



2009 IT Audit/Security Forecast

As organizations gear up for 2009, what risks will continue to haunt management, and what new risks—brought about by changes in the business climate and technology—will need to be addressed?

Risk identification and management have always been daunting tasks, but in 2009 they will become increasingly difficult as risk assessments will require updating to incorporate an ever-increasing number of both business and IT threats. Are you aware of the issues your organization faces? What should be your priorities? How should you allocate scarce resources?

Viruses, malware, and the like will continue to be significant threats. Data theft and leakage, aided by the prevalence of portable storage devices, are becoming more frequent and harmful. News stories of identity theft or inadvertent mishandling of sensitive information have become all too common.

The risks related to the establishment and management of system administrator and super-user privileges will spillover into 2009 due, in part, to continued employee turnover. The failure of third-party service providers to meet management's service levels and control needs may jeopardize an organization's operational, security, and compliance requirements. Finally, the ubiquitous use of spreadsheets and other end-user computing tools, particularly in the financial statement close process, represents an ongoing risk to many companies.

J.H. Cohn's Technology/Security Audit and Control Group has identified five IT audit/security concerns for 2009:

1. Stale Risk Assessments and Audit Plans

Given the current economic environment and the reduction in internal audit staff and budgets, it may be necessary for Internal Audit department heads to update their enterprise-wide risk assessments. Simply executing the same audit procedures from year to year may result in unidentified issues and risks that could adversely impact the organization. Therefore, the updated assessment should take into consideration the organization's appetite for operational, financial reporting, compliance, and reputation risk. Based on this risk assessment, an audit plan should be developed for 2009 that addresses the areas of greatest risk to the organization.

While Sarbanes-Oxley (SOX) has been excellent for reinforcing the need for sound internal controls, and notably information technology controls, addressing the risk of inaccurate or incomplete financial reporting may not be the most appropriate allocation of internal audit resources. Internal Audit departments should reconsider whether the organization's audit resources could be more appropriately focused on higher operational, compliance, or reputation risk areas rather than financial reporting risks or the desire to reduce external audit fees. It may be more appropriate to focus those resources on areas that involve the

organization's key performance indicators, compliance requirements, or privacy concerns.

For example, as a company strives to meet performance expectations and struggles to compete, is management doing enough to ensure that the organization's e-mail system, infrastructure, and critical customer information contained in the customer relationship management (CRM) system are adequately protected from external or internal user security breaches?

As retailers emerge from their most crucial holiday shopping season in years, what impact would a security breach involving customer credit card data have on their reputation and sales results?

2. Viruses and Malware

The applications and systems that allow employees and management to work remotely from anywhere also represent significant threats to the organization's information technology resources if the proper security measures and user education programs are not implemented. If management thinks that a firewall is enough to protect their organization from all threats, they should think again.

Management needs to ensure that adequate antivirus protection is in place and systems are properly patched and updated in a timely manner to help protect against continuous threats and vulnerabilities. Viruses, worms, Trojans, and other malware will continue to evolve and become increasingly "intelligent." Without adequate policies, procedures, and processes in place, it is not a matter of if, but when, the vulnerabilities of an organization will be exploited.

3. Data Theft and Leakage

The physical size and cost of portable storage devices, such as USB drives, will continue to decrease while

the pervasiveness and the risk associated with their use will increase. To their detriment, almost all but the most heavily regulated industries and organizations will continue to effectively ignore the risks associated with the use of these devices, even as reports of laptops, PDAs, flash drives, and data theft continue to appear on the pages of newspapers.

Management needs to formally assess these risks and take sufficient action to help ensure that their financial, proprietary, and customer information is adequately protected and that they do not suffer financial loss or damage to their reputation. Based on the amount of risk senior management is willing to accept, they can choose to allow the uncontrolled use of these devices, implement policies governing their use, or utilize available technology to prevent the use of these devices altogether.

4. Service Provider Issues

As organizations look for opportunities to cut costs, the use of third parties to provide outsourced IT processing, administration, security monitoring, and recovery services will continue to increase. Management will continue to face the risks that the service providers' control environments are inadequate and that management has insufficient processes in place to monitor the service providers' ability to meet their organization's service and control requirements.

Just as with any of their business processes, management should conduct periodic internal audit procedures to determine if their processes to monitor their service providers' performance and controls are adequately designed and effective. A SAS 70 report would be optimal to have in these circumstances, but they are not always available. In their absence, alternative procedures, potentially involving an on-site audit of the service provider, should be performed.

5. End-User Computing Risks

It has been four years since PricewaterhouseCoopers released its influential white paper¹ on spreadsheet controls as they relate to Section 404 of the Sarbanes-Oxley Act, yet misstatements related to lack of adequate controls over end-user computing tools continue to occur. While many consider some of the controls recommended by this white paper to be overly burdensome, ignoring some of its more important and attainable recommendations is foolhardy.

Assuming that the inventory of financially significant end-user computing tools has been identified, adequate security and version control need to be in place along with a sufficient level of both analytical and detailed reviews of the data coming from these tools. If a spreadsheet is too complex for the manual review controls to provide comfort as to the data's completeness and accuracy, then management should consider automating the processes through an existing or new system. This new system should be governed by the controls within a formal system development or change management methodology.

Addressing the Issues: Periodic Internal Audits

In order to gain assurance that the proper security measures have been implemented and are maintained going forward, an organization's Internal Audit department should be charged with performing periodic IT audits, including vulnerability assessments and penetration testing. Any risks identified through these procedures should be prioritized and addressed accordingly. The greatest attention and amount of resources should of course be focused on the highest risks, but this does not mean that lower-risk items

should be ignored or allowed to go unaddressed. A lower risk event that is less likely to occur could still indeed happen, and may have just as significant an impact as a higher-risk item.

It is also important to remember that the technology (i.e., hardware and software) of, threats to, and vulnerabilities of an organization continually change. Therefore it is vital that the frequency and rigor of these IT audits be sufficient.

Conclusion

It may be that through your risk assessment and audit processes you have identified different issues that your organization deems to be of a higher risk. That is not to say that your conclusions are incorrect. In fact, it illustrates that all organizations, whether they be a public company, private company, non-profit organization, or academic institution, differ in their processes, systems, and risk appetites and therefore will never address risks uniformly.

No organization is without its issues. If you are not identifying any threats, vulnerabilities, or risks then you are not looking hard enough or in the right place. Often it is a matter of having a fresh set of eyes or someone with specialized knowledge and a breadth of experience to bring a pragmatic, best practices approach to the organization's risk assessment, management, and IT auditing process— one that will yield the maximum benefit.

*No organization
is without
its issues.*

*Thomas McDermott
IT Manager
J.H. Cohn LLP
tmcdermott@jbcohn.com*

¹ PriceWaterHouseCoopers' white paper titled "The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act" was released in July 2004.

Thomas McDermott
Manager



Thomas McDermott, CISA, is a manager in the Firm's Corporate Governance Services practice and brings to his role over ten years of experience in financial, information technology (IT), security, and internal controls auditing. Tom has been with the Firm since 1997 and is involved in the planning, management, and performance of external, internal, and Sarbanes-Oxley (SOX) compliance audits. He provides specialized services to our clients in a variety of areas, including IT auditing, IT security reviews, e-commerce (Webtrust™), network security, as well as IT general and application controls.

Tom has managed and performed both domestic and international engagements for a number of the Firm's clients. His experience covers a broad range of industries including, but not limited to, manufacturing, retail, financial services, biotechnology, entertainment, and technology.

As a certified information systems auditor (CISA), he is adept in the areas of system development, change control management, information security, computer operations, and disaster recovery. His experience in IT security, IT general controls, and application controls auditing has exposed him to a multitude of applications as well as numerous IT platforms and software environments (e.g., mainframe, mid-range, Windows, server operating systems, Oracle, SAP, PeopleSoft, systems, SQL, and others).

Tom's internal audit and SOX experience spans the entire lifecycle of the control assessment process and leverages the use of the COSO and CobIT frameworks. His involvement includes the planning and management of SOX engagements, the performance and use of risk assessments to develop the engagement approach, the design and implementation of policies and procedures, the development of process flows/narratives and risk control matrices, and the identification and remediation of internal control weaknesses.

Tom also has extensive experience in performing SAS 94 assessments—a specialized audit standard relating to the assessment of the effect of IT on the auditor's consideration of internal control in a financial statement's audit—for a variety of entities, ranging from not-for-profit and manufacturing firms to financial services companies. Additionally, Tom has performed information analysis through the use of audit command language (ACL) to analyze both financial and non-financial data for J.H. Cohn clients in the manufacturing, healthcare, and not-for-profit sectors.

Tom has presented seminars for the New York Society of Certified Public Accountants in information analysis and the use of security tools to analyze organizations' network and system vulnerabilities and the use of ACL and other Computer Assisted Auditing Techniques. He is a member of the Institute of Internal Auditors, the Information Systems Audit and Control Association and has a B.S. in Accounting from Rutgers University School of Business in New Brunswick, New Jersey.

Ranked Among the Top 20 Accounting and Consulting Firms in the United States
www.jhcohn.com 1-877-704-3500



J.H. Cohn LLP is a member of Nexia International, a worldwide network of independent accounting and consulting firms.

How Are You Managing?SM