Global Information Assurance Certification Paper

Developing a Coordinated Defense Strategy

A cross-functional approach to planning Information Security safeguards and management processes.

ABSTRACT

This paper explores some of the coordination issues and gaps that are often revealed when analyzing information security effectiveness in an organization. A Coordinated Defense Strategy is one which takes a cross-functional approach to planning, implementing and managing Information Security. To accomplish this, an approach from three perspectives is recommended: 1) ensuring all functions and all staff in the organization are incorporated into the strategy, 2) ensuring all forms in which information is maintained are examined for potential threats, and 3) ensuring that considerations for safeguarding information are based on either specific organizational needs or external regulatory requirements for a given level of sensitivity of information, rather than a 'one size fits all' approach.

In partial fulfillment of the requirements of the SANS Global Information Assurance Certification, Security Essentials Certification

GSEC Practical Assignment (version 1.4b)
Research Paper option
Jim Rowe
Submitted January 20, 2004

Overview

A coordinated defense strategy approaches the practice of Information Security by looking at threats from all sources -- electronic or otherwise – which might adversely affect the protection of sensitive information. To be effective and consistent, information in all forms must be adequately and consistently protected. For example, it is not enough to firewall an organization's network perimeter if physical access controls permit unauthorized personnel to access server rooms or if sensitive information travels with employees (for example on laptop computers, floppy disk or CDROM) in an unprotected form.

It is also suggested that this strategy be developed in such a manner that it considers everyone within the organization whether or not they would be expected to have access to sensitive information. At the very least, building an awareness of the need to protect sensitive information from disclosure and a common understanding of policies and practices can enhance the maturity of the organization and, ideally, can improve the security posture of the organization by increasing the level of understanding by non-technical staff as to the value of following these policies and practices when they process, transmit or store this information.

The fundamental premise for protecting sensitive information in any organization (commercial, government or other) should be the preservation of Confidentiality, Integrity, Availability and Privacy of critical and proprietary information assets. The level of protection will also be consistent with applicable government legislation and internal policy and based on the organization's appetite for risk. But information itself – and risks that threaten it – both exist in many forms. Only by coordinating all defense mechanisms and ensuring that necessary policies and appropriate compliance measures are in place can a reasonable level of confidence be reached in the overall security strategy.

There are many resources from professional associations (like the SANS Institute), consulting firms, government agencies and educational institutions from everywhere on the planet that offer best practices, guidelines and technical solutions for implementing controls and safeguards. This paper focuses on building a requirements-based security strategy that ultimately may draw on one or many of these resources, but the strategy itself is a precursor to, not a replacement of, the design or implementation of a security architecture.

It is hoped that a security strategy and architecture which follows this process will include a variety of elements including business impact analysis, threat/risk assessment, development of an awareness and education program, the development of policies and standards, conducting of vulnerability assessment and penetration testing and, finally, the creation of a security management methodology that takes the results from preceding steps into account.

Current Reality

Basic Information Security measures are widely deployed based on survey results in the 2003 CSI/FBI Computer Crime and Security Survey[1]. This influential publication says:" Virtually all organizations use anti-virus software (99 percent) and firewalls (98 percent)." Despite that fact, it goes on to say that "Fifty-six percent of respondents reported unauthorized use" which is a clear indication of conventional wisdom that firewalls are not enough. The reality is that firewalls, anti-virus protection, access controls and intrusion detection systems (the four most widely used technology based Information Security solutions reported in the CSI/FBI document) are not enough. Even the reality that more than 9 out of 10 organizations are reported to employ physical security measures isn't enough.

Much has been written about the importance of information in organizations (whether commercial, government or other). In fact, proprietary information is often the lifeblood and, in many cases, the key intellectual property of an organization. Therefore, it follows that information security is a pivotal consideration that cannot be addressed solely by the deployment of technology to protect it. Whether the critical information consists of product designs and software source code, customer lists and pricing information, client's financial transactions and account details or personal information that is held by government, banks, insurance and investment firms and health care practitioners – or any other type of information – there are a number of shared concerns that are typically addressed: Confidentiality, Integrity and Availability.

The United States Federal Information Security Management Act (FISMA) definition of Information Security and these attributes reads as follows:

> (1) The term `information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide--
>
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
>
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
>
> (C) availability, which means ensuring timely and reliable access to and use of information.[2]

Even though personal privacy is mentioned under Confidentiality, given the recent move to implementation and/or strengthening of privacy legislation in many countries, it would seem prudent to focus on this issue in particular.

---

1 2003 CSI/FBI Computer Crime and Security Survey

2 FISMA

Developing a strategy

Definitions

Information Security:

Even though the Generally-Accepted System Security Principles (GASSP) document is many years out of date, the following definition appears to be valid even today: “Information security is a combination of preventive, detective, and recovery measures. A preventive measure is a risk control that avoids or deters the occurrence of an undesirable event.” [3]

Strategy:

According to Roget's Thesaurus a strategy is:

> The science and art of military command as applied to the overall planning and conduct of large-scale combat operations.

Information Security doesn't always involve military command or combat (even though at times it may seem like it), but all the other aspects of that definition make sense. This is a science and an art and it does relate to the overall planning as well as conduct. Many operations are large-scale but even in small organizations the complexity factor that applies to this field is significant.

For simplicity, “Information Security” will be taken to include both the responsibility for protecting sensitive information and the responsibility designing, developing, deploying and supporting Information Technology (IT) Security solutions.

[3] GAASP

Foundation for the strategy

The requirement for development of a strategy prior to implementing an IT Security program is often ignored in the rush to implement technical controls in a new or existing enterprise. We are constantly reminded of the threats which result from having an Internet presence. Clearly this is a significant area of concern, whether it is only for web surfing and exchanging e-mail, or for an enterprise with an e-commerce environment. Also, in a setting with significant Internet-facing resources it is sometimes the quantity of traffic and not the type of traffic that influences the risk. The comprehensive list of categories found below is from a public training reference to SANS GSEC[4] curriculum.

1. Networking Concepts
2. TCP/IP, Routing and Host Security
3. Networking Security Overview
4. Information Warfare and Web Security
5. Internet Security Technologies, Network Vulnerabilities
6. Intrusion Detection and Risk Management
7. Introducing Encryption and Cryptography
8. PKI and Steganography
9. Secure Communications
10. Wireless Security
11. Windows Security
12. Windows XP Security and IIS Security
13. Backing up Windows and Unix
14. Managing Software, Systems Services and Auditing
15. UNIX Security

This list, while comprehensive, will not apply in all cases (for example in an environment where there is no wireless, IIS or Unix) so to make the process simpler a list of 6 broader categories has been created. This simplifies the development of a strategy and removes specific technology from the process.

[4] SmartCertify Direct

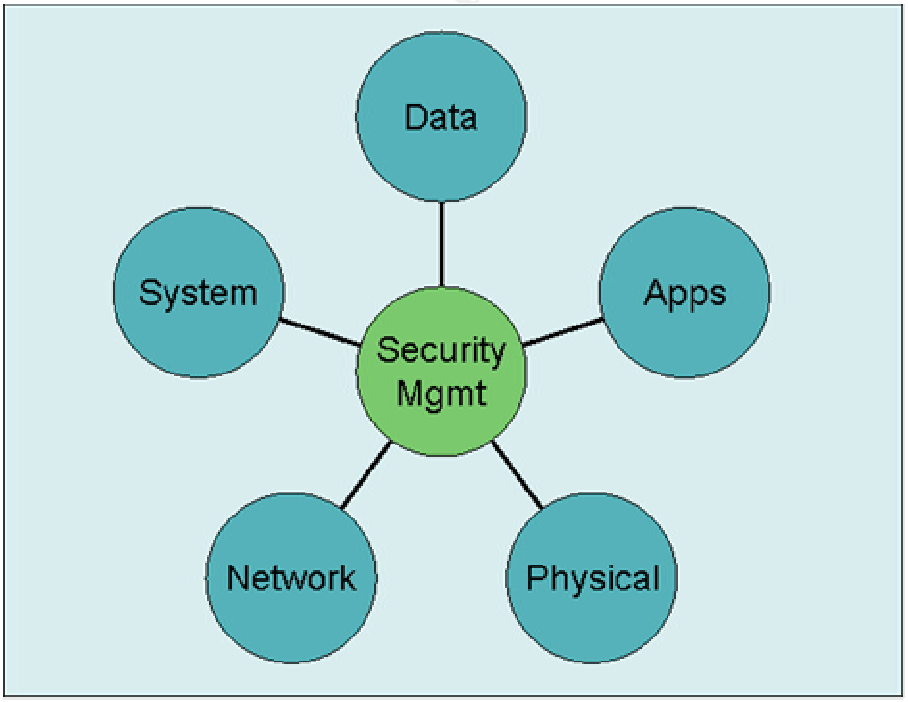
Adapting a well-known model

The list of 'layers' or areas of concern for information security includes security management as the core element, followed by:

1. Physical protection of information assets, media and technology
2. Network (wired or wireless) elements such as routers, firewalls and switches
3. System elements such as servers, workstations, laptop computers, Personal Digital Assistants (PDAs) - including operating system software
4. Applications such as office tools, databases
5. Data – information stored, processed or transmitted electronically

As a reference, this is loosely based on the layered architecture of the TCP/IP protocol[5] and the ISO Open Systems Interconnect (OSI) Reference Model[6] but is related more to the different layers (possibly organizational, definitely different in terms of technology) which exist in most organizations IS or IT departments.

Figure 1 – The different "layers" of information security



[5] Stevens, p. 2

[6] OSI

Rather than show these layers in a stack-based model they are shown with the shared dependency on a strong security management core.

With this model, the basic premise is that protection of the physical layer refers to locks on server room doors, on wiring closets, on locking cabinets, on the ability to prevent unauthorized personnel from entering a building, providing identification badges and the associated monitoring of the physical space.

Although dividing lines between network and system, applications and data can be blurred, it is convenient for the purposes of this model to look at each one for the fundamental reason that safeguards may be different. Access control to a network based on source IP address and login to a Linux system with userid and password are conceptually the same but have different mechanisms.

The same is true for all layers of this model which is shown in Figure 1.

With this model it may also be easier to relate the types of safeguards that need to be in place. A locking mechanism on physical building and room doors is a lock. A password is a lock (as is a token for strong authentication or a digital certificate to decrypt objects in a PKI-based encryption system.

Clearly there are many possible interpretations of what is incorporated in Security Management, but for purposes of this model the intent for Security Management, the hub of the diagram, is to cover a number of elements which include:

- Introduction of an Information Security Program
- Ongoing security strategy development
- Risk Management including Threat/Risk Assessment
- Cost/Benefit Analysis and/or Business Impact Assessment
- Vulnerability Assessment, Patch Management
- Auditing and/or compliance assessment
- Security architecture and design (or the influence on this activity)
- Security policy, standards/guidelines development and security awareness

Depending on the environment and its specific requirements, each of these will be present to a greater or lesser degree. It is beyond the scope of this paper to explore these beyond a superficial level; this paper focuses on development of an preliminary strategy – based on coordinated defense strategy principles.

Combining the multi-layer model with information security core elements

By combining the two groups of previously described factors we can introduce coordination matrix composed of elements from the FISMA Information Security definition and our multi-layer security model.

The matrix, shown below, is the foundation for measuring safeguards and compliance that are key to developing a Coordinated Defense Strategy.

Table 2 - Safeguard evaluation matrix

	Security Management	*Physical Security*	*Network Security*	*Systems Security*	*Application Security*	*Data Security*
prevent unauthorized access						
prevent unauthorized use						
prevent unauthorized disclosure						
prevent unauthorized disruption						
prevent unauthorized modification						
prevent unauthorized destruction						

	Security Management	*Physical Security*	*Network Security*	*Systems Security*	*Application Security*	*Data Security*
provide assured nonrepudiation						
provide assured authenticity						
provide assured privacy						
provide assured propriety						
provide assured timely access						
provide assured reliable access						

This matrix is only one of many tools that will probably be used during the development of the security strategy for a given organization.

The initial challenge may be determining how to start. A top-down approach may be the right one. This involves establishing authority (from senior management delegating responsibility) and often continues with the development of high-level security policies deriving from that authority. Unfortunately, in some cases the start may be as a result of some event that has caught the organization by surprise. In this scenario, analysis of the current reality and identification of critical first steps to correct the problem would be advisable. In the latter situation, the initial focus will be on correcting a known problem rather than proactively establishing or enhancing the organization's structure to define an owner. It is important that once the initial problem is resolved that the remaining elements of the security strategy be undertaken to ensure the coordination benefits of this approach are realized.

In either case, the following sections will address some of the background that may be useful in completing the development of this strategy.

In this model, each aspect of safeguarding and each area of protection would be assessed and rated. For an initial assessment, to determine prioritization of the subsequent work, a subjective rating (High/Medium/Low) could be performed.

The 'why' of a security strategy

Three significant trends in the past decade make it increasingly difficult for IT Security professionals to adequately protect information.

1. Ever-growing ‘connectedness’ to the Internet has raised the potential frequency and impact of network-based threats

2. The migration of information from a resource contained in the datacenter to something that resides on a laptop computer, a personal digital assistant (PDA) or even a cell phone makes the job of protection more complex.

3. As already mentioned, the introduction (and in some cases, strengthening) of privacy legislation adds a fourth component to the three existing principles of Confidentiality, Integrity and Availability that must guide the Information Security strategy as well as its architecture and design.

Over the past several years the visibility and importance of information security – the need for securing information in electronic form, and the technology that processes, stores and transmits this information – continues to accelerate.

What has changed?

Significant improvements have taken place in the decade and a half since the first major IT Security incident on the Internet (then called the ARPANET). In 1988 the Morris worm[7] was an anomaly. At that time, a large amount of sensitive information existed in paper form only. There were no scanners, no webcams, no PDAs, no laptops. Information protection was a different challenge.

In 2004 the typical large private corporate network is more complex than the entire ARPANET was in 1988. There is more computing power in a laptop computer than an 1980's class mainframe. With the massive growth in network size and complexity and the explosion in computing power there certainly are benefits. Business rules can be built into applications. Encryption can be almost seamlessly integrated into applications, online transactions and file systems. Multiple layers of network protection can be achieved without complicated access mechanisms or degraded performance.

[7] CERT

But, with these advantages come added threats. A surprisingly large number of corporate networks still connect to the Internet with little or no protection. Huge amounts of intellectual property are put at risk due to system vulnerabilities which are not corrected, through poor access controls and design limitations.

A co-coordinated defense is a change in paradigm and architecture from previous IT Security defense models. If the typical approach from the 1980's is examined, it was based on a model of Castle and Moat: if you were inside you were trusted, and nothing (or very little) went outside.

In the 1990's, distributed computing and the desktop PC changed that model, but in large part enterprise applications (and their data) remained concentrated in the datacenter. Internet access connected the user to a portal on the perimeter and provided channels of access from the outside in (usually to applications servers located in service networks and restricted operations zones).

For this decade, the trend appears to be toward more ubiquitous solutions. Data is shared (and accessed) in ways that are independent of specific applications, services, platforms or devices. To completely protect the environment, it is necessary to protect the information repositories and the downstream access to information as well as the re-use and re-transmission of information. This shift has made the use of a number of technologies such as encryption, digital rights management (DRM) and content management more important. It has also underscored the need for improved credentials (identity/privilege management and authentication) to ensure that the person who is accessing the data is who they claim to be and that they have been explicitly granted right of access.

The basic principles remain the same

Security professionals often consider a defense in depth strategy to be the same as a coordinated defense strategy, however they differ significantly.

Defense in depth is one of eight security principles (which have appeared in many places without reference, but which appear to have first been published in a well-known security reference in 1995[8]). The complete list is as follows:

- Least Privilege
- Defense in Depth
- Choke Point
- Weakest Link
- Fail-Safe Stance
- Universal Participation
- Diversity of Defense
- Simplicity

[8] D. Brent Chapman & Elizabeth D. Zwicky, Building Internet Firewalls, first edition, <city>, O'Reilly, 1995.

In practice, a "Defense in Depth" approach introduces more than one (and often several) layers of defense for a particular element of security. For example, a simple network perimeter often consists of a single firewall which has an interface to the Internet Service Provider (ISP) on the incoming side and an interface to the private corporate network on the outgoing side.

A defense in depth perimeter typically starts with a screening router which blocks unwanted protocols such as ICMP, followed by a Network Address Translation (NAT) element which translates a private address space on the internal network to those which are registered and published on the Internet. The next layer would potentially be a content filtering engine which blocks specific URLs and ports, as well as specific embedded content, from ever reaching the firewall.

The firewall would be the next layer, performing rule-based access control and probably stateful inspection of packets traversing the firewall. If the firewall supports it, the final layer might be a series of network switches supporting segments that are separated by function: e.g. a restricted operations zone for Internet-facing services, a service network which further directs and filters traffic destined for the internal network or other restricted segments.

The corporate network is built in the same manner with perimeter protection at a suitable level of protection to safeguard the information contained within the network. Additionally, systems which are used to access, process or transmit this information are hardened to reduce risk of unauthorized access to the systems by external hackers and by internal staff.

To continue this example, while the previously-described situation can be implemented in many different ways that are equally acceptable; there are a number of potentially serious coordination issues that impact the very same data that is traveling on this network.

Most recently, the increasing acceptance and deployment of wireless networks adds a complex dimension to the existing wired network. Remembering the fundamental goal of protection of information, it is important to know where the user of the data will be located. It is possible to have an authorized user with valid credentials accessing corporate data on an approved platform (e.g. a laptop computer equipped with adequate firewalling and virus protection) and still have a serious threat to the Confidentiality of the sensitive information being protected. An example of this would be the use of this laptop in a public place (outside the normal workplace with its physical access controls and inherent trust relationship with other colleagues that work for the organization). Even though the data is being accessed by a trusted individual, the environment in which it is being viewed is not trusted. The most likely mechanism would be someone, unknown to the user, looking over the shoulder of the user and viewing the information.

The statistics for an occurrence like this one are not well publicized, but anyone who has ridden a bus, train or airplane recently has probably observed -- without

any effort and without meaning to observe – the use of laptop computers, PDAs as well as binders, notebooks and other carriers of information in public areas.

In reality there are certainly many situations where this practice does not result in loss of confidentiality of sensitive information.

Aside from network perimeter protection, consider the overall goals of building a secure perimeter (which may vary between organizations). Fundamental to these goals will probably be the protection of the internal network from accidental or malicious attack from the Internet or other external network connections (such as business partners). Additionally, to meet the objectives “prevent unauthorized disclosure” and “provide assured propriety” (from Table 1) it should be as important to ensure that the network perimeter does not permit information to be sent from the inside out (again either for accidental or malicious causes).

The “prevent unauthorized disclosure” portion appears straightforward on the surface but it presumes that the organization maintains records of information properties (at least in groupings if not individual documents) that include the related identity management and privilege management attributes. If the identity of the person accessing the document, for example a spreadsheet with sensitive financial data, is not clear due to anonymous access rights then it is not possible to establish privilege management (rights that a user possesses in respect to that information)

To further complicate this example, a database, document repository or disk volume may be configured with appropriate access controls for transmitting sensitive information (again, the spreadsheet) as a file using FTP or a similar network service or as an e-mail attachment but may present no restrictions on local operations with that document. If the user (authenticated or not) can readily transfer a copy of the document to a floppy disk or CDROM or USB stick then the safeguards have not been adequately coordinated.

In reality, much of these safeguards need to be ‘administrative’ in nature rather than technical solutions otherwise the information sharing and business operations effectiveness will be severely impacted. If it is not feasible due to technology or cost constraints to actively prevent an action, an administrative control advises staff by means of a policy or standard that unauthorized copying or distribution of certain documents is prohibited, with repercussions that are based on Human Resources (or Legal) consequences.

It is, perhaps, easier with this explanation to see the implications and risks for potential breaches of Confidentiality, Integrity, Availability and Privacy of sensitive information through this illustration. The ability (based on the lack of safeguard) to manipulate and share information across the physical, network, system, application and data layers of the model in Figure 1.

Implementing safeguards based on IT Security technology

The implementation of a successful IT Security program depends on a number of factors. Before getting to specifics of policies or safeguards that may be put in place, it is important to do a needs analysis of what specific resources are being protected. As previously mentioned, many tools are available to support that activity; often the difficulty is selecting the ones that fit. In addition, the ability to generate an up-front snapshot of the current reality of the state of information security safeguards, policies, practices and requirements can be challenging.

Much in the same way that the GIAC Security Essentials certification material covers a wide range of disciplines for a well-rounded education, it is important to consider a number of aspects of information protection. In some organizations this will require collaboration between multiple teams and departments that have security responsibilities that impact each other.

For example, physical security and IT security are often handled independently and yet the potential impact of deficiencies in physical security on IT Security effectiveness is significant. As an example, consider a server room that has no access controls on doors, thereby permitting entry from any staff member. The potential categories of risk to information stored on the servers ranges from

- availability (someone might inadvertently or maliciously disrupt electrical power in the room),
- confidentiality (unauthorized person might see information displayed on a screen due to an open application running on a sensitive network segment or system) or
- integrity (a malicious intruder might steal disk drives and destroy the data contained on them to reuse the drives in his own machine)

It is for all of these reasons that the coordinated defense strategy is proposed. It can be a useful tool whether applied to gain a snapshot of existing controls or as a maturity or compliance measurement tool. In the former situation a somewhat subjective (or at least superficial) approach can be taken. In the latter case this tool can be used to generate a single ‘dashboard’ of compliance or of progress toward that goal.

Clearly, the overall task of planning for security enhancements would benefit from the use of more formalized methodology such as business impact analysis, threat risk analysis, vulnerability assessment and many other processes beyond the scope of this paper. In the final analysis, this tool may be useful as a first step, as a reporting mechanism or to support use of other analysis processes.

In Conclusion

Effective Information Security protection is a complex discipline which covers a broad range of activities. By merely protecting systems which are used to store (or process) information or networks which transmit information only a portion of the total risk picture is addressed. A coordinated defense strategy provides protection to sensitive information by first understanding the need for protection and then establishing safeguards for the information in all forms and in all places.

Such a strategy is a precursor for designing an overall security architecture so that different platforms and elements of the solution interoperate. Once developed, a security environment can be designed to establish specific controls or safeguards either driven by policies or assured by technology-driven solutions.

Finally, a comprehensive security management function can track the ongoing effectiveness of these safeguards with periodic reviews and by incorporating the security strategy and architecture as an input to further implementations of applications and infrastructure elements. Feedback from this process is most valuable when it is used to adjust the content of the overall security program so that changes which might put sensitive information at greater risk are identified and incorporated into the environment as it evolves.

List of References

1. CSI, “2003 CSI/FBI Computer Crime and Security Survey”, http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf (20Jan2004)
2. US Government of Homeland Security, Federal Computer Incident Response Center, “Federal Information Security Management Act”, http://www.fedcirc.gov/library/legislation/FISMA.html (04Jan2004)
3. Massachusetts Institute of Technology (for I2SF), GAASP (Generally-Accepted System Security Principles) Version 2.0, http://web.mit.edu/security/www/GASSP/gassp11.html (04Jan2004)
4. Curriculum list taken from SANS GSEC Certification Training Course description, SmartCertify Direct, http://www.ffg.com/products/sans-gsec.asp (10Jan2004)
5. Stevens, Richard. TCP/IP Illustrated, Volume 1. Reading: Addison-Wesley, 1994. 2-3
6. “The OSI Reference Model – A Clear and Concise Illustration”, http://www.thecertificationhub.com/networkplus/the_osi_ref_model.htm (17Jan2004)
7. CERT Coordination Center, “Frequently Asked Questions”, http://www.cert.org/faq/cert_faq.html#A8 (30 Dec 2003)
8. D. Brent Chapman & Elizabeth D. Zwicky, Building Internet Firewalls, 1st edition, O'Reilly, 1995.

Additional References

National Institute of Standards and Technology, Computer Security Division, http://csrc.nist.gov/

SANS Institute, Information and Computer Security Resources, http://www.sans.org/resources/