Information Security Governance: Toward a Framework for Action

BSA

Business Software Alliance

Information Security Governance: Toward a Framework for Action

As the barrage of information security intrusions and losses has escalated, so too has the number of information security reports, laws and regulations. According to Carnegie Mellon University's CERT Coordination Center, the quantity of cyber security incidents reported has roughly doubled every year since 2000 – jumping from nearly 22,000 incidents for all of 2000 to 76,000 in the first half of 2003 alone. A survey of the literature reveals that this increase has been mirrored in the growth of reports and guidelines. Congress and state legislatures have responded with several major information security bills and are considering more.

Given this activity, why hasn't more progress been made to secure our information systems? After all, the problem is well known; many solutions have been proposed; the technologies are proven and readily available; and the consequences of inaction are becoming clearer every day.

The Business Software Alliance formed the Information Security Governance Task Force with that question in mind. Our goal is to frame a response in terms that organizations can understand and readily implement. We are committed to delivering quality software that enhances the security of our customers, but are convinced that technology alone cannot address all of our needs. Ultimately, information security is not solely a technical issue, but a corporate governance challenge. While there is broad consensus on the actions needed to create strong security, too often responsibility is left to the chief information officer or the chief information security officer. In fact, strong security requires the active engagement of executive management. By treating these challenges as a governance issue and defining specific tasks that employees at all levels of an organization can discharge, enterprises can begin to create a management framework that will lead to positive results.

In this white paper, we have distilled the lessons contained in other policy reports, legislation, and guidelines and found broad consensus on what needs to be done. In order to ensure that these policies are more effectively implemented, we have developed a preliminary information security governance framework for action that outlines specific roles for business unit heads, senior managers, CIOs, and the CEOs themselves. By doing so, we hope to more actively engage executive management and government policymakers, and to advance the public-private partnerships that are necessary to make real progress. BSA will work closely with other industry groups and with government to refine and advance this framework.

Bill Conner

Bill Conner
Chairman and CEO
Entrust, Inc.
Task Force Co-Chair

Tom Noonan
Chairman and CEO
Internet Security Systems
Task Force Co-Chair

Robert Holleyman

Robert W. Holleyman, II
President and CEO
Business Software Alliance

Executive Summary

Because today's economy depends on the secure flow of information within and across organizations, information security is an issue of vital importance. A secure and trusted environment for stored and shared information greatly enhances consumer benefits, business performance and productivity, and national security. Conversely, an insecure environment creates the potential for serious damage to governments and corporations that could significantly undermine consumers and citizens. For firms engaged in critical activities, such as electrical power generation, banking and finance, or healthcare, the stakes are particularly high.

Where do we stand in the effort to bolster information security? If the stakes are so high, why haven't we made more progress? In attempting to answer these questions, the task force identified four findings.

Findings:

1. ***Government has already established a significant legislative and regulatory regime around IT security, and is considering additional action.*** Many companies are actively addressing their information security needs. What is not as widely recognized is the fact that Congress and state governments have already passed into law several bills that govern how companies must address information security issues.

2. ***Information security is often treated solely as a technology issue, when it should also be treated as a governance issue.*** The CIO alone cannot remedy the problem; the board of directors and executive management must also be actively engaged.

3. ***There is already broad consensus on the actions necessary to remedy the problem.*** A review of literature shows that most guidance documents and other reports recommend a common solution and support the approach reflected in ISO 17799 and the Federal Information Security Management Act (FISMA).

4. ***Lack of progress is due in part to the absence of a governance framework.*** If progress is to be accelerated, a management framework that instructs personnel at different levels about how to implement solutions is crucial.

Each of these findings is discussed in more detail below.

Recommendations:

1. Government and industry should recognize that a significant regulatory regime already exists for information security. Some laws address information security directly; others address it indirectly through such issues as financial governance, privacy, or reporting requirements. Taken together, they have a broad impact on the US private sector, and companies should begin developing programs to comply with them. A summary of these laws is provided in Table 1.

RECENT LEGISLATION	WHO IS AFFECTED?	WHAT DO THE SECURITY PROVISIONS COVER?	WHAT ARE PENALTIES?	WHEN IS IT IN EFFECT?
Sarbanes-Oxley Act of 2002	All public companies subject to US security laws	Internal controls and financial disclosures	Criminal and civil penalties	Current law
Gramm-Leach-Bliley Act of 1999	Financial institutions	Security of customer records	Criminal and civil penalties	Current law
Health Insurance Privacy and Accountability Act (HIPAA)	Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties	Final security rule takes effect in April 2005
California Database Security Breach Information Act (SB 1386)	State agencies, persons, and businesses that conduct business in the State of California	Reporting of breaches of unencrypted personal information	Civil fines and private right of action	Current law
Federal Information Security Management Act	Federal agencies	Federal information, information systems, and security programs	Loss of IT funding	Current law
Bottom Line	**Significant impact on US private sector and governments**	**Financial, customer, health, personal and government information**	**Criminal and civil penalties and private right of action**	**Most provisions are already in effect**

Table 1: Impact of Recent Information Security Legislation

2. Industry should develop an information security governance framework that organizations can readily adopt. The Federal Information Security Management Act (FISMA) and International Standards Organization (ISO) 17799 serve as good inputs to this framework. FISMA provides a management template for federal government agencies that can be adapted to private sector needs. ISO gives broad guidance for implementing information security, but must be tailored to fit each company's needs according to their risk assessment.

To promote this effort, the task force has developed a preliminary governance framework, for comment and refinement by public and private organizations. A summary of the framework is provided below. A more complete discussion is provided in Table 4 on page 7. A variety of related activities are being undertaken by other organizations, and this effort is designed to complement those activities. BSA will work closely with other industry groups and with government to refine and advance this framework.

Actors/Actions	**Corporate Executives**	**Business Unit Head**	**Senior Manager**	**CIO/CISO**
Governance/Business Drivers	***What am I required to do?*** ***What am I afraid not to do?***			
Roles and Responsibilities	***How do I accomplish my objectives?***			
Metrics/Audit	***How effectively do I achieve my objectives?*** ***What adjustments do I need to make?***			

Table 2: Preliminary Governance Framework

Information Security Governance: Toward a Framework for Action

Detailed Discussion of the Four Findings

1. Government has already established a significant legislative and regulatory regime around IT security, and is considering additional action.

Information security is important. Companies and individuals want more security in the products and networks they buy. Vendors are responding with more secure products. Industry and consumers alike recognize the need for information security – consumers from the viewpoint of keeping their information private and businesses from the perspective of its importance to long-term growth of the IT sector. Even though there is a heightened awareness of the importance of security, many factors have contributed to the perception that progress has been slow. For example, the cost of security is not cheap and demonstrating return on security investment is sometimes difficult. The good news is that industry and government are actively engaged in addressing the information security challenge.

Increasing public concern has not only prompted industry to begin to work on this problem, but also has led legislatures to take action. Three examples serve to illustrate. On the national level, the Public Company Accounting Reform and Investor Protection Act (also known as Sarbanes-Oxley) requires firms to certify as to the integrity of their financial records, their information disclosure controls, and internal controls. This certification arguably cannot be made without serious attention having been paid to electronic information security.

A second national law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), established standards for protecting health information about individuals. A principal motivation behind HIPAA was concern about the possible privacy impact on individuals of unauthorized sharing of personal health information. The Department of Health and Human Services recently issued detailed computer security regulations that organizations handling personal health information must follow.

On the state level, California's Database Security Breach Notification Act, which went into effect in July 2003, requires companies to notify customers if they believe a systems breach has led to the release of their personal information.

As concern about the issue continues to grow, more attention and action by legislators and regulators can be expected. Recent identity theft cases in both the private and public sector have caused some in Congress to discuss whether legislation is necessary at the federal level. Senator Dianne Feinstein of California is considering a bill modeled after her state's law. There also have been discussions in Congress on whether disclosure of information security vulnerabilities by companies should be mandated by Congress or required by the SEC.

Thus far, the Bush Administration has taken a non-regulatory approach to information security. It recognizes that private companies on the front lines are best equipped to deal with the challenge and has encouraged companies to voluntarily share information on security breaches, while opposing legislation to force companies to report such incidents. That course could change if there is a major cyber attack that damages national critical infrastructure. Areas where regulation may occur include deployment by companies of specific security measures, reporting on intrusions, and reporting of vulnerabilities.

These laws and regulations, and the potential of additional government intervention, create uncertainty about the costs of compliance and potential liability. As with any uncertainty, this may have the effect of limiting investment by firms in advanced technologies, slowing productivity growth, and reducing the availability of electronic services to citizens and consumers. Additionally, because organizations vary greatly in size, the kind of information they handle, their exposure to threats, and the complexity of their information systems, no uniform regulatory regime can efficiently enhance information security across the board. Indeed, regardless of legislation, regulation, or other guidance, there is no substitute for the effective and consistent application of sound risk management practices at the operational level.

2. Information security is often treated solely as a technology issue, when it should also be treated as a governance issue.

In looking at the growing abundance of rules, regulations, and guidelines, it quickly becomes clear that information security is not solely a technical issue, but a corporate governance challenge.

Businesses today face increased scrutiny when it comes to corporate governance, accountability, and ethics. Laws such as Sarbanes-Oxley are creating a legal obligation at the CEO and board level to pay attention to information security. Two years ago, the National Association of Corporate Directors, in collaboration with the Institute of Internal Auditors and the government's Critical Information Assurance Office, published "Information Security Oversight: Essential Board Practices." The report advised that, "In any organization, directors need to ensure that managers take all necessary measures to secure key information and the systems and networks that store, manipulate, and transmit it. Furthermore, the directors need to ensure that these efforts are continuously underway."

Implementation of an effective IT security program is ultimately a matter of enlightened organizational self-interest. Companies are taking action to protect their own information and information entrusted to them by customers, suppliers, and other partners. They are establishing responsibility for information security in their companies and adopting programs to evaluate and address the vulnerabilities and the internal and external threats to their electronic information.

However, within many organizations, two important barriers to effective computer security exist:

- First, responsibility is too often delegated to the chief information officer or the chief security officer, who suffer conflicting demands with regard to IT functionality and costs and who may not be in a position to leverage the resources and authority necessary to address the problem across multiple business lines or divisions. Because all too often little attention is given to this issue at the CEO or board level, information security efforts are frequently under-funded in proportion to the risk and magnitude of the harm that incidents could produce. Responsibility for the right level of security is a business decision based on risk assessment.

- Second, is the lack of a framework for action – how to set priorities, assign tasks, get started, and monitor implementation. To aid organizations in attacking the problem, numerous guides have been developed. These documents range from detailed technical guidance to high-level principles. But there is no recognized, standard approach at an organization-wide level to help determine what should be done and who should do it. Without such an approach, firms are unclear how to allocate information security funding and energy, and how to measure the return on investment.

The advice of the National Association of Corporate Directors, a leading authority on corporate governance, is all the more true today. To make real progress, firms must address information security, not solely as a technology issue, but as a matter of "corporate best practices" (covering people, processes, and technology) and frame solutions in terms that are broadly relevant to business operations.

3. There is already broad consensus on the actions necessary to remedy the problem.

A thorough review and analysis of the existing literature leads to three conclusions:

- First, remarkable convergence exists across the documents regarding recommended security practices. There is a broad consensus among the experts as to what kinds of measures should be undertaken by organizations.

- Second, no single document provides the necessary governance framework for information security. The existing guidance is either too detailed or not actionable in a comprehensive manner from the top to bottom of an organization.

- Third, ISO/IEC 17799 and FISMA provide a good substantive basis for creating such a framework. However, the current version of ISO 17799 is overly detailed for CEO consumption and application, and FISMA, as written, is too detailed and government-specific to be applied uniformly across all organizations.

Various initiatives, both in the private sector and in government, have addressed the issue of security program management. These initiatives describe proposed management structures, give security checklists, offer best practices, and, in the case of government – legislation. Because the ultimate goal of BSA's analysis of IT security governance documents and activities was to identify or develop a governance framework without duplicating existing work, a key component of the project was the completion of a survey of existing governance and framework documents.

The first part of the effort was the identification of those documents that address the need for a framework for IT security governance in public and private sector enterprises. Indeed, many worthwhile and comprehensive documents emerged during this phase of the project. Publications included in the study are listed in Appendix 1. Once this body of literature was identified, criteria were developed to assess the applicability and coverage of each document.

The analysis was seeded with two primary "reference" documents – the international standard ISO/IEC 17799 Code of Practice for Information Security Management and the newly minted Federal Information Security Management Act (FISMA). Additionally, the National Institute of Standards and Technology's (NIST) Special Publication on Generally Accepted System Security Principles and Practices (GSSP) was also used as a baseline for the analysis. These sources were selected as reference documents because of their comprehensive coverage of the subject matter and their level of general acceptance in the IT security community.

The ISO standard is a benchmark recognized internationally and used by multiple industries, from finance to healthcare, to define IT security effectiveness. This document serves as the baseline reference for the people-operational, people-tactical, process-operational, process-tactical, technology-operational, technology-tactical, and technology-strategic dimensions of the matrix. The ISO standard is extremely detailed at the operational level yet is vague about senior management responsibilities.

FISMA contains high-level management guidance that assigns responsibility at appropriate levels for specific aspects of an organization's information security program. FISMA is used as the baseline reference for the people-strategic and process-strategic dimensions of the matrix. While it is too detailed and government-specific to be directly applied to private sector organizations, it provides a useful benchmark at the strategic level.

The NIST document, an anchor in most government security programs, was used in concert with the other baseline references.

The contents and recommended practices proposed by these publications were examined in detail. The analysis can be conceptually depicted by a three-by-three matrix having the dimensions of people-process-technology and operational-tactical-strategic. The people-process-technology side of the matrix refers to type: people (who), process (how), and technology (what). The operational-tactical-strategic side of the matrix refers to the extent of the strategic nature of recommendations: operational (daily), tactical (review/follow-up), and strategic (annual reviews, establishing policies, organizational view).

	Operational	Tactical	Strategic
People	Ref = ISO 17799	Ref = ISO 17799	Ref = FISMA
Process	Ref = ISO 17799	Ref = ISO 17799	Ref = FISMA
Technology	Ref = ISO 17799	Ref = ISO 17799	Ref = ISO 17799

Table 3. IT Security Governance Document Analysis

Nearly 20 information security initiatives were reviewed. The documents were analyzed using a set of comparative criteria. These criteria included scope, comprehensiveness, level of detail, intended audience, acceptance, impact, transparency, inclusiveness of the development process, the type of sponsoring organization, and the maturity of the effort.

The documents examined fall into three categories: (1) Information Security as a Fundamental Governance Issue; (2) Organizing for Information Security—Essential Program Components; and (3) Governance Documents Under Development.

The first category of documents, "Information Security as a Fundamental Governance Issue," reflects the initiative of the Critical Infrastructure Assurance Office (CIAO), then of the Department of Commerce, to frame IT security as a significant management challenge for public and private sector organizations. Beginning in 1999, the CIAO, in association with a variety of groups (such as the National Association of Corporate Directors (NACD), the Institute of Internal Auditors (IIA), the IT Governance Institute, and others), instituted a program intended to frame IT security as a fundamental governance issue. Several documents stressing this theme were prepared and widely circulated. In 2000, the CIAO, in association with the NACD and the IIA, sponsored a White House conference on the subject. The White House conference was subsequently followed by a series of "summit conferences" and focus group meetings held throughout the country. In 2002, the federal government built on this work by creating the National Strategy to Secure Cyberspace, which states:

> "The cyber security of large enterprises can be improved through strong management to ensure that best practices and efficient technology are being employed…" (page 39)

When viewed in their entirety, the documents represent an important landmark in the evolution of the IT security governance problem. They are very strong on identifying the IT security problem and the need to address this as a fundamental management challenge. But these documents do not provide the necessary framework for the establishment and operation of an enterprise-wide IT security program.

The second category of documents, “Organizing for Information Security,” is focused on the practical aspects of actually implementing an organizational IT information security program. These documents present valuable insights into what programmatic elements should be included in such a program. Each publication represents an important contribution to the evolving field of information security.

Several other efforts to develop guidance are being undertaken by various public and private sector groups. It is hoped that these forthcoming efforts will also build upon the foundations established by previous efforts and will provide a further impetus for convergence among all parties as to the appropriate framework for organizational IT security governance.

4. Lack of progress is due in part to the absence of a governance framework.

With such a broad consensus on the kinds of measures that need to be taken to secure our information systems, why haven’t we made more progress? The conclusion of the BSA task force is that we are still missing a vital piece of the puzzle – an information security governance framework that private industry can readily adopt. Governance entails the systematic oversight and execution of information security functions. As a result, it operationalizes the information security effort. By themselves, recommended practices – no matter how strong the consensus is for them – are not enough; they must be married with an information security governance framework that assures effective implementation. What many of the reports on information security overlook is that a well-developed information security governance framework already exists in the form of the Federal Information Security Management Act (FISMA). This framework was developed for the Federal government. While overly detailed for the private sector, its principles can be applied to all organizations. It is especially good at defining the people and process aspects of information security governance, which is exactly where many of the reports on this topic fall short.

Purpose of a Governance Framework

A governance framework is important because it provides a roadmap for the implementation, evaluation and improvement of information security practices. An organization that builds such a framework can use it to articulate goals and drive ownership of them, evaluate information security over time, and determine the need for additional measures. One of the most important features of a governance framework is that it defines the roles of different members of an organization. By specifying who does what, it allows organizations to assign specific tasks and responsibilities. A common element in almost all security best practices is the need for the support of senior management, but few documents clarify how that support is to be given. Fortunately, FISMA does. Adapting the FISMA management framework to the private sector provides the missing link to industry’s information security efforts. FISMA divides management functions into four categories, which, translated into business terms, are the following: 1) CEO, 2) business unit heads, 3) senior managers, and 4) the CIO/CISO. The security governance role of each is described below:

<u>The CEO</u> (or most senior executives who report to the board of directors) has responsibility for

- Oversight and coordination of policies

- Oversight of business unit compliance
- Compliance reporting
- Actions to enforce accountability

The business unit head (or executives with bottom-line responsibilities) has responsibility for

- Providing information security protection commensurate with the risk and business impact
- Providing security training
- Developing the controls environment and activities
- Reporting on effectiveness of policies, procedures and practices

The senior manager (those reporting to the business units heads) has responsibility for

- Providing security for information and systems
- Periodically assessing assets and their associated risks
- Determining appropriate levels of security for the information in their systems
- Implementing policies and procedures to cost-effectively reduce risk to acceptable levels
- Periodically testing security and controls

The CIO and/or CISO (or most senior manager with IT security responsibilities) has responsibility for

- Developing, maintaining, and ensuring compliance to the security program
- Designating a security officer with primary duties and training in IT security
- Developing the required policies to support the security program and business unit specific needs
- Developing the information use and categorization plan
- Assisting senior managers with their security responsibilities
- Conducting security awareness program

The Components of a Security Governance Framework

FISMA also specifies the core components required in a security program, as do many other documents, including ISO/IEC 17799. To be effective, however, each information security program must be tailored to the needs of the individual business and industry in which it operates. What is needed is a framework that specifies what corporate executives, business unit heads, senior managers, and CIOs/CISOs should do; that identifies business drivers, clarifies roles and responsibilities, recognizes commonalities and defines metrics; and that is flexible enough to apply to different business models.

We have provided the beginnings of such a framework below in a brief but comprehensive chart. (See below.) The horizontal axis identifies different management levels. The vertical axis identifies the business drivers, responsibilities, and metrics. It is important to note that the first and third criteria on the vertical axis (Governance/Business Drivers and Metrics/Audit) are specific to individual businesses and will change according to individual business and industry needs. For example, the governance and business drivers for the financial sector will likely differ from those of the health care industry as will the metrics used to calibrate their results. By contrast, the middle item (roles and responsibilities) is common to almost all businesses and thus can be widely applied.

The task force identified that considerable additional work is needed to develop useful metrics that enable managers to quantify the return on investments in information security and the effectiveness of information security programs and measures. Several public and private sector organizations are investigating this field. The task force looks forward to the products of those efforts.

Toward a Framework for Action on Information Security Governance

Actors\Actions	**Corporate Executives**	**Business Unit Head**	**Senior Manager**	**CIO/CISO**
Governance/Business Drivers These tend to be sector- or organization-specific.)	***What am I required to do? / What am I afraid not to do?***			
	Legislation, ROI	Standards, policies, budgets	Standards, audit results	Security policies, security operations, and resources
Roles and Responsibilities (These tend to be generic across industries and organizations.)	***How do I accomplish my objectives?***			
	• Oversight and coordination of policies • Oversight of business unit compliance • Compliance reporting • Actions to enforce accountability	• Provide information security protection commensurate with the risk and business impact. • Provide security training • Develop the controls environment and activities • Report on effectiveness of policies, procedures and practices	• Provide security for information and systems • Periodic assessments of assets and their associated risks • Determine level of security appropriate • Implement policies and procedures to cost-effectively reduce risk to acceptable levels • Periodic test of security and controls	• Develop, maintain, and ensure compliance to program • Designate security officer with primary duties and training • Develop required policies to support security program and business unit specific needs • Develop information use and categorization plan • Assist senior managers with their security responsibilities • Conduct security awareness
Metrics/Audit (These tend to be sector- or organization-specific.)	***How effectively do I achieve my objectives?***		***What adjustments do I need to make?***	
	Financial reporting, monetizing losses, conforming to policies	Policy violations, misuse of assets, internal control violations	Risk assessment and impact analysis, control environment activities, remedial actions, policy and procedure compliance, security and control test results	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

Table 4. Preliminary Information Security Governance Framework Interpreting the Framework

Interpreting the Framework

This framework is a work in progress. It is designed to be a tool to guide and encourage senior corporate executives and managers to adopt corporate best practices for security. The framework represents a two-fold benefit to those organizations that adopt it. First, it identifies cornerstone security practices that nearly all organizations are following. Second, it makes recommendations about where in the organization the responsibility best fits so that the integration of those practices evolves into a corporate climate of security. The framework poses three sets of questions, with regard to information security:

1. What am I required to do?/What am I afraid not to do?
2. How do I accomplish my objectives?
3. How effectively do I achieve my objectives?/What adjustments do I need to make?

At each level of the organization, these questions result in different answers, yet all can yield a consistent response to information security responsibilities. The first set of questions identifies the drivers behind security objectives – drivers that will be different for different businesses and industries. For example, is adherence to regulations or legislation driving the need for security controls? Or is the driver a market condition such that a company will experience significant brand erosion in the event of a cyber attack? The second question refers to the programs and processes to be put in place to accomplish organizational security objectives. These programs are common to almost all organizations, no matter what their market. The last set of questions focuses on assessing risk, measuring the effectiveness of security controls, and making improvements as necessary. Like the first set of questions, these tend to be more company and industry specific.

Because the framework describes proactive actions that managers at various organizational levels can take to secure their information systems, it not only clarifies roles and responsibilities, but also helps management select a security practice reference (like ISO 17799) that is appropriate for their organization.

Consistent with Key Security Practices

This framework includes the key practices that our analysis of information security reports uncovered. A survey of the literature shows that almost all of the reports on information security cite the following four information security requirements:

1. The need for risk assessments. Risks must be understood and acknowledged, and the security measures that are taken must be commensurate with these risks.
2. The need for a security organizational structure.
3. The need to create, communicate, implement, endorse, monitor, and enforce security policies across an organization.
4. The need to make every member of the organization aware of the importance of security and to train them in good security practices.

In addition, four other recommended practices were frequently cited:

5. The need for access controls to make certain only identified and authorized users with a legitimate need can access information and system resources.
6. The need to consider security throughout the system life cycle.
7. The need to monitor, audit, and review system activity in a routine and regular function.
8. The need for business continuity plans that are tested regularly.

Each of these is included as part of the roles and responsibilities section of our framework. The important lesson is not the list of these practices, which numerous reports have cited, but putting them in a context that defines what level of management is responsible for them.

Conclusion

Our analysis of information security efforts found no ready governance framework or discussion of strategic roles and responsibilities. In FISMA, the U.S. federal government has a model that can be readily adapted to private sector needs. In this paper, we have proposed a preliminary framework for information security governance that builds on the lessons of FISMA and ISO 17799 and the consensus recommendations contained in information security reports. In releasing this preliminary framework, executive management can become more actively engaged and advance the public-private partnership that is necessary to make real progress in information security governance.

This paper was prepared with the assistance of McConnell International, LLC, a Washington-based technology and policy consulting firm. www.mcconnellinternational.com.

*The Business Software Alliance (**www.bsa.org**) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC Software/Mastercam, Entrust, HP, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, Novell, PeopleSoft, RSA Security, Sybase and Symantec.*

BSA member companies that participated in developing phase one of the task force and white paper include: Autodesk, Cisco, Entrust, Intel, Internet Security Systems, Intuit, Microsoft, Network Associates, Novell and Symantec.

APPENDIX 1

INFORMATION SECURITY GOVERNANCE BIBLIOGRAPHY

I. INFORMATION SECURITY AS A FUNDAMENTAL GOVERNANCE ISSUE

The documents listed below are focused on the need for responsible senior corporate officers and members of boards of directors to recognize information security as a strategy that requires the attention of senior officials. These publications argue the case for addressing information security as an integral organizational governance issue. Such publications include:

–Information Technology Governance Institute (founded by the Information Systems Audit and Control Association <ISACA>), "Information Security Governance: Guidance for Boards of Directors and Executive Management", 2001.

–Institute of Internal Auditors, "Information Security Management and Assurance: A Call to Action for Corporate Governance", 2000.

–Ibid., **"Information Security Governance: What Directors Need to Know", 2001.**

–National Association of Corporate Directors, "Information Security Oversight: Essential Board Practices", December 2001.

II. ORGANIZING FOR INFORMATION SECURITY—ESSENTIAL PROGRAM COMPONENTS

The documents listed below focus on the programmatic aspects of information security. These publications appear to be based on the assumption that senior management does understand the need for an effective enterprise information security program and focuses on the components of this activity:

–Business Industry Advisory Council/International Chamber of Commerce, "Information Security Assurance for Executives: An International Business Commentary on the 2002 OECD Guidelines for the 'Security of Networks and Information Systems: Towards a Culture of Security'", April 22, 2003.

–Business Roundtable, "Building Security in the Digital Resource: An Executive Resource", November 2002.

–General Accounting Office, "Federal Information System Controls Audit Manual", January 1999.

–Information Security Forum, "The Standard of Good Practice for Information Security", Version 4, March 2003.

–Information Technology Governance Institute, "Governance, Control and Audit for Information and Related Technology (CoBIT)", 3rd edition, July 2000.

–International Chamber of Commerce, "ICC Handbook on Information Security Policy for Small to Medium Enterprises", April 11, 2003.

–International Information Security Foundation, “Generally Accepted System Security Principles”, Fall 2000.

–International Standards Organization (ISO) and the International Electrotechnical Commission (IEC), “Code of Practice for Information Security” (ISO/IEC 17799), May 5, 2003 (final coordination draft).

–Internet Security Alliance, “Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices”, 1st edition, July 2002.

–National Institute of Standards and Technology, “Automated Information Security Program Review Areas,” July 27, 2002.

–National Institute of Standards and Technology, “Generally Accepted Principles and Practices for Security Information Technology Systems,” September 1996.

–Organization of Economic Cooperation and Development, “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security”, adopted 25 July 2002.

–The World Bank, (Thomas Glaessner, Tom Kellermann, and Valerie McNevin), “Electronic Security: Risk Mitigation in Financial IT Transactions”, June 2002.

–U.S. Congress, “Federal Information Security Management Act of 2002 (FISMA)”, 2002.

III. GOVERNANCE DOCUMENTS UNDER DEVELOPMENT

This section enumerates information security governance documents that are currently under development.

–Business Roundtable, “Information Security Addendum to Principles of Corporate Governance,” announced April 2003.

–Information Systems Security Association (ISSA), “The Generally Accepted Information Security Principles (GAISP)”, in preparation.

–TechNet, CEO Cyber Security Task Force, Announced April 2003.