their accuser. Many recent Computer Incident Response Actions have been caused by perpetrators committing their crimes anonymously, sometimes over distances of thousands of miles, and across hundreds of Judicial and Regulatory Jurisdictions. Determining which agency had responsibility for prosecuting these crimes has been a trial in itself. Assisting Corporations in recovering lost or stolen data that was transported across international lines has proven, in some cases, virtually impossible.

Due to the increase in workplace violence in recent years, it is incumbent upon the Incident Responder to be prepared for any type of problem that might occur during a Response Action. Often, employees engaged in improper activity at work have personal issues that will directly affect their decision making processes at work. This can place the Incident Responder in a very dangerous position. Particularly once the unstable employee has been made aware of the Response Action.

Unfortunately, other types of activities have also crossed into the workplace. Those who would engage in deviant sexual or social behavior now have the tools to do so anonymously, and to the great detriment of their co-workers. Increasingly, Corporate Security Officers and Investigators have been asked to take on the role of Orwell's "Big Brother" character, often equipped with sophisticated surveillance devices to monitor employee activity. Entire Judicial Agencies are now having their Internet access monitored, and some of them are plenty unhappy about it. [1]

Thankfully, most situations never reach this level of severity, with the notable exception of the employee stalking or spousal abuse cases Responders are increasingly faced with. Still, understanding the rules and regulations surrounding the private persons powers of arrest is vital to the overall investigation and successful search and seizure of equipment related to the case. Where possible, local Police and or State and Federal agencies should be consulted prior to any corporate involvement where a criminal investigation may result. But for Civil Litigation cases, there really are very few things a private person can not do in the course of an investigation. A well written employee agreement will allow for the placement of any type of surveillance device necessary to properly monitor an employees activity, including the use of Keystroke Loggers, cameras, microphones, GPS devices, and any number of other devices for monitoring what a subject has been doing with the corporate property assigned to their use.

The most difficult part of any type of Computer Response Action in the "Information Age" is finding a good source of information concerning the current laws regulating the activity or type of activity being responded to. This means contacting local, state, federal, and corporate officials for advice and procedures with which to conduct your Response Action. As these entities may not have the time to guide a Responder, finding someone you can trust who has experience with the Laws in your jurisdiction may not be an easy task. Barring having the ear of your local magistrate, the Incident Responder must call upon the time-tested and proven investigative techniques

[1] http://www.newsbytes.com/news/01/169357.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

with which to garner the evidence necessary for use in the ensuing investigation. Additionally, without a clear understanding of the computer as an "instrument of the crime", most Corporate Security Investigators must rely on the more technical staff members of the Corporation for assistance in retrieving the evidence of an incident. This is where a well-defined and well-trained Computer Incident Response Team can be invaluable.

Involving more technically oriented workers in the investigation may cause problems as well. Having employees of the Corporation involved in sensitive Human Resources issues can cause problems with confidentiality, as well as the technical staff misunderstanding their role, and not having a good grasp of proper chain of custody and investigatory issues. Essentially, any Corporate Incident Responder charged with assisting an investigation into all types of cases should be well versed in Law Enforcement, have an excellent grasp of local, state, and federal laws in their area, and be at a minimum, SANS certified for competence with information technology and Computer Security Incident handling.

Public Agencies like the Police, District Attorney, and Judicial Authority, have restrictions placed upon their regulatory powers with the intent to provide U.S. Citizens with a balanced and fair legal system where no single agency or entity has control over all of the aspects of a case. The local Police Agency is given one set of responsibilities and rules of conduct, the local District Attorney some more/others, the Judicial Authority still more/others, and finally the District Appeals judiciary still more/others. For instance, the local Police are charged with patrolling within their geographical jurisdiction to prevent illegal activity by their presence, and to arrest perpetrators who have violated local, state, or federal laws. They are not responsible for prosecuting the suspects, only collecting the evidence necessary to assist the District Attorney in doing so. Conversely, Judicial Authorities are charged with being the impartial "trier of fact", interested only in preserving the legal rights of all parties in a case, and in determining the outcome of legal cases over which they are given jurisdiction. A Judge will never travel to a crime scene to collect evidence, as that is not their role in the process.

Federally, the system continues, with local level Federal Judiciaries being given power regulated by Federal jurisdictions and regulatory statutes, which sometimes supercede, sometimes exceed, and sometimes even contradict those at the state level. There are many instances where a Federal Judge has reversed the decision of a State Court, or returned a case to an Appeals Court for clarification of technicalities that it feels were not properly addressed, or to give direction in the interpretation of higher laws of the nation in the decisions rendered in those cases under it's jurisdiction. All of these checks and balances are there to provide us, the citizenry, with a system where a balance of power is supposed to prevent the abuse of that same power. In many cases it succeeds; in others, it fails miserably. An unfortunate example of this is the Rodney King case, where several Police Officers, during the performance of their duty to arrest perpetrators of crime, abused that authority in overcoming resistance to a lawful arrest, resulting in charges being filed against the officers for assault under color of authority. The Local Judicial action resulted in a Jury ruling that the Officers had acted in accordance with the training they had received, and that the law was not specific enough for the jury to convict the officers of the charges against them. A Federal Court determined that they had violated a higher law, the Bill of Rights, and sentenced them to serve time in a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Federal Correctional Institution for doing so. A Civil Court was not given the opportunity to rule in the Civil case filed on behalf of Mr. King because a settlement was reached with the LAPD prior to trial.

Key issues to consider when planning a Response Action are jurisdiction, amount and type of loss, type of data damaged/stolen, ways the access occurred, geographical limitations, time zone issues, equipment compatibility, company policy, and legal ramifications. Bringing a public agency into your Response Action at the wrong time can completely disable the ability of your corporation to protect itself, both civilly and criminally. If you bring the Public Agency into your Response Action before you have exercised all of your rights to search and discover as a private citizen, then the Public Agency, tied by the constraints of the fourth amendment and specific jurisdictional policies, may not be able to achieve the legal level of intervention necessary to collect the evidence they need to bring your investigation to a successful conclusion. Additionally, as their goal will always be the prosecution of the suspect according to the criminal law statutes they are charged with enforcing, Public Agencies may hamper, damage, or even negate the ability to bring civil charges and recover Corporate losses during their own case-building efforts.

Understanding the Private Person's Powers of Arrest in your State is the Key to proper Search and Seizure Procedures. While most Computer Incident Responders for a private Corporation would have little use for this information under normal circumstances, it should be said that once you involve them in this type of possibly criminal investigation, it is your duty to inform them of their rights, and your requirements of them, and you must give them the ability to "opt out" of the investigation if they are concerned about their own liability. The use of proper search and seizure techniques may prevent you from losing the admissibility of evidence in a court of law at a later time, but anyone can sue anyone else for any reason, and at any time, so precautions must be taken to allow your responders to protect themselves from liability. In other words, if you use proper search and seizure techniques, and you therefore notify the person to be Searched of the intent to search their system/drawers/person and areas under their direct control, of the reason for the search, and provide the reason in the form of a memorandum from upper level management or HR commanding the employee to submit to the search under penalty of termination, then the individual has no choice but to submit to the search, or risk the loss of their job.

This must be very carefully researched prior to enactment however, as the definition of custody defines physically restraining a person as actually placing them in custody, so the appearance to the subject of your Response Action must always be one of "I am free to move about and leave at any time" or the corporation risks the accusation of false arrest. Hopefully, this is never necessary, as most searches of an employees computers and direct access machines can be performed remotely, quietly, and often without the employee's knowledge.

The primary consideration in any High Technology Incident Response Action should always be "what is the goal of the Response Action." This is perhaps the most important piece of information to have firmly entrenched at the very beginning of any Response Action. An Action with a goal of determining how much, and which, data was taken by a departing or former employee in order to pursue the Civil Law process will have drastically different procedures than one in which the goal is criminal prosecution

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

by local, state, or federal authorities. The investigator will want to make certain they have the guidance of their supervisors, or whomever may have the most vested interest in the investigation from the Responder's Employer's point of view. The Responder must have a thorough understanding of what the goal of the investigation is in order to properly process the evidence. The Responder must also be trained to recognize when to "cut your losses" and just walk away from an incident where just blocking the attack is much more important than allowing it to continue to a level where sufficient evidence to identify the attacker has been captured. Once the goal of the Response Action has been established, the next steps to take are based on that goal.

If the goal of the Response Action is to provide information to the local or Federal agency responsible for the criminal prosecution of Computer Crimes in that area, then vastly different procedures need to be taken from those which will enable your private corporation to recover lost or stolen data from malicious individuals. The Justice System is designed with the goal of deterrence, and barring that, incarceration of criminals for their actions. The Civil System is designed to provide recourse to those who have suffered a civil wrong. The rules of evidence in each of these arenas are vastly different, and as such, need to be approached accordingly.

It is vital that the corporation have a firm understanding with the Law Enforcement agency assisting in the case what level of publicity can/will be brought to bear on the case, as more damage can be done by an errant news report about the safety of the corporation's information protection capabilities than may be recovered in a lengthy investigation and trial.[2]

"Code of silence"
Companies are facing more and more threats of computer crime. But they fear reporting incidents because of negative publicity that could jeopardize stock prices or make their systems increasingly vulnerable to hackers."

However, if you bring Law Enforcement into your Response Action too late, you run the risk that the suspect will flee before apprehension, leaving an ether trail that may or may not lead to a successful conclusion of the investigation. There may be legal liability issues here as well, as negligence may be alleged in too lengthy a delay prior to notification of the proper authorities.

There are also cases where using only private citizen powers have led to evidence being determined to be inadmissible as well. Most notably, in instances that would normally require a warrant for Law Enforcement authorities. If consent of the subject is not received prior to the search, the citizen also may not search the subject. The following case illustrates this:[3]

"The site was intended only for certain pilots who were required to log in with a user name and password.

---

[2] SOURCE: Chicago Business http://www.chicagobusiness.com/cgi-bin/news.pl?post_date=2001-09-08&id=3277&feature=1

[3] http://www.siliconvalley.com/docs/news/tech/026405.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The lawsuit said an airline official gained access to the site and alerted the union to it after asking a pilot who was eligible to view it for permission to use the pilot's user name and password. Konop accused officials of violating the Wiretap Act and the Stored Communications Act by reading the private information under false pretenses. The lawsuit also claimed that in contacting the union about the Web site, the Honolulu-based airline violated the Railway Labor Act, which bars carriers from interfering with employees' selection of union representation. The January decision noted that the Wiretap Act allows any person to read Web sites that are intended for and readily accessible to the general public, but said Konop's site did not fit those criteria."

Some of what this paper addresses has been alternately called "brilliant investigative work" and "dirty pool". Combining a good understanding of the difference between the rights of a private citizen to recover property and data via online investigative techniques, and a good understanding of the limitations rightfully placed on Public Agencies to prevent abuse of authority, you can plan a two-tiered investigation that will allow you the fullest prosecution possible available under current Law, and the maximum return on the Corporations' Civil Prosecution investment as well.

It has only been recently, with the advent of the laws surrounding DNA Evidence admissibility that we have begun to see a swing in the ways our Court systems deal with unknown perpetrators. A judge recently issued a warrant for the "to be located" match of DNA at a crime scene:[4]

> **"SACRAMENTO, Calif. (AP) — A judge late Friday upheld an arrest warrant issued against a rape suspect identified only by a genetic code in what is believed to be the nation's first ruling of its kind.**
>
> **Superior Court Judge Tani Cantil-Sakauye said she was doing what has never been done before.**
>
> **"This is uncharted water. It's a novel theory," she said after a daylong hearing in a case testing fundamental constitutional rights.**
>
> **Prosecutors nationwide are watching the case and say a favorable ruling would provide them with a powerful tool as modern databases become filled with criminals' genetic codes. "**

This type of action was necessary to prevent the criminal from escaping prosecution by remaining unknown for a long enough period of time to allow the Statute of Limitations to expire on their case, barring any successful prosecution of them at a later date. Still, one would argue that issuing a warrant for "that guy who did it when we catch him" is a little ridiculous. It is amazing to think, however, that with DNA in hand,

[4] http://www.courttv.com/news/forensics/022601_dnawarrent_ap.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

we are doing little more than finding Cinderella with her glass slipper. DNA is a little more accurate fit, however, so it has been increasingly acceptable to issue warrants in this manner.

This issue goes more to the "spirit of the law" than the "letter of the law" in that judges deciding to allow the issuance of criminal warrants seeking the match to the unknown DNA are assuming that the writers of the statute of limitations were intending to keep our court systems from being clogged by haphazard, malicious, or unprovable accusations. Findlaw defines the Statute of Limitations as "a statute establishing a period of time from the accrual of a cause of action (as upon the occurrence or discovery of an injury) within which a right of action must be exercised",[5] hence the decision to remove any case from prosecution when a period of time has passed that indicates it is unlikely the case will ever actually be prosecuted in any manner. It should be noted that the most important use for DNA may still be to exonerate the innocent. Too often, investigators lose track of their duty to find evidence of the facts, and instead lean toward finding evidence of their suspicions. This leads to tragedies like the following:[6]

> **"OKLAHOMA CITY (AP) _ Three months after a prisoner's rape conviction was set aside after DNA testing, an inmate already serving time has been linked to the crime, authorities said. In May, Jeffrey Todd Pierce was released from prison after serving 15 years of a 65-year term for a rape at an Oklahoma City apartment complex. Tests showed that semen and hair samples taken from the crime scene didn't match his DNA profile.**
> **The evidence was tested against all convicted violent offenders in an Oklahoma State Bureau of Investigation database and was found to match a man serving a 45-year sentence for rape and robbery, bureau spokeswoman Kym Koch said Tuesday."**

Since this type of warrant has been allowed in criminal cases not involving computers, it is possible that they could now be used in cases which do involve computers. Specifically, we could soon see warrants being issued for a specific "fingerprint" or handle associated with the author of a particularly malicious type of computer program, like a virus, or it could define the subject of the warrant as the owner of a particular IP address or range, or a physical MAC address of hardware used in a crime.

Finding the balance of enforcement vs. deterrence can be difficult as well. While hard and software devices may provide you with a taller fence, it is increasingly common for an intruder to take advantage of an exploitable security hole in a common software package to burrow under, rather than climb over, your walls. Increasingly, the use of personal firewall software, Ethernet and cable switches and routers, and other devices for the continuous real-time blocking of access to your system from the outside in are now just automatically considered when setting up the always on connection to the internet. This is a good thing, but it is sad that it has become necessary in the first place.

---

[5] http://dictionary.lp.findlaw.com/scripts/results.pl?co=dictionary.lp.findlaw.com&topic=33/339dc5812f50d9638ce513acd35931c7

[6] http://news.findlaw.com/ap_stories/l/0000/8-29-2001/20010829083511200.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It is only now, with Law Enforcement and the Judicial System completely overwhelmed, undermanned, under-funded, and woefully inadequately equipped, that Private Corporations have begun looking to their own, internal, private investigations teams to provide them with the protection and assistance that Public Agencies can simply no longer provide. As such, the rights of the common man to interrogate, frisk, search, surveil, and otherwise monitor their fellow man are increasingly being tested in our Corporate Environments. Things like Non Disclosure Agreements have been around for a long time, but the enforcement of them has come full circle. Gone are the days when managers wandered among the cube farms looking for "unauthorized" reading material or other evidence of quality company time being wasted. Now, it is common for Corporations to provide their employees full time access to the internet, often encouraging them to try and handle their affairs in a discreet, timely manner, via the internet rather than take valuable days off to deal with traditionally "business hours only" activities. Additionally, with code sections like 14489 of the Ca. Corporations Code, which states:

"14489. Whenever the registrant or any member of any corporation or association which is the registrant takes an oath before any magistrate that he has reason to believe and does believe that any supplies are being unlawfully used, sold or secreted in any place, the magistrate shall issue a search warrant to discover and obtain the supplies and may also bring before him the person in whose possession the articles are found."

Corporations can now take suspicious activity directly to a Judge, requesting a search warrant for an employees home, car, briefcase, or any other area under that employees control, and the magistrate can, I did not say will, issue a search warrant allowing the Corporation to search the area listed, and bring the items and person responsible back to the court for judgement.

So now, for the first time, corporations and civilians are finding themselves in an awkward position. Unless a certain amount of loss occurs, most federal agencies will not pursue a computer crime for a corporation or civilian, with notable exceptions, like financial institutions. Oftentimes, local agencies simply don't have the training to assist, and more often, simply don't have the resources or equipment. So, Corporations and civilians are increasingly forced to find their own resources to complete investigations into computer crimes. This leads to an amazing amount of ingenuity on the part of the individuals tasked with Responding to the Incident, and has resulted in the true testing of the limits of our written laws concerning search and seizure.

For instance, in California, private citizens are empowered by law to stop a criminal offender and even take them into custody, after which they are to deliver them posthaste to the nearest magistrate for prosecution. Built into the laws which empower these citizens are certain restrictions, and a noticeable lack of others. For example, a Police Officer in California may arrest a person for an outstanding warrant, whereas a private citizen may not. However, a private citizen may search an individual for any reason, provided the person consents, and anything the citizen finds in their search is admissible as evidence, whereas a Police Officer must obtain a warrant for any search

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

that is not pursuant to an arrest, or to check for weapons which might threaten the safety of the Officer. This precludes the Officer, however, from using any evidence found during a search for weapons, which could not have been mistaken for a weapon, and therefore dutifully retrieved, as illustrated below:[7]

> **"Because the object of the "frisk" is the discovery of dangerous weapons, "it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer." 12 If, in the course of a weapons frisk, "plain touch" reveals presence of an object that the officer has probable cause to believe is contraband, the officer may seize that object. The Court viewed the situation as analogous to that covered by the "plain view" doctrine: obvious contraband may be seized, but a search may not be expanded to determine whether an object is contraband. "**

Obviously, a Police Officer would have difficulty convincing a jury that a floppy disk or CD-Rom felt like a weapon, or for that matter, contraband.

But wait, you say, how can it be that a private citizen can do things even the Police aren't allowed to? It's really very simple. They are not subject to Miranda, the 4th amendment, or any other restriction Law Enforcement or Government Representative's have policing their conduct because they aren't any of those things. So essentially, as long as the person you are investigating gives you permission, you can perform whichever search and seizure procedures you choose. All of the evidence is admissible because you are not providing hearsay evidence, you are providing direct evidence you collected yourself, and with the cooperation of the District Attorney, this can be a very powerful tool.

There is a fine line here, though, as "cooperation" with the District Attorney can readily be argued to make you be an "agent" of the state, which does make you susceptible to the legal restrictions of Miranda, the 4th amendment, and the like, so it must be something you did for your own good/need, and then gave to the District Attorney after completion. Asking the D.A. for direction in the collection of evidence in a case is quite a bit different than taking orders from the D.A. on exactly how and what to collect, and in what order.

Most corporations can provide the perfect environment for use of this amazing tool through the extended use of the Employment Agreement. Essentially, Corporations have the power to place wording in their employment agreement which negates any individual's rights to privacy while using corporate assets or while on corporate property. This is a very powerful tool which, when used properly can allow a Corporate Security Investigator all the leeway they need to complete a very thorough investigation comprised of every bit of data needed to convict or exonerate a suspect. The local Police could never achieve this level of intrusive search agreement, with the exception of a Search Clause appended to a Parole Agreement assigned to an individual being released from a prison sentence.

[7] http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Since we are not taking a person into custody, unless they are physically restrained, we are not terribly concerned with the statutes concerning this, except as it goes to our ability and power to actually approach a suspect and interrogate, search, or seize whatever that suspect will allow. If the suspect is asked for permission to search their cubicle, pockets, jackets, bags, lockers, drawers, and any corporate assets they are assigned control to, and they consent to that search, anything the person searching finds is admissible in court as direct evidence. If a Police Officer were to attempt that search, the following would preclude any evidence found under that search from being admissible as evidence:[8]

"There is no comparable justification, however, for routinely searching any room other than that in which an arrest occurs--or, for that matter, for searching through all the desk drawers or other closed or concealed areas in that room itself. Such searches, in the absence of well-recognized exceptions, may be made only under the authority of a search warrant."

If the suspect refuses our Corporate Security request to search, they are subject to whatever penalties the company has dictated in the employment agreement concerning the right of the company to search the employee, including termination for refusal to cooperate with a corporate investigation, at which time the suspect can be either arrested for trespassing and searched anyway, or removed from the property, whereby the Corporation may search any of the items left behind. Either way, most of the information the Investigator needs will be made available. In fact, everything except what the employee has in their pockets or other personal possessions will then be available for search. Of course, a Police Officer could never do this, and in reality the employee may deny the Investigator access to any and/or all of the areas demanded in the memorandum, but doing so will result in their immediate termination, leading to the employee being escorted from the property, and leaving the investigator to complete their search unhampered. A Police Officer would not have any authority to enforce compliance with Company Policy, and a refusal by the employee to allow a search would, in the absence of a warrant, end the Officer's involvement in the evidence collection process. This is further illustrated in the restrictions placed upon an Officer of the Government in describing the protections of the 4th amendment provided an individual:[9]

> **"The test propounded in Katz is whether there is an expectation of privacy upon which one may "justifiably" rely. 36 "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." That is, the "capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was reasonable expectation of freedom from governmental intrusion.""**

[8] http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
[9] http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Notice the use of the phrase "governmental intrusion". As non-governmental employees/designees/agents, Corporate Incident Responders are not subject to this restriction. However, it would still be best to attempt to garner the permission of the employee prior to any search.

Let us explore this with a scenario. An employee of ABC Inc. has been accused of downloading pornographic material on company equipment in his cubicle, inside a company owned facility. The complaint is logged as an incident and a Response Action plan is laid out with goals provided by Human Resources and Corporate Security. They decide the charge is serious enough to warrant a search of the employee computer. Calling Law Enforcement at this stage in our investigation would achieve little, as not enough information has been received to allow for the issuance of a warrant. We decide instead to ask the System Administrator charged with providing the employee access to the company internet connection to provide us an Administrator level user account on the employee computer, and a password to log in. We clear with HR and Management to place a keystroke logger on the employee machine in an effort to achieve one of two goals. If the employee is in fact innocent of the charges, we will be able to determine that by monitoring their online activity for a short period of time. Conversely, if the employee is guilty of the charges, we will be able to determine that as well. We log into the computer and conduct a preliminary search for suspect files, like JPEG and AVI files for instance. Then we place the keystroke logger in a directory on the employee hard drive, modify a registry setting so that the keystroke logger will be activated the next time the employee computer is rebooted, and then we wait for the employee to reboot. All of this activity is performed remotely, with Management and HR agreement and permission, in writing. Once the employee reboots their computer, the activity is logged to a file which we periodically copy and download for review. If we find no improper files on the drive, and the activity appears to indicate the employee is not guilty of the accusation, we can remove the keystroke logger and the registry setting, and the next time the computer reboots, the activity logging will stop. If we find improper files or the activity appears to indicate the employee is guilty of the accusation, a decision is made, with Management and HR approval, to pursue the goal of the Response Action, which is to notify Law Enforcement and ask for their assistance in prosecution of the employee, for this case. If the activity had indicated felonious activity was in progress, and Management and HR agreed it was warranted, the employee might have been suspended immediately, his computer seized and held for Law Enforcement, and depending on Company Policy, a decision made to immediately involve Law Enforcement, even initiating a private person's arrest of the employee by the Responder, if Management and HR agreed that was necessary.

None of this activity would be possible for Law Enforcement to perform without several warrants. One giving them access to the Company Network. One giving them permission to attach a "wiretap" device to the Company Network, one giving them permission to seize, and search both the computer and the employee, and one for the arrest of the employee. None of those would be easily gotten based solely on what may have been an anonymous accusation in the first place. It is highly likely, in fact, that armed only with an accusation, most Law Enforcement officials would decline to assist in this case without additional incriminating evidence provided by either Corporate Security or the Company, which would necessitate taking all of the steps we listed above anyway.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Additionally, if a Police Officer and the Corporate Security Investigator walked up to the employee's cube at the same time, armed with only an accusation, and both said, "I believe there may be criminal activity occurring here and I want to search you and your computer for evidence of it.", and the employee stated, "no", the Police Officer would have to leave, secure a warrant, and return to complete the investigation. The Corporate Investigator could, depending on company policy and cooperation with HR, order the employee to leave the building, conduct his search of the area, and conclude his investigation at that time, resulting in the capture of timely information, and preventing the possible removal or destruction of the evidence possible during the delay caused by the Police Officer having to obtain a warrant.

An interesting California Penal Code section is section 835, which states, "An arrest is made by an actual restraint of the person, or by submission to the custody of an officer. The person arrested may be subjected to such restraint as is reasonable for his arrest and detention." This code section gives the private person the right to escalate the use of force to whatever level is necessary to reasonably overcome the resistance of a suspect to a lawful arrest. This would seem to be a section rife with possibilities of abuse by the overzealous employee, and in fact is a big liability issue where large corporations are concerned. However, with proper training, most arrests, where actually necessary, can be affected with little or no force used at all, especially where employees are involved. In fact, more often than not, the Police are called and the arrest is not even made until they are ready to take the suspect into custody for the arresting person, thus negating any physical confrontation with the suspect and the private person in the first place. A well trained and restrained corporate Security response will resolve most issues very peacefully.

California has several Penal Code Sections which define an arrest, and the conditions under which it is permissible for a private citizen to arrest another. They define an arrest as (penal code section 834) "taking a person into custody, in a case and in the manner authorized by law. An arrest may be made by a peace officer or by a private person." The Supreme Court has further defined an Arrest or Seizure of a Person as:[10]

"only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave."

A Fourth Amendment "seizure" of the person, the Court determined, is the same as a common law arrest; there must be either application of physical force (or the laying on of hands), or submission to the assertion of authority. California Penal Code Section 837 provides the following as the rules surrounding the arrest of a person by another:[11]

"Private Person Arrest
837. A private person may arrest another:
1. For a public offense committed or attempted in his presence.
2. When the person arrested has committed a felony, although not in his presence.
3. When a felony has been in fact committed, and he has reasonable

[10] http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
[11] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

cause for believing the person arrested to have committed it."

While this is an interesting tidbit of information, it has no bearing on most of the investigations corporations are engaged in as they usually provide information to the Police, who approach the District Attorney for a warrant and the suspect is arrested and tried in a court of law at that time, and in that manner. However, it does show how similar the powers of arrest of a Police Officer and a Private Citizen really are.

Another interesting Penal Code Section from California defines how an individual may request assistance in the arrest of another, so as to assure their safety in the actual arrest of a perpetrator:[12]

" **Summon Assistance**

839. Any person making an arrest may orally summon as many persons as he deems necessary to aid him therein."

This section provides the Corporate Incident Responder with the ability to ask others in his department or division to assist him in any means necessary to overcome the unlawful resistance of a suspect to be arrested. Again, not the usual course of action for the Computer Incident Responder in most private corporations, but this is becoming more of an issue every day, it seems.

There are still requirements on a private person making an arrest, however, one of them being the Duty to Inform:[13]

"**Duty to inform**

841. The person making the arrest must inform the person to be arrested of the intention to arrest him, of the cause of the arrest, and the authority to make it, except when the person making the arrest has reasonable cause to believe that the person to be arrested is actually engaged in the commission of or an attempt to commit an offense, or the person to be arrested is pursued immediately after its commission, or after an escape.

The person making the arrest must, on request of the person he is arresting, inform the latter of the offense for which he is being arrested."

These last California Penal Codes show just how much power a Private Person may have in pursuing the perpetrator of a serious offense:[14]

"**Use of force..**

844. To make an arrest, a private person, if the offense is a felony, and in all cases a peace officer, may break open the door or window of the house in which the person to be arrested is, or in which they have reasonable grounds for believing the person to be, after having demanded admittance and explained the purpose for which admittance is desired.

---

[12] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
[13] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
[14] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

845. Any person who has lawfully entered a house for the purpose of making an arrest, may break open the door or window thereof if detained therein, when necessary for the purpose of liberating himself, and an officer may do the same, when necessary for the purpose of liberating a person who, acting in his aid, lawfully entered for the purpose of making an arrest, and is detained therein.
846. Any person making an arrest may take from the person arrested all offensive weapons which he may have about his person, and must deliver them to the magistrate before whom he is taken."

Obviously, this is an extreme situation. But similar liberty could be deprived from an individual suspected of perpetrating any Felony, provided the skilled and well-trained Responder follows the letter of the law, there really is no place where a private employee would have a reasonable expectation of privacy within the corporate confines if a serious enough crime had been committed, and the investigator had reasonable cause to believe the employee to have committed it, and the Employment Agreement was properly written.

This last Penal Code Section shows just how serious a situation can be, however, if a person is falsely accused and arrested. Laying hands upon the person of another so as to restrict their movement is all that is technically needed to effect an arrest, so Corporate Responders need to be very carefully trained in the legalities surrounding a search and seizure operation. Obviously, this section is designed to eliminate the potential of a Police Officer being held financially culpable should a private arrest be deemed improper, and the subject of that arrest decide to sue the arresting party. This is why it is vital that an arrest never occur unless it is absolutely necessary. All other avenues should be pursued in order to avoid this potentially dangerous and very litigious situation.[15]

"847. A private person who has arrested another for the commission of a public offense must, without unnecessary delay, take the person arrested before a magistrate, or deliver him or her to a peace officer. There shall be no civil liability on the part of, and no cause of action shall arise against, any peace officer or federal criminal investigator or law enforcement officer described in subdivision (a) or (d) of Section 830.8, acting within the scope of his or her authority, for false arrest or false imprisonment arising out of any arrest when any one of the following circumstances exist:
(a) The arrest was lawful or when the peace officer, at the time of the arrest had reasonable cause to believe the arrest was lawful.
(b) When the arrest was made pursuant to a charge made, upon reasonable cause, of the commission of a felony by the person to be arrested.
(c) When the arrest was made pursuant to the requirements of Section 142, 838, or 839."

[15] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Perhaps the most interesting Penal Code pertaining to this particular line of study, is Section 142:[16]

"Duty to receive
142. (a) Any peace officer who has the authority to receive or arrest a person charged with a criminal offense and willfully refuses to receive or arrest such person shall be punished by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison, or in a county jail not exceeding one year, or by both such fine and imprisonment.
(b) Notwithstanding subdivision (a), the sheriff may determine whether any jail, institution, or facility under his direction shall be designated as a reception, holding, or confinement facility, or shall be used for several of such purposes, and may designate the class of prisoners for which such facility shall be used."

This section places a Law Enforcement Officer in jeopardy of arrest and prosecution for refusing to take custody of a private person's arrestee. This may be the only example in our history of public officials being forced to assist private citizens in the doing of their preference, even if the Officer feels the arrest to be without merit, in which case their only recourse is to take custody of the arrestee and immediately release them pursuant to Penal Code Section 849(b). But the arrest still holds, even if the District Attorney does not prosecute the suspect, the arrest will remain on their record in a manner viewable only by other Law Enforcement officials, and some Background Investigators. This provides a multitude of liability issues to the Corporation employing the Responder forced to make an arrest, but it also protects the Responder from the Police Agency with little interest in performing their duty to assist, as large Police Agencies have become more resistant to assist private security with their efforts to perform private party arrests. It is fascinating to think, however, that with only a little over half a million uniformed Police Officers in the United States, and more than 4 million Uniformed Security Officers, the ones actually deterring crime by their uniformed presence, by sheer numbers alone, must be the Private Security Officers. It should be plain for the Police to see how much more work they would be called upon to perform if it weren't for the Security Officer already doing it for them. Still, agencies will sometimes resist their duty to assist with a private person's arrest.

There have been many cases in which Police Officers have simply refused to take custody of an individual rightfully arrested by a Private Person, giving no reason other than they are "too busy", which may very well be true. As the Official charged with this particular duty, they have the discretion to perform their duties as they see fit, leaving a Corporation with no other recourse than a complaint to the Officer's Supervisor, which will usually lead to even worse treatment the next time an Officer is called to assist. Often, the agency may have had experience with an improperly trained Security Guard, or been included in a lawsuit as a result of a Private Person's arrest. It is a Corporations

[16] http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

right to employ a Private Security force for their own protection, and the local Police should provide them with assistance when needed.

Building a trusting relationship with the Local Authorities is vital to any Incident Response team. Once the Officers in your community see the level of experience and training you have undergone, they will be much more likely to assist you when needed. You may even find them calling you for assistance with more complicated cases than they are technically able to deal with.

In any case, most Corporations will never face this type of problem, as most computer incidents are resolved on-site through the use of Human Resources policies and regulations, or civil recourse agreements. It will be more commonplace to handle these situations in-house as the level of training and complexity grows with the types of incidents occurring. Eventually, most Corporations will simply build into their budget the cost of Information Security Analysts tasked with providing supervision over the Internal Affairs of the Corporation. Many of the crimes we see being charged by Public Agencies will be handled by the Corporation, with punitive civil measures being taken against the offenders, rather than involving the Police at all.

In fact, as the Police are faced with ever-growing changes in their responsibilities, their budgets will remain "cause of the year" based. For instance, money allocated to a High Tech. Crimes Investigator last year will almost certainly be re-allocated to some of the new and interesting responsibilities being foisted on Local Agencies by the State of our Nations' terrorist vulnerabilities. In order to justify the pennies in their budget, they will be forced to resist growth in the High Technology Crime arena, in order to better focus their budget dollars on the Security of our Nation, forcing them out of the High Tech. ballgame altogether. This will leave a highly trained international group of private Incident Responders to handle most Computer Crimes amongst themselves. This is not necessarily a bad thing, however, as most Information Security Analysts are poorly prepared to guard our property and people against a terrorist attack, and most Police Officers are poorly prepared to respond to a Computer Crime Incident. It is only natural that those with the proper talent be utilized in the proper arena.

Either way, the careful planning, integration, training, and support of a multi-disciplined group of Incident Responders will continue to be the last line of defense for most Corporations, and the better their relationship with the Local, State, and Federal Agencies they work with, the better the success of both their proactive and reactive activities.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

List of References

1. Krebs, Brian. "Judge Slams Monitoring of Court Staff Web Use". NewsBytes. August 23, 2001. URL: http://www.newsbytes.com/news/01/169357.html
2. Richardson, Patricia. "Code of Silence". Crain's Chicago Business Newsroom. September 8, 2001. URL: http://www.chicagobusiness.com/cgi-bin/news.pl?post_date=2001-09-08&id=3277&feature=1
3. Associated Press. "Appeals Court reworking opinion in Pilot Lawsuit". Knightridder.com. August 28, 2001. URL: http://www.siliconvalley.com/docs/news/tech/026405.htm
4. Unnamed Author, Court TV Online. "Judge upholds arrest warrant issued against DNA code". Courttv.com. February 26, 2001. URL: http://www.courttv.com/news/forensics/022601_dnawarrent_ap.html
5. Mirriam-Webster, Inc.. "Statute of Limitations". Findlaw.com. 1996. URL: http://dictionary.lp.findlaw.com/scripts/results.pl?co=dictionary.lp.findlaw.com&topic=33/339dc5812f50d9638ce513acd35931c7
6. Unknown Author, Associated Press. No Title Given. Findlaw.com. 1999. URL: http://news.findlaw.com/ap_stories/l/0000/8-29-2001/20010829083511200.html
7. Case law. "Detention short of arrest: Stop-and-Frisk". Findlaw.com. 2001. URL: http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
8. Case Law. "Search Incident to an Arrest". Findlaw.com. 2001. URL: http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
9. Case Law. "Search Incident to an Arrest". Findlaw.com. 2001. URL: http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
10. Case Law. "Search Incident to an Arrest". Findlaw.com. 2001. URL: http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#1
11. State of California. "837". California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
12. State of California. "839" California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
13. State of California. "841" California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
14. State of California. "844" California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
15. State of California. "847" California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html
16. State of California. "142" California Penal Code. 1999. URL: http://caselaw.lp.findlaw.com/cacodes/pen/833%2D851.85.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced