Winter 2008

Building an Effective Internal Audit Function: Learning from SOX Section 404 Reports

Dana R. Hermanson
Kennesaw State University, dhermans@kennesaw.edu

Daniel M. Ivancevich
University of North Carolina - Wilmington

Susan H. Ivancevich
University of North Carolina - Wilmington

Building an Effective Internal Audit Function: Learning from SOX Section 404 Reports

Dana R. Hermanson, Dinos Eminent Scholar Chair of Private Enterprise, Professor, Department of Accounting, Kennesaw State University

Daniel M. Ivancevich, Dixon Hughes Faculty Fellow, Professor, Department of Accountancy and Business Law, Cameron School of Business, University of North Carolina Wilmington

Susan H. Ivancevich, Dixon Hughes Faculty Fellow, Associate Professor, Department of Accountancy and Business Law, Cameron School of Business, University of North Carolina Wilmington

We thank Tim Ils, Graduate Assistant from the University of North Carolina Wilmington, for his help in data collection for this project.

Abstract

In the wake of the major accounting scandals, internal auditing has emerged as a powerful force in promoting effective controls, risk management, and governance in U.S. companies. This article highlights recent internal audit-related problems that were revealed in SOX Section 404 reports and offers specific recommendations for building an effective, value-adding internal audit function.

Introduction

Since the major accounting scandals in 2001 and 2002, as well as the passage of the Sarbanes-Oxley Act of 2002 (SOX 2002), the internal auditing profession has experienced unprecedented growth and prominence. Internal audit budgets, staffing, and boardroom exposure have increased (Carcello, Hermanson, and Raghunandan 2005), and the Institute of Internal Auditors (IIA) has seen an explosion of membership and interest. In fact, one prominent CFO stated, "[Internal] auditors are rock stars now. This is their day in the sun" (Liebs 2004).

Internal auditors are experts in governance, risk management, and internal control—areas that many companies have emphasized to achieve compliance with SOX. Many public companies have dealt with SOX Section 404 audits of the effectiveness of internal control over financial reporting, and a host of organizations are

exploring the implementation of enterprise risk management tools. On top of these challenges, the pressure to produce reliable financial reports has caused many audit committees to lean more heavily on their internal auditors for information and technical guidance related to risks and controls.

Given recent developments, we believe that almost any organization can benefit from an effective internal audit function. In this article, we (a) describe the role of internal audit in the organization, (b) highlight some recent internal audit problems revealed in SOX Section 404 reports, and (c) offer practical suggestions for building an effective, value-adding internal audit function. We hope that the insights provided will be useful to managers and audit committee members in a variety of organizations.

The Role of Internal Audit

The IIA (2007b) defines internal auditing as follows:

> *Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

The key to internal audit adding value is that it provides objective evaluations of an organization's processes and operations. The main focus is on improving risk management, internal controls, and governance so that stakeholders' value is preserved. In other words, internal audit seeks to improve the organization's operations and to reduce the chance of negative surprises, including those created by unreliable financial reporting. Through its monitoring efforts in such areas as fraud prevention, improving business processes, and promoting reliable information (including financial reports) and sound controls, a properly designed and functioning internal audit group can add significant value to an organization. Effective internal audit functions also can contribute greatly to SOX Section 404 audits, performing some work on which the external auditor can rely. Such arrangements can reduce Section 404 compliance costs.[1]

New York Stock Exchange companies are required to have an internal audit function. For other U.S. companies, internal audit is a voluntary mechanism. Internal auditing appears to be growing rapidly in popularity, whether implemented as an in-house function or outsourced to an accounting firm or other provider. Research suggests that there is significant protection in having an internal audit function. For example, Beasley, Carcello, Hermanson, and Lapides (2000) found that the presence of an internal audit function was much less common in companies that had been accused of accounting fraud by the Securities and Exchange Commission. The differences between fraudulent and non-fraudulent firms

Internal auditors are experts in governance, risk management, and internal control—areas that many companies have emphasized to achieve compliance.

were particularly noticeable in two industries. In the technology industry, none of the fraud firms had an internal audit function, versus 82 percent of the no-fraud firms. In the healthcare industry, 13 percent of the fraudulent firms had an internal audit function, versus 74 percent of the non-fraudulent firms. Clearly, there is a strong association between the presence of an internal audit function and reduced accounting fraud risk.

Recent Internal Audit Problems

We believe that one way to learn how to "do internal audit right" is to study cases where there have been internal audit-related problems. To highlight deficiencies in the internal audit arena, we recently searched SOX Section 404 internal control reports for cases where there were material weaknesses in internal control related to the company's internal audit function.[2]

Section 404 of SOX requires the external auditor to test the company's internal control over financial reporting, and to highlight any material weaknesses that existed as of the end of the fiscal year. Compliance with Section 404 currently is required for public companies with over $75 million in public float and will be required for smaller public companies in the future.

According to PCAOB Auditing Standard No. 2 (PCAOB 2004, para. 10), "A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected." The standard states that one strong indicator of a material weakness is (para. 140): "The internal audit function or the risk assessment function is ineffective at a company for which such a function needs to be effective for the company to have an effective monitoring or risk assessment component, such as for very large or highly complex companies." [3]

The Audit Analytics database revealed 16 public companies from late 2004 through mid-October 2006 with internal audit-related material weaknesses or remediation plans. In each case, either the Section 404 report highlighted an internal audit-related material weakness, or management's plan to remedy a material weakness included some discussion of enhancing the internal audit function. While these 16 companies represent a very small percentage of public companies subject to SOX Section 404, we believe that these weaknesses illustrate important issues for managers and audit committee members to consider.

Exhibit 1 provides an overview of the 16 companies' size, industry, auditor, and material weaknesses. The companies are reasonably large, with median market value, revenues, and assets in the $500 million or higher range, and they are primarily manufacturing or financial firms. Most of the companies have Big 4 external auditors and typically have other internal control problems in addition to their internal audit issues (the median number of material weaknesses per company is 4.5, with a range of 1–10).

Exhibit 1
Sample Description – Companies with Internal Audit-Related Problems (n = 16)

Panel A: Company Size ($000s)

	Median
Market Value (n = 14)	798,959
Revenues (n = 15)	482,619
Assets (n = 15)	684,094

Panel B: SIC Codes

	N
1000–1999 Mining and Construction	1
2000–3999 Manufacturing	6
4000–4999 Transportation and Communication	1
5000–5999 Wholesale and Retail	2
6000–6999 Financial, Insurance, and Real Estate	4
7000–7999 Services	2
Total	16

Panel C: External Audit Firm

	N
Big 4	9
National Firms, Non Big 4	3
Local Firms	4
Total	16

Panel D: Total Number of Material Weaknesses

Median number of material weaknesses per company	4.5
Range of material weaknesses per company	1 – 10

Exhibit 2 presents wording quoted or adapted from the 16 companies' 10-Ks (which contain the management and external auditor reports on internal control) that describes the internal audit problems and management's efforts to fix/remediate the problems. While many of the disclosures do not provide much detail (we provide the full text of the relevant portions in Exhibit 2), some interesting overall patterns emerge from reviewing this table.

In terms of material weaknesses, the most commonly cited issue is the lack of a comprehensive or effective internal audit program/function (seven companies). This problem generally refers to a pervasive failure to implement effective internal auditing, which means that internal auditors do not adequately monitor key risks and controls. This problem also can result from internal audit getting "sidetracked" by management requests. For example, the disclosure for Ligand Pharmaceuticals Inc. indicates that the internal audit department was redirected to help with the company's restatement of its financial statements, the Director of Internal Audit resigned, and the company did not complete much of its internal audit work.

Other problems with internal audit include (a) a lack of independence in the internal audit function (Composite Technology and Ligand Pharmaceuticals), (b) insufficient oversight of internal audit/internal audit focus (Cellstar and Ultra Petroleum), and (c) issues related to inadequate auditing of international operations (H. B. Fuller and Thermadyne Holdings). Other problems mentioned include having too few internal auditors, having inexperienced internal auditors, not having an internal audit function at all, or internal audit failing to address problems found in control testing.

Exhibit 2
Internal Audit-Related Control Weaknesses in SOX 404 Reports

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
99 Cents Only Stores 2004	• Did not have a sufficient number of or appropriate depth of experience for accounting and finance, inventory management, real estate management, information technology, or internal audit personnel. • Did not have an adequate monitoring program, including full testing of its internal control systems and a comprehensive internal audit function.	• Adequately staffing its accounting and finance, inventory management, real estate management, information technology and internal audit departments. • Developing an adequate monitoring program, including full testing of its internal control systems and a comprehensive internal audit function.
Accupoll Holding Corp. 2005	• The insufficient or lacking procedures and structures include, but are not limited to (1) a failure to authorize and empower standing committees of the Board, including an audit committee and a compensation committee, (2) a failure to approve governance structures including charters, delegations of authority, codes of ethics and appropriate conduct for officers and directors, controls regarding conflicts of interest, definition of roles and responsibilities, approval of budgets, and (3) a lack of an internal audit function.	• An internal audit function will be developed to perform periodic reviews to evaluate adherence to formalized procedures and controls over the financial reporting processes performed by the Company.
Aspen Technology, Inc. 2005	• No specific mention of internal audit in material weaknesses.	• Hired additional accounts receivable, tax and internal audit personnel, including a Director of Internal Audit and a Director of Tax.

(continued)

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
Bally Technologies, Inc. 2005	• Ineffective controls at the entity level: As evidenced by the material weaknesses described above, and management's final assessment of our internal controls, we have determined that our entity-level controls related to the control environment, risk assessment, monitoring function and dissemination of information and communication activities did not operate effectively, resulting in a material weakness in each COSO component (COSO 1992). Such entity-level controls, and a comprehensive monitoring of internal controls by the internal audit function, are part of the framework to ensure that the designed system of internal control is operating effectively to ensure that significant transactions are adequately identified, recorded and disclosed.	• *No remediation efforts related to internal audit.*
Bristow Group, Inc. 2005	• *No specific mention of internal audit in material weaknesses.*	• Internal audits are planned to ensure that the compliance program is followed.
Cellstar Corp. 2004	• The Company did not maintain effective controls over the focus of the internal audit function.	• Increasing the level of monitoring through the internal audit function.

Clearly, there is a strong association between the presence of an internal audit function and reduced accounting fraud risk.

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
China Energy Savings Technology, Inc. 2005	• Lack of Internal Audit System. The internal audit department was ineffective in preventing and detecting control lapses and errors in the accounting of certain key areas like revenue recognition, purchase approvals, inter-company transactions, cash receipt and cash disbursement authorizations, inventory safeguard and proper accumulation for cost of products, in accordance with the appropriate costing method used by the company.	• Evaluating the internal audit function in relation to the Company's financial resources and requirements.
Clifton Savings Bancorp, Inc. 2005	• The Company's internal audit program was not sufficient to provide management a basis to assess the quality of the Company's internal control performance over time. Accordingly, management concluded that the monitoring component of the Company's internal control over financial reporting was not effective. Internal control monitoring involves assessing the design and operation of internal control on a timely basis, and taking necessary corrective actions.	• We will review the need for additional compliance/internal audit personnel. • We will request testing reports from our internal auditor on a regular basis.
Composite Technology Corp. 2005	• The Company did not have an independent internal audit function due to the small size of the organization.	• Evaluating the internal audit function in relation to the Company's financial resources and requirements.

(continued)

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
Flagstar Bancorp, Inc. 2004	• Management believes that the deficiencies noted above may have been the result of weaknesses such as (1) certain personnel lacking sufficient expertise in areas of U.S. GAAP, (2) inadequately trained employees, such as personnel who perform certain accounting functions that rely heavily on supervisors to identify problems and errors, (3) lack of communication between certain departments, (4) internal audit's failure to address certain issues identified in the internal controls testing and (5) security around user access rights to certain application systems.	• *No remediation efforts related to internal audit.*
H. B. Fuller Company 2004	• In its assessment as of November 27, 2004, management identified as a material weakness, insufficient supervision and oversight of certain local accounting personnel in its Chilean accounting operations. Specifically, Company policy did not provide for regional financial management or internal audit review of the local books and records of the smaller locations within the Company's Latin America region, which includes the Chilean operations. As a result of this material weakness in internal control, H.B. Fuller Company's financial statements were misstated due to the intentional recording of incorrect accounting entries by local accounting personnel under the supervision of the	• The company is in the process of expanding internal audit resources in the Latin America region.

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
H. B. Fuller Company 2004 *(continued)*	Chilean financial controller beginning in 1999, and continuing through the third quarter of 2004. These incorrect accounting entries resulted in the overstatement of other current assets and income taxes payable, the understatement of notes payable and trade payables, and a cumulative overstatement of net income during the aforementioned period amounting to $3.1 million.	
Impac Mortgage Holdings, Inc. 2004	• *[After a discussion of a material weakness]* We also noted significant deficiencies in that our internal audit function did not provide an adequate or effective monitoring of our controls, and we needed to evaluate whether we have appropriate internal resources to manage and monitor work performed by our outsourced tax compliance function.	• We hired outside consultants to assist our internal audit group in documenting our accounting and business processes and identifying areas that require control or process improvement. • We hired a Director of Internal Audit whose primary responsibilities are to perform risk assessment and monitoring of our system of internal controls and, in addition, to oversee the establishment of formal policies and procedures throughout our organization.
Ligand Pharma-ceuticals Inc. 2005	• Internal Audit. The Company did not maintain an independent effective Internal Audit Department. This material weakness resulted from the fact that: 1) the Internal Audit Department was redirected during the second, third and fourth quarters of 2005 to assist with the restatement of the Company's consolidated financial statements,	• Internal Audit Plan. As discussed under the caption Remediation Relating to Accounting Personnel, the Company is in the process of recruiting a Director of Internal Audit and such position is targeted to be filled during the second quarter of 2006, or as soon as possible thereafter. Until the position is filled, the Company has engaged a nationally

(continued)

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
Ligand Pharma-ceuticals Inc. 2005 *(continued)*	and 2) the Director of Internal Audit resigned December 2, 2005. As a result, the Company's Internal Audit Department executed only a small portion of the activities contemplated to be performed pursuant to the 2005 internal audit plan. In late December 2005, the Company engaged a nationally recognized consulting firm to perform the planned activities of the Internal Audit Department, most notably the Company's compliance efforts with respect to Section 404 of the Sarbanes Oxley Act of 2002. While this material weakness did not result in adjustments to the Company's 2005 consolidated financial statements, it is reasonably possible that, if not remediated, given the importance of a functioning effective Internal Audit Department in the maintenance of effective internal controls over financial reporting, this material weakness could result in a material misstatement of the Company's financial statement accounts that might result in a material misstatement to a future annual or interim period.	recognized external consulting firm to perform the functions of the Internal Audit Department. It is anticipated that the 2006 Internal Audit Plan will be approved by the Audit Committee in the second quarter of 2006, and until the Director of Internal Audit is hired, the Company will continue to utilize the consulting firm to implement and execute the 2006 internal audit plan. • Monitoring Controls. As discussed under Internal Audit Plan above, the Company is in the process of recruiting a Director of Internal Audit. Additionally, and until the Company has hired the Director of Internal Audit, the Company has engaged a nationally recognized external consulting firm to implement and execute the 2006 internal audit plan starting in the second quarter of 2006. As part of the internal audit plan, these consultants will be responsible for assisting management with updating and maintaining the Company's documentation of internal control over financial reporting. The consultants will also be used until and after the hiring of the Director of Internal Audit to assist with the testing of such internal controls and in monitoring the progress of any ongoing and newly identified remediation efforts to help ensure the timely completion of the Company's 2006 monitoring program.

While the scope of the internal audit function will vary greatly across organizations, we believe that just about every organization can benefit from effective internal auditing.

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
Riggs National Corporation 2004	• As of December 31, 2004, the Company's internal audit program was not sufficient to provide management a basis to assess the quality of the Company's internal control performance over time. Accordingly, management concluded that the monitoring component of the Company's internal control over financial reporting was not effective. Internal control monitoring involves assessing the design and operation of internal control on a timely basis, and taking necessary corrective actions.	• The Company enhanced the internal audit program during 2004 and has now completed implementation of that program. However, as of December 31, 2004 the updated internal audit program was not in place for a sufficient time period to fully determine its effectiveness. The Company will continue to enhance its internal audit function in 2005 by expanding the scope of certain internal audits, enhancing the tracking of outsourced audit work, and modifying its existing internal audit plan as necessary. This will also include continued focus and review of regulatory risk through the use of internal audit, including outsourced internal audit resources.
Thermadyne Holdings Corp. 2004	• During the year-end financial statement close process, we identified unexpected variations in the balance sheet data provided from our Brazilian subsidiary. After a rigorous internal audit at this subsidiary, it was concluded that certain period costs were improperly capitalized and included in inventory and intangibles. In addition, certain contingent tax refunds were improperly recognized prior to being received. In response to the errors identified at our Brazilian subsidiary, we performed internal audit procedures at our South African subsidiaries and determined that key	• In order to remediate our insufficient controls relating to the oversight and monitoring of our smaller international locations, we will augment internal audit work already performed with a more extensive internal audit program for 2005 that will include work performed at our smaller foreign locations, and additional audit resources.

(continued)

Company	Deficiencies related to internal audit	Remediation(s) related to internal audit
Thermadyne Holdings Corp. 2004 *(continued)*	account reconciliations were not being performed in accounts receivable, inventory, and accounts payable. The internal audits at these locations resulted in adjustments recorded during the fourth quarter of 2004 to accounts receivable, inventory, prepaid expenses, intangibles, goodwill, and cost of sales. We have concluded that a material weakness exists due to insufficient controls relating to the oversight and monitoring of our smaller international locations.	
Ultra Petroleum Corp. 2005	• The Company did not maintain effective company level controls. Specifically, (1) certain of its accounting personnel in key roles did not possess an appropriate level of technical expertise, and (2) the Company's monitoring of the internal audit function was not sufficient to provide management a basis to assess the quality of the Company's internal control performance over time.	• Increasing training for the Company's current accounting personnel, hiring additional accounting personnel and engaging outside consultants with technical accounting expertise, as needed, and reorganizing the accounting department to ensure that accounting personnel have adequate experience, skills and knowledge relating to the accounting and internal audit functions assigned to them.

Note: The wording above is quoted or adapted from the companies' auditor reports or management reports on internal control.

Management's discussion of any remediation efforts most commonly addresses staffing issues—hiring an Internal Audit Director, hiring additional internal audit staff, or engaging an outside consultant. Having the right people in place is absolutely critical to effective internal auditing, but internal audit talent is in high demand in today's market. Thus, it is challenging for some companies to attract and retain top internal audit talent.

Other remedial steps cited include:
- enhancing international auditing efforts,
- evaluating the overall internal audit function in light of company characteristics,
- developing/enhancing a comprehensive internal audit function, and
- addressing such issues as compliance auditing, additional testing/scope, greater communication through internal audit reports, better tracking of outsourced internal audit work, and increased training.

Suggestions for Managers and Audit Committee Members

How can organizations build their internal audit functions to provide maximum value? Based on the types of weaknesses identified in Exhibit 2, as well as our own experience researching internal audit issues for several years, we offer the following suggestions for management and audit committee members. We also encourage interested readers to consult a host of IIA resources available online at http://www.theiia.org/theiia/about-the-profession/about-the-internal-audit-profession/ and the AICPA's (2004) Evaluating the Internal Audit Team: Guidelines and Questions.

- **Setting up an Internal Audit Function.** Some organizations do not yet have an internal audit function, due to small organization size or lack of management or board support. While the scope of the internal audit function will vary greatly across organizations, we believe that just about every organization can benefit from effective internal auditing. Those beginning the process of establishing an internal audit function are encouraged to visit the IIA website (see Establishing an Internal Audit Shop, IIA 2007a) for tips in this regard. This process may start with one internal auditor, perhaps even part time, but we believe that this function is critical to effective governance, risk management, and control in the organization.

- **A Clear Internal Audit Charter.** The internal audit charter should clearly establish the role and responsibilities of the internal audit function. If the charter is deficient, it increases the chance that internal audit will be sidetracked into non-core activities or simply fail to comprehensively monitor the organization's risks and controls. The charter should unambiguously describe the scope of internal audit's activities—both for the benefit of keeping internal audit on task, as well as informing others of the role of internal audit (see Tarr (2003) for specific guidance).

- **The Right People.** If internal audit is going to be a major player in the organization, getting the right people on board is critical, especially in the Director of Internal Audit role (referred to as the "Chief Audit Executive"

in IIA professional standards). Organizations need to consider the quantity of internal audit personnel needed, which may be less than some would imagine. Also critical are desired skill sets, which should match the types of risks faced by the organization. Some internal audit groups may require people with backgrounds in environmental issues, complex financial instruments, healthcare regulations, etc. Organizations need to recognize that internal audit talent can be expensive in today's market. Finally, the organization should carefully consider whether internal audit will be an in-house function or will be outsourced to major accounting firm or other provider. There are advantages and disadvantages to each structure (see Rittenberg 1997; Rittenberg, Moore, and Covaleski 1999).

- **Carefully Constructed Reporting Channels.** To whom does internal audit report? An internal audit group cannot easily provide objective oversight of management if the Chief Audit Executive reports only to management. After all, it is difficult to be the watchdog of one's boss. What many, including the IIA, have called for is primary internal audit reporting to the audit committee, with administrative reporting to management (CFO, Controller, or even CEO) since the audit committee is not on-site most of the time. If the internal audit function is to be sufficiently independent, then it is critical that it report to the audit committee and not be under the control of management. Currently, the pendulum clearly has swung toward audit committee (rather than management) oversight of internal audit. Many of internal audit's activities now are related to performing assurance work for the audit committee, rather than "internal consulting" or special projects for management.

- **Covering International Risks.** As indicated by two of the companies in the sample, covering international risks can be a challenge for internal audit. Remote locations often involve language and culture issues, as well as significant travel and time costs. Despite these challenges, it is worthwhile to carefully consider international risks and to appreciate the implications of a reduced emphasis on international operations due to the hassle and cost of auditing them. Problems in an international location can become significant corporate issues.

- **Monitoring the Internal Audit Function.** Once the internal audit function is designed and operational, it is important to continue to monitor internal audit's activities. Both the audit committee and top management may participate in this monitoring, as each party benefits from internal audit's efforts. Questions to consider in this monitoring process include the following:

  - Are we comfortable with the quality of internal audit's work? Are we learning new things from internal audit's reports?
  - Does the scope of internal audit's work seem adequate? Does it appear to match our understanding of organizational risks?
  - How is internal audit viewed in the organization? Is internal audit a major

"player" in organizational decisions? Do people in the organization seek internal audit's advice, or do they avoid internal audit at all costs?

- Does the internal audit staffing level appear adequate? Does the internal audit budget consider all essential areas? Does management try to constrain internal audit through budgetary means?
- Have internal audit's findings and recommendations been communicated to us in a timely and understandable manner? Have the recommendations resulted in value-adding changes in the organization?
- Does the Chief Audit Executive communicate well with the audit committee? Does this person appear to have the respect of management and the external auditor?
- Has internal audit's work improved our understanding of the organization's internal controls and risks?
- Is internal audit responsive to audit committee requests for work in certain areas?
- Is internal audit responsive to audit committee suggestions for improvement?
- Do we perceive that the benefits of the internal audit function outweigh the costs of the function? Do we gather any metrics that are used in making such an assessment of internal audit costs and benefits?

Conclusion

Internal audit can be a powerful tool for improving operations, enhancing controls, managing risks, and promoting sound corporate governance. In the current environment of high accountability and continuing governance failures (e.g., stock option backdating), such elements are vital to organizational success.

Our review of recent internal audit problems cited in SOX Section 404 reports illustrates that not all companies have implemented effective internal audit functions. We believe that companies can learn from these problems, and we have offered several suggestions to managers and audit committee members for building an effective, value-adding internal audit function. We hope that these suggestions will help to drive future internal audit improvements.

References

1. American Institute of Certified Public Accountants (AICPA). (2004). *Evaluating the Internal Audit Team: Guidelines and Questions,* New York: AICPA. http://www.aicpa.org/Audcommctr/guidance_resources/ia_and_audit_cmte/15.htm.

2. Beasley, M. S., J. V. Carcello, D. R. Hermanson, and P. D. Lapides. (2000). Fraudulent Financial Reporting: Consideration of Industry Traits and Corporate Governance Mechanisms. *Accounting Horizons,* (December), 441–454.

3. Carcello, J. V., D. R. Hermanson, and K. Raghunandan. (2005). Changes in Internal Auditing During the Time of the Major U.S. Accounting Scandals. International *Journal of Auditing,* (July), 117–127.

4. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). *Internal Control—Integrated Framework,* New York: COSO.

5. Institute of Internal Auditors (IIA). (2004). *Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002*, Altamonte Springs, FL: IIA. http://www.theiia.org/download.cfm?file=1655.

6. Institute of Internal Auditors (IIA). (2007a). *Establishing an Internal Audit Shop,* Altamonte Springs, FL: IIA. http://www.theiia.org/guidance/standards-and-practices/additional-resources/establishing-an-audit-shop/.

7. Institute of Internal Auditors (IIA). (2007b). *International Standards for the Professional Practice of Internal Auditing,* Altamonte Springs, FL: IIA.

8. Liebs, S. (2004).New Terrain, *CFO.com,* (February). http://www.cfo.com/printable/article.cfm/3011491?f=options.

9. Public Company Accounting Oversight Board (PCAOB). (2004). *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements*, Washington, DC: PCAOB.

10. Rittenberg, L. E. (1997). *The Outsourcing Dilemma: What's Best for Internal Auditing,* Altamonte Springs, FL: Institute of Internal Auditors.

11. Rittenberg, L. E., W. Moore, and M. Covaleski. (1999). The Outsourcing Phenomenon. *The Internal Auditor,* (April), 42–46.

12. Sarbanes-Oxley Act (SOX). (2002). *Public Law No. 107-204,* Washington, DC: Government Printing Office.

13. Tarr, R. (2003). *Establishing an Internal Audit Activity Manual,* Altamonte Springs, FL: Institute of Internal Auditors.

Endnotes

[1] See IIA (2004) for details on the role of internal audit in Section 404 audits.

[2] We examined management's internal control report and the auditor's opinion on internal control over financial reporting, which often contain identical language to describe the material weaknesses. Typically, the auditor identifies the material weaknesses.

[3] See COSO (1992) for discussion of the internal control framework and the importance of monitoring internal controls over time. Internal audit often takes the lead in monitoring the control system.

Exploring Internet Abuse in the Workplace: How Can We Maximize Deterrence Efforts?

Joseph C. Ugrin, Department of Accounting,
College of Business & Administration, Southern Illinois University

J. Michael Pearson, Department of Management –
Information Technology, College of Business & Administration,
Southern Illinois University

Abstract

To advance our knowledge about Internet abuse in the workplace, this study examines how deterrence mechanisms commonly used within organizations impact individual decisions to abuse the Internet. The study uses a policy-capturing approach to test the relative degree of deterrence imposed by common components of Internet acceptable use policies **(AUPs).** The results provide evidence that an AUP that defines acceptable Internet usage, imposes potential sanctions, and implements detection (or monitoring) mechanisms is an important deterrent of Internet abuse. In addition, these mechanisms are most effective when they are actively enforced. The study provides valuable insights and considerations for drafting and implementing an AUP in an organization.

Keywords: Non-work-related computing, general deterrence theory, Internet abuse, Internet acceptable use policy, self-control

Introduction

The Internet and its associated technologies have created a revolutionary change in the way business information flows. With the click of a button, we can communicate, order products, or track competitor activities, among other things. However, the Internet can be misused. The U.S. Treasury Department found that non-work-related computing **(NWRC)**, such as online shopping, checking personal finances, answering personal emails, and using chat rooms, accounted for 51 percent of an employee's time online (Davis, 2001). Urbaczewski and Jessup (2002) refer to the lost productivity that takes place directly after granting employees Internet access as a "productivity vacuum," where the easy access to non-work-related activities is too tempting for employees to resist. In addition to the lost productivity, misuse of the Internet can cause other problems such as security concerns and reduced bandwidth, along with legal issues such as racist, sexist, and offensive materials being transmitted via email (Case and Young, 2002a, 2002b). This gives management motivation to try to reduce or eliminate NWRC.

Some organizations try to curb NWRC by blocking access to unauthorized Internet sites; but due to the dynamic nature of the Internet, keeping a list of unauthorized sites updated can be difficult and time consuming. Instead, many organizations rely primarily on Internet acceptable use policies (AUPs). AUPs attempt to control NWRC by providing guidelines on appropriate computer use, and outline how the organization will monitor, enforce, and punish non-work-related activities (Lee and Lee, 2002; Woon and Pee, 2004). Despite the widespread use of AUPs[1], NWRC has continued to grow (Lee and Lee, 2002; Lee, Lim, and Wong, 2005; Urbaczewski and Jessup, 2002). In addition, managers encounter a catch-22 when introducing AUPs. Potential positive effects of AUPs, such as keeping employees on task, can be counteracted by reduced workplace satisfaction and trust (Urbaczewski and Jessup, 2002). Despite the high degree of abuse shown in many studies, employees often use the Internet for short personal tasks or during breaks, which are not detrimental to the organization and would be consumed by other non-work-related tasks if the Internet were not available (Urbaczewski and Jessup, 2002). Thus managers must make a decision about the amount of NWRC they are willing to tolerate to balance productivity and morale.

This paper helps resolve this paradox by providing insights into how effectively various components of an Internet acceptable use policy deters non-work-related computing. In other words, which components of an AUP give managers the most "bang-for-the-buck?" By using a multi-criteria decision-capturing approach (policy capturing), this study addresses these issues by examining how specific components of an AUP stack up against one another in deterring an employee's intention to perform NWRC.

Internet Acceptable Use Policy (AUP)

Organizations are concerned about the consequences of NWRC, including lost productivity, potential legal liability, and poor corporate image. Many are resorting to AUPs for deterrence (Case and Young, 2002a; Greenfield and Davis, 2002). Typical components of an AUP are:

1. an explanation of the scope of the AUP, (e.g. who and what does it apply to)
2. a statement defining appropriate use
3. examples of appropriate versus inappropriate use
4. a statement defining punishment for inappropriate use
5. a statement about the extent of monitoring, and
6. a signature of the reader acknowledging that they have received and understand the policy (Siau, Nah, & Teng, 2002)

Even though AUPs are widespread, most companies do not actively enforce their policy (Greenfield and Davis, 2002). Despite the lack of enforcement, the mere adoption of an AUP by an organization has been shown to mitigate NWRC behavior due to increased employee awareness of the policy (Harrington, 1996; Lee and Lee, 2002; Lee et al., 2005). However, as mentioned in the introduction,

...non-work-related computing (NWRC), such as online shopping, checking personal finances, answering personal emails, and using chat rooms, accounted for 51 percent of an employee's time online.

Urbaczewski and Jessup (2002) suggest that regardless of their potential benefits, AUPs can reduce workplace satisfaction and trust; this is particularly exacerbated by monitoring mechanisms. Thus, it is important that firms do not implement deterrence measures haphazardly and instead try to implement mechanisms that have the greatest ratio of deterrence to dissatisfaction. To this end, the current paper presents an exploratory study to answer the research question:

> *What is the relative impact of specific control mechanisms commonly found in AUPs on deterring NWRC?*

AUPs from a General Deterrence Perspective

General deterrence theory **(GDT)** provides a theoretical foundation for proposing and evaluating deterrence components within an AUP, and based on GDT we are able to hypothesize the relative importance of several of the deterrence components. Under general deterrence theory, individuals make rational risk/reward decisions based on their expected gratification from taking advantage of opportunities, versus their perceptions of the likelihood and severity of potential consequences. GDT has long been the foundation for crime prevention. It provides insights on how security measures can discourage illicit behaviors. GDT has been used by criminologists to examine the effects of laws on crime, but it has only recently been used to look at workplace issues such as NWRC (Lee et al., 2005; Lee and Lee, 2002; Woon and Pee, 2004).

AUPs comply with GDT because they clarify unethical Internet use and raise employee consciousness to the potential for negative repercussions for abusive behavior. Specifically, AUPs explicate the potential severity of consequences, and by revealing the existence of security and detection systems, they create awareness to the likelihood of consequences coming about.

Researchers who have examined the impact of penalties on intentions to perform NWRC found that the mere awareness of others being reprimanded for performing NWRC reduced user intentions (Lee and Lee, 2002; and Woon and Pee, 2004). This is an intuitively logical finding and we conjecture that enforcement is the key determinant on deterring user intentions. Even when an individual is likely to get caught performing NWRC (for example, by detection systems) and potential ramifications are severe, those mechanisms will have relatively little salience without enforcement. This can be easily illustrated with a short analogy. Imagine that fines for highway speeding and the number of highway patrol officers are greatly increased. Yet you are not aware that the speed laws are ever enforced; everyone just gets a warning. Would you expect drivers to be compelled to comply with speed limits in this case? Probably not.

Kelman (1958) was one of the first to use this line of thinking. Kelman found that individual beliefs tend to change to conform with another party's rules when the other party is able to deliver punishment, is described to be socially acceptable, or is described to be highly credible. This has been extended to the business context by various authors (Tyler 2001; Tyler and Blader, 2005).

Based on this, we conjecture that the awareness that sanctions are being enforced will make the threat of sanctions more credible and increase perceptions about the likelihood of punishment, and will thus be the most salient deterrent on NWRC.

H1: Enforced sanctions will have the greatest degree of deterrence on NWRC.

Even without awareness of enforcement, we expect that the threat of sanctions will still have a relatively strong impact on deterring NWRC, particularly if the level of sanction is strong, such as getting fired. GDT suggests that individuals weigh potential sanctions against the gratification received from an illicit act. Thus, these sanctions are important in a decision maker's mental account. Based on this, we suggest that the threat of sanctions, regardless of whether or not a decision maker is aware of the sanctions being enforced, will have a high level of deterrence on NWRC as compared to other common components of an AUP.

H2: The threat of sanctions will have a high degree of deterrence on NWRC relative to other components of an AUP.

We also expect detection systems to have a strong affect. Detection systems increase perceptions of the likelihood of sanctions being enforced (Hollinger and Clark, 1983). Based on this we expect detection systems to have significant impact on deterring NWRC relative to other common components of an AUP.

H3: Detection systems will have a high degree of deterrence on NWRC relative to other components of an AUP.

Signing an Internet acceptable use policy may not link directly to general deterrence theory, but we expect it to enhance other control mechanisms. For instance, signing a statement saying that one has read and will comply with the AUP will make the individual more mindful of the AUP's components. Case and Young (2002b) found anecdotal evidence that deterrence will be enhanced when employees are required to sign a statement indicating that they agreed to comply with the AUP at their organization. They found that 60 percent of participants who were required to sign their Internet use policy felt the policy was an effective deterrent. However, since signing a statement does not deter non-work-related computing itself, we do not expect it to have a strong relative impact on NWRC.

Finally, an AUP that merely outlines acceptable use may affect NWRC intentions by raising awareness to what type of behavior is acceptable to the employer. Using Kelman's perspective, this would have an impact if the respondent feels that it is socially desirable to follow the rules outlined in the AUP. However, the pervasiveness of NWRC seems to indicate that it is developing into a socially acceptable behavior. Based on this, we expect that merely outlining acceptable behavior will have a low relative impact on NWRC.

The Study

The study used a procedure for examining multi-criteria decisions (policy capturing) that is most commonly used to develop an understanding of the relative salience of available pieces of information on a decision (e.g. Butler and Cantrell, 1984; Pearson, Crosby

and Shim, 1996). The results of a policy-capturing analysis provide an additive linear model that illustrates how a decision-maker weighs available information (cues) to arrive at a decision (Karren and Barringer, 2002). Kline and Sulsky (1995, p. 394) state that "the goal of this approach is to understand an individual's decision-making "policy" by observing the relationships between the decision cues given to the individual, and the final decision made by the individual and then modeling that relationship using an idiographic multiple regression analysis (i.e., regression analysis carried out for a single individual). The results of the analysis provide a description of how the individual decision-maker weights the various cues to arrive at his or her decision. Thus, within the constraints of the cue information presented, each individual's decision-making "policy" can be observed."

The cues (or independent variables), in this study are:

1. the perceived existence of an acceptable use policy
2. the degree of punishment for performing NWRC
3. awareness of others receiving punishment for NWRC
4. evidence of detection systems, and
5. a signature by the participant (employee) on the acceptable use policy, which indicates that they have received it.

The final decision (or dependent variable) is the individual's intention to perform NWRC.

We surveyed 87 people at 12 companies representing a wide variety of industries throughout the Midwest. Participants were given 20 unique scenarios[2] covering all combinations of the independent variables with the existence of each independent variable, or cue, indicated by a yes or no statement. Considering each scenario, respondents were asked a question about whether or not they would use their company's resources for personal use. The respondents were also asked whether or not they would use their company's resources for personal use if they worked in a cubicle or an office (Appendix 1). In addition to the scenarios, basic demographic information was collected, along with open-ended questions about how the participants felt about NWRC in general and whether or not they felt NWRC was an inappropriate behavior.

The policy-capturing analysis involved performing a multiple regression for each respective participant on each of the 20 scenarios. The relative salience of each cue is represented by the average of the individual beta weights. The pairwise differences of the average beta weights were tested for statistical significance using Tukey's honestly significant difference **(HSD)**.

Results

In general, enforcement resulted in the greatest reduction on intentions to perform NWRC. Enforcement was initiated by presenting respondents with a scenario that indicated that others had been fired for NWRC. This was followed by sanctions (possibly getting

fired or not), detection systems, an AUP that merely communicates what types of computing is acceptable, and finally signing or certifying that one has read, understands, and will abide by the policy (Exhibit 1). This hierarchy did not change considering the participant's perceived level of privacy, an office or a cubicle.

The test of pairwise differences indicates that the marginal impact of sanctions, detection systems, and enforcement activities were not significantly different from one another, and the impact of sanctions, detections systems and outlining acceptable Internet use were not different from one another. Requiring individuals to sign a statement indicating they had read, understand, and will abide by the policy *had the smallest marginal impact* and was significantly different than the other cues.

Exhibit 1. Study Results

Independent Variables Decision Cues (Deterrence Measures)	DV1 (Overall Likelihood to perform NWRC)		DV2 (Overall Likelihood to perform NWRC if in an Office)		DV3 (Overall Likelihood to perform NWRC if in an Cubicle)	
	Beta Mean	Group Rank	Beta Mean	Group Rank	Beta Mean	Group Rank
You are aware of others within the organization being fired for performing non- work-related activities on their computers.	-0.381	1	-0.375	1	-0.381	1
The company's Internet use policy contains a statement stating that you may be fired if you perform non-work-related activities on your computer.	-0.292	1,2	-0.264	1	-0.285	1
The company employs security detection systems capable of monitoring your computer usage.	-0.268	1,2	-0.271	1	-0.261	1
The company employs an Internet use policy that states what types of Internet use are acceptable.	-0.248	2	-0.259	1	-0.260	1
You are required to sign the Internet use policy indicating that you have read, understand, and will abide by the policy.	-0.100	3	-0.097	2	-0.089	2

*** Group Rank 1 is the highest rated group and is significantly different from 2 and 3; 2 is the second highest rated group and is significantly different 1 and 3; and 3 is the third highest rated group and is significantly different from 1 and 2. Cues that are rated 1, 2 are significantly different from only the cue rated 3.

Analysis and Discussion

As we conjectured, the components of the AUP that could be linked to GDT—sanctions, detection systems, and enforcement—were highly salient. The component that doesn't seem to have a link to GDT is the signature requirement, which was the lowest-rated cue and was significantly different from the other four cues. Surprisingly, implementing a policy that merely outlines what type of behavior is acceptable was equally as effective as sanctions and detection systems statistically.

From a policy-maker perspective, this seems to indicate that severe sanctions that are likely to be enforced are relatively effective ways to deter NWRC. This gives a signal to employers that if NWRC is a significant problem within their **organization**, they may want to implement a policy that includes potential sanctions that the employer is prepared to enforce. However, if NWRC is only a minor issue within their organization, a policy that merely outlines acceptable use may suffice and, in fact, may have the most cost benefit considering the potential loss of workplace satisfaction and trust that can occur when more intrusive mechanisms are introduced.

To give additional insight into the results, we solicited open-ended responses related the participant's feelings on the topic, and they yielded many interesting comments. In general, employees felt that occasional use of the Internet for personal purposes is not a problem. They seem to feel that employer's demands have increased over the years; thus the separation of work and personal time gets blurred and employees have no choice but to manage some personal issues while at work. However, many employees felt that their employer should have a policy as long as it is fair. For example, one employee states, "there needs to be a policy, but a policy that can be fair and enforced." There were also many comments about pornography. and in general employees feel it should not be tolerated. It seems the general attitude among the employees surveyed is that NWRC is not a problem, which is contradictory to Davis's (2002) findings. However, the employees seem to feel that a policy is still in order. This seems to indicate that employees feel that certain types of NWRC are acceptable, while others are not. Exhibit 2 illustrates respondent's general concerns towards NWRC. These concerns give some insight into how workplace norms may be developing.

Exhibit 2. Employee Concerns

1. Occasional use of the Internet for personal purposes is acceptable.
2. Pornography should not be tolerated.
3. Increasing employer demands are forcing employees to manage personal issues at work.
4. The feel that the NWRC is not a major issue.
5. Even though the NWRC is not a major issue, a policy is still in order.

Management Implications and Directions for Future Research

The implication of these results for practitioners is that an Internet acceptable use policy outlining acceptable uses does provide a degree of deterrence, but the effectiveness of the AUP can be enhanced by including a statement indicating severe consequences (e.g., you may be fired for viewing pornography). With that said, the employer must be prepared to enforce the policy since the most salient component to our participants was the awareness of enforcement. In addition, security measures that increase the likelihood of detection are important relative to other AUP components.

Yet despite the understanding that this study gives us about the relative importance of deterrence measures, managers are still left with a dilemma about which components to implement and how severe to set the punishment, since enforcement does not come without cost and as mentioned previously, monitoring activities can create employee discontent (Urbaczewski and Jessup, 2002).

There are several items that management should consider when implementing an AUP (see Exhibit 3).

- First, what type of employees does the firm have? If the typical employee's job requires considerable use of the Internet, an AUP may be a more practical solution to NWRC deterrence as compared with technology-based solutions such as access restriction, where keeping a restricted website list can be time consuming.

- Next, what type of culture does the organization have? Would employees accept an AUP? If employees are accustomed to a relaxed environment, implementing a restrictive policy could create disgruntlement, particularly if it involves monitoring Internet activity.

- Third, the punishment should fit the offense. It would seem to be impractical to threaten dismissal for relatively small infractions such as managing personal finances or emailing friends, as compared to more serious issues such as viewing pornography.

  However, habitual use of any kind can cause a productivity issue. We suggest NWRC infractions of any kind should be carefully documented in employee personnel files. This will allow the organization to more easily recognize those that are repeat offenders and give adequate documentation in case ramifications are in order.

- Next, what is the cost of implementation, particularly the implementation of detection measures?

- Finally, if the firm has decided to implement an AUP, management should create buy-in. Surprising employees with a new policy such as an AUP could exacerbate potential employee dissatisfaction. We suggest that firms make their employees fully aware of implications and ramifications of an AUP, and

employees be given an opportunity to voice opinions before the AUP is implemented. However, we propose that as AUPs continue to become more common in the workplace, employees will be more familiar with AUPs and employee dissatisfaction will diminish.

Despite our findings, there are still unanswered questions that could impact many organizations. We suggest that the salience of the AUP components examined here will change if they are implemented to different degrees. For example, at what level of punishment does the threat lose its effectiveness? Future researchers should extend this study by focusing on the impact of different levels of AUP components.

We also question how well an AUP will work on employees that work from home. We have suggested that the level of privacy, either in an office or a cubicle, has no bearing on the salience of AUP components. However, we recommend that future researchers examine other settings, such as a home office.

Finally, due to the global nature of business and the Internet, we feel it is important to understand how AUPs are accepted in different cultures. For example, are individuals in cultures that rate higher in uncertainty avoidance more likely to find the mere existence of a policy more salient, or do the findings about the lack of difference between men and women hold in cultures that are more or less masculine? We suggest that future researchers test our model globally.

Limitations

The study has several limitations, most notably measuring participant intentions rather than actual behavior. However, research in many contexts; including ethics, have relied on the theory of planned behavior (Ajzen, 1991) to understand how behavioral intentions lead to action.

The next limitation is that this study treats all forms of non-work-related computing equally, as if time wasted shopping or browsing stock

Exhibit 3. Management Considerations

1. What type of employees does the firm have? Is it feasible to restrict Internet usage?
2. What is the corporate culture? Will it accept an AUP?
3. The punishment should fit the crime.
4. Document all NWRC infractions.
5. What is the cost?
6. Create buy-in.