



White Paper

ENTERPRISE INFORMATION SECURITY: A SYSTEMS ENGINEERING PROCESS

Disclaimer

This is one of a series of articles detailing information security procedures as followed by the INFOSEC group of Computer Technology Associates, Incorporated, also known as CTA. These articles are copyright by Computer Technology Associates and may not be reproduced or used for profit without the expressed written permission of CTA or as included in contractual arrangements with clients of CTA.

For further details as to the process and the procedures followed, contact:

Computer Technology Associates, Inc.
INFOSEC Group
7150 Campus Drive, Suite 100
Colorado Springs, CO 80920
(719) 590-5100

The Challenge:

Enterprises today operate in a high tech, open networked environment. Enterprises depend on IT to successfully compete in domestic and international markets. Most enterprises do some business electronically. More and more enterprises are losing millions of dollars due to high-tech crime and IT misuses and abuses. The crimes include financial fraud, telecommunications fraud, theft of proprietary information, computer viruses, thefts of computers and their components, and sabotage of data or networks. The cyber terrorism threats to critical infrastructure IT assets are real. The threats come from many sources: human intentional and unintentional, environmental, and structural. Furthermore basic operating systems for desktop computers and other commercial software is produced, delivered and implemented with an alarming number of security weaknesses. Enterprises are concerned about Enterprise IT Security and what do to about it.

Unfortunately, today's information security practice in many organizations is in a similar state to that of system development 20 years ago when the focus was oriented toward isolated individual systems solving narrow problems rather than enterprise level interoperable solutions. This approach is often the result of a knee-jerk reaction to discovered security vulnerability from external and internal sources threatening to disrupt and/or violate the confidentiality, integrity and/or availability of critical information system resources. It is supported and encouraged by an industry focused on providing point solutions. The result in many organizations is a piece-meal solution, which addresses security problems as they are encountered using a diverse set of products with little or no interoperability. While this approach is initially expedient, it eventually evolves into a complex set of diverse products with an ever-increasing set of issues and costs that must be managed and maintained. It either fails or inadequately addresses many of the fundamental security issues including appropriate policy and procedure documents, awareness, and training, and also makes comprehensive auditing difficult at best and impossible at worst. A disciplined systems level approach to security focused at the enterprise level and addressing the entire problem, can bring order to this complex area. As with any good systems engineering effort, it should be methodology-based with the methodology tailored to each individual situation. This approach will identify the real security requirements, along with the information to be protected, and lead to a comprehensive solution with known interactions and independencies with various systems, processes and individual solutions. With new efforts the approach should begin at the system requirements level and include security as an integral part of the overall system engineering process. This approach is equally applicable to existing systems and can provide a comprehensive security roadmap that can be implemented based on risk tolerance, time and budget. It is only through this type of disciplined approach that a comprehensive, cost-effective and manageable security can be deployed for the long-term.

Until enterprises take a more disciplined and structured approach to information security through a fully implemented entity-wide security program, there is a significant increased risk that controls will not be adequate, properly implemented or applied consistently across each of its domains. The CTA Enterprise Information Security Systems Engineering (SSE) Methodology depicted in the accompanying diagram is such an approach. (The graphic may be printed for easier viewing. Return to the Solutions, White Papers and Case Studies page and select Security SEM Graphic.)

The Solution:

With our Enterprise Information Security Systems Engineering Methodology, we have the "yardstick" for the lifecycle development of Enterprise IT Security. The process is applicable to any type of business. CTA applies the process to enterprise information assets at state governments, corporations, or health care facilities with equal success. CTA uses standard methodologies and practices across the enterprise designed to ferret out the security functional and performance requirements driven by a systematic analysis of the value, sensitivity and criticality of system information assets and services, the threats to the enterprise, and the vulnerabilities of each of its domains. The method is driven by the fact that the enterprise's connected assets are only protected to the strength of the weakest link in the enterprise. The enterprise inherits the risks of all its organizations that share resources.

The CTA methodology consisting of the procedures, processes, tools, products and standards depicted in the diagram is modular. The overall process is based on a repeatable, proven risk management approach. The process reflects military and commercial "Best Business Practices" for INFOSEC. The process results in the systematic allocation of functional and performance requirements to hardware (processors, routers, physical access and detection controls, etc), software (encryption, password management, etc.) and operational (personnel, procedures, administration, etc.) control elements which balance cost and acceptable risk.

The Security Systems Engineering (SSE) Process:

The SSE process has four phases. During Phase I, we establish a well-defined set of security functional and performance requirements designed to ensure the integrity, confidentiality and availability of systems and data supporting the enterprise's critical operations and assets. We develop an Enterprise Security Policy and identify what needs to be done to satisfy the Policy. Our SSE establishes a risk assessment framework beginning with the identification and prioritization (sensitivity, criticality, etc.) of all assets, nodes, networks, and associated infrastructure dependencies and interdependencies that comprise the critical elements of the enterprise to be secured. A risk model of the enterprise is developed which establishes key security requirements commensurate with asset/domain sensitivity and/or criticality. Phase II includes the development of a security architecture comprised of procedures, layered hardware/software defenses and the high-level allocation of functional and performance requirements to this architecture. Generally security architectures are reflections of best practices/standards designed to be commensurate with the protection levels required of the specific system assets. At the highest level, these architectures include **preventive** measures (training, vulnerability scans, network administrative procedures, etc.), layered **protection** mechanisms (firewalls, routers, encryption, VPNs, etc.), **detection** mechanisms (IDS, system logging, context filtering, alarms, etc.), **reaction** mechanisms (automated system reconfigurations, execute manual contingency plans, etc.) and **reconstitution** of system services in the event of a disaster. We interview organizations, develop an INFOSEC Program approach, and perform a macro risk assessment against the Program as a result of using the recommended approach to assure the acceptability of residual security risks.

Phase III, the detailed design phase, involves the allocation of requirements to the "Right Bucket" based on their common functional and/or performance characteristics (hardware/software/operational procedures). The design process is supported by detailed risk assessment for each organization of the enterprise. We produce assessments of Agencies/Departments against Program requirements, a Criticality and Sensitivity Assessment of Data by agency/department, and the Enterprise Security Policy.

The product of the detailed design phase is a set of recommend solutions and approaches to help protect the Enterprise and address specific security issues. We produce Enterprise Security Issues Policy Templates that address subjects such as Internet use, Intranet use, LANs, access control, and other security subjects. We also produce an Independent Assessment of Products to solve specific security issues. The products may include security policy enforcement tools for servers, virus products, firewalls, intrusion-detection system, and other products. Since CTA's is not a VAR for any product, nor does it have exclusive alliances with any vendor, we can recommend the best products for the customer's environment.

Phase IV is IMPLEMENTATION. During Implementation, CTA provides the strategy, schedule, cost estimates, personnel, and program management to implement the Enterprise Security Program. CTA produces a prioritization of program activities, schedule/milestones, costing information, and implementation assumptions/constraints

CTA also provides support to assess and evaluate security products in its laboratory, to integrate security products into the environment, to perform integration test, to assess security, to train personnel, and to monitor firewalls and intrusion detection tools.