The Information Criminologist: Litigation Services in the EDP Environment.

Patrick R. Wheeler,(accprw@gsu.edu), Georgia State University
Ram S. Sriram,(rsriram@gsu.edu), Georgia State University

Abstract

Prior research has concentrated on either the conventional skills of forensic auditing or the impact of information technology on accounting. Little has been attempted by way of synthesizing these two areas; i.e., identifying specialized skills required of the forensic auditor operating in an EDP environment. This article focuses on a sub-category of forensic auditing, litigation services, as a first step toward achieving such a synthesis. First, the unique characteristics of the EDP environment and their affect on the nature of fraud are examined. Second, the skills of conventional litigation experts are analyzed to see whether they are adequate for practice in the EDP environment. Third, it is found that several new skills are required for the litigation expert to operate effectively against computer-aided crime. Finally, the new and conventional skills are combined into a more comprehensive framework.

Introduction

In the past three decades, much has been written about the impact of information technology on accounting. The primary focus of this writing has been on internal controls: How have computers affected the internal controls that, after centuries of testing by trial-and-error, were instituted to protect assets and promote accurate reporting? Protection and reporting, however, represent only one side of the problem. Equally important to achieving the overall objectives of accounting and accountability are detection and litigation services. While a considerable literature has developed on forensic auditing, little has been written on the affect of computers on forensic auditing, and even less has appeared in accounting research on litigation services as a distinct aspect of the investigative professions. The following article contributes toward filling these gaps.

Although litigation services offered by an accountant or other expert are often referred to as forensic accounting, litigation services are narrower in scope than forensic accounting. Litigation services include accounting and consulting services performed by an expert in connection with a pending or potential lawsuit. The expert may perform such services for either a client or an attorney who employs the expert as a consultant or an expert witness. Unlike conventional accountants, experts who specialize in litigation services must possess special skills and must be knowledgeable in the areas of law, legal
procedures, rules of evidence and testimony.

The simultaneous development of computers and litigation accounting is not coincidental. Both reflect a society undergoing fundamental change, especially in the role of information in business. Computers have been instrumental in making information a primary asset in all sectors of the business. The emergence of litigation services as a distinct service has largely been a response to the increase in information crimes (See Romney 1995, Paskel-Mede 1994 and MacGough and Brown 1990 for recently published data on white collar crimes and their impact on business). While criminal activity has always existed, in the information age, it has now taken on a different nature and an enhanced seriousness.

Litigation experts in accounting, because of their special auditing skills and knowledge of litigation procedures, can make significant contributions toward investigation and prosecution of computer-aided crimes. Other writers have recognized the seriousness of computer crimes and the need for specialized training but did not attempt to unite the issues of computer-aided crimes and litigation services under a single perspective. For example, the Peat, Marwick, Mitchell & Co. sponsored publication Management Fraud: Detection and Deterrence (Elliott and Willingham 1980), with its article on “Computer-Related Management Misdeeds” points to the seriousness of computer crimes and the need for specialized training to adequately deal with such crimes, but offered little practical advice. More recently, Bologna and Lindquist (1995) in Fraud Auditing and Forensic Accounting extensively analyze the role and skills of forensic accountants. Although Bologna and Lindquist discuss conventional business frauds and the role of forensic accountants, they do not indicate how the litigation expert can help in the area of “EDP frauds”. Information processing in the EDP environment is different from that in conventional environment. Similarly, litigation experts differ in their skills and services from conventional accountants. Therefore, this article examines how the special skills of litigation experts can enhance the investigation and prosecution of EDP crimes. Specifically, it is asked, what skills are required of a litigation expert in dealing with computer crime?

The EDP Environment and Fraud

The critical difference between the EDP environment and the non-EDP environment is in the approach to information processing. Although, information has always been important to business, computer use in information technology (IT) have made qualitative changes to the business environment. Information has taken on a synergistic and catalytic aspect that it did not previously possess. While still a means to a business-related end, information per se has become an asset of overwhelming significance in most, if not all, businesses. However, the change itself is not merely technological. It involves alterations in the entire system and environment. Thus, it is necessary to move beyond a narrow focus on technology, IT, to an information systems (IS) perspective in order to capture the nature of the new business environment. It is meaningful and practical today to think of businesses as information systems in a way that it was not even in the recent past. By extension, this radical change in businesses and information correspondingly affects the nature of many of the crimes committed in that environment.

Some researchers contend that there are no substantial differences between EDP fraud and conventional fraud (Menkus 1990; Bologna and Lindquist 1995). Undoubtedly, all fraudulent activities share certain common aspects. However, the EDP environment possesses a significant number of unique characteristics. In Table 1 presents a comparative list of the unique characteristics of the EDP environment and the risks that these characteristics introduce. Many of the special characteristics of EDP environment affect the nature of any criminal behavior carried on within that environment.

Prior research has shown that there are also differences in the characteristics and psychology of the criminals involved in different
### Table 1
#### The EDP Environment and EDP Fraud

<table>
<thead>
<tr>
<th>Unique Characteristics of the EDP Environment</th>
<th>Risks of EDP Fraud due to Environmental Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concentration of data in one location</td>
<td>Enhanced access vulnerability</td>
</tr>
<tr>
<td>Time/distance of reduced significance</td>
<td>Mitigation of traditional deterrents</td>
</tr>
<tr>
<td>Visible records are often lacking</td>
<td>Lack of evidence of fraud</td>
</tr>
<tr>
<td>Audit trail is incomplete and confused</td>
<td>Inability to trace fraudulent transactions</td>
</tr>
<tr>
<td>Loss of separation of duties</td>
<td>Loss of traditional internal controls</td>
</tr>
<tr>
<td>Changes can be made almost instantly</td>
<td>Reduced exposure of the criminal while committing the crime</td>
</tr>
<tr>
<td>Increased ease of access</td>
<td>Increased vulnerability of assets</td>
</tr>
<tr>
<td>Computers not widely understood</td>
<td>Competitive advantage to trained criminals</td>
</tr>
<tr>
<td>Computer literacy/user-friendliness</td>
<td>Increased opportunities for fraud</td>
</tr>
<tr>
<td>Increased volume of data processed</td>
<td>Increased exposure of assets</td>
</tr>
<tr>
<td>Security systems not always built-in</td>
<td>Loss of traditional internal controls</td>
</tr>
<tr>
<td>Performance and security trade-off</td>
<td>Circumvention of internal controls</td>
</tr>
<tr>
<td>Networks increase risks</td>
<td>Increased access problem</td>
</tr>
<tr>
<td>Internal controls altered or overridden</td>
<td>Internal controls made ineffective</td>
</tr>
<tr>
<td>Reduction in human intervention</td>
<td>Less monitoring of transactions</td>
</tr>
<tr>
<td>Functional complexity</td>
<td>Loss of traditional internal controls</td>
</tr>
<tr>
<td>Technical complexity</td>
<td>Competitive advantage to trained criminals</td>
</tr>
<tr>
<td>No evidence of data changes</td>
<td>Lack of evidence of crime</td>
</tr>
<tr>
<td>Trusted personnel circumvent controls</td>
<td>Break-down of internal controls</td>
</tr>
<tr>
<td>Storage media are vulnerable</td>
<td>Increases ease of crime</td>
</tr>
<tr>
<td>Volatility of the IT/IS industry</td>
<td>Multiple exposures to risk of fraud</td>
</tr>
</tbody>
</table>

Types of fraud (Saunders 1980; Romney et al. 1980; Bintif 1993). These studies have suggested that it is helpful to distinguish between those committing computer fraud for personal gain from those who engage in this type of criminal behavior for the benefit of the company. The demographics of the pilferer taking home a pirated copy of a program and the executive smoothing profits on a performance report are distinct. However, these differences are often overemphasized. White-collar crime, of which computer fraud is a subset, is so widespread that it now encompasses a large cross-section of the population. Studies confirm that:

When fraud perpetrators were compared with other incarcerated property offenders (burglars, bank robbers, etc.) and college students, it was found that they were much different than other property offenders and more closely resembled the college students...From these results it can be concluded that the detection of potential perpetrators of fraud will not be an easy task because their demographic and psychological profiles reveal that they are very much like most other citizens. (Romney et al. 1980, pp. 64-65)

To the extent that computer specialists are a separately identifiable subgroup of the overall population, it may be inferred that they have unique demographic characteristics. They are, for example, more highly trained and educated. Yet, with the spread of computer literacy and the increased use of PC's, computer crimes have spread beyond this subgroup of computer specialists. Add to this the fact that computer fraud can be committed quickly and at a seemingly safe distance, and it becomes obvious that these crimes are a temptation to an ever widening segment of the population.
This creates an important corollary: just as there are no unique demographic features of those who engage in computer fraud, so there are no unique motivational characteristics. The general stream of motivations that influences the behavior of the average citizen is more or less identical to that of the computer criminal. These individuals are rarely driven by psychotic impulses. They generally act from self-interest, whether for immediate personal gain, as in the case of embezzlers, or for indirect profit, as in the case of those who commit management fraud. It is, therefore, more instructive to view the information criminal as a product of the rational economic man mentality than of psychosocial deviant thought-processes.

If fraud is a rational crime, embarked upon because expected rewards exceed expected costs (punishment), then the establishment of severe punishments and the implementation of strategies that maximize the probability of detection are the best courses of action, especially since there is little that can be done to reduce the expected reward side of the utility equation. An understanding of the psychology of the computer criminal leads to the conclusion that greater emphasis must be placed on fraud detection. Consequently, increased importance must be placed on the litigation expert.

The non-distinctiveness of computer crime perpetrators in terms of their demographics and their motivation makes the task of preventing this type of criminal activity more difficult. It is often contended that the pre-hiring screening of potential employees can serve as a primary means for reducing the threat of computer fraud (Romney 1995). However, if their are no unique, definable characteristics of computer fraudsters, then screening will be ineffective for this purpose. Thus, it will not be possible to significantly reduce computer fraud by controlling the problem at its source; i.e., reducing the influx of potential perpetrators. This places the onus of EDP fraud prevention on controlling the problem internally (internal controls), detecting the problem after the fact (auditing) and prosecuting it as a crime (litigation).

**Litigation Experts and Investigating Fraud**

Investigating fraud is important for the prevention of fraud for three reasons. First, it provides feedback so that weaknesses in the internal controls that allow fraud to occur can be corrected. Most models of fraud include opportunity as one of the main elements in fraudulent activity (Romney et al. 1980; Doost 1990). The elimination of any of these elements will prevent fraud but the suppression of opportunity is clearly the one most controllable by the corporation. Second, fraud investigation sends a signal to those engaging in this activity that they are being actively pursued. It increases their risk of detection and will thereby act as a deterrent. Third, if the criminal is caught, then he or she can be fired and prosecuted. The former directly reduces the occurrence of such crimes in the organization, at least to extent of the criminal activity of that one individual. This, in turn, sends a signal to the remaining undetected information criminals which will act as a deterrent.

Consideration of the last two reasons stated above bring forward some of the misconceptions surrounding fraud investigation. Corporations routinely assume that in catching one fraud perpetrator they have solved most, if not all, of their problems (Menkus 1990). The facts show the opposite. White-collar criminal activity is so widespread that catching one criminal has minimal direct impact. However, it is often helpful in locating the internal control flaw that is being exploited. This knowledge is of major benefit to the company, since it may allow them to catch more criminals and to reduce fraud due to that particular weakness. Another misconception is that the company benefits by not prosecuting those engaging in fraud. Statistics show that less than one percent of those caught are prosecuted. Corporations believe that prosecuting will adversely affect client confidence, their public image and their insurance premiums. This is short-sighted reasoning, as the ever-increasing costs of fraud to the business world demonstrates. The only way to effectively influence the motivation behind these crimes is to convince the criminals that the potential costs outweigh the
expected benefits.

The job of the conventional auditor is to test the reliability of accounting controls and financial statements. The litigation expert’s function is more specialized. His or her job involves understanding fraud in relation to accounting controls and financial statements. The litigation expert’s role has both proactive and reactive aspects. Proactively, the litigation expert is often called-in while the fraudulent activity is being perpetrated in the corporation. The criminal activity may be suspected at this point but has not been explicitly discovered. Here the litigation expert overlaps in duties with the fraud auditor. Reactively, the litigation expert is called in ex post. Clear evidence of the crime and/or the criminal has surfaced. In this case, the job of the litigation expert is to gather evidence, analyze the nature of the crime and testify in court as an expert witness. The reactive role of the litigation expert is sometimes given the general title of forensic accounting (Bologna and Lindquist 1995).

Litigation experts have a different perspective than conventional auditors. Conventional auditors are primarily concerned with occurrences that have a material impact on the financial statements. They focus on the big picture. Litigation experts, on the other hand, concentrate on immaterial oddities that are generally not investigated during routine audits. It is often such oddities that lead to the detection of criminal activity. Many authors (Bologna and Lindquist 1995; Mintz 1993) believe that it is this special mind-set—and not any specific set of skills—that makes the litigation expert unique. For example, it has been argued that it is easier to make a criminal investigator into a litigation expert than it is to make a conventional accountant into one (Bologna and Lindquist 1995). The litigation expert must have a sixth sense about crime that cannot, so it is maintained, be taught (Mintz 1993).

In a similar vein, Bologna and Lindquist (1995) believe that the underlying psychology of financial auditors and litigation experts are fundamentally different. Using Jungian psychology and neurological research, they state that both types of investigators are left-brain dominant (rational, analytical, sequential and logical); but that financial auditors are sensation/thinking types, while litigation experts are intuition/thinking types. Thus, financial auditors see events in terms of their overt aspects (i.e., structural considerations such as financial resources, performance standards and efficiency measurements) whereas litigation experts view them in terms of their covert aspects (i.e., behavioral considerations such as attitudes, feelings and values). While there may be much truth in this approach, it is important not to lose sight of the fact that litigation services, like financial auditing, nevertheless requires a set of specific skills, and, thereby, expertise and professionalism in applying these skills.

In general, the litigation expert must possess knowledge of the following broad areas: (a.) Accounting including professional standards, rules and regulations that govern public interest, integrity, objectivity, and due care; (b.) Auditing and internal controls including professional standards that govern these areas; (c.) Criminology and investigation; (d.) Law, regulations and the rules of evidence; (e.) Individual and social psychology; (f.) Motivational theory and deviant behavior theory; and (g.) Organizational theory. It may be noted that it is items c through g that distinguish the litigation expert from the conventional financial auditor, although the latter cannot be totally ignorant of these areas.

Specific skills required of the litigation expert that stem from these broad areas may be listed as follows (Mintz 1993; Bologna and Lindquist 1995). These skills have been divided into those that fall within and without the purview of conventional auditing. This dichotomy is not exact since the degree of expertise is often the distinguishing characteristic. See the list on page 68.

EDP Fraud Investigation

Previous researchers have either concentrated on conventional auditing or on EDP
Illustration 1
Specific Skills Required of Litigation Experts

I. Litigation service skills that overlap conventional accounting and auditing skills:
   a. General requirements such as competency, objectivity, ability to avoid conflict of
      interest, and maintain confidentiality
   b. Adequate knowledge of professional standards including: GAAP, GAAS, SAS,
      SSARS, etc.
   c. Auditing skills including (i) the ability to review and evaluate internal controls and
      (ii) a sufficient understanding of efficient management and organizational policies/
      procedures

II. Special litigation-related skills that are outside conventional auditing:
   a. Conduct interrogations
   b. Do background searches
   c. Apply laws and regulations
   d. Apply rules of evidence
   e. Detect destruction of evidence
   f. Provide testimony in the courtroom
   g. Design scenarios to identify weaknesses in internal controls that could result in fraud
   h. Identify unusual transactions and situations in account balances
   i. Distinguish between erroneous and fraudulent account entries
   j. Trace and review documentation for questionable transactions
   k. Gather evidence of fraud
   l. Document fraud for court
   m. Examine the company's motivational and ethical culture

fraud investigation, but not on a synthesis of the two; i.e., how conventional auditing expertise

Many of the skills innate to conventional auditing techniques are directly applicable to the
EDP environment and to EDP fraud auditing. Specific applications are:

(a.) The litigation expert's ability to focus on minute, immaterial details and oddities is especi-

(b.) The litigation expert's knowledge of crimi-

(c.) The litigation expert can apply his or her expertise with the nature of evidence to the

(d.) similarly, the fact that the litigation expert is knowledgeable in accounting and auditing, yet
also trained to look beyond accounting and auditing when conducting an investigation, helps
him or her deal with the compacted, non-traditional condition of the separation of duties in
the EDP environment

(e.) the litigation expert can apply his or her IS/IT expertise to problems that arise from the
functional complexity of computerized systems except here the litigation expert's knowledge of
organizational theory also comes into play.

Unfortunately, there are several unique characteristics of the EDP environment, along
with their associated risks of fraud, that are not covered by these traditional skills of the litigation
expert. Those mentioned in the preceding para-
Additional Skills for Litigation Experts

To safeguard those areas in the EDP environment left vulnerable by traditional fraud auditing skills, litigation experts require additional skills. In general, these new skills and attitudes center around information systems (IS) and information technology (IT). The litigation expert working in an EDP environment must be knowledgeable of computers, advanced technologies and the systems that have grown up around these. This states the obvious; however, three further observations may be more beneficial. First, a general knowledge of computers is not sufficient. The litigation expert needs to concentrate and specialize his or her additional training to certain aspects of IS/IT. Second, training in computers, even if properly specialized, will not completely prepare the litigation expert to confront all of the unique characteristics of EDP fraud. There are other areas that the litigation expert needs to develop beside those specifically related to computers. Third, IS does not equal IT. IS is the crucial concept in this regard and is broader than IT. Computers and advanced technologies (IT) are only one part of the overall information processing network (IS).

There are numerous new skills and attitudes that will be of benefit, if not necessity to a litigation expert investigating in an EDP environment:

(a.) Concentrated training in the problem of computer access. The EDP litigation expert must be able to test a system's integrity. This requires expertise in access. Access is the quintessential problem for the information criminologist.

(b.) Shift focus from documents to the system; e.g., information systems and systems theory. This reorientation will help the auditor overcome the problems of disappearing audit trails and lack of traditional evidence.

(c.) Detailed knowledge of the various techniques used to commit EDP fraud; e.g., Trojan horse, salami, round down, trapdoor, superzapping, software piracy, data diddling, data leakage, piggybacking, masquerading, hacking and eavesdropping. It is important that some of these techniques involve advanced technologies other than computers.

(d.) Updated education in organizational theory to deal with the extensive decentralization that corporations have recently undergone due in part to PC's, networks, and other IT innovations. Computers and IS have radically altered the workplace. The auditor must have a firm grasp on these changes and their implications for criminal activity within the workplace.

(e.) Knowledge of the different types of computer environments. It is important to realize that there are several types of IS/IT environments: service centers, microcomputers, minicomputers, batch systems, distributed systems, real-time/online systems, mainframes, database systems, PC's, LAN's, WAN's, internet, intranet, etc. Each environment has unique characteristics than affect the nature of fraudulent activity occurring within that environment.

(f.) Training in computer security systems. The EDP litigation expert must be up-to-date in the latest developments of computer security systems since the criminal is sure to be.

(g.) Training in internal controls unique to EDP auditing. The accounting profession has made significant advances in EDP internal controls, especially in how they differ from traditional internal controls. The EDP litigation expert must
exploit this comparative advantage over the EDP fraudster.

(h.) Develop a more sophisticated mental approach. In the detection of fraud, litigation experts have generally claimed that their operation by instinct and by a sixth sense has given them a distinct edge over conventional auditors tied to red-flag checklists, the documentation of working-papers and the need to focus on materiality. However, the information criminal is much different than the common criminal and the current “average man” computer criminal is different than the “computer geek” computer criminal of the past. The EDP litigation expert must be careful when relying on conventional detection techniques, even instinctual ones. He or she needs to stay current with the various models and theories being developed by researchers in this area.

(i.) Be knowledgeable of IS as a distinct discipline. IS is the not the same as IT; nor is IS or IT the same as computers. An awareness of this and its extensive ramifications will help the EDP litigation expert understand the EDP environment and the unique role that information has assumed in it.

Table 2 on page 71 summarizes the preceding two sections and ties it in with the earlier discussion of the unique characteristics of the EDP environment (table 1). Especially note the number of “unique characteristics of the EDP environment” (column 1) that are left exposed (blank) by “traditional auditing skills” (column 2).

Conclusion.

EDP fraud is a special subset of both fraud in general and white-collar fraud in particular. Similarly, EDP fraud investigation is a subset of conventional auditing and fraud investigation. Rarely has it been attempted to bring these two unique realms together into a single synthesis, although the need is obvious since EDP fraud is a major problem to the business community. To arrive at the point of attempting this synthesis, it was first necessary to examine the unique characteristics of the EDP environment in order to achieve an understanding of the special nature of the computerized environment in which the auditor must work when conducting an EDP audit. Subsequently, the focus shifted to the litigation expert, who was distinguished from the conventional auditor by analyzing the unique skills of the former. This made it possible to make the synthesis that was a primary objective of the article: the litigation expert in the EDP environment. It was found that, while conventional litigation experts traditionally possesses numerous skills required for operating successfully in this environment, they need to develop several additional skills to achieve maximum effectiveness in the detection and deterrence of EDP fraud.

Suggestions for Future Research.

The above discussion has identified specific areas in which litigation experts need to develop new skills in order to be optimally effective in an EDP environment. This result suggests several avenues for future research. First, litigation services is only one aspect of the expertise related to fighting computer-aided crime. Additional research is needed to expand the above results into this wider sphere. Specifically, work can be done to achieve a similar synthesis for non-litigation services performed by forensic auditors.

Second, the EDP environment is rapidly changing. Continual research is therefore required to keep-up with the advances in information technology and to examine how these affect the above results. The internet, for example, provides new opportunities for fraud. What new skills are needed by the forensic auditor to combat internet-aided crime?

Third, behavioral research is called-for in order to study the nature of individuals that engage in computer-aided crime. Specifically, it needs to be established whether such criminals have unique profiles and, if so, how such profiles change along with the IS/IT environment. If so, then their special characteristics may be used to
### Table 2
Fraud Auditing Skills in Relation to the EDP Environment.

<table>
<thead>
<tr>
<th>Unique Characteristics of the EDP Environment</th>
<th>Applicable Traditional Auditing Skills</th>
<th>New Skills and Training Need by the Litigation expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concentration of data in one location</td>
<td>Conventional investigative skills</td>
<td>Shift from documents to systems focus</td>
</tr>
<tr>
<td>Time/distance of reduced significance</td>
<td>Training in accounting plus expanded outlook</td>
<td>IS training</td>
</tr>
<tr>
<td>Visible records are often lacking</td>
<td></td>
<td>Shift from documents to systems focus</td>
</tr>
<tr>
<td>Audit trail is incomplete and confused</td>
<td></td>
<td>More sophisticated attitude; EDP auditing internal controls training</td>
</tr>
<tr>
<td>Loss of separation of duties</td>
<td></td>
<td>Knowledge of techniques of EDP fraud</td>
</tr>
<tr>
<td>Changes can be made almost instantly</td>
<td></td>
<td>Access expertise</td>
</tr>
<tr>
<td>Increased ease of access</td>
<td></td>
<td>Types of computer environments</td>
</tr>
<tr>
<td>Computers not widely understood</td>
<td></td>
<td>Types of computer environments</td>
</tr>
<tr>
<td>Computer literacy/user-friendliness</td>
<td></td>
<td>Shift from documents to systems focus</td>
</tr>
<tr>
<td>Increased volume of data processed</td>
<td></td>
<td>Training in EDP auditing internal controls &amp; security systems</td>
</tr>
<tr>
<td>Security systems not always built-in</td>
<td></td>
<td>Training in EDP auditing internal controls &amp; EDP fraud techniques</td>
</tr>
<tr>
<td>Performance and security trade-off</td>
<td></td>
<td>Updated organizational theory</td>
</tr>
<tr>
<td>Networks increase risks</td>
<td></td>
<td>Training in EDP auditing internal controls &amp; security systems</td>
</tr>
<tr>
<td>Internal controls altered or overridden</td>
<td></td>
<td>More sophisticated attitude</td>
</tr>
<tr>
<td>Reduction in human intervention</td>
<td>Organizational theory and accounting training</td>
<td>Updated organizational theory</td>
</tr>
<tr>
<td>Functional complexity</td>
<td>Training in evidence</td>
<td>IS training</td>
</tr>
<tr>
<td>Technical complexity</td>
<td></td>
<td>Shift from documents to systems focus</td>
</tr>
<tr>
<td>No evidence of data changes</td>
<td>Criminology and psychology</td>
<td>Updated organizational theory; more sophisticated attitude</td>
</tr>
<tr>
<td>Trusted personnel circumvent controls</td>
<td></td>
<td>Types of computer environments</td>
</tr>
<tr>
<td>Storage media are vulnerable</td>
<td></td>
<td>IS training</td>
</tr>
<tr>
<td>Volatility of the IT/IS industry</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

detect and prevent their criminal activity.

Finally, empirical research needs to be done in order to test the framework developed above. Case studies and field work are probably best initial approaches, since they are especially helpful in identifying the key factors. Surveys would also prove useful in finding these variables, at least as perceived within the practitioner community. After these types of research have established a foundation, hypothesis testing from collected data should be feasible.  

**References**


