The auditing profession has incurred increasing responsibilities due to the proliferation of legal liability and the special role of computer technology in today's business environment.

White-collar Computer Crimes:

A Threat to Auditors and Organization

Nazik S. Roufaiel and Vernon Dorweiler

Managerial Auditing Journal, Vol. 9 No. 3, 1994, pp. 3-12
© MCB University Press, 0268-6902

Introduction

An earlier article[1] described the characteristics of computer crime, features of the perpetrators of such crimes, and generic methodologies of such crimes. Additionally, the design features – physical, technical, and administrative – of internal control systems and audits were presented for the detection and prevention of computer crimes.

A range of cases involving *computer-related crime*, and the legal literature, were studied in an attempt to develop a comprehensive analysis of the dimensions of this crime. From the resulting analytical framework, the auditor's responsibility can be defined, along with the positions of legal and professional authorities in an audit failure. Emphasis is placed on the legal-judicial position placed on the victim in computer-related crime.

This article further addresses the broader aspects of *responsibility* for injury from white-collar and computer-related crime. The historic development of the auditor's responsibility gives a basis for viewing recently legislated criminal statutes. The most recent emphasis has been on legislating for the organization's responsibility. The recency of this development can be viewed by the activity of the United States Sentencing Commission, established in 1984, which focused on individuals' sentencing and which has only addressed the sentencing of organizations since 1988.

There is an urgent need to sensitize practitioners, academicians, students, and standard-setting authorities, to these added responsibilities. The proliferation of liability, and the special role of computer technology, in the accounting profession has raised vigorous challenge and responsibility – to be faced in the decade of the 1990s.

The Auditor's Responsibility

It is becoming nearly impossible to predict the future standards to which the public and the courts will hold the auditing profession responsible. A particular focus is computer-related crime (that is, *computer fraud*) which is easy to commit but hard to detect. Auditors can expect to be increasingly challenged to define their responsibility for computer fraud. Otherwise, they will find others (complainants, courts, legislators) defining their responsibility for them. If that happens, it will be a substantial threat to standard-setting authorities and to the independence and the credibility of the auditing profession. Public and professional emphasis already exists on increasing auditors' responsibility. Auditors currently practise in a climate where national public policy emphasizes protection for clients against substandard work by professional malpractice generally (see the section on Public Precepts).

The determinative question at this point is the definition of the nature and extent of the auditor's opinion. Such a definition must cover the auditor's responsibility to prevent or detect computer fraud, and the extent of such responsibility. There is now a big gap between what the public expects of CPAs and what the CPAs expect of themselves. There is also a gap in court rulings that draw on the auditor's opinion which, on financial statements, is considered "expert testimony". This testimony should be considered only as being persuasive but not conclusive. This evidentiary rule follows from the standards employed by auditors; that is, in the absence of specific rules or customs, the required standard of communication and reporting is measured by generally accepted accounting principles and generally accepted auditing standards. In courts, such standards are not accepted because they are not based on specific rules and prohibitions. Thus, *legal liability* may follow the accountant in rendering any professional service.

In the USA, auditors can be sued under common law (tort, contract, and in equity), statute (the Securities Acts of

1933 and 1934 and the Foreign Corrupt Practices Act of 1977) and criminal laws. Negligence and not exercising "due professional care" are particularly applicable in cases of undetected computer fraud. Under common law, auditors could be used successfully for ordinary negligence, gross negligence or fraud. This is the least burdensome path for suit because carelessness is usually easier to prove than recklessness or intent to deceive.

Thus, auditors can no longer benefit from the common law protection previously available. In the complex world of auditors' business and legal environments, their responsibility to the public is ever expanding. The Treadway Commission[2] recommended a *professional understanding* of the complex regulatory and law enforcement framework. In addition, professionals and business and accounting students should gain an overall sense of what will be expected of them, legally and professionally, in their accountability to the public. To emphasize the auditor's changing responsibility, the following sections describe prevailing legal and public precepts, as well as current professional standards of auditors' responsibility.

Legal Precepts

The position of law enforcement bodies towards victims of computer fraud is based on statutory provisions and specific elements. Analysis of these legal provisions and the elements can be used to indicate the auditor's responsibility as perceived by law enforcement bodies. At the outset, these legal precepts are tempered by general public precepts regarding fault. Both *fault* and *civil liability* (tort and contract based) are considered next.

Caveat Emptor

The most elementary understanding of *caveat emptor* is a warning to read, investigate and examine before reporting, where assets are involved. Those who choose to disregard such an admonition to do so at their own risk and liability (i.e. they assume the risk). Victims of computer crimes stand accused of being neither careful enough, smart enough, nor honest enough to deserve the protection of society.

Incredulity towards Fraud Victim

The general incredulity focused on victims who did not discover fraud seems to derive from two widely held beliefs[3]:

(1) This crime does not happen except to those of questionable character.

(2) Only those who have shown an exceptional disregard for simple rules of conduct become victims of fraud.

Auditors' reports on the internal control system, and financial statements with no qualifications, may provide a basis for believing that evidence collected and data disclosed are fairly representing the business operations. these can contain fraud of any type considered earlier[1], perpetrated on those who have been deceived. Such a crime has, therefore, happened because of the victim's apparent failure to observe some basic rules of conduct (obtaining sufficient competent facts).

Erosion of Fault-and-causation Concept

Many legal actions (and prosecutions) stem from the erosion of the fault-and-causation concept of liability. Focusing on the accounting profession, the litigation issue is related to the role and scope of auditor responsibility. In some cases, auditors have been accused of negligence, for ignoring the "early warning" of fraud and business difficulty. Auditors thus assume the role of business forecaster, and run the risk of being the ultimate insurer of business success and being at *fault for not preventing failure*[4].

Adoption of (Victim's) Negligence Concept

Adopting the negligence concept has the same effect in fraud cases as it has in rape cases[5]. Thus, the more careless, co-operative or negligent the victim's behaviour can be characterized, the less culpable and more acceptable the perpetrator's conduct becomes. In its most extreme form, the negligence concept can be seen to shift responsibility for the act away from the offender to the victim.

Contributory Negligence

The criminal justice system's response to white-collar crime includes a consideration of the part played by the victim of such crimes which influences the level and kind of sanctions imposed on the offender[3]. When a victim is considered to co-operate and ease the arena of crime by negligence or ignorance, the law mitigates the sanction against offenders.

The issue of victim involvement is particularly enlightening, and has consistently intrigued social scientists. Studies of the dynamics of this involvement in various crimes have yielded such interesting concepts as victim participation, victim precipitation, and victim proneness. However, victim actions rarely nullify or excuse the criminal acts. Thus, contributory negligence (victim co-operation) is not excusatory in criminal law. However, it may totally or partially excuse in civil tort actions; comparative negligence (partial excuse) has replaced contributory negligence (total excuse) in most states in the US.

Erosion of Privity-in-contract Provision

Privity of contract (that is, where only parties to the contract have rights under the contract) has been eroded in a few states. Courts have moved towards the view that all third parties who were "foreseeable users" (a negligence basis) of the audited financial statements should be allowed to sue on the ground of negligence.

Auditors' responsibilities have been extended beyond their immediate clients who have a privity relationship. Auditors became responsible to foreseeable third parties who are reasonably expected to see the audited financial statements, and to act (or refrain from acting) in reliance on them.

Joint and Several Liability Provision
Auditors have been required to pay not only for losses caused by their negligence, but also for those caused by a bankrupt professional co-defendant, under the joint and several liability standard. Under this standard, defendants are "jointly" responsible for the entire judgement, as well as "severally" (individually) liable for that share of the damages caused by their own acts. Where the bankrupt co-defendant is excused, and joint and several liability becomes total liability of the remaining auditory (see the section on Public Precepts).

Absence of a Corpus Delicti
In fraud cases, proof of *corpus delicti* is as likely to verify the behaviour of the victim as it is to obfuscate and nullify the offender's guilt[5, p. 43]. The focus is on looking at what total circumstances contributed to such crime. Paucity of evidence about the fraud (certainty and amount), and leniency of prosecution are directly related to the lack of public protection. Society looks at computer crime offenders as somewhat intelligent and as folk heroes.

Anti-racketeering Legislation
The auditor has been caught up in the current period of litigation known as the "litigious society". This societal stance has blossomed through the use of anti-racketeering legislation (the Racketeer Influenced and Corrupt Organization Act (RICO) in business situations)[6]. This federal law, passed in 1970, is extremely broad in its definition of *racketeering activity*, including securities transactions and mail fraud. The statute provides for awarding private civil lawsuits with treble damages as well as criminal sanctions. This legislation was originally intended to be used against organized crime. However, a recent Supreme Court decision allowed private civil action to be applied to commercial disputes reflecting such activity. RICO, lately, has been used in suit against the auditing profession. The fact that juries consider accounting firms to be well financed, and backed by insurance, has provided additional inducement for suits against them, and RICO civil suits have become a very attractive avenue.

Public Precepts

The auditory, as part of the larger accounting profession, is on the anxiety-provoking ground of increasing liability for action and opinion. Historically, public interest has been protected by state law, requiring public accounting practice to be a private partnership (or alternatively, a sole practitioner or professional corporation) – without protection of limited liability. Not only does this requirement make practitioners liable for their own practice, but they are also jointly and severally liable for that of partners. The extent of this liability stretches beyond assets of the partnership to personal assets of the partners.

This requirement deprives practitioners of limited liability, as enjoyed in the corporate form of the organization. With the growing areas of liability, the accounting profession has been developing a consensus within its members which permits limited liability. This position can (will) be used against lawmakers in individual states, to change statutory requirements regarding the regulation of accounting practice. Strong counter-arguments are known to exist, concerning the erosion of professional standards and the influence of public (non-professional) investors. How these positions, and the nature of the practice, evolve will determine the path the accounting and auditing profession will take during the 1990s[7].

Professional Standards

The extant law's position is increasingly aggressive in accusing the auditor of negligence for not exercising professional "due care" in fraud cases involving audit failure. As a British court noted, "There is no remedy for the man who trusted the word of a liar"[8]. Nonetheless, the exact extent of the auditor's responsibility in detecting such fraud is still unclear according to current professional standards.

For many years, accounting pronouncements have stood regarding the proper selection of auditing standards. Accounting bodies have an important role in reducing the likelihood of harmful behaviour through enforcing standards, rather than through prosecution for actions which breach standards and have harmful consequences. Professional standards should provide consistent and identified measures of responsibility. However, existing standards do not consider such measures and, instead, simply guide performance.

Responsibility in case of fraud due to audit failure has generally been generated and expanded by new auditing standards and the recommendations of the Treadway Commission.

Auditing Standards
Ten new standards, effective for audit periods beginning on or after 1 January 1989, have been pronounced. These new standards broaden the auditor's responsibility for assessing:

(1) The status of the organization's internal control and accounting system.

(2) Inherent risk.

(3) The materiality of audited items.

(4) Required documentation of audit procedures before planning the audit.

In the following, selected new standards are compared with corresponding old ones, as related to the auditor's responsibility. The new standards have extended the auditor's responsibility for detecting and reporting fraud and illegal acts; evaluating the system of internal control; and considering and disclosing doubts about a company's ability to continue in existence[9].

SAS No. 53, "The Auditor's Responsibility to Detect and Report Errors and Irregularities", supersedes SAS No. 16, "The Independent Auditor's Responsibility for the Detection of Errors and Irregularities". SAS No. 16 required the auditor to plan the audit to search for errors and irregularities, reporting and mentioning the *inherent limitations* to discovering errors or irregularities in the engagement letter. This presumed management and employees to be honest until found to the contrary. However, SAS No. 53 requires the auditor to design the audit to provide *reasonable assurance* of detecting errors and irregularities which have material effect on financial statements. Moreover, it clearly invalidates the provision of inherent limitations of the audit, and emphasizes affirmative auditor's responsibility and careful study of questionable management integrity.

SAS No. 55, "Consideration of Internal Control Structure in a Financial Statement Audit", supersedes SAS No. 1, "The Auditor's Study and Evaluation of Internal Control". SAS No. 1 required that "there is to be a proper study and evaluation of the existing internal control as a basis for reliance thereon, and for determination of the resultant extent of the tests to which auditing procedures as to be restricted". SAS No. 55, however, redefines "internal control" and expands the auditor's responsibility for internal control in two ways. First, it broadens "internal control" into "internal control structure", which is subdivided into control environment, accounting system and control procedures. Second, it requires an increase in the knowledge the auditor should have concerning the internal control structure when planning an audit. This means that the auditor should carefully consider and understand how internal control policies and procedures are designed, and determine whether they are in operation. SAS No. 1 did not require an understanding of the control environment or accounting system to help identify possible misstatement. It did not require any understanding of control procedures unless the auditor planned to rely thereon.

SAS No. 55 also requires the auditor to obtain sufficient knowledge and understanding of the classes of transaction, and how they are initiated; and accounting records, supporting documents and machine-readable information, including how the computer is used to process data. In determining if there is sufficient understanding to plan the audit, auditors should incorporate into the assessment of internal control the concept of SAS No. 31, "Evidential Matter", and SAS No. 47, "Audit Risk and Materiality", and the complexity and sophistication of operations and the accounting system. In addition, SAS No. 55 requires documentation of the internal control procedure, even if the auditor did not plan to rely on it.

SAS No. 59, "The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern", supersedes SAS No. 34, "The Auditor's Consideration when a Question Arises about an Entity's Continued Existence". This increases the auditor's responsibility for assessing an organization's status as a going concern, and he or she must evaluate whether there is substantial doubt about this ability for a reasonable period of time (minimum of one year). This assessment is based on collected evidential matter supported by additional information which reduces the auditor's doubt. If the auditor concludes that there is substantial doubt, appropriate disclosure should be considered (an explanatory paragraph following the opinion paragraph). This extension in the auditor's responsibility could lead to unwarranted requests and expectations for additional auditor assurance.

SAS No. 60, "Communication of Internal Control Structure Related Matters Noted in an Audit", supersedes SAS No. 20, "Required Communication of Material Weaknesses in Internal Accounting Control", and paragraphs 47 to 53 of SAS No. 30, "Reporting on Internal Accounting Control". This broadens auditors' responsibility by requiring them to report significant deficiencies in the control environment, accounting system and control procedures. These deficiencies are those which could adversely affect the entity's ability to record, process, summarize and report financial data in the financial statements. SAS No. 20 only required auditors to inform management and the board of directors (or its audit committee) about any material weaknesses in internal accounting control procedures which the auditor uncovered.

While the new statements of auditing standard have broadened the auditor's responsibility towards the public and their clients, they are still only guidance..More positive enforcement to comply with such responsibility is needed. A critical look at the standards of professional conduct is essential. It should be emphasized that CPAs should be diligent and competent in carrying out their responsibilities. They should know their limitations and seek consultation when necessary. Lacking qualifications to serve the contemporaneous computer environment is not an excuse for audit failure.

Under Rule 201, "General Standards" (a part of the code of professional ethics), a member and a member's firm:

> shall comply with the following standards and any interpretations thereof by bodies designated by Council:
>
> (a) Professional competence. Undertake only those professional services that the member or the firm can reasonably expect to complete with professional competence.
>
> (b) Due professional care. Exercise due professional care in the performance of professional service.
>
> (c) Planning and supervision. Obtain sufficient relevant data to afford a reasonable basis for conclusions or recommendations, in relation to any professional service performed. If the CPAs believe that they cannot obtain the necessary technical information they need to conduct a specific audit task, they should refer the engagement to, or work with, someone else who has such competence.

National Commission on Fraudulent Financial Reporting
This commission was formed in 1985 to develop initiatives for the prevention and detection of fraud[2]. To extend the auditor's responsibility, the Commission recommended that the standard report should explain that an audit is designed to provide "a reasonable, but not absolute", assurance that financial statements are free of material misstatement arising as a result of fraud or errors. The report should also describe the extent to which the auditor has reviews and evaluated the system of internal control. The Commission also recommended that professional codes of competence and ethics should not only identify the required level of proficiency but also refer to a body of technical standards to be observed.

The Commission's recommendations have increased the interaction between the internal auditor and the external auditor as a single team. The internal auditor is the first line of defence against fraud. The independent public accountant's role, while secondary to that of management and the board of directors, is crucial in detecting and deterring fraudulent financial reporting.

The Commission recommended changes to ensure and improve the effectiveness of the independent public accountant. The changes involved auditing standards and procedures which enhance audit quality and that better recognize the independent public accountant's responsibility for detecting fraudulent financial reporting. The standards should require the independent auditor to take affirmative steps to assess the potential of fraudulent financial report, and to design tests to provide reasonable assurance of detection. The independent public accountant should make greater use of analytical review procedures, and should review quarterly financial data before their release, to improve the likelihood of early detection.

Securities and Exchange Commission
The SEC, in its Accounting Series Release in 1940, cited as a major purpose of audit the expectation that the auditor will uncover an overstatement of assets and understatement of liabilities[10]. However, there is no guideline to determine the responsibility of the auditor to discover such fraud, particularly in the light of modern, sophisticated fraud instruments as in *EDP* accounting systems, *ATM*, and *EFT*. The SEC has authority to sanction or suspend practitioners from performing audits for "registered" companies. Rule 2(e) of the SEC's Rules of Practice provides that "the commission may deny, temporarily or permanently, the privilege of appearing before it in any way, to any person who is found by the commission...(1) not to possess the requisite qualifications to represent others, or (2) to be lacking in character or integrity or to have engaged in unethical or improper professional conduct"[7]. Many auditing professionals are trying to disavow the SEC's extension of responsibility, though this responsibility cannot be ignored due to the increasing number of audit failures, and particularly due to computer fraud. The concomitant awareness by the accounting regulatory bodies, reflected in court decisions and the interest of society, further recognize the massive danger from this problem.

Foreign Corrupt Practices Act of 1977
The Act, passed by Congress to affect SEC-registered companies, affects auditors through their responsibility to review and evaluate an organization's internal control system as a part of a financial statement audit. While some auditors deny their responsibility in reviewing, in particular, internal control systems, the new SAS No. 55 is expected to broaden their responsibility, thus increasing the number of law suits for audit failure under the Act[7].

Organizational Responsibility

Organizational Culpability

The growing list of federal criminal statutes (see the Appendix) has given increased attention to the culpability of the business organization. Statutes such as the Criminal Fine Enforcement Act of 1984, the Criminal Control Act of 1984, the Narcotics Enforcement Act, the Criminal Forfeiture Act, the Money Laundering Control Act of 1986, the Major Fraud Enforcement Act of 1988, have made it possible for courts to impose fines of meaningfully large amounts on convicted organizations.

The major thrust towards *procedural recognition* of the organization's criminal liability – whether individuals may or may not be simultaneously convicted – comes with the Federal Sentencing Reform Act (of 1984). Under the Act, the United States Sentencing Commission was established to promulgate sentencing guidelines and policy statements for all federal courts, and for the United

States probation system[11]. Its statutory foundation (policy) is uniformity and predictability and, hence, its aim is to create a system which is easier to apply. Guidelines for sentencing of *individuals* were promulgated on 1 November 1987.

For purposes of the Act, an organization is defined as a *person*, other than an individual, such as a corporation, an association or a partnership. A variety of situations provides a basis for prosecuting and sentencing the organization. However, the legal principles involved are:

(1) *Imputation* of criminal conduct and intent of the organization (including benefiting, assenting, collective knowledge).

(2) *Attribution* of criminal conduct to individuals of the organization (including direct and indirect participants) and in complicity[8].

Hence the interaction of *individual* and *organizational* culpability is, for the first time, addressed in criminal prosecution and sentencing. Presently, criminal prosecution generally concerns the individual, while only about 300-350 sanctions are imposed per year on organizations. A breakdown of these by category is given in Table I, for 1988.

The Act provides that:

(1) Benefits derived from criminal activity are to be disgorged (and distributed to victims).

(2) Assets will be seized, for fines, from the *whole* where several are culpable.

Table I. *White-collar Crime Statistics*

	%
Areas of prosecution (1988)	
Anti-trust	30
Government fraud	25
Private-fraud	10-15
Environmental crimes	10-15
Other	15
	100
Areas of conviction (1988)	
Fraud	33
Anti-trust	29
Environmental crimes	9
Export control	5
Tax evasion	4
Other	20
	100

Source:[11]

(3) Collective guilt is ascribed where individual guilt may not be established, to vindicate the criminal statute.

It further aims to provide an incentive to owners and managers, to install mechanisms to prevent, detect and punish criminal activity.

Organizational Sentencing

After conviction of the organization for criminal conduct (the offence itself), the sentencing guidelines provide the following *sentencing* categories:

(1) Restitution, to victims of the criminal activity, with probation permitted as a condition to supervising the restitution.

(2) Remedial order to correct the anomalous situation and to prevent further of future harm (for example, to establish a trust fund for victims).

(3) Probation, as an independent sentence (under the guidelines), on a *fines* basis (guaranteeing payment), and requiring *internal change* (with a concomitant demand to establish and report on required plans).

(4) Community service as an expeditious way of repairing harm to specific victims, approximately an indirect monetary sanction (though charitable contributions are not included, unless specifically directed).

(5) Notice to victims (limited to those reasonably identifiable).

(6) Fines, on the same basis as individuals. (This is the largest category.)

Discretion of the court is mandated regarding restitution, community service, and notice to victims. Likewise, probation must be justified by the court, as needed:

(1) To guarantee payment of fines.

(2) To ensure compliance with remedial orders.

(3) As a condition of restitution.

These performance-based sentences severely intrude into the business affairs of an organization and demand the reporting, examination and interrogation of financial status; notice of change in condition (material adverse change); and the implementation of a compliance plan, with approval, and subsequent reporting and examination.

External officials participate who are appointed by the court, probation officer, auditor or expert. Such sentences are extraordinary in judicial administration – with competence and fee liability creating objective issues. Consequently both the discretion and justification of the court is required to impose these sanctions.

Fines represent "market-based", "pro-market" incentives to the organization to deter criminal activity, and

introduce a whole discipline into the enterprise (previewed above as a compliance plan). The sentencing guidelines represent a *systematic* approach to establishing a *range of fines*, which is detailed in Table II, with fine *amounts* listed against offence level. The computation of the fine for an office proceeds as follows:

(1) Determination of the "offence level", with the individual's status taken into account and recognizing special characteristics of the offence and multiple counts.

(2) Determination of the amount of the fine, as the *greater of*:

- the amount related to the offence level (see Table II);
- gross pecuniary loss caused by the criminal activity; or
- gross pecuniary gain to the defendant from the criminal activity.

(3) Adjustment of this *fine amount* by:

- Aggravating factors – eight factors, and
- Mitigating factors – four factors

with the adjustment on either of two bases:

Option I, as +/– the percentage of the fine amount; and

Option II, as +/– level of offence.

where aggravation adds (+), and mitigation subtracts (–), the stated amounts under the two options.

(4) Determination of residual amount of loss not ordered restituted or gain not disgorged.

(5) The range of the fine then is set as:

([2] +/– [3] + [4]) *M where M is 2.0, for minimum and 3.0 for maximum of the range.

(6) Fines to the organization are offset by fines to individuals (to prevent double counting), and by punitive amounts paid to government agencies (not to private parties).

Under the sentencing guidelines, the court must sentence within this range or state, on the record, specific reasons and other aggravating/mitigating circumstances for departure. Such circumstances include substantial assistance to authorities, and risk of death or serious bodily injury.

Table II. *Table of Fines*

Offence level	Amount $	Offence level	Amount $
1	500	21	400,000
2	1,000	22	500,000
3	1,500	23	600,000
4	2,000	24	700,000
5	3,000	25	800,000
6	4,000	26	900,000
7	6,000	27	1,000,000
8	8,000	28	1,500,000
9	10,000	29	2,000,000
10	12,000	30	2,500,000
11	15,000	31	3,000,000
12	20,000	32	3,500,000
13	30,000	33	4,000,000
14	50,000	34	5,000,000
15	75,000	35	7,000,000
16	100,000	36	10,000,000
17	150,000	37	12,000,000
18	200,000	38	15,000,000
19	250,000	39	20,000,000
20	300,000	40 & above	25,000,000

Range to be determined from: (1) amount of fine; (2) pecuniary gain or loss from the offence: and (3) loss of gain not subject to restitution or disgorgement.

Organizational "Code of Conduct"

While the sentencing approach treats aggravating and mitigating factors as procedural adjustment to *offence levels* or to *fine amounts*, the areas of organizational conduct described are more in the nature of a code of conduct.

Mitigating factors are:

(1) Prompt reporting of the offence to government authorities (prior to the onset of official action);

(2) Lack of knowledge of the offence (on a reasonable basis);

(3) The act of being an isolated incident of criminal activity, given *bona fide* policies and programmes of substantial effort to prevent such conduct;

(4) If substantial steps have been taken to prevent recurrence, such as monitoring procedures and disciplining individuals.

From the affirmative requirement (for mitigation), a proactive stance and code are defined.

On the other side of codification are the proscribed activities:

(1) When high level management aids or abets, knowingly encourages or condones the conduct or obstructs the investigation or prosecution.

(2) Where the offence was in violation of a judicial order, or within 15 years of the violation of a judicial or administrative decision (ten years of similar offence).

(3) Where the injury involved:

- Official bribery.

- Targeting a vulnerable victim.
- Substantial risk to a financial or consumer market.
- Substantial risk to national security.

From the prohibited limitations (for aggravation), parallel remedies are available to the court, beyond fines. Note that *victims* related to restitution, remedial orders, community service and notice to victims; and *management conduct and past incidents* relate to probation and the requirement to install internal changes.

A code of conduct for the organization is then formulated, incorporating positive, affirmative actions and prohibitions, which is fully amenable to the internal control system.

Code of Conduct versus Fiduciary Duty
Directors and officers have extended responsibility under the federal sentencing guidelines. The net result of discharging this responsibility is to reduce fines *to zero* – as against increasing them by up to four times the actual amount of injury caused by the offence. As noted, further intrusive remedies can be forestalled.

On the other hand, the fiduciary duty of directors and officers is to assure the assets, and performance of assets, of the organization[12]. Then, if the proper exercise of their *business judgement* is to "stand and fight", this position opens several avenues of liability. Loss of mitigation can cripple the organization, as can notice to victims (initiating private and class lawsuits). Derivative action can be brought against individual directors by shareholders[13].

Some balance of the two duties is found in *parsing* out offending officers, managers and supervisors. It should be noted that such an action satisfies mitigating factor (4), mentioned previously, and simultaneously discharges (to some extent) the fiduciary duty of directors and officers.

An Auditing Perspective for the 1990s

The proliferation of computer technology and related crimes has created a rigorous challenge, and has imposed a threatening extension of the auditor's responsibility to discover financial fraud. Side by side with this technology, auditing professional standards have been changed to broaden this responsibility. A precipitous change in the legal environment towards increased auditors' liability (the burden of internal control scheme, the erosion of privity of contract provision and adoption of contributory negligence concept), in the vastly expanded environment of organizational criminal activity, has extended the potential for successful lawsuits against auditors.

Audit failure cases, trials and huge increases in judgement awards (particularly following civil RICO suits) are positive affirmation of such threat. The absence of *corpus delicti* in computer fraud cases, and the societal perception of the fraud victim (viewed with incredulity) and computer fraud offender (seen as "slick") have narrowed the means by which auditors may defend themselves. Insurance premiums are escalating, and coverage is shrinking, as carriers have ceased to offer liability insurance. The AICPA liability insurance plan premium in 1980, for firms with 25 professionals, was about $64 for each professional per $1 million in coverage. By 1986, the premium had risen to about $1,160, with the deductible amount doubled.

Recommendations

All of the above mandate careful consideration by professionals, standard-setting authorities and educators, regarding what should be done to avoid (or at least minimize) such expanding responsibility.

The profession has a number of existing quality standards. What the profession needs, to regain and maintain its quality and credibility, is a system of sanctions for non-compliance and non-adherence to such standards. The profession should not stand by those who are violating its standards. If it does so, society will not long tolerate the outcome.

Auditors should carefully examine an organization's internal control system and assess the integrity of management. While internal auditors are the first line of defence against such crimes, nevertheless, external auditors have the main responsibility to uncover such fraud. Computer fraud is easy to commit but hard to detect. There is no fool-proof method to prevent or detect fraud. However, the awareness of certain indicators and the development of a detection mentality will be helpful for auditors when conducting an examination (see[1]). The more proficient auditors become in discovering ways to infiltrate a computerized information system, the better they will be at uncovering computer fraud. Auditors should plan and implement defence techniques to detect the incidence of such a sophisticated crime. They should develop *mental* detection techniques which require a heightened degree of professional scepticism. While detection is an after-the-action line of defence, however, awareness of physical, technical. and administrative techniques could help in reducing the incidence of such crimes (see [1]).

Prevention mechanisms are primarily actions of internal auditing, which restrict or control accessibility to computer hardware and software. Auditors must be proficient in evaluating those prevention techniques and the degree of compliance therein. A new generation of

competent auditors who possess technical and professional skills are needed to meet the challenge of the increasing complexity of the audit environment.

Education and professional examinations confer entry to the profession. They aim to ensure that those entering the profession are competent and capable of applying their knowledge and carrying out duties in a sophisticated area of business. An auditing curriculum should devote a specific course to computer technology and computer-related crime. Graduates should develop a mental and professional attitude towards discovering such crimes. Computer courses, system analysis and design, and the development of ethical values, should be integrated into the accounting curriculum, and should be required by professional societies. Though it is acknowledged that these requirements are cumbersome to accounting education, and may affect the number of students recruited, quantity should be sacrificed for competence in crucial skills. In the alternative, the profession will lose credibility. What could make that target attainable in the future is AICPA membership requirements. The coming 150 credit semester hours, in the year 2000, could be used to include specialized areas of expertise. Credits required for continuing professional education should include coverage of an EDP unit.

Question the integrity of management sceptically and professionally □

Auditors should be trained to develop a sense of integrity, and ethical (and moral) standards of commitment to the profession. Such ethical standards might be the transcendent objectives of their particular responsibility. Studying audit failure cases, and the positions of the court and society, is one of the best resources in educating and training auditors in this area of responsibility.

Conclusion

The success of the perpetrators of white-collar crime and computer fraud, in committing and concealing their crimes, depends mainly on the ignorance of the victim. According to the perceptions of the public and the law, such ignorance facilitates criminality, and contributes to criminal schemes.

The contributory negligence provision can be used as a ground to mitigate the sanction *against the offender*. Thus, a primary technique to avoid responsibility for contributory negligence is for the auditors to vastly expand their knowledge of the client's business, management and computer technology.

A second technique, and second line of defence, is to follow professional standards, and employ only qualified personnel to carry out sophisticated tasks. Those professionals should be trained and supervised carefully before any assignment. Professional standards require collecting evidence and documenting the work properly, and seeking legal and technical consultation, as needed. A pervasive requirement is to recognize and articulate wisely the difference between business failure and audit failure. This explanation should be followed by a clear corresponding statement in the engagement letter.

A last, but unending, requirement is to question always the integrity of management, sceptically and professionally. This can involve collecting sufficient competent evidentiary matter about their background, and past history. Note that this is consistent with integration organizational liability.

Criminals and amateurs, outwith and internal to the organization are an everyday threat, coming with new techniques to penetrate the accounting system and to challenge its security. Auditors' awareness of these techniques is the only key to developing detection and prevention mechanisms. This reduces the looming accusing hand – and avoids establishing auditors as business guarantors and insurers.

References

1. Roufaiel, N.S., "Computer-related Crimes: An Educational and Professional Challenge", *Managerial Auditing Journal*, Vol. 5 No. 4, 1990, pp. 18-25.
2. "Report of the National Commission on Fraudulent Financial Reporting", *Journal of Accountancy*, November 1987, pp. 39-48.
3. Geis, G. and Stotland, E., *White-collar Crime: Theory and Research*, Sage, Beverly-Hills, CA, 1980, p. 46.
4. Staats, E., "Why Today's Audit is More Difficult", *The Internal Auditor*, April 1987, pp. 31-3.
5. Edelhertz, H., *The Nature, Impact and Prosecution of White-collar Crime*, Government Printing Office, Washington DC, 1970, p. 23.
6. Staats, E., "Why Today's Audit is More Difficult", *The Internal Auditor*, April 1987, p. 31.
7. Neebes, D. *et al.*, "Explaining the Auditor's Obligations under SAS No. 54", *Journal of Accountancy*, January 1991, pp. 82-93.
8. Brickey, K., "Corporate Criminal Liability", Colloghan & Co., New York, NY, 1988, p. 992.
9. "ASB Makes Auditing History: 10 New SAS's Herald Far-reaching Changes", *Journal of Accountancy*, July 1988, pp. 144-97.

10. Cascini, K., "FCPA: The American Antibribery Legislation", Third Annual Internal Auditor Education and Training Colloquium, 1990, pp. 1-11.
11. *US Sentencing Commission Guidelines Manual*, Government Printing Office, Washington DC, 1987.
12. Knepper, W., *Liability of Corporate Officers and Directors*, Allen Smith & Co., New York, NY, 1978 (updated 1985).
13. DeMott, D., "Shareholders' Derivative Actions", Colloghan & Co., New York, NY, 1987 (updated 1990).

Appendix: Array of Federal Criminal Statutes

The organization is, in many instances, involved in "interstate commerce", and consequently is subject to federal statutes and regulation. Even "closely held corporations" are found in these federal "streams of commerce". This brings into effect many federal criminal statutes, and the application of federal sentencing guidelines.

The array of federal criminal statutes gives a clear picture of the range of commercial activity[12]:

Conspiracy (general, and anti-trust).

- RICO (different from civil RICO suits by victims).
- Schemes to defraud. Federal securities (including insider trading)

  Mail Fraud
- Foreign corrupt practices act
- Sensitive domestic payments

  Federal Election Campaign Act

  Lobbying activities

  Bribery and gratuities
- Administration of internal revenue laws

  Major tax fraud

  Slush funds and improper payments

  Bank Secrecy Act
- Obstruction of justice

  Perjury, false statements, fraudulent reporting.

Culpability of the organization for acts of officers, managers, supervisors, employees and agents, has been defined in terms of specific criminal elements:

(1) Imputation of criminal conduct to the organization.

(2) Imputation of criminal intent to the organization.

(3) Attribution of criminal conduct conduct to officers, managers, and supervisors of the organization.

Thus, when reviewing the array of criminal activities – at the federal level – and the facility to attribute criminal liability to both the organization and to individual participants, the responsibility of the organization and the Author is indeed significant.

Nazik S. Roufaiel is Associate Professor of Accounting at the School of Business, Ithaca College, New York and Vernon Dorweiler is Associate Professor of Management and Law at the School of Business, Michigan Technological University, Houghton, USA.