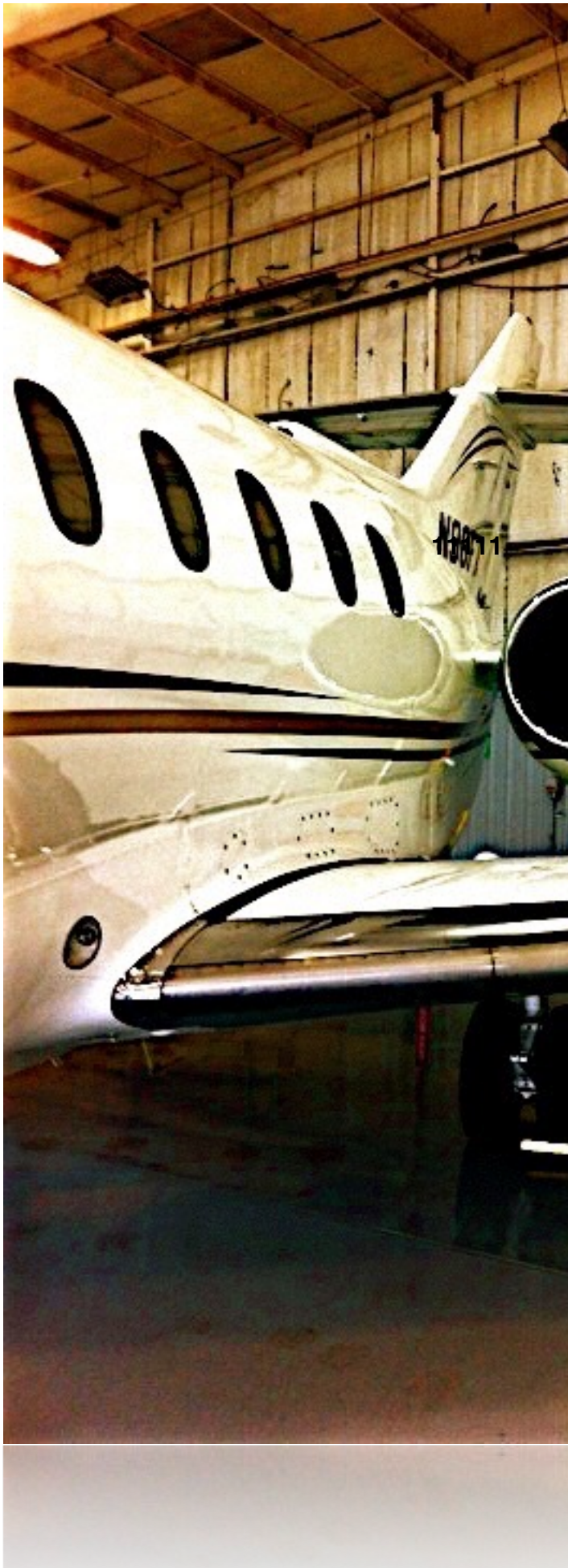
Corporate Security Guideline

Prepared for:

Prepared by: Eagle Eye International



Executive Summary-Corporate Security

Objective

Corporate Security identifies and effectively mitigates or manages, at an early stage, any developments that may threaten the resilience and continued survival of a corporation. It is a corporate function that oversees and manages the close coordination of all functions within the company that are concerned with security, continuity and safety. Our Objective is to:

- reduce / zeroize existing losses (using ASIS standards)
- identify and evaluate potential threats
- minimize danger and risk

Goals

1. To convince employees across the company to deliver security through their everyday actions and decisions – not try to do security to or for the company.

2. Security is there to help the company to take risks rather than prevent them and should therefore be at the forefront of new business development.

3. Security constantly responds to new business concerns and, as such, the portfolio of responsibilities and their relative importance will change over time. Security departments should never stand still or become fixed entities. In many companies today, its role is more concerned with overall corporate resilience than 'traditional' security. YOU SHOULD stay flexible and learn to accept security as a way of business continuity.

4. Security is both a strategic and operational, and departments must distinguish between these two layers. Dover will become that!

5. The power and legitimacy of the security department does not come from its expert knowledge, but from its business acumen, people skills, management ability and communication expertise. Our goal is to make sure everyone understands this.

Core elements of Corporate Security are:

Personal security

Physical security

Information security

Corporate governance

Compliance and ethics programs

Crime prevention and detection

Fraud deterrence

Investigations

Risk management

Business continuity planning

Crisis management

Personal Security

Security as it relates to personal protection is a constant learning process . One has to try and teach the Principle/Employees one is charged with protecting, to accept a discernible degree of responsibility for their own security awareness and actions and ultimately arrive at a place where both Principle and Bodyguard agree about what their individual and unique security applications should be.

General Guidelines:

I. Observation and Vigilance

II. Action

- weakness
- vulnerability
- escape route

III. Family Considerations

IV. Threats

V. Domestic Arrangements

VI. Raising the Alarm

- postal deliveries
- check list
- action
- never rule

VII. Telecommunications-Security Awareness

VIII. Anonymous - Annoyance Calls

IX. Security Applications with respect to Children

X. Security Provisions for the Home

XI. Travel

XII. Rules and Guidelines for Security Drivers

Physical Security

Physical security systems for protected facilities are generally intended to:

- deter potential intruders (e.g. warning signs and perimeter markings);
- distinguish authorized from unauthorized people (e.g. access badges, keycards)
- delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes);
- detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems); and
- trigger appropriate incident responses (e.g. by security guards and police).

It is up to security designers, architects and analysts to balance security controls against risks, taking into account the costs of specifying, developing, testing, implementing, using, managing, monitoring and maintaining the controls, along with broader issues such as human rights, aesthetics, health and safety, and societal norms or conventions. Physical access security measures that are appropriate for a high security prison or a military site may be inappropriate in an office, a home or a vehicle, although the principles are similar.

Elements and design

XIII. Deterrence methods

A. Physical barriers

B. Natural surveillance

C. Security lighting

XIV. Intrusion detection and electronic surveillance

A. Alarm systems and sensors

B. Video surveillance

XV. Access control

A. Mechanical access control systems

B. Electronic access control systems

C. Identification systems and access policies

XVI. Assessments

XVII. Emergency and Contingency Planning

XVIII. Periodic Review

Information Security - Cyber

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal,

inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)

Two major aspects of information security are:

- IT security: Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.
- Information assurance: The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

Governments, military corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, not to mention damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years.

Core Concepts:

- Key concepts
- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation
- Information security analysts
- Risk management
- Controls
- Administrative
- Logical
- Physical
- Defense in depth

- Security classification for information
- Access control
- Cryptography
- Process
- Security governance
- Incident response plans
- Change management
- Business continuity
- Disaster recovery planning
- Laws and regulations
- Information Security Culture
- Sources of standards

Corporate Governance

Corporate governance refers to the system by which corporations are directed and controlled. The governance structure specifies the distribution of rights and responsibilities among different participants in the corporation (such as the board of directors, managers, shareholders, creditors, auditors, regulators, and other stakeholders and specifies the rules and procedures for making decisions in corporate affairs. Governance provides the structure through which corporations set and pursue their objectives, while reflecting the context of the social, regulatory and market environment. Governance is a mechanism for monitoring the actions, policies and decisions of corporations. Governance involves the alignment of interests among the stakeholders.

There has been renewed interest in the corporate governance practices of modern corporations, particularly in relation to accountability, since the high-profile collapses of a number of large corporations during 2001–2002, most of which involved accounting fraud. Corporate Scandals of various forms have maintained public and political interest in the regulation of corporate governance. In the U.S., these include Enron Corporation and MC inc.(formerly WorldCom). Their demise is associated with the US Federal Govt. passing the SO act in 2002, intending to restore public confidence in corporate governance. Comparable failures in Australia are associated with the eventual passage of the CLERP 9 reforms.

I. Corporate governance models around the world

- Continental Europe
- India
- United States, United Kingdom

II. Regulation

- Legal environment – General
- Sarbanes-Oxley Act of 2002

III. Codes and guidelines

- OECD principles
- Stock exchange listing standards
- Other guidelines

IV. Parties to corporate governance

I. Responsibilities of the board of directors

II. Stakeholder interests

III. Control and ownership structures

A. Family control

B. Diffuse shareholders

IV. Mechanisms and controls

- Internal corporate governance controls
- External corporate governance controls
- Financial reporting and the independent auditor

V. Systemic problems of corporate governance

VI. Debates in corporate governance

- Executive pay
- Separation of Chief Executive Officer and Chairman of the Board roles

Compliance and Ethics Program

There has been a long history of business and government excesses and subsequent legal, public and political reaction. Response to criminal misconduct has resulted in legal sanctions, governance practices, compliance standards and cultural transformation. Over the last 40 years, several major events in American business and subsequent legislation and regulation have shaped the way organizations do their business. The events with the most significant impact and influence in the development of ethics & compliance programs are the Foreign Corrupt Practices Act, the Committee of Sponsoring Organizations, and the Federal Sentencing Guidelines.

I. Foreign Corrupt Practices Act

II. Committee of Sponsoring Organizations

III. Federal sentencing guidelines for organizations

IV. Effective program design

A high-performing compliance and ethics program is best organized as an integrated capability assigned to business functions/units while managed and overseen by individuals with overall responsibility and accountability. Compliance can be a daunting challenge, but it is also an opportunity to establish and promote operational excellence throughout the entire organization and significantly improve the overall operational performance.

Broadly understood, compliance is an important mechanism that supports effective governance. Compliance with regulatory requirements and the organization's own policies are a critical component of effective risk management. Monitoring and maintaining compliance is not just to keep the regulators happy, it is one of the most important ways for an organization to maintain its ethical health, support its long-term prosperity, and preserve and promote its values.

On a more practical level, a compliance and ethics program supports the organization's business objectives, identifies the boundaries of legal and ethical behavior, and establishes a system to alert management when the organization is getting close to (or crossing) a boundary or approaching an obstacle that prevents the achievement of a business objective.

Once an issue is detected, management must be prepared to respond quickly and appropriately to minimize the impact on the organization (and the community, as appropriate). Management should continuously improve its compliance and ethics program. This will enable it to better prevent, detect, and respond to similar misfeasance and/or malfeasance in the future.

Like any other core capability and/or process, the compliance and ethics program should strive to deliver tangible benefits and outcomes to the organization. Every organization is unique and has its own objectives. As such, several objectives of the compliance and ethics program will be unique as well. That said, there are a few universal program outcomes/objectives that a compliance and ethics capability should deliver. These include an enhanced culture of trust, accountability and integrity; prevention of noncompliance, preparation for when (not "if") noncompliance occurs, protection (to the extent possible) from negative consequences, detection of noncompliance, response to noncompliance and improvement of the program to better prevent, protect, prepare, detect and respond to noncompliance.

An important aspect of a high-performing program, and one that cannot be overstated, is enhancing the culture. A strong culture that provides important benefits would including a "safety net" for when formal controls are weak or absent, and an open environment of trust, accountability and integrity – all of the ingredients that help drive overall workforce productivity.

A well-designed compliance and ethics program is only half the picture. Critical to its success and its ability to meet the challenges of constant change, increasing complexity, rapidly evolving threats, the need for continuous improvement requires organizations to have the commitment of both senior management and the board, adequate authorization and funding, the appropriate tools to facilitate measurement and rolling-up information, comprehensive training on the measurement process and an early socialization of approach.

V. Effective program implementation

VI. Measuring program performance

VII. Future outlook for ethics and compliance programs

Crime Prevention, Detection and Workplace Violence

I. Crimes related to office

II. Bribery

III. Abuse of personal data

IV. Harboring a criminal

V. Forgery of official documents

VI. Blackmailing

VII. Preventing Workplace Violence

- A. Organize a WPV Team
- B. Develop and disseminate a Policy against it
- C. identify and Evaluate potential threats of violence
- D. Provide mechanisms for reducing or eliminating threats

VIII. Preventing Sexual Harassment Lawsuits

- A. Policies
- B. Benefits to Employer
- C. Zero tolerance
- D. Clear Definitions
- E. Specify Consequences
- F. Monitoring

G. Training

H. Discipline

I. Retaliation

J. Complaint Procedure and investigations

K. Complaint Procedures

IX. Workplace Hostage Situations

A. Training/Active Shooter

B. Establish verbal and written SOPS

C. Crisis Management Program

D. COMM Plan

E. Safe Havens / Areas

F. Leaders and Followers

Fraud Deterrence

Fraud deterrence has gained public recognition and spotlight since the 2002 inception of the Sarbanes-Oxley Act. Of the many reforms enacted through Sarbanes-Oxley, one major goal was to regain public confidence in the reliability of financial markets in the wake of corporate scandals such as Enron,WorldCom and Waste Management. Section 404 of Sarbanes Oxley mandated that public companies have an independent Audit of internal controls over financial reporting. In essence, the intent of the U.S. Congress in passing the Sarbanes Oxley Act was attempting to proactively deter financial misrepresentation (Fraud)

in order to ensure more accurate financial reporting to increase investor confidence. This same concept is applied in the discussion of fraud deterrence.

Until recently, fraud deterrence has not been specifically identified under one common definition. While it has been discussed by many authoritative sources such as the American Institute of Certified Public Accountants (AICPA) Practice Aid Series, "Fraud Detection in a GAAS Audit: SAS No. 99 Implementation Guide," (explicitly) The Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Internal Control – Integrated Framework," (implicitly) and the National Association of Certified Valuation Analysts Certified Fraud Deterrence Analyst (CFD) designation (recently merged into the Certified Forensic Financial Analyst (CFFA) designation), an actual definition of the term "fraud deterrence" has been difficult to find.

I. Deterrence vs. Prevention

II. Fraud Triangle

    a. Breaking the Fraud Triangle

III. SAS 99

IV. The COSO Model

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring
- Insurance Fraud

Investigations

Corporate Investigations practice helps companies assess allegations of corporate fraud or financial mismanagement and respond to government regulator requests. The CSO should work work directly with their corporate personnel such as the Chief Ethics and Compliance Officer, General Counsel, legal department personnel, the Internal Auditor, or other investigation team members when pursuing or processing a case.

Some investigations also require that the CSO work closely with audit committees and outside counsel.

Internal Investigations

An effective internal investigations program should have a wide range of investigative tools at its disposal, such as assisting the HR department with background and personality investigations; carrying out covert surveillance of suspect areas and personnel; the development of an internal intelligence network, through the establishment of an anonymous reporting mechanism (hotline, email), recruitment of informants, exit interviews of outgoing employees and undercover operations. The development of a sophisticated and effective intelligence apparatus not only allows for the company to initiate legal measures against the perpetrators, but will also help in identifying undetected vulnerabilities, allowing the company to develop proper countermeasures to ensure that other employees cannot take advantage of that opportunity anymore. Furthermore, these actions will provide a strong deterrent to other employees that might be contemplating a crime or are already in the process of carrying it out.

Intellectual property

- Product counterfeiting
- Diversion/parallel imports

- Patent/trademark/copyright infringement
- Stolen product resale
- Truck theft
- Warehouse/Plant theft
- Expired/Returns theft
- Waste/disposal theft
- Insider / outsider espionage
- White/Grey/Black market inspections
- Product Loss

Background Investigations

- Strategic Planning and Project Management
- Field investigations
- Finding and buying product for evidence/confirmation
- Investigation of suspects and businesses
- Covert and undercover operations
- Electronic and physical surveillance
- Special/proprietary Information
- Confirmation on product existence before raid
- Personnel and suspect interviews / polygraphs
- Intelligence data basing, analysis and dissemination

• Liaison & coordination with authorities

Risk Management

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards.Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

The strategies to manage threats (uncertainties with negative consequences) typically include transferring the threat to another party, avoiding the threat, reducing the negative effect or probability of the threat, or even accepting some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits).

Certain aspects of many of the risk management standards have come under criticism for having no measurable improvement on risk, whether the confidence in estimates and decisions seem to increase

Process

- Establishing the context
- Identification

- Assessment

Composite Risk Index-Risk Options

- Potential risk treatments
- Create a risk management plan
- Implementation
- Review and evaluation of the plan

Limitations-Areas of risk management

- Enterprise risk management
- Risk management activities as applied to project management
- Risk management for megaprojects
- Risk management regarding natural disasters
- Risk management of information technology
- Risk management techniques in petroleum and natural gas
- Risk management as applied to the pharmaceutical sector

Business Continuity

Business continuity planning (BCP) "identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity". It is also called business continuity and resiliency planning (BCRP). A business continuity plan is a roadmap for continuing operations under adverse conditions such as a

storm or a crime. In the US, governmental entities refer to the process as continuity of operations planning (COOP).

Any event that could impact operations is included, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing/network resource). As such, risk management must be incorporated as part of BCP.

I. Business impact analysis (BIA)

II. Threat and risk analysis (TRA)

III. Impact scenarios

IV. Recovery requirement

V. Solution design

VI. Implementation

Testing and organizational acceptance

- Tabletop exercises
- Medium exercises
- Complex exercises

VII. Maintenance

VIII. Information/targets

IX. Technical

X. Testing and verification of recovery procedures

Crisis Management

Types of crisis

1. Natural crises
2. Technological crises
3. Confrontation crisis
4. Crisis of malevolence
5. Crises of organizational misdeeds

- Crises of skewed management values
- Crisis of deception
- Crises of management misconduct

1. Workplace violence
2. Rumors
3. Crisis Leadership

- Sudden crises
- Smoldering crises
- Signal detection
- Preparation and prevention
- Containment and damage control
- Business recovery

- Learning
- Crisis communication

1. Models and theories associated with crisis management

- Crisis Management Model
- Crisis Management Planning
- Contingency planning
- Business continuity planning
- Structural-functional systems theory
- Diffusion of innovation theory
- Role of apologies in crisis management
- Crisis leadership
- Unequal human capital theory
- Social media and crisis management

Summary:

For many years corporate security has been dominated by a ‘defensive’ approach, focused on protection and loss prevention. The head of security was seen as little more than the ‘guard at the gate,’ someone whose actions invariably stopped people doing their jobs instead of enabling the business to function more effectively. Typically, heads of security came from a narrow talent pool, namely police, armed forces or intelligence.

There are many reasons companies tend to recruit security managers from these backgrounds. The police and armed forces churn out individuals with intensive training in the practice of security and protection, and have hands-on experience that is rarely available elsewhere. There are a number of reasons greater diversity is essential within the corporate security function.

There is a growing recognition of the strategic importance of security and as a result security departments need to operate at a much more senior level.

Matrix organizations require a particular approach to management and leadership, which can be antithetical to those with police or armed services backgrounds. In today's corporate environment, the impact of the security department is proportionate to its ability to persuade individuals and teams all over the company to collaborate and cooperate. This means that dialogue between security specialists and non-specialists is essential.

Traditional security skills are associated with an approach where security is perceived as a 'dis-enabler' of business. Those with formal security training can tend to be risk averse, while businesses need to take calculated risks to stay ahead of competitors, break into new markets and maximize profits.

The corporate security function needs people who are happy breaking rules, innovating and thinking outside the box. Studies of security-related professions such as the police, the ambulance service and local authority emergency planning departments have suggested that 'too much' experience in a traditional security context can inhibit people from making innovative responses to security incidents. Heads of security consistently rated qualities such as independent thinking, willingness to challenge assumptions and behaviors and innovation as being ones they value most in their team. One said: 'I'm looking for people who push the boundaries and constantly challenge the way we work.'

There is a growing recognition of the value of 'the human element'. According to experts, many security professionals are typically trained to address security incidents and

emergencies in ways that fail to factor in the human dynamics of such situations, including the impact of emotions, perceptions and fear on people's behavior. Emotional intelligence is critical to effective alignment, but the human element of security and risk management is routinely overshadowed by the emphasis on technical security skills.

For security to be aligned with the business, security managers must understand the business and how they contribute towards its objectives.

The Chief Security Officer (CSO) is the corporation's top executive who is responsible for security. The CSO serves as the business leader responsible for the development, implementation and management of the organization's corporate security vision, strategy and programs. They direct 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, and personal risk; establish appropriate standards and risk controls associated with intellectual property; and direct the establishment and implementation of policies and procedures related to data security.

END OF DOCUMENT