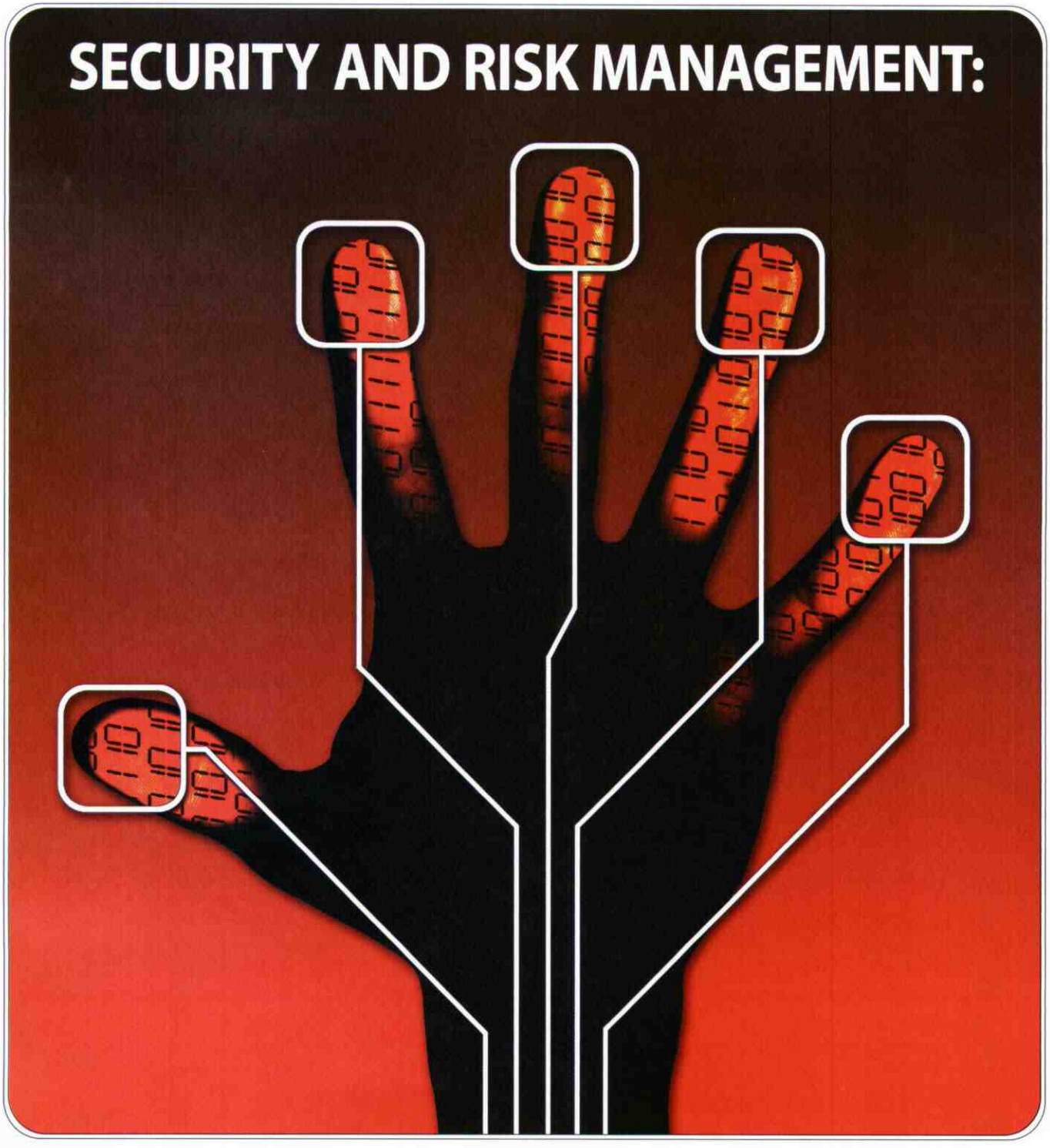
SECURITY AND RISK MANAGEMENT:



A FUNDAMENTAL BUSINESS ISSUE

All organizations must focus on the management issues of security, including organizational structures, skill sets, processes, and methodologies for managing security and risk management

Arthur C. McAdams

According to a report by The Computer Security Institute, 251 of the organizations polled lost $202 million in 2003 due to computer crime. While this loss rate is down from 2002, it is still significant, and many of the companies said they were not able to quantify their losses. International finance and operations executive Oscar Kolodzinski states, "most incidents of cybercrime go unreported because the individuals and businesses affected want to avoid the negative publicity." Therefore, experts believe the real loss is probably greater than stated, and it includes only the losses that are recognized (whether reported or not).

According to Lawrence Gordon and Martin Loeb's article "The Economics of Information Security Investment," there is a void in the research on creating a framework for an economic model that establishes the appropriate investment in security programs. Gordon and Loeb say that most proposed methodologies favor too much spending on certain countermeasures. In "The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officer," Andre Liebenberg and Robert Hoyt note that there is also a dearth of research on enterprise risk management and cite several reasons for an integrated risk management program. If they were aware of it, this information would probably alarm chief executive officers (CEOs) and other leaders enough for them to order further studies.

At the Core

This article

- clarifies the challenge of managing risk in organizations
- provides an organizational framework for successfully managing risk
- describes the evolving role of a chief security officer
- recommends an integrated approach to security using existing methodologies

Security and Risk Management

The American Dictionary of the English Language formally defines "risk" as "the possibility of suffering harm or loss; danger." "Management" is defined as "the practice of managing, handling, or controlling something." The definition of "security" is "freedom from risk or danger." With these terms formally defined, the blended definition roughly describes risk management and security as the practice of controlling and mitigating the amount of loss an organization will have to endure because of any adverse action or situation, whether intentionally or unintentionally initiated. This interrelationship between security and risk management should prompt a convergence that would then lead to a combined effort to address these issues in an integrated manner within an organization.

Organizations have to deal with managing risks as a regular part of conducting business. In the article "Security in Enterprise Systems," published in *The ISSA Journal*, P. Tippet says risk can be defined as "annualized loss expectancy."

Liebenberg and Hoyt note that certain industries have created well-established risk management specialties to address specific types of risk. For instance, a bank may address credit risk with one group of experts, interest rate risk with another, and information risks with yet another group. Ultimately, the organization may have several disparate sub-groups (e.g., facilities, information technology, compliance, human resources), each managing risk by leveraging its own subject-matter experts (e.g., in this scenario – and in any similar situation – the organization will only be as strong as its weakest link).

A painful reality for most organizations is that staff are often more responsible than intruders for data and information loss. According to Ivan Arce and Elais Levy, the workstation offers the most opportunity for exposure in the information technology (IT) area. If an organization has placed updated antivirus and encryption software on the workstation, then it has implemented a single-dimensional level of effort, note S. Liu, J. Ormaner, and J. Sullivan in "A Practical Approach to Enterprise IT Security." If the single-dimension solution were to significantly improve the security of a single component (in this case, the desktop), then something else may become the new weakest link. Therefore, the weakest link may continually shift from the technology area to the physical area, to the human resources area, to the policy area, and so on. Arce and Levy also emphasize the temporal aspect of vulnerabilities. In particular, they suggest that the weakest link can shift from the desktop operating systems to the individuals operating them. Determining the appropriate countermeasures and monetary investment that should be calculated at the highest level in the organization to ensure an effective overall security program is important. Without a high-level view, an organization may over-invest in areas that are not the weakest links.

The Chief Risk/Security Officer

This need for a centralized view of security has led to a worldwide rise in interest in the position of chief risk officer (CRO). In his *Financial Director* article, Elspeth Wales states that there are now more than 200 companies with a board-level CRO, primarily in the financial services sector, with the primary responsibility of integrating credit, market, operational, and economic risk within the organization. This new CRO position, also referred to as chief security officer (CSO), is still developing as the need to address the entire organization, or enterprise, gains attention. For instance, Liebenberg and Hoyt cite an organization's ability to improve both strategic and operational decision-making (especially in highly leveraged organizations), which leads to improved earnings, decreased costs, and lowered stock volatility, through the implementation of a formal enterprise risk management position. The CSO may report to the CEO, the chief financial officer (CFO), the chief legal executive, the chief operating officer (COO), or any other executive-level officer. This placement varies by industry and by importance of security within a specific organization.

James Lam lists the following responsibilities for CROs:

- Provide overall leadership
- Establish an integrated framework
- Develop policies
- Implement metrics
- Allocate capital to business activities
- Develop training programs
- Develop support systems for the program

These responsibilities can fall directly on one security officer individual in the security department.

Finally, the appointment of a high-level risk manager shows some shift from the normal defensive risk position to a more offensive and strategic position.

Discussion of security falls into two categories: high-level awareness and low-level technology solutions. The former category relates to the general understanding of security, executive-level strategy, regulations, and corresponding policies on security; the latter refers to tactical single-point technology solutions such as antivirus software and firewalls. Building a bridge between the two extremes is a challenge for CSOs. In an *IT Pro* article, "Post 9-11 Security: Few Changes, Business as Usual Rules," L. Paulson says this dilemma is further exacerbated because many middle managers have no incentive to raise awareness as they fear that this might put their jobs at risk.

Paulson also points out that part of the communication challenge is related to the ironic state of affairs in that an effective security program is transparent to the organization. Ideally, a good security program protects corporate assets without hindering productivity or placing too much burden on employees or customers. The responsibility of communicating these ideals to the organization's top executives falls on the organization's senior security officer.

Communication skills are important for security officers because many security practitioners and researchers believe that an effective security program must start at the top of the organization. In the article "Five Dimensions of Information Security Awareness," Mikko Siponen states that awareness is the first dimension to be addressed, and soliciting senior-level commitment from management and gaining clarity on the requirements and components is critical to success.

In their book, *Principles and Practices of Information Security*, Linda Volonino and Stephen Robinson echo Siponen's assertion that getting management's attention and commitment to embrace organizational risk management is the first step in addressing the security issue. In this scenario, Paulson says an organization could embrace security as a core value much like customer service rather than merely as an adjunct support activity. With the support and commitment of senior management, the organization would be adequately prepared to build an organizational structure to facilitate the design and implementation of a robust security program. Top management may realize a strategic-level commitment to customers' information.

In his 2003 *CSO* magazine article, Thornton May states that CSOs need to learn how to market their product in the same way that chief information officers (CIOs) sell technology-related projects. CIOs educate and align themselves with the business executives in a way that makes every technology project a business project. Using this thinking, May explains that security officers need to do the same. May says it is ironic that security officers cannot sell security-related projects at a time when security has garnered a significant amount of general awareness that has been further bolstered by the news media. In fact, the disconnect may be similar to the situation faced by IT leaders seven years ago concerning the Y2K issue, which was initially viewed as a technical issue, not a business issue, and this led to ambiguous ownership and sponsorship of the problem. The Y2K effort improved measurably once the emphasis shifted to business. The CSO needs the skills to lead the transition from security projects to business projects. Given the importance of organizational knowledge for market leverage and competition, top mangers should see the need to protect "leaky" knowledge sources.

According to S. Hazari's article "Reengineering an Information Security Course for Business Management Focus," educators are beginning to change security courses to expand this new holistic view of security to include topics such as encryption, physical security, risk analysis, and human compliance. In this scenario, Hazari notes that a security manager must be knowledgeable in a wide array of skills, which include technology, policy and legal matters, and softer skills such as communication and management. CSOs lacking business acumen will run the risk of being viewed as narrow, single contributors, which may ultimately limit the security program to a technical problem.

The evolution of a security manager beyond a single specific skill has similarities to other disciplines (technology and finance), which now commonly have a chief position within an organization. For instance, Carol Brown's article "The Successful CIO: Integrating Organizational and Individual Perspectives" asserts that the gradual shift from data processing manager (with a purely technical skill set) to CIO, which calls for forging partnerships across the organization and more of a governing role than a dictating role. In his *Research Technology Management* article "The Chief Technology Officer: Strategic Responsibilities and Relationships," Roger Smith echoes this need for skills in business strategies for emerging CTOs as a leading success indicator.

Finally, the CFO role has gone "beyond bean counting," according to P. Favaro's *Strategy and Leadership* article. Favaro states that the role of the leader in finance has expanded from keeping tabs on the money to becoming a strategic member of the executive team and a visionary capable of communicating and providing a framework for financial governance within the organization.

These examples may serve as good indicators of what the CRO's role will evolve into over the next few years.

Security Standards and Methodologies

Even with the role of a CSO established, it is still challenging to integrate security within the organization's processes. For instance, in his *Darwin Magazine* article "Calculating an ROI for Data Security," Larry Ponemon says the interrelationships between the people, the IT infrastructure, and the business processes create the greatest challenge to understanding risk valuation. This is an extremely difficult task given the limited research on security issues within processes and work systems.

Fortunately, there are predefined methodologies for addressing the management of security. One comprehensive standard is ISO 17799, which offers a template for guiding an organization to a successful security program. In his article "ISO 17799: A Standard for Information Security Management," M. Hoffman writes, "improving information security is at the forefront of every IT decision-maker's mind. But tackling this task without a sound framework can be overwhelming. It doesn't have to be with ISO 17799."

In "The Unlikely Heroes of Cyber Security," ISO 17799 is praised because it helps security experts make professional, consistent assessments of organizations for insurance purposes. According to the article, "Some insurance providers regard ISO 17799 as the most important tool organizations have for meeting cyber insurance coverage requirements," and in almost all cases insurance companies require organizations to follow the ISO 17799 guidelines. It is hard to imagine that a resource as important as information – with massive amounts of it coursing through, into, and out of the organization – could be treated in what is often a cavalier approach with regard to the cyber placement issues focused on hard equipment.

Hoffman asserts that ISO 17799 calls for the following 10 security controls:

- *Information security policy* – helps management define what security means to the organization
- *System access control* – detects and prevents unauthorized access to information, computer areas, and mobile users
- *System development and maintenance* – ensures that controls are in place for every stage in the life cycle of an application
- *Personnel security* – emphasizes reducing exposure to human error as well as fraud, theft, and misuse of company property
- *Physical and environmental security* – addresses physical access to certain areas and items such as workstations
- *Security organization* – addresses the roles and responsibilities for key security personnel and any ongoing committees required to maintain the organization's security program
- *Asset classification and control* – ensures that the organization has the tools and practices to protect its assets
- *Communications and operations management* – focuses on the organization's operational procedures, change control, incident management, segregation of duties, capacity planning, etc.
- *Business continuity management* – includes building a business continuity plan, testing the plan, and building processes to ensure that it is maintained
- *Compliance* – ensures that the organization meets its regulatory requirements, does not violate any laws, and follows its internal policies

This established standard is invaluable to a CSO because it frames the security program in a universal manner. The CSO will probably need to customize the framework to match the individual needs of the organization, but the basic structure can remain the same. The CSO is the primary architect, and a well-designed security program will significantly improve the likelihood of a successful implementation effort, much the same way good technical architectures will provide foundation for successful application systems.

Organizational Synergy

Integrating security into the organization and hiring the best people is the most important part of building a security program, notes Mathew Schwartz in his article "Put a Good Security Staff in its Place." Schwartz says the CSO must present a cohesive view of the security program to the executives and must develop a security program that does not encourage organizational fiefdoms. Therefore, the CSO must prevent building organizational silos within the security department while implementing a security program. For instance, the security department would develop work requests for the various departments (e.g., IT, facilities) that are required to satisfy the security issue. In this way, the security department will focus on its expertise and source the other work to the appropriate areas.

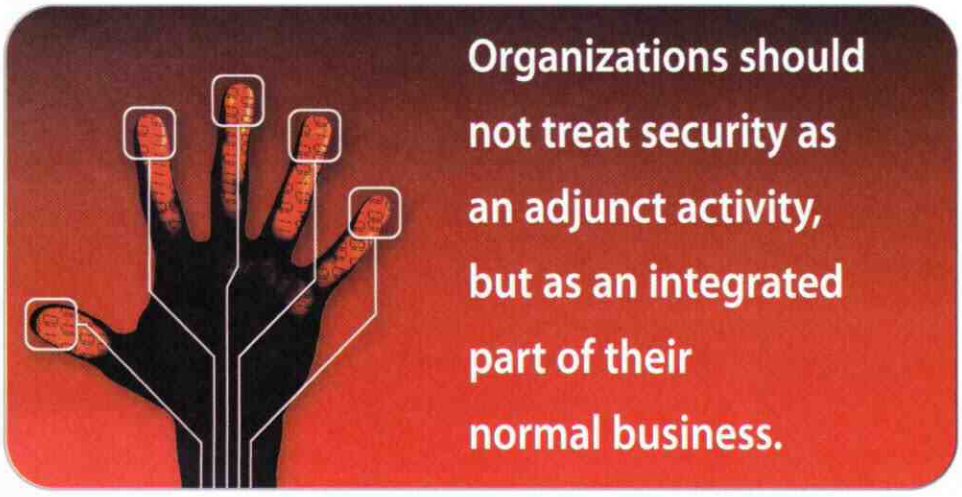
Ponemon suggests five steps to prioritize security spending:

- Assessing vulnerabilities to the infrastructure
- Understanding the risks of regulatory non-compliance
- Understanding employee-related risks

- Determining the cost of business interruption
- Measuring compliance to the security program

Many of the steps require quantifying risk and valuating corporate assets, including intellectual property. The CSO may need to leverage the existing knowledge and structures within the finance department rather than build a new finance area in the security department, suggest D. Geer, K. Hoo, and A. Jaquith in their article "Information Security: Why the Future Belongs to the Quants."

The risk manager, with the help of other subject matter experts, will then need to quantify the threats and vulnerabilities. In their article "IT Security Is IT Risk Management," B. Blakley, D. Geer, and E. McDermott note that this process includes technology, processes, and physical mechanisms, and it should reduce the probability, as well as seek to minimize the magnitude of any adverse event. Research and experience also point to internal sources as a high-risk area (including mistakes and ignorance) and should not be ignored during this step, according to M. Whitman's article "Enemy at the Gate: Threats to Information Security." The CSO will need to establish roles and responsibilities as well as the terms of engagement among the security department and the other departments to manage these aspects of security effectively.



In addition to defining the security culture and facilitating the quantified risk formula, the CSO is charged with building the security policies. These policies should align with the organizational culture, which should be improved by the CSO's direct access to the CEO, assert T. Begley and D. Boyd in "Moving Corporate Culture Beyond the Executive Suite." Also, the policy must be legally sound and immaculately consistent in its writing and enforcement, according to F. Nah, K. Siau, and L. Teng's "Acceptable Internet Use Policy." This effort will require interaction with the legal department. Once completed and approved, the security program should be disseminated throughout the organization as an awareness phase, which outlines employees' responsibilities and mechanisms for reporting violations, note S. Liu, J. Ormaner, and J. Sullivan in their article "A Practical Approach to Enterprise IT Security." Heightened communication may leverage an existing corporate mechanism, such as human resources or corporate communications.

With this framework set, security-related matters should continue to follow the normal path that the organization uses for implementing initiatives. For instance, in "How to Improve Your IT Security Policy: A Six Sigma Approach," Karen Avery and Gary Lynch suggest bringing security into the organization's continuous improvement program to ensure the security program is assignable, executable, enforceable, and measurable. In other words, organizations should not treat security as an adjunct activity, but rather as an integrated part of their normal business. In this manner, an organization could add security into the project management methodology as a mandatory step rather than an afterthought at the end of a project. A continuous improvement methodology could be employed after the initial implementation to ensure the program stays current.

The Software Engineering Institute (SEI) recommends the following ongoing steps: identify, analyze, plan, track, and control, with communication as the common thread. In this case, according to J. Lanz, security could be analyzed along with availability, integrity, and maintainability. Similarly, the return on investment (ROI) phase of a project would be handled using the normal people and processes.

Calculating ROI on security projects is a subject unto itself, but the process of calculating ROI for the organization should be consistent with other efforts. Risk and security could also be introduced into the system development methodology to ensure risk is addressed during every phase of the effort, contends S. Maguire in "Identifying Risks During Information System Development: Managing the Process." Appropriate technology choices should follow the risk analysis and the policy, which should follow the appointment of a senior-level security officer.

The specific methods and technologies used are not the most important factors in successful risk management. Rather, success is driven by business needs, and successful implementation should leverage the existing processes and expertise within the organizational structure to ensure a consistent, sustainable, and enterprise-wide solution. Things that also must be addressed include details of the policy, the asset valuation (acknowledging the difficulty with intangible items), IT production procedures, and the technology applied to mitigate the threats and vulnerabilities.

It may be time to stop treating security and risk management as separate activities that cannot be integrated into any current organizational structures. Research shows that the best solution calls for a primary sponsor and owner (CRO or CSO) to lead the organization with business savvy and general governance while blending with the culture and operating environment. This structure and integrated implementation methodology would lead to a process-oriented solution versus a silo-based, task-oriented approach. The latter relies on the individual efforts of a few security professionals and creates duplication and possible gaps in the overall organizational work system. By integrating security and risk management into the organization and its ongoing processes, these important functions will become a way of doing business.

***Arthur C. McAdams**, Adjunct Professor at Fairfield University in Fairfield, Connecticut, is a strategic architect, general manager, educator, and author with experience working in large corporations, small businesses, and academia. He also worked as the Chief Information Officer for Strategic Security Computing in Bridgeport, Connecticut. He may be contacted at* amcadams@stagweb.fairfield.edu.

References

Arce, Ivan and Elais Levy. "The Weakest Link Revisited." *IEEE Computer Society.* March/April 2003.

Avery, Karen and Gary Lynch. "How to Improve Your IT Security Policy: A Six Sigma Approach." CXO Media Inc. 2002. Available at *www.cioinsight.com/article2/0,3959, 1217371,00.asp* (accessed 29 April 2004).

Begley, T. and D. Boyd. "Moving Corporate Culture Beyond the Executive Suite." *Corporate Governance.* 2002.

Blakley, B., D. Geer, and E. McDermott. "IT Security is IT Risk Management." *NSPW'01.* September 2002.

Brown, Carol. "The Successful CIO: Integrating Organizational and Individual Perspectives." *Association for Computing Machinery.* 1993.

"Cyber Attacks Continue, but Financial Losses Are Down." Computer Security Institute. 2003. Available at *www.gocsi.com/awareness/fbi.jhtml* (accessed 29 April 2004).

Favaro, P. "Beyond Bean Counting: the CFO's Expanding Role." *Strategy and Leadership.* September/October 2001.

Geer, D., K. Hoo, and A. Jaquith. "Information Security: Why the Future Belongs to the Quants." *IEEE Security and Privacy.* July/August 2003.

Gordon, Lawrence, and Martin Loeb. "The Economics of Information Security Investment." *ACM Transactions on Information and Systems Security.* November 2002.

Groves, Shanna. "The Unlikely Heroes of Cyber Security." *The Information Management Journal* 37. May/June 2003.

Hazari, S. "Reengineering an Information Security Course for Business Management Focus." *Journal of Information Systems Educator* 13. 2002.

Hoffman, M. "ISO 17799: A Standard for Information Security Management." The Info-Tech Research Group. 2003.

Kolodzinski, Oscar. "Cyber-Insurance Issues: Managing Risk by Tying Network Security to Business Goals." *The CPA Journal.* November 2002.

Lam, James. "Enterprise-wide Risk Management and the Role of the Chief Risk Officer." *ERisk.* 2000. Available at *www.erisk.com/Learning/Research/011_lamriskoff.pdf* (accessed 28 April 2004).

Lanz, J. "Worst Information Technology Practices in Small to Mid-Size Organizations." *The CPA Journal.* April 2002.

Liebenberg, Andre and Robert Hoyt. "The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officer." *Risk Management and Insurance Review* 6. Spring 2003.

Liu, S., Ormaner, J., & Sullivan, J. "A Practical Approach to Enterprise IT Security." *IT Pro.* September/October 2001.

May, Thornton. "Why Security Needs to Blow Its Own Horn." CSO. June 2003. Available at www.csoonline.com/read/060103/horn.html (accessed 28 April 2004).

Maguire, S. "Identifying Risks During Information System Development: Managing the Process." *Information Management and Computer Security.* 2002.

Nah, F., K. Siau, and L. Teng. "Acceptable Internet Use Policy." *Communication of the ACM* 45. January 2002.

Paulson, L. "Post 9-11 Security: Few Changes, Business as Usual Rules." *IT Pro.* July/August 2002.

Ponemon, Larry. "Calculating an ROI for Data Security." *Darwin Magazine.* 2003. Available at *www.darwinmag.com/read/090103/ secureroi.html* (accessed 28 April 2004).

Robinson, Stephen and Linda Volonino. *Principles and Practices of Information Security.* Upper Saddle River, N.J.: Pearson Prentice Hall, 2004.

Schwartz, Mathew. "Put a Good Security Staff in its Place." *101 Communications LLC.* 2002. Available at *www.esj.com/Columns/article.asp?EditorialsID=62* (accessed 28 April 2004).

Siponen, Mikko. "Five Dimensions of Information Security Awareness." *Computers and Society.* June 2001.

Smith, Roger. "The Chief Technology Officer: Strategic Responsibilities and Relationships." *Research Technology Management* 46. July/August 2003.

Tippet, P. "Security in Enterprise Systems." *The ISSA Journal.* August 2003.

Wales, Elspeth. "Rise of the Chief Risk Officer." *Financial Director.* 2002. Available at *http://financialdirector.co.uk/Features/1128771* (accessed 28 April 2004).

Whitman, M. "Enemy at the Gate: Threats to Information Security." *Communications of the ACM* 48 (August 2003).