

WHITE PAPER

PRESENTED BY :



CREATING AN INFORMATION SECURITY AND INFORMATION ASSURANCE CULTURE

MEETING ENTERPRISE SECURITY NEEDS

Dr. Jim Heimberg, ABC, Ph.D., ISSO

May 12, 2008

Introduction

Leverage Information Systems, Inc. (Leverage) Information Security (INFOSEC) Services is pleased to present this white paper that describes its approach and methodology for creating an INFOSEC / Information Assurance (IA) culture within an enterprise.

INFOSEC Services prepared this white paper to describe how it can assist enterprises in creating the type of culture that will protect information and information systems throughout an enterprise. This is accomplished through a series of processes that may include staff augmentation, training, provision of security awareness training and briefings, and/or specific INFOSEC/IA tasks that the enterprise needs to have accomplished, for which there is not knowledgeable human assets to complete the work. The maturity of the culture will determine what recommendations are made.

Based on industry agreement that the largest threat looming for an information enterprise is the internal threat, creation of an appropriate protective culture may be the single most effective weapon in the fight to protect information and information systems and resources.

Culture – Defined

The United Nations Educational, Scientific and Cultural Organization (Unesco) (2002) described culture as follows: "... culture should be regarded as the set of distinctive spiritual, material, intellectual and emotional features of society or a social group, and that it encompasses, in addition to art and literature, lifestyles, ways of living together, value systems, traditions and beliefs".

UNESCO, of course, was determining culture on a global scale based on nations, geographic areas, and vast populations that may or may not be under a single rule of law. In the world of business and government today, cultures are set within parameters of management's ability to communicate to its stakeholders (e.g., employees, shareholders, and public) to demonstrate how it wants business performed and/or mission fulfilled within the organization. Each organization has a responsibility for managing assets, processes, and information that are needed to fulfill mission assignments and/or to compete in the business arena. Whether governmentally based or commercially based, the parameters do not change from management of assets, processes, and information.

Management can only manage through a process of management communications, the ability of management to oversee and direct business workflow. The phrase "business workflow" is used to define the day-to-day business operations of the organization; in other words, the work the organization does to meet its goals and objectives, to fulfill its mission, and commercially to remain competitive. This is true whether the key organizational goal is a product, service or other accomplishment. Another way to view it is to understand that management is getting things done with people. Organizations must be able to get the cooperation of people both inside and outside the organization in order to achieve their objectives. Thus, it is a management imperative to create a culture within the organization that stakeholders are expected to respect and adhere to when working for the organization.

Compliance Requirements and Culture

During the last 20 years, there have been a spate of laws, rules, regulations, and codes established in the Information Technology (IT) arena based on the exposure of data and information in the computerized world. This includes creation of:

-] Computer Security Act of 1987 (CSA)
-] Information Technology Management Reform Act of 1996 (ITMRA) (aka the Clinger Cohen Act)
-] Health Insurance Portability and Accountability Act of 1996 (HIPAA)
-] Gramm-Leach-Bliley Act of 1999 (GLBA) (aka Financial Modernization Act of 1999)
-] Federal Information Security Management Act of 2002 (FISMA)
-] Sarbanes-Oxley Act of 2002 (SARBOX or SOX) (aka Public Company Accounting Reform and Investor Protection Act of 2002)
-] National Infrastructure Protection Plan (NIPP) (2005)
-] Federal Information Processing Standard (FIPS) 200 (Minimum Security Requirements for Federal Information and Information Systems (2006)

For example, the following table describes some of the requirements of the laws, rules, regulations, and codes described above. It also maps nicely to the training those who hold these roles should receive.

COMPLIANCE REQUIREMENT	C S A	I T M R A	H I P A A	G L B A	F I S M A	S A R B O X	N I P P	F I P S 2 0 0
Information System Security Officer (ISSO) Role Training								
Risk Management	X	X	X	X	X	X	X	X
Vulnerability Management	X	X	X	X	X	X	X	X
Disaster Recovery Planning (Incident Response & Contingency Planning)		X			X		X	X
Business Process Management		X			X	X		X
Audits & Surveys			X		X	X	X	X
Knowledge Management		X			X			X
Configuration Management		X			X			X
C&A (C for both) and/or Security Test & Evaluation (S)		C	S	S	C	S		X
Solutions Management	X	X			X			X
Strategic Planning		X						X
Information System Security Engineer (ISSE) Role Training								
Test & Evaluation		X	X	X	X	X		X
Vulnerability & Penetration Testing		X	X		X	X		X
Forensics	X	X	X	X	X	X		X
Architecture & Design		X			X	X	X	X

Nowhere is this more stringent than in the Federal government where the protection of national security rests on the protection of information and information systems. However, many states have enacted

similar requirements on information and information systems and business has come to realize that the ability to maintain competitiveness and productivity relies heavily on information systems and protection of the data and information they hold.

Some organizations unknowingly take unacceptable risks with customer data. They assume certain technologies provide greater levels of security than they actually do or that a process is not vulnerable to a breach. Those assumptions often lead to breaches that lead to bad publicity and can result in significant financial losses.

How Can an INFOSEC/IA Culture be Created

One of the key functions within an INFOSEC/IA culture is implementation of a Defense in Depth approach. Defense in Depth is a strategy in which multiple layers of defense are placed throughout an IT system. It addresses security vulnerabilities in personnel, technology, and operations throughout the system's lifecycle. It is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations. The following figure demonstrates this graphically.



The use of technology is based on smart decision making in the IT management area of the organization. The reliance on operational control stems from management's ability to communicate its desires and goals to those working in the enterprise. The people issue is twofold. The first is based on ensuring that only trustworthy people are given access to sensitive data and information and to the information systems on which the information and data resides. It is the responsibility of both Human Resources and the access control system. The second part is the receptiveness of the people to taking direction, understanding INFOSEC/IA sufficiently to perform their tasks safely and securely, and being sufficiently iterative to apply best practices for INFOSEC/IA in the absence of specific direction. This is accomplishable through development and delivery of a comprehensive set of policies and procedures directed at safe, secure management of information and information systems; training and awareness being provided; development of a comprehensive access control system; a functioning change control and change management system; and security administration. The following figure demonstrates the balance required for the people portion of the Defense in Depth approach.



Policy and Procedure Development

Direction from management can take many forms; however, for semi-permanent directions, the clearest method to use is the development of policies and procedures. Policies with regard to IT security should be developed as simple minimally sized documents with a single topic in that document. Typically they should be no more than two pages even with formatting and boilerplate. Procedures should be tied to policies with the policy either as the driver of the procedure or as the way of ensuring valid processing within constrained paths. A procedure should be developed with two audiences in mind. First and foremost, the people who will be performing the procedure, who need step-by-step instructions that only assume the level of knowledge required by their assigned job description. Secondly, the procedure should consider managers of the various departments and how the steps interface between departments. In this case, the steps should be organized by department or branch.

ISSOs should be involved in drafting policies and procedures for INFOSEC/IA issues.

Business Process Analysis

To adequately understand business workflow, ISSOs must be involved in Business Process Analysis (BPA) for any process that includes INFOSEC/IA issues. Specifically this means reviewing or developing procedural flow charts, building project plans for specific efforts, and reviewing all documentation that drives how the efforts will be performed by knowledge workers. ISSOs must be knowledgeable in working with business processes beyond the scope of INFOSEC/IA.

Training and Awareness

According to the National Institute for Standards and Technology (NIST), security awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the

effectiveness of the awareness and training program. This is also true for a successful IT security program. Thus, everyone involved in INFOSEC/IA effort as an end-user of IT systems, administrator, or any other role must be provided with training and awareness if they are to function properly in their roles.

Because the human factor is typically your weakest link, well-educated and security-aware employees go a long way in the securing of your environment. -- ComputerWorld 2007

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.

Nearly all organizations provide annual security awareness briefings under compliance requirements. These briefings are the best tool to preventing the social engineering of personnel by competitive-, criminal-, or espionage-related attempts.

Most organizations attempt to either train security professionals within the organization or attempt to hire trained individuals from outside the organization. In the short term, that is a good approach, but professionals need to remain vigilant and up to date with regard to INFOSEC/IA issues as the technology changes rapidly. Thus, training must be an ongoing effort within the organization.

Each organization should have a plan in place that outlines how awareness and training will be performed within the organization.

Configuration Management (including Access Control and Change Management)

Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, details the importance of Configuration Management to INFOSEC/IA. This is based on providing an up-to-date description of the organizations IT systems, detailing how access control to the information and systems is performed, and conducting change management and change control efforts throughout the lifecycle of each system.

A well-conceived Configuration Management system will contain as Configuration Items (CIs) specifications of hardware and firmware, digital copies or originals of software and the lines of code used in firmware, and documents that describe products in use throughout the organization. It should also contain as CIs test reports from product tests and Security Test and Evaluation (ST&E), leading up to authorization to operate on an operational system. At the Federal level, ST&E is further documented through a Certification and Accreditation (C&A) process and the documents that result from that process should also be managed as CIs.

This view of as-is systems can then be used to manage change, whether in the form of the processing of a change request or determining the best methods for managing patches and upgrades to operational software. Generally, these changes are managed through a series of boards with the Configuration

Management Board (also known as the Change Management Board) at the top level and Configuration Control Boards for large complex systems the require intimate knowledge and separate expertise from the rest of the enterprise.

Finally, the Configuration Management organization often oversees and manages the Access Control System ensuring that access control efforts are handled with the same level of expertise as changes to existing systems.

INFOSEC/IA Administration

Administration of these types of efforts are handled and managed by a designated person who is responsible for all INFOSEC/IA issues. That person may have the role of Chief Security Officer, Chief Information Security Officer, Chief Information Assurance Officer, Information Security Manager, or any number of other similarly functioning named titles.

The guide under which all of this occurs is usually a single document, which may be called the Security Program Plan (SPP). The SPP should detail all areas of INFOSEC/IA responsibilities and the level of effort required to ensure proper functioning.

Success Criteria

For a security manager to determine what constitutes success is going to be one of the most difficult tasks the manager will undertake. Existing metrics and dashboards do not cover the wide array of INFOSEC/IA responsibilities as detailed in FIPS 200, which for the purposes of this white paper are considered best practices for the breadth of an INFOSEC/IA practice.

IT systems operate on binary principles, meaning that data is preserved and evaluated based on being either a 1 or a 0, signifying a YES or a NO. Building an array of questions that get at the complexity of INFOSEC/IA responsibilities would be extremely difficult and there are no magic boxes into which a checkmark indicates success. From senior management's perspective, the balance is between exposure and the number of breaches, time and assets required as opposed to delays in workflow processes, and the costs of a breach based on the likelihood of occurrence. However, that obviates two categories, one called errors of judgment (whether intentional or unintentional) and the other is unforeseen risks.

Management looks to INFOSEC/IA professionals to provide them with the information they need to operate and manage the organization. The best approach is to tightly manage the process using a common body of knowledge and a history of security issues as the guide to the processes that must be managed well to avoid breaches. This is a knowledge management task. Some of this information can be garnered from public sources such as the Federal Bureau of Investigation's (FBI's) Computer Emergency Response Team (US CERT) at <http://www.us-cert.gov/current/index.html> or the CERT Coordination Center at Carnegie Mellon University (URL: <http://www.cert.org/>).

The key is to have a good plan, follow that plan as closely as possible, and have positive results including no damage to workflow processes.

The Leverage Approach

Leverage has the pre-requisite experience working with customers to mentor security managers, teach security professionals, augment staff, and/or undertake specific projects on behalf of a customer. We evaluate all the work we do both internally and for our customers to determine how effective it is. We have a cadre of knowledgeable, skilled professionals in the full breadth of INFOSEC/IA efforts as specified in FIPS 200 all under a single INFOSEC Services umbrella.

Typically, we recommend that our customers undergo an operational risk assessment that focuses not only on the highly visible risks that are very apparent, but that also gauges how well the organization can incorporate a culture that includes sensitivity to all facets of an INFOSEC/IA program.

From that point, we can mentor an existing staff member who will have INFOSEC/IA responsibilities or augment the IT staff with a knowledgeable senior ISSO to oversee the process of putting together a security program and the SPP that will describe it.

As the practice is put into place, further support for augmentation or handling of specific security tasks can be accomplished until the organization is happy with the make up of its INFOSEC/IA practice.

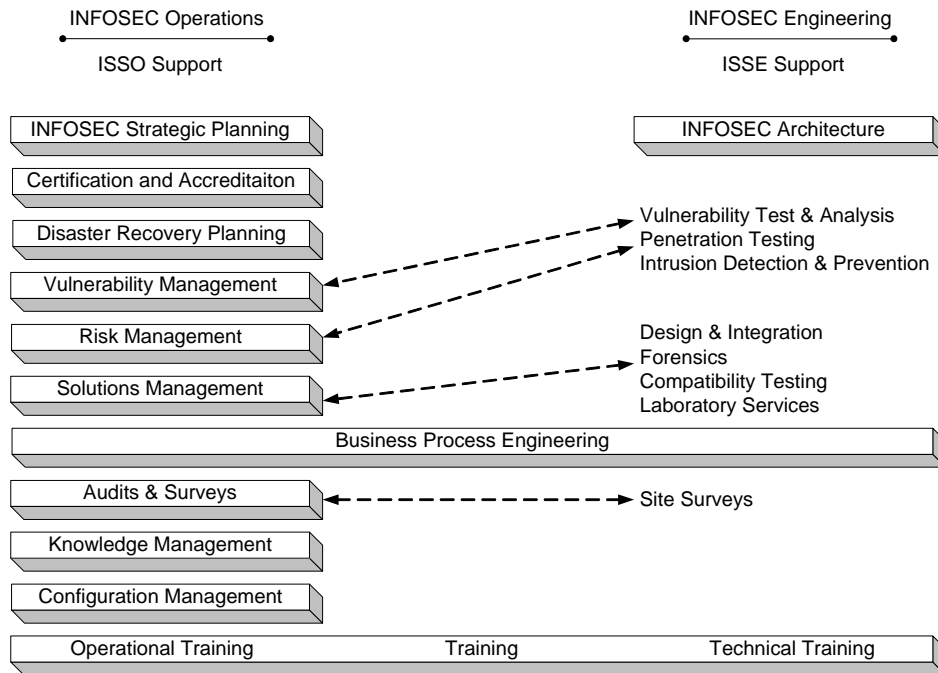
Leverage Support Services and Product Offerings

If planned and executed appropriately, developing this type of program can ensure that information, information systems, and the people involved with those systems are secure and safe as a result of the organizations ongoing IT operations.

Leverage's INFOSEC Services organization specializes in providing ISSOs and Information System Security Engineers (ISSEs) to perform this work and to ensure that potential risk conditions are identified and that best security practice protection mechanism and remediation solutions are presented to the customer. INFOSEC Services operates from a holistic approach to INFOSEC, which means a balanced approach with the breadth of coverage for all areas that should be managed under and INFOSEC/IA organization.

The following graphic describes the offerings of INFOSEC Services and the breadth of the practice.

INFOSEC Services Offerings



For more information on Leverage’s INFOSEC capabilities and service offerings, refer to the contact information provided on our Website: www.INFOSEC.leverageis.com. A representative is ready to provide additional information.