

Norwich University
Master of Information Assurance Program
Seminar Five Final Paper

Preparing for the In-House Digital
Investigative Function

Suzanne Widup

Table of Contents

Executive Summary	3
Introduction	4
Management Commitment	5
Policy	6
Process	8
Personnel	14
Infrastructure	16
Methodology	18
Employment and Privacy Law	22
Conclusion	25
Appendix A: Summary of Recommendation	26
Appendix B: Prioritized Recommendations	28
Works Cited	32

Executive Summary

A part of doing business and having employees is the likelihood that allegations of misconduct will arise from time to time. While these allegations may or may not all warrant investigation, the business must develop a process for handling these events. In the course of this, the company may decide to handle internal digital investigations themselves, rather than outsourcing the function to a third party. When this is the case, there are steps that the company must follow to protect itself against improperly handled investigations.

The corporation must develop policies that address the employee expectation of privacy, as well as controls that reinforce those policies. The business must also develop policies and processes around conducting investigations. They must determine the evaluation criteria for an event requiring an investigation; for who makes that determination; who assigns the approved cases out; who conducts the investigations; and what methodology they use. The company must have the support of management to conduct all of these steps, for without that it is destined to fail.

The business must put in place sufficient infrastructure, tools and equipment to allow the investigators to complete their tasks in a timely manner. They must adequately staff the group who will perform these investigations and provide for ongoing training. They must provide a secure environment for performing the data analysis, and storing evidence and case files.

Finally, the company must ensure that their policies and methodologies are compliant with the current regulatory environment. They should also keep up with regulations that may affect the way they conduct investigations in the future.

Introduction

This paper addresses the steps required for preparing a company to conduct internal workplace investigations. However, the question of why a company may want to perform investigations must first be addressed. There are as many reasons as there are trigger events—those events that make the employees of the company think that perhaps an investigation is warranted. An example of a trigger event would be an employee bringing charges of sexual harassment against a supervisor. The company must then decide if an investigation is warranted. One criterion for evaluating whether to perform an investigation is if there is a legal duty to do so (Dewey Poteet).

“One of the first issues an employer should address is to determine if it has a legal duty to conduct the intended workplace investigation. There are circumstances where an employer may have a legal duty to investigate employee misconduct. That is, in the cases the decision to investigate is no longer discretionary. A duty to investigate, for discussion purposes here, may arise from statutes and regulations, contracts with employees, and common law duty to properly screen and supervise employees (Ferraro, 2006).”

The hypothetical trigger event listed above—sexual harassment—is a case where the company has a legal duty to investigate; since the allegation falls under the heading of statutes and regulations. In fact, according to PPS, decisions by the Supreme Court provide compelling reasons for employers to perform investigations. A good investigation can protect your organization, while a bad one can become an employee relations fiasco. If you follow the proper process, your investigations should result in the “right” decisions.

Since there are many pitfalls in performing investigations properly, it is important to note that if a company is going to perform their own internal investigations, significant preparation is required **prior to the first trigger event**. As there is no way to determine when the first trigger event will occur, if the company is not prepared, an outside consulting firm should be considered as an option until the appropriate steps have been completed.

“A good investigation can help you make sound employment decisions. However, poorly conducted internal investigations often result in low morale, negative public relations, and litigation. Therefore, you should have a well-defined process to specify the circumstances in which you will conduct investigations and to help you make confident, fair decisions (PPS, 2006).”

When a company determines the need for a digital investigative function staffed by corporate employees, much preparation must occur prior to the first investigation to ensure that the company does not cause damage to their reputation or incur legal liabilities. These preparations must include developing

the appropriate management commitment, policies, processes, personnel and infrastructure to support the investigative function. All of these activities must ensure that the methods utilized comply with existing employment law and privacy regulations. It should be noted that without a solid commitment from management to developing the policies, processes and infrastructure to support the digital investigation function, the effort is likely to fail.

This paper addresses the series of steps a company must complete in order to prepare for performing internal digital investigations. They include developing policies and controls that dispel the employee expectation of privacy, defining standards of appropriate behavior, and defining the way that investigative activities will be handled within the company. The company must define the process for when a trigger event occurs that determines if an investigation is warranted, as well as the processes around which investigations are approved and assigned. Employee redress once an investigation completes and findings are presented must be defined to ensure the accused have a way to present their side of the story.

The company must develop the organizational infrastructure, hire, and train the staff on the chosen investigation methodology to ensure that their staff conduct investigations in the approved manner. The business must develop the technical infrastructure to support the digital investigative function, which consists of specialized computer hardware and software. The company must also determine how investigators will obtain access to the systems in the event of an investigation, since privileged access is typically required. The company must determine the investigative methodology that investigators will use to conduct investigations, including provisions for evidence collection and preservation, case file management, and document retention.

Finally, the company must be cognizant of the regulatory environment in which it operates. A brief survey of several of the applicable laws is presented, and policies and processes must be evaluated to ensure compliance.

I. Management Commitment

Management commitment to the purpose of having an in-house internal digital investigations unit is critical to the success of all subsequent steps. Without this commitment in both funding and resources, the function will be unable to perform their chartered duties.

“Computer forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by constructing a comprehensive training program for examiners, sound digital

evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency (TWGEDE, 2004).”

The support must come from the highest levels of management to ensure cooperation with the needs of the investigators when a timely response is necessary. If the management of the company is not prepared to commit to support the necessary policy changes and controls, as well as the funding required to staff and equip the personnel designated to carry out investigations, then the investigations performed may not live up to their expectations.

II. Policy

Companies use policies to define a standard of conduct in many situations. There are many different types of policies, but those dealing with computers are of the most interest to this topic. Companies with systems, networks and data need policies outlining what types of behavior are appropriate, and what types are not. “In short, an employee has a right to know what is expected of him or her and what the consequences of not fulfilling these expectations will be. The employer has a duty to establish a system which provides adequate notice to employees as to what behavior is acceptable and what behavior is not acceptable (Freedman, 1994).”

A. Acceptable Use Policies

A good starting point for policy development is to look at defining acceptable use of the systems, networks and data a company owns. According to Stephenson, “a common error of many organizations is to assume that because they own the computers, the network, and the other corporate information assets, that employees using those assets must do so for business purposes. Failure to use them properly subjects the wrongdoer to disciplinary action. To assume that such automatically is the case is in error.” To that end, included in any acceptable use policy should be a section informing employees that the company monitors all activity on their systems. Companies should require new employees to read and sign a paper indicating their understanding of the policies and acknowledging that there are penalties for noncompliance. Spell out those penalties in the policies in plain, easy to understand, language. Companies must be prepared to enforce these penalties evenly across all segments of their employee base—if the company enforces them inconsistently, it may appear

as discriminatory. Therefore, do not put in penalties that the company does not really want to enforce.

B. Countering the Expectation of Privacy

Many states have privacy protection laws, and in general, unless a company has a policy in place, the court may find that the employee had a legitimate expectation of privacy.

“All individuals, in absence of a strong policy to the contrary, have an expectation of privacy in their daily lives, even if those lives belong, for an eight hour workday, to their employers. The extent of that expectation and the extent to which their lives belong to the employer is a source of debate, often in front of a judge and jury (Stephenson, 2001).”

Having developed the acceptable use policies that indicate the company monitors all activity is a good beginning. However, if a control can be designed that requires employees to acknowledge that they are subject to monitoring each time they use a system or application, it goes a long way to ensuring they cannot later claim ignorance. For instance, many companies use a proxy server (a system that stands between the employee's system and the internet and performs their requested actions on their behalf). The company's technical staff should determine if the proxy server can be configured to pop up a window that the employee must click through prior to being taken to the web site they have requested. The language displayed on that window is up to the company, but should mention that the employee's activity is subject to monitoring. This way, the employee must acknowledge the monitoring policy each time they try to access the internet. The company would do well to implement similar controls where the potential for abuse is highest, designed to interfere with regular business operations as little as possible.

C. Investigation Policy

Before investigations begin, it is important to define the investigative process, the methodology used, and the goals of investigations. Having this in a written policy tells employees what to expect (whether they are the target of the investigation or a witness), and emphasizes the process objectivity. According to

PPS, the policy should outline steps for initiating the process, the actual investigation (including fact finding and interviewing witnesses), proper documentation, the final decision, and the communication of the results.

The policy should also grant the investigators the authority to conduct their investigations. In many cases, investigators must contact other groups to provide log files or other access that requires elevated system privileges. The policy should clearly state the process for involving other groups and the logistics required for escalation. “The policy should also account for the fact that during the process, investigators commonly encounter indicators of wrongdoing that were not known at the outset. If such evidence is unearthed, the plan should allow for appropriate arrangements to be made for investigation of these new lines of inquiry (Dewey and Sprunk, 2005).”

III. Process

The company will have to determine the processes surrounding investigations. For instance, how do they want investigations initiated? Some companies have employee hotlines in place or other methods for anonymous tips to report employee misconduct. Others channel employees through a specific department, such as Human Resources or Legal. Once a tip comes in, someone must determine if it warrants an investigation. Some companies require the approval of other groups prior to the initiation of an investigation, such as Human Resources. A company must settle these issues prior to advertising the investigative function.

A. Initiating Investigations

Employees may not feel comfortable taking their concerns to their supervisor or even Human Resources. For this reason, many companies establish a method for employees to report their concerns while remaining anonymous. Tip telephone lines or drop boxes are a common implementation of this. However, this is not likely to be the preferred method for initiating investigation requests.

Having a standard form that requestors must fill out is a way to help standardize the documents surrounding investigations. The company can define the workflow that best suits their needs.

Where the investigation request comes from will help determine the path the investigation takes. If it comes from Legal, it may require no further approvals. If it comes from the tip line, it may require Human Resources and / or Legal to approve further investigation.

1. Human Resources

Human Resources investigations often involve allegations of time wasting, abuse of system resources, and even threats. They frequently start with a manager of an employee having suspicions about the behavior that employee is exhibiting. For instance, if a manager notices an employee spends large portions of their day surfing the web and has problems meeting their deadlines, the manager may talk to Human Resources about having their computer usage habits investigated.

“At some point, every manager or HR professional will face a situation that requires investigation before any employment action can be taken. Typically, the investigation will be necessary to respond to complaints or suspicions of workplace misconduct, rule or policy violations, or even criminal acts. Performed systematically, investigations can prevent potential morale problems, resolve efficiency problems, and prevent legal and financial losses (PPS, 2006).”

2. Legal

Many of the investigations from Legal follow the e-discovery path rather than the traditional investigation path. Litigation where the company is a named participant frequently requires preservation of email and other electronic data for analysis. However, this does not preclude traditional investigations centered on specific individuals from initiating from this department.

3. Corporate Security

Cases where an investigation handled by the physical security investigators branch out into the digital realm are not uncommon. The investigators may need to determine if evidence of a crime is located on the computer systems that the suspects had access to, and thus initiate a digital investigation.

4. Incident Response Team

Incidents of malicious computer attacks frequently involve the collection and preservation of digital evidence. Investigations from

this source can be the most challenging, particularly if the attacker is highly skilled.

B. Approving Investigations

Once an investigation request has been initiated, someone must determine if there is a basis for an investigation, and approve or deny the request. The company must determine who this should be performing this critical function, and what criteria should be evaluated in making the decision. “A crucial issue for the policy to cover is who will supervise the investigation. This person will have the power to determine whether the investigation will be a fair and thorough exercise or whether it will simply reach a preordained result (Dewey and Sprung, 2005).” This may be the manager of the Investigations group, or Legal and Human Resources may handle it—the company will have to answer this question and incorporate it into their workflow for the process.

Once the “who will decide” question is answered, the next step is to define the criteria by which the decision to investigate or not will be based upon. Here are some criteria (the company will ultimately have to determine this on their own) to consider when making this decision:

- Which specific policy does the alleged behavior violate?
- Is the company incurring a financial loss?
- Is there a safety issue to others or the employee?
- Is there criminal activity occurring?
- Is this a simple issue or a complex one?
- Is there a pattern of behavior or is the incident isolated?
- The degree of the behavior (minor, moderate, extreme)
- Are all the facts known about the situation?
- Will outside expertise be required? (Dewey Poteet, 2001; PPS, 2006).”

Companies should not take this decision lightly. They should also document the reasoning behind the decision to investigate, or not investigate so that should this end in litigation, there is a record of the logic. In fact, according to PPS, “both the complaining party and the accused wrongdoer may sue if an investigation was conducted in a shoddy manner or if a decision appears to be unfounded. Significantly, courts tend to punish employers that do not conduct thorough investigations. In addition, employee morale may suffer if employment decisions appear unfair or arbitrary

because investigations are not thorough or objective. Most employees value fairness and will respect their employers' decisions if they are based on a structured investigative process.”

The company's legal team can determine if there are applicable laws requiring an investigation. However, in general, if an employer knows of (or should know of) discrimination, harassment, threat or safety issues faced by their employees, they have a duty to take prompt action to remediate the problem. In these cases, the only way to know what the appropriate action is would be to initiate the investigation and act on the findings. Employers who fail in their duty to investigate frequently lose the litigation brought by the employees in response to their lack of action (Texas Workforce, 2006).

C. Assigning Investigations

Once the appropriate groups approve an investigation request, the company must determine where it goes for assignment. The company must determine for purposes of workflow who should handle assigning each case to the investigators available. They should also be responsible for following up on status of cases, and communicating to the requestors of the case so that the investigator is able to continue their work.

The investigators on staff will have a mix of skills. They will have their strengths and weaknesses, and the person charged with assigning out cases should keep this in mind when selecting the right investigator for the job. For instance, if the investigator has their own bias, they may discourage victims, even unconsciously. If the victim is not likely to feel comfortable talking to the investigator, the investigation may not successfully gather the required information. This may cause the employer to make a decision based on faulty or incomplete data gleaned from an inadequate investigation (Freedman, 1994).

“Impartiality is the innate ability to separate one's self and self-interests from the investigation and its outcome. It is not a common trait, nor is it human nature. Because the human spirit is possessive by nature, we tend to take ownership (and pride) in the things we do. The greater the investment of time and resources, the greater that ownership becomes. Investigations are no different. The professional fact-finder must divest herself from any interest in the outcome of the investigation. This is not to say one may not be interested in

the outcome or take pride in her work. No, the fact-finder must instead be impartial and not allow her loyalty and self-interests to interfere with the fact-finding process or the investigation's ultimate outcome (Ferraro, 2006)."

Just as important as the potential bias is the level of skill an investigator has in the type of investigation in question. According to Ferraro, insisting on or allowing an investigator without the proper skills to conduct an important investigation is a recipe for disaster. Companies should resist the temptation to use an investigator just because they are the one with the highest availability at the time. For best results, match the skill of the investigator to the type of project undertaken.

There are several factors the person tasked with doling out the cases should evaluate prior to assignment. They include:

- The investigator's responsibilities in relation to the work area, employees, etc.—are they familiar with the people or setting? Have they worked in similar settings before on other cases?
- Ability to understand and identify the purpose of the investigation. Is this someone who gets sidetracked by the details? Are the goals of the investigation clearly defined enough for this person to handle?
- Knowledge of the company's policies and procedures. How well versed is the investigator? Are they new to the company?
- How good are the investigator's interviewing skills? How well does this person relate to others socially?
- Credibility, impartiality, and ability to maintain confidence.
- Effectiveness as a potential witness. This person may end up testifying on behalf of the corporation. Are they believable? How comfortable are they with public speaking? Are they articulate?
- Organizational skills and attention to detail. Does this person take accurate notes? Does this person keep accurate records? (Barowicz and Rupe, 2006)

In addition, the combination of more than one person handling the case may tend to help counter both bias and lack of specific skill sets. By pairing off investigators who have complimentary skills, the company can provide both the opportunity for cross training and objectivity. This is a technique frequently employed by law enforcement.

Why is it so important for a company to choose the right investigator for the case? It is because the company has liability for the actions of that person taken on behalf of the corporate during the investigation. According to Ferraro, under the doctrine of *respondeat superior*, a principal is vicariously liable for the actions of its agents that are committed within the scope of employment or engagement. An employer-employee relationship is a principal-agent relationship as the employer has control over the methods of work and performance outcomes. An employee-investigator conducting a workplace investigation on behalf of the company is an agent of the company, and the employer may be held liable for any misconduct.”

So, since the investigator is a company employee, the actions that person takes in the course of the investigation may make the company vulnerable to litigation. For this reason, it is imperative that personnel are properly trained in the appropriate methodology, and the expertise of the individual is taken into consideration prior to case assignment.

D. Performing Investigations

Who performs the investigations? Is there one group that handles all investigations no matter the type? Or do different types of investigations get handled by different groups? Jurisdiction in the event of multiple groups must be spelled out in the policy on investigations. Without that, turf wars are an activity that wastes time and can cost the company.

Additionally, it should be noted that investigations will likely involve personnel not used to performing investigations—whether as witnesses or as someone who must provide privileged access to a system. For these personnel, it is critical to stress that all investigations must be kept strictly confidential, particularly if they rarely participate in them. In general, the fewer personnel outside of the investigative workflow who must be utilized, the better for confidentiality purposes (Ferraro, 2006).

E. Employee Redress Options

The investigation is completed and the findings report delivered to the appropriate parties. Now the employee learns of their fate regarding this investigation. What happens next? Does the employee have the right to rebut the findings? Can they tell their side of the story? In some cases, the employees were not even told about the investigation prior to the findings. In others, they were interviewed by the investigator. If the company wants to have a process for the employee to address the concerns and justify their behavior, this will need to be developed.

“The employee has a right to consistent and predictable responses by the employer to violations of rules of conduct. Indeed, deterrent values increase as predictability increases. And the employee has a right to fair discipline based on the facts discovered in an internal investigation. The employee has a right to question the facts unearthed by the internal investigation and to offer and present his or her defense. In *Banas v. Matthews International*, a Pennsylvania appellate court sustained defamation damages against an employer in a situation where the internal investigation of an alleged misappropriation of company property was negligently conducted and resulted in the wrongful discharge of an employee for theft. An employee has the right to appeal the disciplinary decision under due process of law (Freedman, 1994).”

The company must incorporate the end of the investigation process with their disciplinary process to ensure that employees have a method of telling their side of the story and defending themselves against the allegations as appropriate. Consult the company’s legal team to determine how this should be incorporated to ensure compliance with all relevant regulations.

IV. Personnel

Once all the policy and processes are in place, it is time to start working on staffing the investigative function. The company must determine the number of personnel and the structure of the organization. The company must then develop job descriptions and based on those, post job openings to attract candidates.

A. Defining Qualifications

Because computer forensics/digital investigations are a relatively new specialty, it can be difficult to find and attract qualified personnel. It may be necessary to start with a core team and expand it from there with less experienced personnel that have aptitude and can be trained (Vecchio-Flaim, 2001).

Yasinsac, Erbacher, Marks, Pollitt, & Sommer (2003), recommended a Computer/Network Forensics (CNF) matrix based on levels of sophistication mapped against the tasks required of the practitioner. This matrix can also be used to specify the types of training and experience required to perform the job. It is shown in Table 1:

Table 1: CNF Matrix

Role	Education	Training
CNF Technician	Introductory level: Computer Science, Hardware, Operating Systems, Forensic Science, Civil and Criminal Law	Professional certification training for hardware, network (e., A+, Net+), "bag-and- tag", basic data recovery and duplication
CNF Policy Maker	Information Management, Forensic Science, Information Assurance, Knowledge Management, Enterprise Architecture	Survey/seminar courses in Information Assurance, legal and CNF techniques
CNF Professional	CNF Technician items, upper level courses in IS, Networks, Architecture, and law (civil, criminal and procedural)	CNF Technician training, Advanced data recovery and courtroom training
CNF Researcher	Doctorate level education or master's degree, extensive experience in computer forensics	Hands-on training for specific research areas being pursued

The matrix data can be incorporated into the job postings and combined with the job descriptions can help a company determine what types of expertise they are looking for in an applicant (Kanellis et al., 2006).

B. Training

New members to the team will require training of the team's methodology and core tools. However, since tools, technology, law and policy change quickly in this field, the company should provide funding for refresher training on a regular basis, as well as additional training to keep up with emerging trends (Stephenson, 2001).

V. Infrastructure

It is not sufficient to have the staff prepared to conduct internal digital investigations. It is also important to have the technical infrastructure required. For instance, a secured location for the staff to conduct their work is very important. It is in the company's best interests to limit the number of personnel able to access the location where evidence is kept, and the confidential nature of investigations make control of information critical.

A forensic lab with appropriate physical controls will allow the investigators to perform their analysis without concern of unauthorized personnel observing their activities. It provides a place for the investigators to access the specialized hardware and software necessary to their job. It also provides a good place to establish the evidence storage, since it has restricted access.

A. Hardware and Software

Building and equipping a laboratory for digital forensics investigations requires a significant financial commitment from management. While many of the software tools available are open source and found freely on the internet, the hardware is not. Depending on the tools chosen, some may also require software license purchases.

“As you build your team, you should begin to acquire the tools and equipment that will be needed to conduct a variety of forensic examinations. This step will require a great deal of planning and resources. The forensics team should conduct a thorough analysis of what types of operating systems, hardware, and environments, they will be expected to analyze. This will determine what tools and equipment will be required to conduct their examinations (Vecchio-Flaim, 2001).”

An estimate of hardware and software requirements for equipping a sample forensics lab can be found in Appendix B. The investigative staff should make the determination as to which tools are necessary and present their recommendations to management for approval and acquisition.

B. Document Management

The company should establish a secure location for investigation files and records. For instance, case files should only be accessible by the person(s) conducting the investigation. This means that the case files should be kept in a locking file cabinet when not in use, and a method developed for checking the files in and out so that files can be located when needed. In addition, documentation related to an investigation, even if deemed irrelevant, should not be destroyed. Instead, the company should develop a retention policy addressing long-term storage (Barowicz and Rupe, 2006).

Investigations typically generate records, whether formal or informal, based on the process and policies of the company. Keep in mind that these records, however, they are often discoverable during litigation. This means that there are requirements around preserving the documents associated with a case, and the company should devote significant attention to developing case document management procedures.

“Proper documentation control procedures for creating, labeling, copying, tracking, distributing, and retaining investigative documents should be established. Without such ground rules there are risks. Documentation may be produced that is immaterial or even harmful to an investigation; investigative documents may be inadvertently intermixed with other records and create problems locating and editing them when requested in litigation; vital evidence may not be properly documented; sensitive information may

be too broadly distributed; and critical documents may be lost (Ferraro, 2006).”

This covers not only how the case files are handled, but also where they are stored, who has access to the data inside them, how reports are presented, and how long these files are retained. According to Ferraro, case file retention practices deserve thorough consideration before implementation. Retention of case files for five years from the date of closure is considered the minimum. However, retention policies that exceed seven years are difficult to manage and often do not work.

C. Evidence Storage

The company should provide a suitable secured location for evidence storage. A safe located in the digital forensics lab provides secure storage, but the company should also develop policies around access and maintaining the chain of custody. In addition, retention of evidence is an issue that policy should address. Offsite storage for closed cases that provide sufficient security to ensure chain of custody is preserved will enable the company to retain evidence as long as necessary.

VI. Methodology

Methodology is the procedures by which investigations are conducted. It ranges from how evidence is gathered and handled, to how leads are developed, how analysis is performed, protocols for conducting interviews or interrogations, to what goes into an investigation report. Without these items defined, a company may find that investigators perform their investigations differently, and not necessarily in compliance with how the company would want them conducted.

“Prior to commencing your first computer forensics investigation, your team should have a written methodology for the performing the analysis. This methodology should address the basic fundamental procedures that will be performed for every investigation. The specific tools may differ from case to case, but the methodology should remain the same unless there are specific documented reasons for making modifications (Vecchio-Flaim, 2001).”

Three major areas that must be defined is how the company plans to collect, handle, and preserve evidence, how they will conduct interviews of those involved, and what the final reports should look like. There are

numerous excellent references available on the minute details for conducting the investigations themselves, and companies should consult them for further detail, as they are out of scope of this paper.

A. Evidence

What is evidence? According to Ferraro, evidence is any type of proof that when presented is materially capable of proving or disproving a contention or fact. There are different types of evidence, and rules as to whether it will be admitted in court.

“In order to be used or admissible, the evidence must be material to the matter in question. Thus, materiality speaks to the relevance of the evidence. Direct evidence is that means of proof that tends to show the existence of a fact without the intervention of proof or any other fact, and is distinguished from circumstantial evidence, which is often called indirect evidence. Circumstantial evidence is inferential by establishing a condition or premise from which the existence of the principal fact may be concluded by reasoning (Ferraro, 2006).”

1. Collecting Evidence

Evidence must be collected and handled following some very strict rules. For instance, evidence must be gathered in a manner that does not alter it, thus affecting the integrity.

“When dealing with digital evidence, the following general forensic and procedural principles should be applied:

- Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
- Persons conducting an examination of digital evidence should be trained for that purpose.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review (TWGEDE, 2004).”

If the company does not ensure that those responsible for collecting and handling evidence are properly trained, they can be held liable for evidence spoliation. “Spoliation is the

destruction of evidence and it constitutes an obstruction of justice. Spoliation is also the destruction, or significant and meaningful alteration, of a document or instrument. The rules of evidence impose an obligation to retain and produce evidence deemed admissible and relevant in criminal and civil matters (Ferraro, 2006).”

The company’s liability in regards to spoliation also comes into play in many of the cases that come from Legal. These cases typically start by generating a communication to the groups that are responsible for backups and data preservation in a company to notify them to ensure that evidence is not destroyed in the course of normal business operations. For instance, if the company has a policy for cycling the tapes that are old back into the active pool after a certain amount of time has passed, the notification should cause the operators to set those tapes aside that are identified as potentially containing evidence.

2. Chain of Custody

When evidence is gathered, it does not continue to reside with the person who collected it. When it is transferred from one party to another, there needs to be a record. According to Ferraro, each person who handles or takes control of evidence must be recorded, creating what is called the chain of custody. The chain of custody, sometimes called the chain of evidence, is a document that at a minimum identifies each custodian, when he received the evidence, and to whom he transferred it. The company must develop procedures that assure the chain of custody of all evidence is maintained, even in cases where the case is not expected to go to court. The reality is, it is very difficult to determine which cases will end up in court, and it is in the company’s best interest to treat all evidence with the highest standard of documentation.

If the chain of custody is broken—if there are gaps in the record of who had custody of the evidence at any given time, the opposing counsel will use this as a basis to challenge the validity of the evidence. If a company cannot prove that they can account for the whereabouts of evidence from the time it was gathered to the time it is turned over to the court, then they cannot testify to its continued integrity. “Claims of evidence tampering, alteration or contamination are possible when evidence is mishandled (Ferraro, 2006).”

B. Conducting Interviews

Interviewing witnesses or principles in an investigation is an art unto itself. There are many excellent references written on the topic, and the methods are out of scope of this paper. Suffice it to say the company will need to outline the interview methodology that the team will follow in conducting investigations.

There are some comments that should be made regarding interviews, however. First, every effort should be made to ensure confidentiality while preserving an accurate and complete record. Barowicz and Rupe make the following recommendations:

“In the course of preparing for and conducting interviews, an administrator should:

- *Make an interview outline.* The outline should identify all specific questions or issues that need to be addressed, as well as specific evidentiary matters that may need confirmation or verification. Update outline as needed.
- *Take complete and accurate notes.* Notes should include the names of the person conducting the interview, person(s) being interviewed, and any other persons present at the interview. Notes should also include the time, date and location of the interview.”

The company may want to have interviews conducted with two persons present besides the interviewee. This can provide a witness to what they discussed, as well as allow for another's perspective on the answers.

C. Report Contents

The company must determine the data they want included in the investigation report. The purpose of the report is to document the methods used in the investigation and findings it produced. The company must keep in mind that the report may very well need to be presented and defended in court should the case end up in litigation. As mentioned above, there is no way to determine which cases will end in litigation, so the company should treat each case as though it will.

Stephenson provides an excellent sample table of contents for an investigation report:

Executive Summary

- Description of the event
- Brief methodology of the investigation
- Brief evidence collection and preservation methods
- Conclusion with short, generalized reasons

Methodology details

- Investigation
- Evidence collection and preservation

Finding 1 – Description

- Discussion
- Supporting evidence

Finding 2 – Description

- Discussion
- Supporting evidence

Finding N – Description

- Discussion
- Supporting evidence

Summary and Conclusion

Appendix

- List of interviewees
- Evidence listing
- Software and tools used in the investigation
- Outside experts and consultants
- Contacts at assisting sites (such as intermediate sites)
- Other important listings and information (Stephenson, 2001)”

Whether the company adopts this format or develops another one, a consistent manner of presenting data that allows for all of the evidence to be addressed will provide professional and more easily defended reports.

VII. Employment and Privacy Law

The investigative process requires the accessing of communications and data that employees may consider private. In Section II, recommendations for overcoming that expectation were discussed. This section provides a short survey of some of the laws that may apply to a company in dealing with internal digital investigations. In any case, the company should defer to the advice of their own legal counsel.

A. Right to Privacy

In looking at common law, the first item that must be addressed is the individual's constitutional right to privacy. The case of *Bourke v. Nissan Motor Corporation* (1993) gives us an excellent reference dealing with just this topic.

“Whether an individual's constitutional right to privacy has been violated depends first on a determination whether that individual had a personal and objectively reasonable expectation of privacy which was infringed. (*Alarcon v. Murphy* (1988) 201 Cal.App.3d1, 5; *People ex rel. Franchise Tax Bd. v. Superior Court* (1985)164 Cal.App.3d 526, 540-541.) Nissan maintains that the evidence conclusively establishes that plaintiffs had no reasonable expectation of privacy in their E-mail messages. In support of this contention, they cite the following undisputed facts: (1) Plaintiffs each signed a Computer User Registration Form, which states that “[I]tis company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business.”

Nissan contends that the foregoing uncontroverted facts regarding plaintiffs knowledge that E-mail messages could in fact be read without the author's knowledge or consent establishes as a matter of law that plaintiffs had no objectively reasonable expectation of privacy in those messages.

In the absence of a reasonable expectation of privacy, there can be no violation of the right to privacy. (*Alarcon v. Murphy, supra*, 201 Cal.App.3d 1, 5.) Thus, plaintiffs' causes of actions for common law invasion of privacy and violation of the constitutional right to privacy were properly dismissed on summary judgment.”

This case illustrates how important the policy and controls mentioned in Section II become when faced with litigation. Establishing acceptable use and having employees acknowledge by signing a form established what their expectation level should be in regards to rights to privacy.

B. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act primarily addresses people attacking systems to obtain data without authorization. According to Stephenson, it establishes penalties for people convicted of:

- Accessing a computer and obtaining classified information
- Accessing a computer and obtaining financial information
- Accessing a government computer
- Accessing a computer across state lines
- Trafficking in passwords

C. Electronic Communications Privacy Act

The Electronic Communications Privacy Act is primarily concerned with communications across a wire—in all their many forms. Its importance to companies who want to perform internal investigations is that it determines the extent of the monitoring allowed. For instance, Stephenson indicates it covers owner's rights to monitor their systems, and their right to monitor their employee's communications. For instance, businesses may monitor employee communications on its computer network and systems where:

- Employees have no right to use the computer for any reason;
- Policy states that employer will monitor all employee communications;
- Employee monitors a legitimate investigation of criminal misconduct by an employee using equipment provided by the telephone company.

D. Employee Polygraph Protection Act

According to Ferraro, the Employee Polygraph Protection Act prohibits private sector employers from administering polygraph examinations, creates limited exemptions where it may be used, and sets forth very specific rights of employees who refuse or agree to take the test.

While each company will have to determine their own policy on using polygraphs in investigations, they should be very careful in the manner of usage.

E. Federal Fair Credit and Reporting Act

The implications of the Federal Fair Credit and Reporting Act (FCRA) to those conducting investigations was not fully realized until 1999, when the Federal Trade Commission (FTC) weighed in on the subject in response to what is now known as the “Vail Letter”. In that opinion, the FTC concluded that all workplace investigations, regardless of their purpose or objective, **when conducted by a third party** (identified as Consumer Reporting Agencies or CRAs in the FCRA) for an employer, are subject to compliance with the FCRA (Ferraro, 2006). This meant that the employee’s permission would have to be obtained prior to the company accessing certain financial information, such as their credit report. Interestingly enough, this affected only those investigations handled by a third party, such as a investigative consulting firm.

On March 31, 2004, however, the FCRA was amended and third party workplace investigations are since exempted from the act.

Finally, the nature of law is that it is constantly changing. It is critical that the legal counsel keep the investigators up to date with law that applies to their function. Without this feedback, investigators may find that they are performing their duties in a manner that exposes the company to increased risk of litigation.

Conclusion

Clearly, the task of preparing a company for performing internal digital investigations is a complex one. It involves providing management support, creating policies and controls to dispel the expectation of privacy, and developing the processes, methodology and infrastructure to support those who will be performing the investigations. It requires companies to define the criteria for when an investigation should be performed, to determine the staffing needs for the function to succeed, and provide the appropriate equipment, tools and training to do the job in a manner that will not expose the company to undue risk of litigation.

Appendix A: Summary of Recommendations

1. Management commitment to the purpose of having an in-house internal digital investigations unit is critical to the success of all subsequent steps. Without this commitment in both funding and resources, the function will be unable to perform their chartered duties. Ensure that this commitment has been obtained prior to embarking on the remainder of the steps outlined in this document.
2. The company should develop acceptable use policies governing their systems, network and data—if they are not already present.
3. Included in any acceptable use policy should be a section informing employees that the company monitors all activity on their systems.
4. Companies should require new employees to read and sign a paper indicating their understanding of the policies and acknowledging that there are penalties for noncompliance.
5. Do not include penalties that the company does not really want to enforce.
6. The company should design controls that require employees to acknowledge that they are subject to monitoring each time they use a system or application.
7. The company should create policy around investigations. They should define the investigative process, the methodology used, and the goals of investigations.
8. The policy should grant the investigators the authority to conduct their investigations.
9. The policy should also account for the fact that during the process, investigators commonly encounter indicators of wrongdoing that were not known at the outset. If such evidence is unearthed, the plan should allow for appropriate arrangements to be made for investigation of these new lines of inquiry.
10. The company should define the processes surrounding investigations.
11. The company should have a standard form that requestors must fill to request an investigation. This is good a way to standardize the documents surrounding investigations. The company can define the workflow that best suits their needs.

12. The company should define the criteria by which the decision to investigate or not will be based upon.
13. The business should also document the reasoning behind the decision to investigate, or not investigate so that should this end in litigation, there is a record of the logic.
14. Once the appropriate groups approve an investigation request, the company must determine where it goes for assignment. The company must determine for purposes of workflow who should handle assigning each case to the investigators available.
15. Jurisdiction in the event of multiple groups must be spelled out in the policy on investigations.
16. If the company wants to have a process for the employee to address the concerns and justify their behavior, this will need to be developed.
17. The company must determine the number of personnel and the structure of the investigation organization. The company must then develop job descriptions and based on those, and post job openings to attract candidates.
18. New members to the team will require training of the team's methodology and core tools. However, since tools, technology, law and policy change quickly in this field, the company should provide funding for refresher training on a regular basis, as well as additional training to keep up with emerging trends.
19. A forensic lab with appropriate physical controls should be equipped to allow the investigators to perform their analysis without concern of unauthorized personnel observing their activities.
20. The investigative staff should make the determination as to which tools are necessary and present their recommendations to management for approval and acquisition.
21. The company should establish a secure location for storage of investigation files and records.
22. The company should develop a retention policy addressing long-term storage.
23. The company should develop case document management procedures.
24. The company should provide a suitable secured location for evidence storage. A safe located in the digital forensics lab provides secure storage.

25. The company should develop policies covering evidence access and maintaining the chain of custody.
26. In addition, retention of evidence is an issue that policy should address. Offsite storage for closed cases that provide sufficient security to ensure chain of custody is preserved will enable the company to retain evidence as long as necessary.
27. The company must define how it plans to have investigators collect, handle, and preserve evidence, how they will conduct interviews of those involved, and what the final reports should look like.
28. The company will need to outline the interview methodology that the team will follow in conducting investigations.
29. Legal counsel should keep the investigators up to date with changes in the laws that apply to their function.

Appendix B: Prioritized Recommendations

This section prioritizes the list of recommendations in Appendix A, and provides estimated costs where capital outlay is expected. The recommendations are also broken down into major categories and prioritized within those categories.

Policy Recommendations

These recommendations do not require capital outlay. Their costs lie in the time employees must devote to altering the policies. The amount of time to make the changes recommended varies with the company's existing process for updating policies.

1. Management commitment to the purpose of having an in-house internal digital investigations unit is critical to the success of all subsequent steps. Without this commitment in both funding and resources, the function will be unable to perform their chartered duties. Ensure that this commitment has been obtained prior to embarking on the remainder of the steps outlined in this document.
2. The company should develop acceptable use policies governing their systems, network and data—if they are not already present.
3. Included in any acceptable use policy should be a section informing employees that the company monitors all activity on their systems.
4. Companies should require new employees to read and sign a paper indicating their understanding of the policies and acknowledging that there are penalties for noncompliance.
5. Do not include penalties that the company does not really want to enforce.
6. The company should design controls that require employees to acknowledge that they are subject to monitoring each time they use a system or application.
7. The company should create policy around investigations. They should define the investigative process, the methodology used, and the goals of investigations.
8. The policy should grant the investigators the authority to conduct their investigations.

9. The policy should also account for the fact that during the process, investigators commonly encounter indicators of wrongdoing that were not known at the outset. If such evidence is unearthed, the plan should allow for appropriate arrangements to be made for investigation of these new lines of inquiry.
10. The company should develop a retention policy addressing long-term storage.
11. The company should develop policies covering evidence access and maintaining the chain of custody.
12. In addition, retention of evidence is an issue that policy should address. Offsite storage for closed cases that provide sufficient security to ensure chain of custody is preserved will enable the company to retain evidence as long as necessary.

Process Recommendations

These recommendations involve defining the process changes that must take place to sustain and support the investigative function. Again, they do not have direct capital outlay involved, and mostly represent time spent defining and communicating the changes to existing process. That time varies greatly with each company, depending on variables such as the culture's resistance to change, the number of other processes the changes will impact, and the time it takes to design the process and gain acceptance.

1. The company should define the processes surrounding investigations.
2. The company should define the criteria by which the decision to investigate or not will be based upon.
3. The business should also document the reasoning behind the decision to investigate, or not investigate so that should this end in litigation, there is a record of the logic.
4. Once the appropriate groups approve an investigation request, the company must determine where it goes for assignment. The company must determine for purposes of workflow who should handle assigning each case to the investigators available.
5. The company must define jurisdiction in the event that multiple groups perform investigations.

6. If the company wants to have a process for the employee to address the concerns and justify their behavior, this will need to be developed.
7. The company must determine the number of personnel and the structure of the investigation organization. The company must then develop job descriptions and based on those, and post job openings to attract candidates.
8. New members to the team will require training of the team's methodology and core tools. However, since tools, technology, law and policy change quickly in this field, the company should provide funding for refresher training on a regular basis, as well as additional training to keep up with emerging trends.
9. The company should develop case document management procedures.
10. The company must define how it plans to have investigators collect, handle, and preserve evidence, how they will conduct interviews of those involved, and what the final reports should look like.
11. The company will need to outline the interview methodology that the team will follow in conducting investigations.
12. Legal counsel should keep the investigators up to date with changes in the laws that apply to their function.
13. The company should have a standard form that requestors must fill to request an investigation. This is good a way to standardize the documents surrounding investigations. The company can define the workflow that best suits their needs.

Sample Purchase Recommendations

These recommendations require capital outlay and involve direct purchases of equipment and software. Estimates for each recommended item are provided. Clearly, the size of the team and the volume of cases may require different choices for hardware and software. These are sample figures to start with a small team on a limited budget.

1. The investigative staff should make the determination as to which tools are necessary and present their recommendations to management for approval and acquisition. (This recommendation is planning for the subsequent items, and has no capital outlay itself.)
2. A forensic lab with appropriate physical controls should be equipped to allow the investigators to perform their analysis without concern of unauthorized personnel observing their activities.

Quantity	Description	Cost
2	Computer systems to run forensic tools	\$20,000
1	EnCase Forensic software license/investigator	\$ 5,000/license
5	Hard drives for forensic images	\$ 1,500
1	Forensic Imaging System	\$ 2,000

3. The company should establish a secure location for storage of investigation files and records.

Quantity	Description	Cost
1	Filing Cabinet	\$200

4. The company should provide a suitable secured location for evidence storage. A safe located in the digital forensics lab provides secure storage.

Quantity	Description	Cost
1	Evidence Safe	\$500

Works Cited

Barowicz, Denise A. and Rupe, Manuel R. Internal Investigations: Developing Effective Procedures for Conducting Internal Investigations. Ferris State University. 2006.
<www.ferris.edu/htmls/administration/president/generalcounsel/LaborRelations/InternalInvest.doc>

Bourke v. Nissan Motor Corporation. Court of Appeal of the State of California. Second Appellate District. Division Five. July 1993.
<http://www.loundy.com/CASES/Bourke_v_Nissan.html>

Dewey, Lee M. and Sprung, Peter C. In Readiness for an Internal Investigation BDO International. First Quarter 2005.
<<http://www.bdo.com/about/newsevents/events/InternalInvestigation.pdf>>

Dewey Poteet, Austin. How to Conduct an Effective Workplace Investigation. Akin, Gump, Strauss, Hauer & Feld, L.L.P. April 2001.
<<http://www.akingump.com/docs/publication/293.pdf>>

Ferraro, Eugene F. Investigations in the Workplace. Auerbach Publications. 2006

Freedman, Warren. Internal Company Investigations and the Employee Relationship. Quorum Books. 1994.

Kanellis, Panagiotis; Kiountouzis, Evangelos; Kolokotronis, Nicholas; Martakos, Drakoulis. Digital Crime and Forensic Science in Cyberspace. Idea Group Publishing. London, England. 2006.

Personnel Policy Service, Inc. (PPS) Internal Investigations: Fairness is Key to Success. November 2006.
<http://www.ppspublishers.com/articles/fairness_key_success.htm>

Stephenson, Peter. Investigating Computer-Related Crime. CRC Press LLC. Florida. 2000.

Technical Working Group for the Examination of Digital Evidence (TWGEDE). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice. Office of Justice Programs. April 2004.
<<http://www.ncjrs.gov/pdffiles1/nij/199408.pdf>>

Texas Workforce. Workplace Investigations - Basic Issues for Employers.
November 2006.

<http://www.twc.state.tx.us/news/efte/workplace_investigations_basics.html>

Vecchio-Flaim, Christine. Developing a Computer Forensics Team. SANS GIAC
GSEC Practical. June 2001.

<http://www.sans.org/reading_room/whitepapers/incident/628.php?portal=9b070bc5da6377b993475f5594234d08>