ASIS INTERNATIONAL

Chief Security Officer (CSO) Organizational Standard

ASIS CSO.1-2008

AMERICAN NATIONAL STANDARD

ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS CSO.1-2008

an American National Standard for Security

Chief Security Officer (CSO) Organizational Standard

Approved October 22, 2008

American National Standards Institute, Inc.

Abstract

This Standard is designed as a tool to educate an organization in deciding upon and providing a recommended security organizational architecture characterized by appropriate awareness, prevention, preparedness, and response to changes in threat conditions. This Standard is structured at a high level, although specific considerations and responses are also addressed for consideration by individual organizations based on identifiable risk assessment and requirements.

SAFETY Act Designation

In April 2005, the U.S. Department of Homeland Security (DHS) awarded ASIS International a Designation for its Standards and Guidelines Program under the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technology Act of 2002). This Designation is significant in three ways: (1) it establishes that ASIS standards and guidelines are qualified to be a "technology" that could reduce the risks or effects of terrorism, (2) it limits ASIS' liability for acts arising out of the use of the standards and guidelines in connection with an act of terrorism, and (3) it precludes claims of third party damages against organizations using the standards and guidelines as a means to prevent or limit the scope of terrorist acts.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

ASIS International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a voluntary, nonprofit professional society with no regulatory, licensing or police power over its members. ASIS does not undertake a duty to third parties because it does not have the authority to enforce compliance with its standards. It assumes no duty of care to the general public, because its standards are not obligatory and because it does not monitor the use of those standards.

ASIS disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. ASIS disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. ASIS does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document shall not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-887056-89-2

10 9 8 7 6 5 4 3 2 1

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with the requirements of the American National Standards Institute, Inc. (ANSI) for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 36,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, ASIS leads the way for advances and improved security performance.

The work of preparing ASIS Standards is carried out through the ASIS International Standards and Guidelines Commission committees.

Commission Members

Jason L. Brown, Thales Australia
Steven K. Bucklin, Glenbrook Security Services, Inc.
John C. Cholewa III, CPP, Embarq Corporation
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
Michael A. Crane, CPP, IPC International Corporation
Eugene F. Ferraro, CPP, PCI, CFE, Business Controls Inc.
F. Mark Geraci, CPP, Bristol-Myers Squibb Co., Chair
Robert W. Jones, Kraft Foods, Inc.
Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair
John F. Mallon, CPP, SC Johnson & Son, Inc.
Marc H. Siegel, Ph.D., ASIS Security Management System Consultant
Roger D. Warwick, CPP, Pyramid International

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818.

It is recognized that the following Chief Security Officer (CSO) 2008 Guideline Review Committee Members are responsible for the Chief Security Officer baseline text:

Jerry J. Brennan, Security Management Resources, Inc., Chair
John C. Cholewa III, CPP, Embarq Corporation, Commission Liaison
George K. Campbell, Security Risk Management Consultancy
Robert W. Hayes, CPP, CFE, The Security Executive Council
Don L. Hubbard, PricewaterhouseCoopers LLP
John E. McClurg, Honeywell International Inc.
Mark A. Sanna, CPP, Hyatt Hotels Corporation
Timothy L. Williams, CPP, Caterpillar, Inc.
W. Lance Wright, USEC Inc.

ASIS International would like to express its foremost appreciation to W. Lance Wright, Senior Vice President, Human Resources & Administration, USEC Inc., author of the original Chief Security Officer (CSO) white paper presented at the 2002 ASIS Annual Seminar and Exhibits, for his time, assistance, and use of material, which contributed significantly to the development of the Standard.

At the time it approved this document, CSO Standards Committee, which is responsible for the development of this Standard, had the following members:

Committee Members

Committee Chairman: Jerry Brennan, Security Management Resources, Inc.

Commission Liaison: John C. Cholewa III, CPP, Embarq Corporation

Chuck Baley, Farmers Insurance Group
Howell Barbee, Tishman Speyer
Jay C. Beighley, Nationwide Mutual Insurance Company
Ralph Blasi, Brookfield Financial Properties
John M. Boal, University of Akron
Mark Borchers, Germanna Community College
Tim Bowen, BearingPoint
Thomas C. Browning, AlliedBarton Security Services
Jerry Brennan, Security Management Resources Inc.
James D. Calder, The University of Texas at San Antonio
Julio C. Campos, Aflac Worldwide Headquarters
Joseph J. Cantamessa, Dow Jones & Company, Inc.
Stephen T. Colo, SAIC
Dan Consalvo, State Farm Insurance
Michael J. Daly, Queens Borough Public Library
Barbara A. Felker, EMC Corporation - Federal
Walter N. Fountain, Schneider National, Inc.
Tim Gladura, AIGWIG, Inc.
G. Ernest Govea, Parsons
Jeffrey P. Grossmann, St. John's University
Jeff Gurule', KLA-Tencor Corporation
Robert W. Hayes, Security Executive Council
Joseph Herrity, URS Corporation
John A. Hill, University of Denver
William T. Hill, The Wackenhut Corporation
Greg Hull, American Public Transportation Association
Tim Janes, Capital One Financial Corporation
Michael John, Applied Materials, Inc.
Mike Keenan, Mervyns
David Kent, Genzyme Corporation
Dr. Igor Khripunov, Center for International Trade and Security
Patrick J. Kilgore, Jr., Federal Bureau of Investigation, Buffalo Division
Charles King, Federal Trade Commission
Jed Kirkman, CIA
Kelly S. Klatt, Loews Hotels at Universal Orlando
Barbara Knieff, Federal Aviation Administration
Bryan C. Leadbetter, Bausch & Lomb World Headquarters
Eric L. Levine, The Levine Group, LLC
James P. Litchko, Litchko & Associates, Inc.
Norm Littler, American Bus Association
Thomas J. Mahlik, Federal Bureau of Investigation
Robert Martin, Colgate-Palmolive Company
John E. McClurg, Honeywell International
Clyde D. Miller, BASF Corporation
Paul Nguyen, Neohapsis
John Petruzzi, Simon Property Group
Jeffry J. Pifer, Chemtura Corporation
Robert S. Pocica, McKesson Corporation
Richard S. Post, Post & Post LLC
Chris Richardson, PCG Solutions
Jimmy Salinas, AT&T
Mark A. Sanna, Hyatt Hotels Corporation
Ben Scaglione, New York Presbyterian Hospital
Timothy J. Scott, The Dow Chemical Company
David W. Skidmore, NCR Corporation
Austin L. Smith, Department of Homeland Security
James F. Smith II, AT&T Asset Protection
James M. Sonntag, Honeywell International
David L. Stackleather, Circuit City Stores Inc.
J. Kelly Stewart, Deloitte Services, LP
Robert Stokes, Drexel University
Steve Surfaro, Panasonic
Darryl Thibault, PeXis Investigations & Security
Hector Torres, Banco Popular of Puerto Rico
Lyly Tran, Federal Aviation Administration

Debra van Opstal, The Council on Competitiveness
Tony Vermillion, Emerson
Eva A. Vincze, Security Management & High Tech Crime Investigation
Lee S. Webster, Society for Human Resource Management
John A. Weidner, USEC Inc.
W. Lance Wright, USEC Inc.
Stephen L. Winters, AICPA

Working Group Members

Working Group Chairman: W. Lance Wright, USEC Inc.

Chuck Baley, Farmers Insurance Group
Jay C. Beighley, Nationwide Mutual Insurance Company
John M. Boal, University of Akron
Mark Borchers, Germanna Community College
Stephen T. Colo, SAIC
Dan Consalvo, State Farm Insurance
Michael J. Daly, Queens Borough Public Library
Walter N. Fountain, Schneider National, Inc.
Tim Gladura, AIGWIG, Inc.
G. Ernest Govea, Parsons
Robert W. Hayes, Security Executive Council
Michael John, Applied Materials, Inc.
Mike Keenan, Mervyns
Charles King, Federal Trade Commission
James P. Litchko, Litchko & Associates, Inc.
Thomas J. Mahlik, Federal Bureau of Investigation
John E. McClurg, Honeywell International
Paul Nguyen, Neohapsis
Jimmy Salinas, AT&T
Ben Scaglione, New York Presbyterian Hospital
James M. Sonntag, Honeywell International
David L. Stackleather, Circuit City Stores Inc.
Timothy J. Scott, The Dow Chemical Company
Steve Surfaro, Panasonic
Hector Torres, Banco Popular of Puerto Rico
Debra van Opstal, The Council on Competitiveness
Eva A. Vincze, Security Management & High Tech Crime Investigation
John A. Weidner, USEC Inc.
Lee S. Webster, Society for Human Resource Management

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Security –

Chief Security Officer (CSO) Organizational Standard

1. Scope, Summary, and Purpose

1.1 Scope

The Chief Security Officer (CSO) Organizational Standard is applicable to organizations in the private and public sector environments, which need to evaluate and respond to the ever-increasing and ever-changing multitude of threats to their assets, equities, information, and structure, on both a domestic and global level.

1.2 Summary

This Standard is designed to be a tool to educate an organization in deciding upon and providing a security architecture characterized by appropriate awareness, prevention, preparedness, and necessary responses to changes in threat conditions. This Standard is structured at a high level, although specific considerations and responses are also addressed for deliberation by individual organizations based on identifiable risk assessment and requirements.

1.3 Purpose

This Standard is a model for organizations to use when developing a leadership function to provide a comprehensive, integrated security risk strategy to contribute to the viability and success of the organization. This leadership function is designated the *Chief Security Officer (CSO)*. With respect to this standard, the role may be viewed as a standalone position or as one that has been incorporated within an existing senior-level executive's accountability to the organization's leadership team.

2. Normative References

The following documents contain information, which, through reference in this text, constitute foundational knowledge for the use of this American National Standard. At the time of publication, the editions indicated were valid. All material is subject to revision, and parties are encouraged to investigate the possibility of applying the most recent editions of the material indicated below.

ASIS International. (2008). *Chief security officer guideline*. [Online]. Available:
< http://www.asisonline.org/guidelines/guidelineschief.pdf > [2008, April].

Booz Allen Hamilton. (2005). *Convergence of enterprise security organizations*. [Online]. Available:
< www.asisonline.org/newsroom/alliance.pdf > [2007, November 1].

Booz Allen Hamilton. (2006). *Convergence of enterprise security organizations: International views: an addendum to the 2005 study*. [Online]. Available:
< http://www.aesrm.org/GlobalConvergenceStudyInsightsAddendum.pdf > [2007, November 1].

Business Roundtable. (2005). *Committed to protecting America: CEO guide to security challenges* [revised 2007]. [Online]. Available:
< http://www.businessroundtable.org/pdf/20050503003CEORiskMgmtGuideFINAL.pdf >, [2008, April 16].

NOTE: This online pdf version was revised in March 2007 with additional added material (Chapter 9). The original 2005 version is no longer available on this site.

Council on Competitiveness. (2007). *Transform. The resilient economy: Integrating competitiveness and security*. [Online]. Available:
< http://www.compete.org/images/uploads/File/PDF%20Files/Transform_The_Resilient_Economy_FINAL_pdf > [2007, November 1].

Deloitte & Touche LLP Canada. (2007). *The convergence of physical and information security in the context of enterprise risk management*. Rolling Meadows, IL: The Alliance for Enterprise Security Risk Management. [Online]. Available: < http://www.aesrm.org/AESRM_Convergence_in_ERM.pdf > [2007, November 1].

Foushee Group, Inc. (2007). "Top global security executive (chief security officer)." *2007 Security and Compliance Compensation Survey* (pp.23-24). Matlacha, FL: Foushee Group, Inc.

Hayes, Bob, & Fickes, Michael. (2007, March 1). "Tomorrow's security leader today". *Access Control & Security Systems*. [Online]Available:
< http://securitysolutions.com/mag/security_tomorrows_security_leader/index.html > [2007, November 1].

Lefler, Richard. (2007). *Board level risk focus and the CSO's role*. Marietta, GA: Security Executive Council.

Nortel Networks. (2006). *Integrated Enterprise Security: A Proactive, Cross-Functional Approach for Using Security to Enhance Competitiveness of the Enterprise*. [Online]. Available:
< http://whitepapers.zdnet.com/whitepaper.aspx?docid=315398 > [2007, November 1].

3. OVERVIEW

Increasingly, business risk environments have become more severe, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business today and will continue to be so in the future. Boards of Directors, shareholders, key stakeholders, and the public all expect organizations to identify and anticipate areas of risk, and set in place a cohesive strategy across all functional lines to mitigate or reduce those risks. In addition, it is expected that an organization's leadership will respond in a highly effective manner to events and incidents that threaten the assets of the organization. Thus, a proactive strategy for risk mitigation ultimately creates an increase in profitability and is an organizational governance responsibility of senior leadership and governing boards.

The thesis of this Standard is that the skills and competencies essential to the active protection of an organization, and measurably effective responses to the modern threat environment, are more critical than ever before. Effective leadership within the top levels of an organization, especially its security functions, is imperative. Organizational reputation, the uninterrupted reliability of the technical

infrastructure and normal business processes, the protection of physical and financial assets, the prevention of compromising of trade secrets, the safety of employees and customers, and the preservation of shareholder confidence all rely in some measure upon the effectiveness of a responsible and accountable senior security executive.

Traditionally, what has previously been lacking in most organizations is a single position at the senior governance level having the responsibility for crafting, influencing, and directing an organization-wide protection strategy. In many organizations, accountability is dispersed – possibly among several managers in different departments, who potentially have conflicting security objectives (e.g., employee safety being primary to one, physical assets to another, etc.).

The complexity of today's security risks creates a diverse matrix of interrelated threats, vulnerabilities, and impacts; therefore, the safeguards against these risks are interdependent. While "ownership" of a specific security function in a strict sense is not essential, strategic accountability and effective influence are.

The restructuring and focusing of current efforts through the single senior leadership function of CSO should eliminate the redundant and narrow interests that may be present in vertical departmental structures. The ability to influence business strategy and address matters of internal risk exposure requires a CSO at the appropriate level in the organization.

4. REPORTING RELATIONSHIP

Appropriate reporting relationship decisions for the CSO position should be driven by an evaluation of the current structure of the organization. It is strongly recommended that the position report to a key senior-level executive of the organization so as to ensure a strong liaison with the Board of Directors and its operating committees. This senior position in the organizational hierarchy is a signal, not only of top leadership's commitment and support, but also of the legitimacy ascribed to the security program.

5. MODEL FUNCTION

The diagram following this section illustrates the scope of an organization's security protection program. It includes functional areas of responsibility, key processes, and discussion of work elements that should be found within an organization.

Leadership may take the form of either a Security Council or actual managerial and budgetary accountability for all security functions. Most importantly, leadership should clearly establish strategic accountability and exert effective influence on the security and risk mitigation activities of the organization in order to achieve organizational goals and objectives.

The culture and business model at work within an organization should guide specific decisions seeking to establish the best approach for that organization. This Standard is intended to assist an organization as it considers its best approach; it provides guidance on where the positions should be placed in the

organization, and the skills and competencies the CSO should possess. The concept of an organizational vision and voice for the security mission is the substance of this Standard.

While many different approaches may be taken to align the CSO role within an organization's culture, to aid in understanding and facilitating implementation, this Standard presents a model position description (Annex A). An additional security governance reference model can be found in Annex B, *Next Generation Security Leadership*.

Table 1 - Model Profile of a Chief Security Officer Function

Risk Areas		
Human Resources and Intellectual Assets	Information/Data	Facilities and Premises
Ethics and Reputation	Transportation, Distribution, and Supply Chain	Environmental, Health, and Safety **
Financial Assets	Legal, Regulatory, and General Counsel	Vendor/Outsourcing
** Recognizing that EH&S may be structured outside the scope of security functions, there are still significant risk issues in this category to an organization. Since many organizations have combined their EH&S and security functions, it is presented in this Standard for consideration.		
Benchmark Processes and Services		
Global Security Policy and Procedures Administration	Investigative and Forensic Services	Executive Protection
Technology and Infrastructure Protection	Safe and Secure Workplace Operations	Background and Due Diligence Investigations
Information Risk Management	Tailored Business-Process Safeguards	Business Conduct and Security Compliance
Business Continuity, Crisis Management, and Response	Insurance and Risk Transfer	External and Government Relations
Employee Risk Awareness	Risk Assessment, Analysis, Evaluation, and Testing	Business Intelligence and Counterintelligence Support
Skill Set Required		
Relationship Manager	Develops, influences, and nurtures trust-based relationships with business unit leaders, government officials, and professional organizations. Acts as a consultant to all organizational clients.	
Executive Management and Leadership	Builds, motivates, and leads a professional team attuned to organizational culture, responsive to business needs, and committed to integrity and excellence.	
Subject Matter Expert	Provides or sees to the provision of technical expertise appropriate to knowledge of risk and the cost-effective delivery of essential security services.	
Governance Team Member	Provides intellectual leadership and active support to the organization's governance team to ensure risks are made known to senior management and the Board.	
Risk Manager	Identifies, analyzes, and communicates on business and security-related risks to the organization.	
Strategist	Develops global security strategy keyed to likely risks and in collaboration with the organization's stakeholders.	
Creative Problem Solver	Aids competitiveness and adds value by contributing dynamic, real-time critical thinking and solutions that enable the organization to "prevent" disruptions from occurring and minimize damage when they do occur. Engages in business processes to mitigate risk. Is a positive change agent on behalf of organizational protection.	

6. KEY RESPONSIBILITIES AND ACCOUNTABILITIES

The CSO should be a full partner in the governance infrastructure of the organization. If a comprehensive assessment of any areas of risk (as noted in the above model) supports the need for a function-specific security role, the assignment of high-level accountability better ensures an integrated security strategy, with less duplication of effort and an overall lower cost.

A core responsibility for effective security is the management of effective working relationships among client groups. Front-line accountability for protecting the business should fall to the managers of each operating unit, with the appropriate organization's security function providing the risk assessment, policy, and supporting infrastructure for those managers.

This model requires a senior executive in the CSO position that can lead, integrate, and enable these business lines to achieve the core business objectives of the organization. Being an effective *business process enabler* requires that the incumbent be a creative problem solver and a leader with business acumen who can blend "common sense" controls with efficient and productive business processes.

It is also necessary that the incumbent bring *subject matter expertise* to the position. Ideally, in addition to the pure "generalist" or leadership qualities the CSO should possess, to be effective in the business environment (and in support of the Board Room), it is paramount that the CSO should possess "on demand" competencies, experiences, and advanced working knowledge of contemporary security tradecraft, practices, and applications. The CSO should be recognized and respected within the corporate structure as the executive with commensurate subject matter expertise on security matters.

An effective CSO model is a hybrid that takes into consideration the incumbent's combined leadership talent, business acumen (i.e., background in business or a governance function), and subject matter expertise. While it is likely that the incumbent will have come from a specialized background within the business, a governance function, or some element of the security mission, leadership of a multi-faceted security program requires general business and management knowledge. In addition to this generalist knowledge, any technical or specialized attributes and skills should be given strong consideration in the selection of the CSO candidate. Ultimately, the CSO's resourcefulness and credibility within the organization, and the CSO's vision to craft an integrated, multi-faceted strategy, depends on the incumbent's ability to understand, value, and articulate the varied security threats facing an organization in the context of business model impacts.

6.1 Key Success Factors

The ability to build sustainable competitive advantages through pragmatic, innovative, and business-focused security solutions.

Demonstrated integrity and the ability to maintain principles under internal and/or external pressure.

High-quality analytical skills, management experience, and exceptional relationship management competencies.

Qualitative experience in strategic planning and/or policy development at a senior leadership level.

The ability to anticipate, investigate, influence, and assist the organization in its ability to assess and rapidly adjust to changing conditions and trends of importance (both internal and external) in light of the overall direction of the organization.

Effectiveness in developing, communicating, and executing recommended courses of action for innovative, business-oriented responses.

A commitment for excellence and a demonstrable orientation toward successful staff development.

6.2 Strategy Development

One key responsibility of the CSO is to strategize with senior leadership in order to conceptualize, illustrate, develop, implement, and continuously renew an overall strategy that demonstrates the various processes needed to understand the nature and probability of all risk events within the business context of the organization. The strategy should outline, in detail, the plans to prevent and prepare for an adverse event—including state-of-the-art awareness, training, exercises, and methodologies to inculcate contemporary security programs and processes throughout the organization. The strategy should also include methods for continuity of business operations after any security-related attack or catastrophic event. The CSO should be capable of clearly communicating this strategy, its costs, and its related impact to the highest levels of the organization, the Board of Directors, and its operating committees.

6.3 Information Gathering and Risk Assessment

The CSO is responsible and accountable for systematically gathering, assessing, and synthesizing information related to a wide range of security-related events and threats specific to the organization and its various operations, which may adversely affect the security and safety of personnel and the profitability or reputation of the organization.

In addition, the CSO should also determine the probability of security-related incidents and threats, and develop appropriate strategies consistent with sound business judgment and internal controls to prevent negative impacts on the organization**.** The information necessary to develop these assessments and preventive strategies should come from multiple sources, including organizational records, government and law enforcement (including intelligence) agencies, news organizations, existing security bodies of knowledge, etc. The CSO should be capable of making the links between disparate pieces of information, from multiple sources, in order to understand and assess the data's importance to the security of the enterprise. The CSO should understand and be familiar with both "human capital skills" and technological aids that can assist in this process, and possess both conceptual and critical thinking skills to prioritize risks and develop appropriate preventive strategies across the organization.

6.4 Organization Preparedness

The CSO is responsible and accountable for ensuring that the enterprise is prepared for events or circumstances that potentially disrupt the continuity of business operations. For example, these events include deliberate attacks (physical and cyber) targeted at the organization, catastrophic events

(hurricanes, tornados, earthquakes, etc.), or significant security incidents (for example, white collar crime: the commission of major fraud, major theft, product tampering, sabotage, etc.).

Preparation for these events should involve the development and administration of training plans, programs, procedures, and exercises to establish baseline organizational responses. A process of regular periodic review, testing, and evaluation of organizational readiness in the event of disruptive attacks or events is a key responsibility of the CSO.

6.5 Incident Prevention

The CSO should identify and understand the nature of security risks in the business environment, as well as the application of appropriate financial and managerial controls to mitigate those risks. This will require the CSO to understand how and when to enlist the support of risk management, internal audit, controllers, outside resources, legal, human resources, and other staff functions to mitigate the various risks to the business.

Another key responsibility of the CSO is the analysis of information and the coordination of activities with persons inside and outside the organization to forestall, prevent, or mitigate attacks, incidents, and catastrophic events. This implies the ability to successfully operate independently in fast-paced, matrix-management environments, requiring a high tolerance for ambiguity and positive political skills to drive programs and projects to completion.

6.6 Securing Human Capital, Core Business, Information, and Reputation

The protection of the company's integrity, human capital, processes, information, and assets from harm and loss is a key responsibility of the CSO. While guarding the *financial and physical assets* of the enterprise (i.e., cash, facilities, and equipment) is important, it is equally important that the CSO should also be especially adept at countering the potential risks involved in the loss of *intangible assets* (i.e., reputation and customer and client confidence), intellectual property, and trade secrets. *Human capital* here includes leadership and directors, employees, customers, and any others the organization has a duty to protect.

6.7 Incident Response, Management, and Recovery

In case of an incident of attack or catastrophe, the CSO should be responsible for coordinating the following *critical business processes*:

1) Incident response; and
2) Management and recovery efforts within the organization to:
    a. Restore critical systems; and
    b. Provide facilities needed by the organization to function.

The CSO should coordinate with internal and external resources to ensure adequate medical, financial, and psychological *support assistance* is provided to employees, customers, and others involved in a catastrophic event or an attack on the organization.

The CSO should *coordinate* with local, state, federal, and international government agencies as required.

6.8 Investor Relations, Public Affairs, and Government Relations Coordination

The CSO should closely coordinate with those responsible for investor relations including—but not limited to—public affairs, finance, human resources, operations, and government relations involving events and incidents that threaten the assets of the organization.

The CSO should be required to participate in the development of media interviews and testimony before government regulatory agencies.

7. KEY COMPETENCIES

Generally, the outlook of the CSO should be more strategic than tactical. The position requires an extreme degree of integrity, ethics, responsibility, and dedication, as well as the ability to calmly facilitate the appropriate resolution of difficult ethical and crisis situations. The ability to programmatically and holistically analyze, understand, and explain the value proposition of security initiatives to senior executives and Board of Director members is a key requirement of the position. It is likely that the strategic, business, and interpersonal abilities of a CSO will be of greater importance than their technical security skills (many of which are available through internal subject-matter experts or external consultants). Thus, the CSO should have exceptionally strong business and interpersonal skills.

The ability to communicate clearly and authoritatively, both orally and in writing, should be a core competency of the CSO position. The necessity of interaction with senior executives and Board of Director members means the incumbent should be comfortable in making presentations, as well as fielding questions and challenges concerning the security proposals and recommendations presented.

The CSO will need skills and competencies to accomplish the following:

- Effectively communicate with all levels of the organization—especially senior executives, the Board of Directors, and any operating committees.

  Understand the strategic direction and goals of the business, and how to support the security needs of the organization in order to protect its goals and objectives. (This implies the ability to establish a vision for the global and individual business security programs, and the ability to build support for their implementation and ongoing development. Some demonstration of international experience should be required, based upon the scope and reach of the organization.)

  Understand the impact of ongoing changes in economics, geopolitics, organizational design, and technology, and assess how all of these relate to potential threats and risks to the organization (including their impact on existing security programs and services).

  Investigate and resolve security incidents and related ethical issues without further disruption of operations, and conduct these in a fair and objective manner that is in alignment with the organization's values and code of business conduct.

Use traditional and advanced scenario planning techniques in assessing risks and threats to the organization.

Understand how to successfully develop and network working relationships with key individuals in staff and line positions throughout the organization.

Promote organizational education on security awareness and develop organization-wide knowledge-sharing, as appropriate for the business and the culture of the organization.

Comprehend the need to assess the realistic financial, employee, or customer implications of any security plan or recommendation.

Function as an integral part of the senior leadership team, with regard both to planning and capital expenditures, and the security dimension of such.

A description of the ideal CSO should also include the following professional characteristics of a senior level executive:

Strategic orientation with ability to act tactically (as required).

Adaptable and effective in either a hierarchical or a matrix-management environment.

Global perspective, possessing a multi-cultural understanding and approach.

Detail-focused (as required).

Excellent conceptual and critical thinking skills.

High integrity, ethics, responsibility, and dedication.

Politically astute, but not politically motivated.

Strong negotiator/facilitator and consensus builder.

Understands principles of process management.

Able to interact at all levels of the organization, and sensitive to divisional organization management issues.

Recognized as a change agent.

8. EXPERIENCE

Demonstrated experience in security-related issues is key. Prior experience showing the candidate CSO's ability to effectively assess and determine success factors in the culture of an organization should be critical to the selection process.

A broad and diverse set of skills, education, and experience should be required, depending upon the hiring organization's analysis of the position and security needs. The incumbent should be recognized as a change agent and a highly credible senior-level leadership resource.

Some demonstration of international experience should be required, based upon the scope and reach of the organization. Added value should be given to one or more language proficiencies.

The incumbent should have a range of experience that permits a hiring organization to assess the challenges successfully addressed in prior experience, compared to those likely to be confronted in the future. The desired candidate should be a seasoned executive with a collaborative outlook and a proven track record as a team player and business partner.

9. EDUCATION

CSO is a senior executive leadership position. As with other senior positions, there are significant expectations for the levels of education and experience of the applicant.

Advanced degrees should be highly valued in all industries, and should represent the business connections that would likely enhance the CSO's credentials across many companies. Degrees in law, business administration, accounting and finance, security management, information systems management, or criminal justice are valuable, and should be considered with significant added value.

Professional Certifications in related fields (such as CPP, CFE, CISSP, etc.) should also be considered, as this demonstrates the individual's education, experience, and competence in that field.

With the growing emphasis on information security, degrees in computer science or related areas are highly valued in many industries. The job-relatedness and benefits of education and certification credentials should be balanced against the organization's culture. However, the quality, type of experience, and other directly-related accomplishments should be more compelling credentials for the hiring organization.

10. COMPENSATION

The options for compensating this senior level leader position are varied—and the compensation practices of organizations are too unique—to be stated with confidence here. Recruiters with experience in this area, high-quality annual compensation analyses, and similar organizations that value a highly effective security program should be consulted for benchmarking. Compensation packages should be comparable to other organizational executive leadership positions at the same level. (As a point of reference, the results of the 2007 Foushee Group Salary Study of the top global security executives are attached as Annex C.)

Annex A
(informative)

A. MODEL POSITION DESCRIPTION

A.1 Position Purpose

The incumbent CSO serves as the executive responsible for the identification, development, implementation, and management of the organization's [global][1] security strategies and programs.

A.2 Key Responsibilities

In cooperation with the executive committee, directs the development of an effective strategy to assess and mitigate risk (foreign and domestic), manage crises and incidents, maintain continuity of operations, and safeguard the organization.

Directs staff in identifying, developing, implementing, and maintaining security processes, practices, and policies throughout the organization to reduce risks, respond to incidents, and limit exposure and liability in all areas of information, financial, physical, personal, and reputational risk.

Researches and deploys state-of-the-art technology solutions and innovative security management techniques to safeguard the organization's assets, including intellectual property and trade secrets. Establishes appropriate standards and associated risk controls.

Develops relationships with high-level law enforcement [and international counterparts] to include in-country security [and international security agencies], intelligence, and private sector counterparts [worldwide].

Through subordinate managers, coordinates and implements site security, operations, and activities to ensure protection of executives, managers, employees, customers, stakeholders, visitors, etc., as well as all physical and information assets, while ensuring optimal use of personnel and equipment.

A.3 Key Skills and Competencies

Senior leadership skills to provide direction to the management and professional staff within the organization.

Ability to understand, interpret, analyze, and develop consensus within an organizational climate of diverse operational activities and often-conflicting regulations, imposed by agencies with regulatory jurisdiction.

[1] Bracketed items are dictated by each organization's scope.

Ability to effectively communicate within all levels of the organization (including briefing executive management and governance Board committees) on the status of security and issues surrounding enterprise risk management decisions.

High-quality analytical skills, leadership experience, and exceptional relationship management competencies to understand impact and sensitivity of security issues.

Demonstrate commitment to lead personnel in education and training advancement.

A.4 Qualification Guidelines

At least 3-5 years of direct experience in a significant senior level executive leadership role. Demonstrated ability to develop and manage the functional capital of an executive position and manage an expense budget.

Advanced degree (or equivalent), professional certifications in an area of study relevant to this position, and at least 10-15 years of experience in private sector corporate security or a related public sector organization.

Demonstrated experience and exposure in the international security arena dealing with security-related issues, based on the scope and reach of the organization.

Annex B
(informative)

B. NEXT GENERATION SECURITY LEADERSHIP

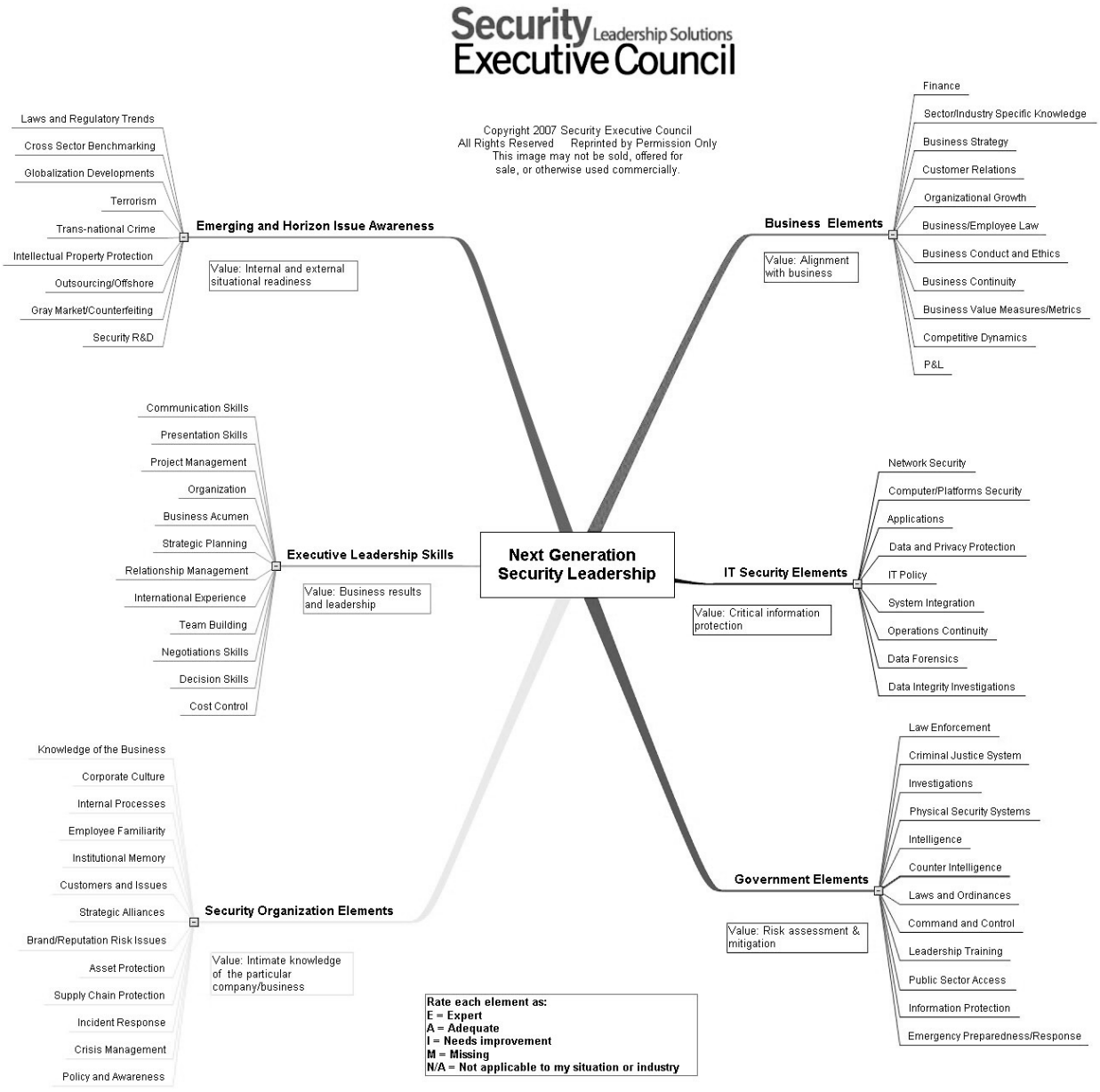
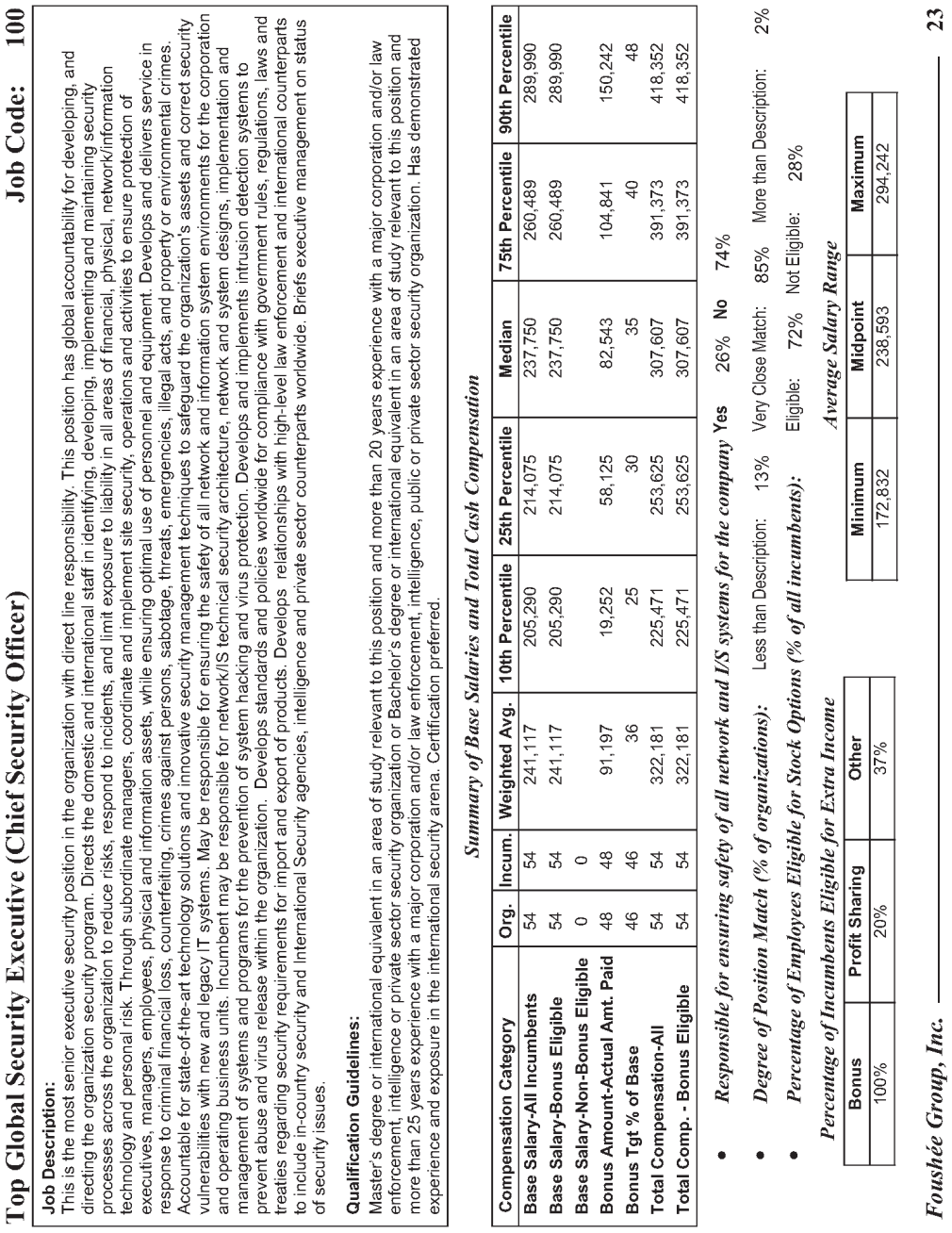


Figure 1 - Next Generation Security Leadership

Annex C
(informative)

C. TOP GLOBAL SECURITY EXECUTIVE (CHIEF SECURITY OFFICER)



Top Global Security Executive (Chief Security Officer) **Job Code: 100**

Job Description:
This is the most senior executive security position in the organization with direct line responsibility. This position has global accountability for developing, and directing the organization security program. Directs the domestic and international staff in identifying, developing, implementing and maintaining security processes across the organization to reduce risks, respond to incidents, and limit exposure to liability in all areas of financial, physical, network/information technology and personal risk. Through subordinate managers, coordinate and implement site security, operations and activities to ensure protection of executives, managers, employees, physical and information assets, while ensuring optimal use of personnel and equipment. Develops and delivers service in response to criminal financial loss, counterfeiting, crimes against persons, sabotage, threats, emergencies, illegal acts, and property or environmental crimes. Accountable for state-of-the-art technology solutions and innovative security management techniques to safeguard the organization's assets and correct security vulnerabilities with new and legacy IT systems. May be responsible for ensuring the safety of all network and information system environments for the corporation and operating business units. Incumbent may be responsible for network/IS technical security architecture, network and system designs, implementation and management of systems and programs for the prevention of system hacking and virus protection. Develops and implements intrusion detection systems to prevent abuse and virus release within the organization. Develops standards and policies worldwide for compliance with government rules, regulations, laws and treaties regarding security requirements for import and export of products. Develops relationships with high-level law enforcement and international counterparts to include in-country security and International Security agencies, intelligence and private sector counterparts worldwide. Briefs executive management on status of security issues.

Qualification Guidelines:
Master's degree or international equivalent in an area of study relevant to this position and more than 20 years experience with a major corporation and/or law enforcement, intelligence or private sector security organization or Bachelor's degree or international equivalent in an area of study relevant to this position and more than 25 years experience with a major corporation and/or law enforcement, intelligence, public or private sector security organization. Has demonstrated experience and exposure in the international security arena. Certification preferred.

Summary of Base Salaries and Total Cash Compensation

Compensation Category	Org.	Incum.	Weighted Avg.	10th Percentile	25th Percentile	Median	75th Percentile	90th Percentile
Base Salary-All Incumbents	54	54	241,117	205,290	214,075	237,750	260,489	289,990
Base Salary-Bonus Eligible	54	54	241,117	205,290	214,075	237,750	260,489	289,990
Base Salary-Non-Bonus Eligible	0	0						
Bonus Amount-Actual Amt. Paid	48	48	91,197	19,252	58,125	82,543	104,841	150,242
Bonus Tgt % of Base	46	46	36	25	30	35	40	48
Total Compensation-All	54	54	322,181	225,471	253,625	307,607	391,373	418,352
Total Comp. - Bonus Eligible	54	54	322,181	225,471	253,625	307,607	391,373	418,352

- ***Responsible for ensuring safety of all network and I/S systems for the company*** **Yes** 26% **No** 74%
- ***Degree of Position Match (% of organizations):*** Less than Description: 13% Very Close Match: 85% More than Description: 2%
- ***Percentage of Employees Eligible for Stock Options (% of all incumbents):*** Eligible: 72% Not Eligible: 28%

Percentage of Incumbents Eligible for Extra Income

Bonus	Profit Sharing	Other
100%	20%	37%

Average Salary Range

Minimum	Midpoint	Maximum
172,832	238,593	294,242

Foushée Group, Inc. **23**

Figure 2 - Top Global Security Executive (Chief Security Officer)

[2] Check the Foushee Group for updated results. < http://www.fousheesurvey.com >

Top Global Security Executive (Chief Security Officer) **Job Code: 100**

TYPE OF ORGANIZATION	Org.	Incum.	*Base Salary* Wt. Average	Median	10th Percentile	90th Percentile	*Total Cash Compensation* Wt. Average	Median
Corporation	50	50	241,964	238,223	206,208	290,739	321,420	320,272
Group/Subsidiary	1	1						
Division/Plant	0	0						
Res. Labs., Gov't., Education	3	3						

REGION	Org.	Incum.	*Base Salary* Wt. Average	Median	10th Percentile	90th Percentile	*Total Cash Compensation* Wt. Average	Median
West Coast	9	9	252,558	255,200	209,080	280,273	350,113	367,764
South Central	13	13	227,739	230,000	195,040	257,316	292,802	272,253
North Central	12	12	250,086	239,850	207,247	294,650	321,377	296,604
Southeast	9	9	256,156	241,241	222,800	301,622	378,180	342,815
Northeast	11	11	225,479	224,000	207,200	248,400	289,107	257,000

INDUSTRY	Org.	Incum.	*Base Salary* Wt. Average	Median	10th Percentile	90th Percentile	*Total Cash Compensation* Wt. Average	Median
Durable Goods Mfg.	5	5	237,859	246,595	218,100	253,120	315,391	319,595
Technology	4	4						
Other	1	1						
Non-Durable Goods Mfg.	14	14	244,810	233,783	197,182	294,681	340,499	306,560
Chemicals	4	4						
Pharmaceutical	4	4						
Other	6	6	233,844	224,783	191,000	285,748	306,916	274,050
Non-Manufacturing	35	35	240,106	237,500	207,760	287,490	315,824	305,300
Ener gy	7	7	248,635	244,920	204,645	289,580	338,775	383,933
Utilities	8	8	251,088	261,757	206,466	289,424	336,055	346,890
Research Laboratories	1	1						
Services	6	6	227,793	222,208	214,000	247,172	293,354	284,289
Other	13	13	234,830	237,500	209,840	257,440	302,195	274,400

FINANCIAL DIMENSION	Org.	Incum.	*Base Salary* Wt. Average	Median	10th Percentile	90th Percentile	*Total Cash Compensation* Wt. Average	Median
Under $500 Million	1	1						
$500 Million < $1 Billion	2	2						
$1 Billion < $3 Billion	2	2						
$3 Billion < $5 Billion	2	2						
$5 Billion < $10 Billion	9	9	226,326	229,566	208,001	242,860	289,217	273,515
$10 Billion < $20 Billion	12	12	239,338	225,000	209,290	284,237	308,312	306,268
Over $20 Billion	26	26	251,008	248,298	206,870	297,560	349,774	350,408

Foushée Group, Inc. 24

Figure 3 - Top Global Security Executive (Chief Security Officer)

Annex D
(informative)

D. USEFUL WEB SITES

The Alliance for Enterprise Security Risk Management (AESRM). < http://www.aesrm.org >

ASIS International. < http://www.asisonline.org >

Booz Allen Hamilton. < www.asisonline.org/newsroom/alliance.pdf > and
< http://www.aesrm.org/GlobalConvergenceStudyInsightsAddendum.pdf >

Business Roundtable. < http://www.businessroundtable.org >

Council on Competitiveness. < http://www.compete.org >

Foushee Group, Inc. < http://www.fousheesurvey.com >

Security Executive Council, Inc. < http://www.securityexecutivecouncil.com >

Annex E
(informative)

E. DEFINITIONS

Business Process Enabler: An individual who can blend "common sense" control with efficient and productive business processes and procedures; requires creative problem solving and business acumen.

Change Agent: An individual who is willing to challenge established business processes and procedures in the pursuit of excellence.

Chief Security Officer (CSO): A leadership function responsible for providing comprehensive, integrated risk strategies (policy, procedures, management, training, etc.) to help protect an organization from security threats.

Critical Business Processes: In terms of security issues, critical business processes include incident response, and the management of recovery efforts within the organization to restore critical systems and provide alternate facilities so that the organization can continue to function.

Financial and Physical Assets: Includes such things as facilities, equipment, inventory, and on-hand cash.

Human Capital: Includes organization staff (leadership, directors, managers, employees), customers, and any others the organization has a duty to protect.

Incumbent: This term is being used in the context of any person currently functioning in the CSO role, being considered for the CSO role via an external recruitment effort, or any existing management team member who will be assigned the accountabilities recommended for the CSO role within this Standard.

Intangible Assets: Includes such things as reputation, customer confidence, client confidence, trade secrets, intellectual property, and goodwill.

Subject Matter Expertise: Competencies, experiences, and advanced working knowledge of contemporary tradecraft, practices, and applications related to the topic of interest.

Support Assistance: Medical, financial, and emotional resources provided to employees, customers, and others involved in a catastrophic event or an attack on the organization.

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 36,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the general public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management*, ASIS leads the way for advanced and improved security performance. For more information, visit *www.asisonline.org.*

1625 Prince Street
Alexandria, Virginia 22314-2818
USA
1-703-519-6200
Fax: 1-703-519-6299
www.asisonline.org