Global Information Assurance Certification Paper

SANS - GSEC PRACTICAL ASSIGNMENT

Integrated Security - Getting from A to Z

Establishing metrics to improve the current condition

By Matthew P. Malvaso

ABSTRACT/SUMMARY

This paper discusses the importance of understanding some of the most relevant challenges in existence today with regard to securing enterprise systems.[1] It includes establishing performance metrics to assist enterprises in reaching higher security standards. Securing enterprise systems perfectly is not achievable, however, approaching this ideal should be the goal of every organization that wishes to thrive in today's competitive and hostile computing environment. While security products can assist in protecting the computing environment, it takes much more than a "quick fix" tool to protect complex organizations with a myriad of systems, processes, and personnel to manage. The overarching philosophy within this paper is to treat security not just as a product, but rather as a process to be managed within the larger framework of an enterprise architecture.

CURRENT ENVIRONMENT AND SECURITY RISKS

In order for an enterprise to grow and stay competitive in today's business environment, the risk inherent in opening up a network is a **necessary** risk.[2] Collaboration tools, i.e. sharing documents and exchanging e-mails using client-server and web-based systems, are standard ways of communicating with colleagues, clients, and suppliers. These technologies are necessary tools used to support the business activities in a normal business enterprise. However, the benefits derived from making information more easily accessible to remote employees and enabling speedy data exchange with clients and suppliers must be balanced against the risks inherent in opening up corporate networks.

Some "high level" risks associated with opening up a network and potential impacts of each risk:

- Unwanted person(s) accessing private corporate data can compromise:
  - Corporate computer code
  - Receivable/payable accounts
  - Intranet/message dissemination to employees
- Unwanted person(s) accessing employees' personal data can compromise:

[1] [Note]: The material that follows is based on observations, analysis, and recommendations resulting from work with several clients of my company as well as intensive internet and book research. While some of the information is client-specific, many of the security problems presented in this paper exist in most enterprises. My intentions are to provide a security analyst with an approach that may enable him to tackle the more common security problems that will confront him.

[2] Schneier, Bruce "*Secrets and Lies: Digital Security in a Networked World*", August 2000, pg.176.

- Taxpayer Data
- Social Security Accounts
- Retirement Accounts
- Medial Records

Some possible mitigation strategies for dealing with the above-mentioned risks[3]:

- Conduct system-wide risk assessments
- Identify and prioritize company essential operations and assets and determine a restoration priority for each.
- Establish information security policies and procedures that are commensurate with the identified risks.
- Provide adequate computer security training to employees.
- Institute a process to ensure the security of services provided by a contractor.

When talking about security, it's important to understand that more than just IT systems security is involved. For purposes of this paper, the basic concept is explained below.

INTEGRATED SECURITY CONCEPT

This concept includes the three key elements:

Physical security–that element of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against sabotage, damage, and theft.

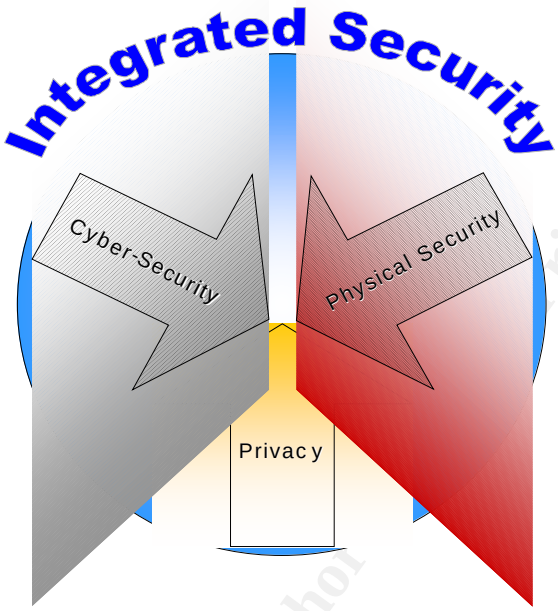
Privacy–ensuring the prevention of the unauthorized access, disclosure, or use of identifying information.

Cyber-security–the protection of confidentiality, integrity, and availability of information technology assets.

These elements must be integrated to achieve a meaningful view of security at any large corporation or enterprise. Figure 1 depicts the conceptual relationship.

[3] GAO-03-303T, Computer Security, *Progress made, But Critical Federal Operations and Assets Remain at Risk*, November 19, 2002.

Figure 1-Integrated Security Concept



Viewing security in a cohesive manner and formulating an overarching security strategy is a preliminary and necessary step for controlling the three above-mentioned security elements. All three elements must be considered when formulating the strategy. If any one of them is not properly controlled or given a set of adequate mitigation strategies, the integrated security concept is weakened. For example, having the most robust firewalls and intrusion detection systems in place, without adequate control over who is permitted access through the front doors of an enterprise, is a contradiction in practice. In other words, a sound practice or policy in one area could be cancelled out by the lack of a policy in another area. Again, a comprehensive security strategy must be thought of in a way that integrates all the key elements.

SECURITY AS AN INTEGRAL PART OF THE ENTERPRISE ARCHITECTURE

SECURITY AND THE ENTERPRISE FRAMEWORK

An enterprise's architecture provides a framework for analyzing an organization's overall security posture, i.e., *the enterprise architecture…defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing needs of business.*[4]

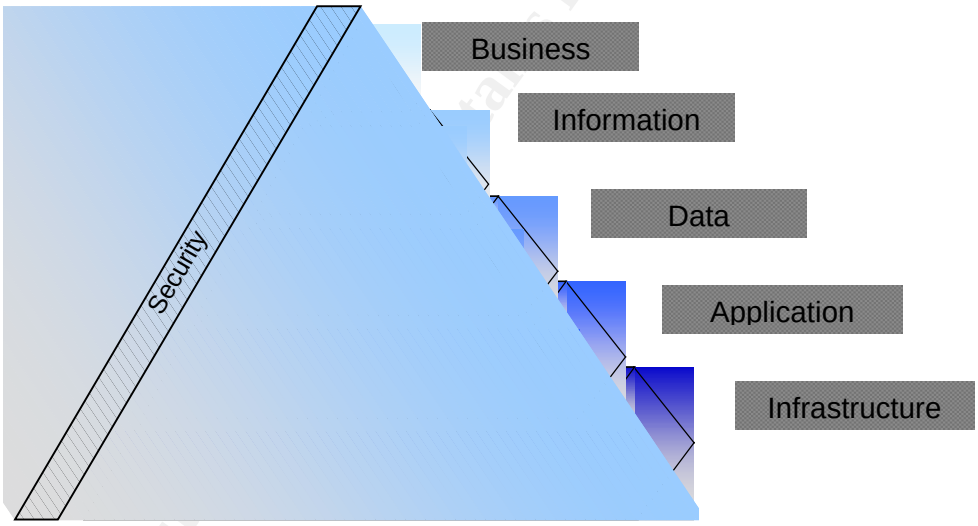
[4] CIO Council, Federal Conceptual Model Subgroup, *Federal Enterprise Architecture Conceptual Framework*, August 1998.

Use of an enterprise approach facilitates the analysis of system efficiencies, platforms, and communications, in alignment with the business needs of an organization. Moreover, it ensures a structured and comprehensive process for evaluating the impact and consequences of changes in technology and business processes. Thus, we can use it to communicate and validate requirements, select a solution, or design a new system.

FRAMEWORK

A framework enables us to focus on security while maintaining a sense of the whole enterprise. Figure 3 depicts a proposed framework.

Figure 3-Conceptual Relationship of Security in an Enterprise Architecture



The framework comprises five separately defined but interrelated architectural layers. The layers are connected in that any change in one layer will impact another layer. The resulting impact can be either positive or negative. For example, an operating system (OS) upgrade (Infrastructure layer) will impact all software in the application layer that operate using an OS. While a change in the requisite data or information necessary to run a business might call for change in the supporting applications or even the network infrastructure.

As depicted in the diagram, security cuts across the entire architecture. It both affects and is affected by each layer. Each of the layers has components that relate to integrated security. The following are examples of each layer's attributes to be identified, inventoried, and related to enable an enterprise-wide view of integrated security:

- *Business architecture*—hierarchy of roles and responsibilities, an organization's business and administrative functions with legislated or directed security or control practices.

- *Information architecture*—identifies processes, information flows, information requirements, and relationships among other business areas, functions, and processes. Major influences on the information architecture are people, culture, internal policies, budget, organization, and technology drivers.

- *Data architecture*—ability to create, read, update, and delete data.

- *Application architecture*—access control lists, user login.

- *Infrastructure architecture*—Basic Service Areas, e.g., firewalls, access control, and virus protection.

The security dimensions of an enterprise architecture have the same characteristics of functional dimensions found in many enterprise architecture models. The security dimension begins with security business functions that contribute to integrated security. These functions, constrained by the security principles will drive all security decisions made in each architectural layer.

A good starting point from which to derive a reasonable set of security functions would come from functions defined in the Executive Order that established the Office of Homeland Security. Other congressional mandates, e.g., security-driven Presidential Decision Directives and GAO reports generated by Congressional testimonies, could also be used to further develop a comprehensive set of security functions.

Successfully integrating security into enterprise architecture is probably the most challenging of the major issues facing enterprises attempting to secure their systems.

Integration of security into a robust Enterprise Architecture is often lacking or non-existent largely due to lack of time, money or narrow mindset of agency Chief Information Officers (CIOs). It is crucial that CIOs comprehend that weaknesses in one area cascade to other areas undermining the integrity of several layers within the enterprise. (*e.g. poor distribution power distribution will adversely impact consumers relying on a steady energy supply into their homes which could, in effect, cause unexpected health problems*). This is just one example which shows the cascading nature of highly complex and integrated systems and a major reason that proper foundation building ("the architecture") from the outset is so necessary for the successful security of systems.

Without ensuring integrity of data, the building blocks of any enterprise, how can we ensure a sound information infrastructure? The component pieces of any system are as essential as the whole system. The data that reside in that system must be trusted in order to trust the system itself and the products created by it. This again leads us to the statement that possessing a comprehensive enterprise architecture necessitates integrating security into the overall architecture approach.

To construct an architecture that will enable organizations to both analyze security needs and deploy security measures, it is necessary to consider the entire network

structure, and then separate that structure into discrete entities, (*e.g. internet, intranet*). These entities are both physical and conceptual. A security risk analysis will determine levels of security exposure for each entity and then appropriate controls can be implemented for each one.

MANAGING CHANGE IN THE ENTERPRISE

Enterprises—whether a government agency or private organization—often undertake activities to improve information technology (IT) within a functional area (e.g., personnel, payroll, grants). A change in the IT services in one functional area may affect other aspects of the enterprise.

For example, a major staff reduction of an IT Call Center without a business process change would likely have a negative impact on its customer response time. However, implementing a more efficient trouble response process using a new and improved trouble-tracking system might counter the productivity loss of a reduced Call Center staff.

One method for quantifying the risks of change could be to use a cost-benefit analysis approach. In the case of responding to a violated system, a security analyst has two very basic options:

1. Do something (e.g. install a firewall, proxy server, or IDS)
2. Do nothing

While option two does not appear reasonable, it may in fact be the most suitable in certain situations. Why? The costs of implementing security systems may be steeper than the costs of losing data or having it compromised. It is recommended that this general type of analysis (with much greater emphasis on potential actions and related costs) be performed on all enterprise assets vulnerable to compromise.

As stated previously, one of the major challenges in IT analysis is to determine specifically what the impacts of change will be. Determining likely impacts requires understanding the interrelationships of an enterprise's functional and technical environment. A comprehensive and effective IT analysis should include a security assessment that cuts across the enterprise architecture layers.

ANALYTICAL APPROACH TO ENTERPRISE-WIDE SECURITY

The described analytical approach deals with the complex interrelationships of guidance, organizations, business functions, business processes, and data, and the information technology that supports them. This approach to analyzing the architecture of an enterprise has five steps:[5]

1. *Establish Security Guidance and Objectives*. Develop a set of guiding principles or high-level requirements or both. These principles show how the

[5] Requirements are continually being identified and documented in every step.

organization must operate using congressional mandates and agency directives as the two major drivers. The security constraints are further defined by agency-created performance metrics. They are used to evaluate the existing architecture and to identify deficiencies that, when corrected, will lead to an effective target architecture.

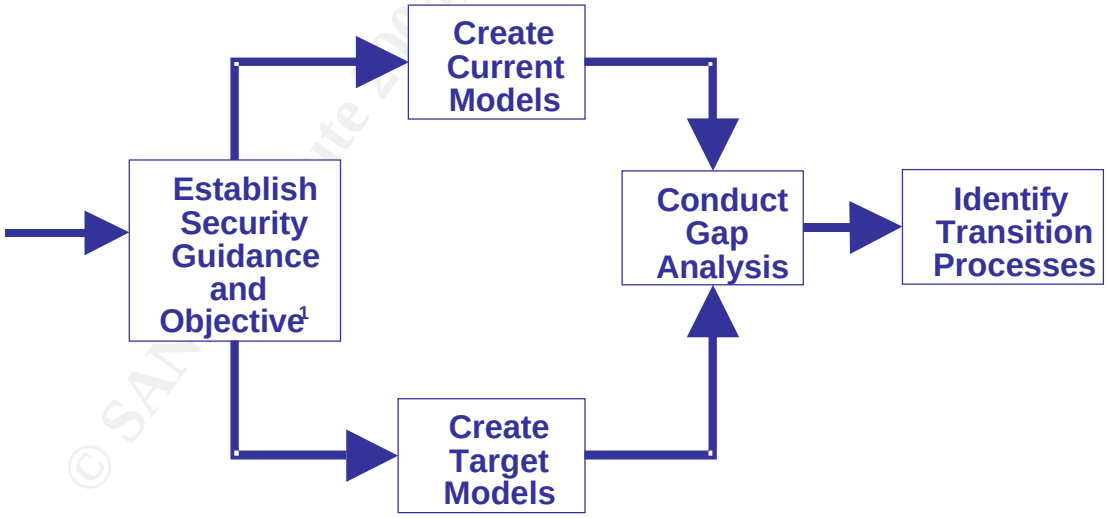
2. *Document the current architecture*. Describe the concept of operations and document the architectural layers (business, information, data, application, and infrastructure) of the current environment.

3. *Develop the target architecture*. Develop the concept of operations and the business, information, data, application, and infrastructure architectural layers of the desired environment, using the guiding principles and the findings from the analysis of the current environment. Develop transition strategies that will be used to move to the target architecture.

4. *Conduct gap analysis*. Identify opportunities for improving the current environment, using the guiding principles and best practices as the basis for analysis.

5. *Identify Transition Processes*. Develop approaches to closing the gaps. Figure 4 depicts the approach.

Figure 4-Analytical Approach



[1]Based on established metrics

This approach is based on previously tested models and has proved successful in identifying gaps between current and target architectures. The most important aspect of this model, seemingly simple, is to know where one wants to arrive at, i.e. where to take the enterprise. Developing a strong set of guiding principles, as previously mentioned is probably the most crucial step in arriving at where one wants to go. Performance metrics, which will be discussed in a later section, ensure that enterprises hold themselves accountable for getting there. To provide a starting point, I'll provide a few basic issues that many enterprises are faced with today.

PREVAILING SECURITY ISSUES

Listed below are eight examples of challenging security issues that require consideration when developing a security program. This list is by no means exhaustive, but rather, consists of an array of some of the most common issues facing enterprises today. *(The section immediately following this one describes performance metrics and how they can be applied to handle some of these issues).*

1 - SECURITY POLICY DOES NOT EXIST.

Security policies are documents derived from business security needs. They lay out the guiding principles ensuring enterprise security. A growing organization and its ever-changing initiatives that involve a shift in the *modus operandi* or current way of thinking, require policies to enforce the importance of the change. The existence of a robust security policy (and management's buy in and enforcement of it) is necessary to have any hope for integrated security in an enterprise. It is important that a newly crafted policy address an organization's unique business and security needs, not just follow the trend of addressing industry "best practices". The right level of detail should be built into a policy, and enable an enterprise to focus on only the most important security concerns. A balance must be met among the security and business objectives of the enterprise[6]. In other words, if a policy is too tight, this translates into resources wasting time filtering the relevant information from the garbage. It is not practical to attempt to screen everything. If a security policy is too restrictive, it will be subverted over time as users try to accomplish business objectives despite the policy. Conversely, too loose of a policy will translate into too little or no guidance for system designers and administrators to follow. While flexibility is important, being overly flexible invites problems. For example, it would not be prudent to construct policy that permits the system administration staff of an organization to choose willy-nilly which software features of an application to enable or disable. First, it is important to survey the business needs of an organization and identify the inherent vulnerabilities that enabling these features would present. If there's no business need to justify the software feature, do not turn it on!

2 - MANAGEMENT SUPPORT FOR POLICY IS LACKING.

While a policy may have been developed, that is still not enough. Policies are only good if enforced properly by management and people follow them -- oftentimes this is the weakest link -- people agree to policies they do not understand or are unwilling to faithfully comply with them. Employees must feel a sense of ownership in the enforcement process by understanding the benefits to themselves and the organization, and being actively engaged in enforcing the policies themselves.

[6] Schneier, Bruce "*Secrets and Lies: Digital Security in a Networked World*", August 2000, pg.155.

Oftentimes, initiatives start on track, intentions are good and things fall apart. Why does this happen? When it comes to the complexity of securing an enterprise system it's important to stay the course, keep employees engaged, and constantly remind all involved of the purpose of their work. Why are we securing the system? To protect ***data***, the heart and soul of an enterprise -- data integrity must be maintained.

3 - SECURITY CONCEPT IS REACTIVE ALONE.

It is very important that when the overarching security policy is created and implemented it address not only reactive methods for responding to breaches and attempts, but proactive methods as well[7]. A reactive policy always puts the enterprise in a defensive position, expecting and responding to intrusion attempts. In order to develop a more comprehensive and robust strategy for protecting the assets of an organization, the security team and infrastructure must be prepared with the knowledge and cutting edge technology to anticipate intrusions, thereby reducing the number of reactive measures needing implementation.

4 - SECURITY PRODUCTS ARE WEAK.

Ok, so a great new product that claims to protect against all the latest viruses and hackers has been installed, now what? This could be a security problem in and of itself -- the "security product" could be a *perfect* tool to protect "other" software applications (which is highly unlikely) and have bugs in its own software code. Design flaws provide a perfect avenue for hackers to exploit. How can one avoid this security weakness? Test, test, re-test and have a lot of faith. Only time will tell how well built the product is. Since systems (and connecting systems) are dynamic and ever-changing it's important to ensure that the security product has maintained the capability to secure the systems it intended to. Hopefully, the product has fared well at other enterprises and the vendor has a reputation for building robust products. Outside of that, a fair amount of trust must be left with the vendor.

An organization's security must be thought of as a system or process, not a technology. Not one security product, e.g., a strong firewall, IDS or proxy server, can protect an enterprise against security breaches. Each of these tools measures a technology. They do not come close to measuring a security process.[8] Security products, by nature, are forms of reactive responses to outside threats. What happens if the threat comes from the inside or from an individual (e.g. ex-employee, contractor) who is intimately familiar with the internals of an organization? A comprehensive process must be set in place to preempt or mitigate opportunities for security breaches. This means educating the workforce and raising the level of awareness to enable creation of a robust system from the outset. Security is a process, not a product -- as a process it has many components -- the better they fit together, the better the process works -- often it's the interfaces between the components that are the least secure.[9]

5 - SECURITY PROCESSES ARE WEAK.

Audit the process as well as the product. Is there a sound policy in place? Does top management proactively support it? Is the organization using multiple products to

[7] Rob Hale, Ian Poynter and Char Sample, "Holistic Security", Jerboa Inc., 2001, pg. 1.
[8] Rob Hale, Ian Poynter and Char Sample, "Holistic Security", Jerboa Inc., 2001, pg. 1.
[9] Schneier, Bruce "*Secrets and Lies: Digital Security in a Networked World*", August 2000, pg.84.

protect itself from various attack types? Is the workforce truly educated on security "best practices"? Is there a sufficient level of expertise and training in the hands of the security folk to "do the job"? These are questions enterprises should be asking themselves in addition to employing the latest and greatest technological tools to fight against system intrusion. Is this enough? No. The enterprise must continuously evolve and react to its ever-changing environment to properly defend against all intrusion types.

6 - DEFENSE-IN-DEPTH PRACTICE NOT FOLLOWED.

A good security system provides multiple layers of security, e.g. one that requires multiple logons for accessing several systems or integrating several intrusion detection systems into a network architecture. We can define a system as "a collection of things or elements which, working together, produce a result not achievable by the things alone."[11] A good security system is much more than just a collection of various technologies and features. It includes the technologies, the process framework that the technologies support, and the environment in which they can all work together to exceed their individual capabilities.

Single sign-on provides a convenient way to eliminate ID and password memorizing, but also contributes to the possibility of a "single point of failure". It is unrealistic to presume that It will be able to handle all the interface programming needed to "tie" legacy and modern systems together.

7 - REQUIREMENTS GATHERING PRACTICE IS INSUFFICIENT.

A thorough requirements gathering process is fundamental to building a system architecture that fulfills the organization's objectives. Building a robust security architecture from the outset is necessary to keep system re-designing to a minimum. Requirements should map to processes/activities that support the overall mission of the organization. Are the security requirements too general? It is important to map the requirements back to the specific missions, goals, and objectives of the enterprise to ensure that only those activities or data supporting the overall mission are protected. What is the use of protecting non-pertinent data, e.g. data/documents not supporting the mission? It is important not to waste resources safeguarding non-essential areas, or an organization should at least tailor the security system to use more resources in those areas where data integrity is most critical.

8 - LACK OF RESPECT FOR THE WEAKEST LINK.

Corporations have spent millions of dollars to beef up security. A big portion of the money is spent on technical solutions such as firewalls, anti-virus programs, intrusion detection systems, etc. The common belief is that the information security problem is best managed by throwing more money at it; protection is directly correlated to the amount of hardware and software deployed to hold back attackers. However, the reality is quite different.[12] Organizations can strengthen their overall security position if they use the resources required to properly secure themselves not just from a technical perspective, but also a human perspective. Since humans either create or comprise all

[10] CIO Council, Federal Conceptual Model Subgroup, *Federal Enterprise Architecture Conceptual Framework*, August 1998.
[11] Rechtin, Eberhardt and Maier, Mark W., "The Art of Systems Architecting", CRC Press, 1997, pg. 254.
[12] http://www.giac.org/practical/Chan_Lieu_GSEC.doc

systems requiring security it is fundamental that adequate respect be given to this most crucial link in the security chain.

SECURITY PERFORMANCE METRICS

As FAR 37.601[13] states:

> Performance-based contracting methods are intended to ensure that required performance quality levels are achieved. Performance-based contracts
>
> a) describe the requirements in terms of results required rather than the methods of performance of the work;
>
> b) use measurable performance standards (i.e., terms of quality, timeliness, quantity, etc.) and quality assurance surveillance plans (see 46.103(a) and 46.401(a));
>
> c) include performance incentives where appropriate.

It is my contention that if a metric-based approach can be used to measure contractor performance, then some of the same principles could be applied to gauge an organization's own performance in the security arena.

Each performance requirement contains the two elements below. In each case, the elements taken together constitute the components of a performance requirement.

- **Performance Requirements** are statements of outcome or results expected of the organization. Performance requirements specify what is to be done; they do not specify how it is to be done.
- **Performance Standards** are the targeted levels of required acceptable performance for determining the accomplishment of specified performance requirements. These may or may not be the same for each performance requirement.

When specified, performance standards may be used to achieve a variety of goals. These include:

- Collection of data to test the practicality of a performance requirement,
- Identification of a performance requirement of less than 100 percent compliance,
- Emphasis on the most critical performance objectives,
- Collection of data to support vulnerability remedies—including the evaluation of past performance, and other similar goals.

Table 1 below links back to the security issues described previously and displays potential performance requirements and standards for each issue. It is important to

[13] http://www.arnet.gov/far/current/html/Subpart_37_6.html

keep in mind that this is just a starter list of possible metrics. The requirements and standards are intended to "set in motion" an enterprise's security program, not solve all potential problems. An important objective when establishing a new program such as this is to establish and maintain momentum. There are a multitude of ways to solve security problems; respond to incidents. The performance metric approach does not constrain "the performer", but rather, encourages his creativity.

Table 1. Security Performance Metrics

Issue	Performance Requirement	Performance Standard
1. Security policy does not exist.	The enterprise shall produce a comprehensive security policy unique to the agency in that it is business process driven and based on guiding principles.	The enterprise shall perform an enterprise systems assessment every six months to evaluate the effectiveness of the performance requirements.
2. Management support for policy is lacking.	The enterprise shall create position descriptions with responsibility given to the hired individual(s) to ensure policy permeates the organization.	
3. Security concept is reactive alone.	The enterprise shall be able to demonstrate its "security awareness" through a well thought security policy as well as during quarterly training sessions.	
4. Security products are weak.	The enterprise shall make testing purchased and in-house created products a continuous process.	
5. Security processes are weak.	The enterprise shall ensure the policy addresses its evolving process change needs due to an environment in constant transformation.	
6. Defense-in-Depth practice not followed.	The enterprise shall demonstrate its use of multiple layers of security protection.	
7. Requirements gathering practice is insufficient.	The enterprise shall demonstrate an ability to map security requirements to business processes and activities.	
8. Lack of respect for the weakest link.	The enterprise shall be prepared to articulate its posture for securing itself against "social engineering".	

SUMMARY

Implementation of a strong security program spanning the enterprise architecture is fundamental to an organization's responsibility to protect its enterprise-level systems. If the above-mentioned prevailing issues are promptly and appropriately handled, without being given time to grow into bigger, more complex problems, an enterprise is well on its way to a secure system. Instituting metrics into the picture will hold organizations accountable in much the same way government contractors are held accountable in sizeable performance-based contracts. Throughout the "life" of any organism or material structure, it is the foundation that is the most important building block enabling a higher probability of reaching its full potential. Building a robust security product and process is no different. While this does not guarantee a secure system, the absence of a program in today's hostile environment assuredly guarantees an insecure one.

REFERENCES

1. Schneier, Bruce "*Secrets and Lies: Digital Security in a Networked World*", August 2000.
2. GAO, Computer Security*, "Progress made, But Critical Federal Operations and Assets Remain at Risk"*, November 19, 2002.
3. CIO Council, Federal Conceptual Model Subgroup, "*Federal Enterprise Architecture Conceptual Framework"*, August 1998.
4. Rob Hale, Ian Poynter and Char Sample, "*Holistic Security*", Jerboa Inc., 2001.
5. Rechtin, Eberhardt and Maier, Mark W., "The Art of Systems Architecting", CRC Press, 1997.
6. Fingar, Pete. Enterprise Architecture for Open eCommerce." URL: http://online.securityfocus.com/library/1418
7. Schneier, Bruce. "Managed Security Monitoring, Network Security for the 21st Century." URL: http://www.counterpane.com/msm.pdf
8. Microsoft, Inc. "Best Practices for Enterprise Security." 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpent/bpentsec.asp
9. Aberdeen Group. "Infrastructure Security: Description." URL: http://www.aberdeen.com/ab_company/researchareas/security-infra-description.htm
10. Hemmendinger, Eric. "Automating Security Patches: A Two-Billion-Dollar Business Opportunity." June 2002. URL: http://www.aberdeen.com/ab_abstracts/2002/06/06020006.htm
11. FAR Manual. "Subpart 37.6- Performance-Based Contracting." URL: http://www.arnet.gov/far/current/html/Subpart_37_6.html
12. Lieu, Chan. "Social Engineering – Attacking the Weakest Link." URL: http://www.giac.org/practical/Chan_Lieu_GSEC.doc