Global Information Assurance Certification Paper

The Holistic Attributes of Information Security

Clint Brady GIAC-GSEC
GSEC version 1.3

Table of Contents

I. Abstract

This paper will discuss the essential components of a solid information security infrastructure. The components covered are personnel, training, education, and security management. Security must be approached with a holistic viewpoint. For the purpose of a simplistic comparison, Information security principals can be compared to home security. With home security, the defense is against intruders entering your home and gaining access to valuables. With information security the defense is against the intruder entering your network and systems and gaining access to valuable information. It all starts with a risk assessment and a policy. A home security policy is not necessarily documented in the tradition sense. However, the goal is to protect the people and valuables within the home. If the home has no people or valuables then the impact of the risk of an intruder is very low. Most homes are packed full of valuable personal belongings and people, therefore the impact and risk is high. Information contained on networks and computers in most cases has a value. This information must be protected in the same sense as the valuables in a home. A home with no doors or windows installed in the openings will attract vagrants and intruders especially if valuables are in the house. This is the equivalent to a network and systems being connected directly to the Internet with no controls. Anybody may view, steal, or destroy information and utilize systems for their own purpose. When doors, windows and curtains are installed, this is the first layer of defense against intruders. A potential intruder will visually inspect the home and may be deterred. The installation of locks, deadbolts, chains, barred windows, and a security system adds more layers of defense to protect and deter. A locked car with the alarm enabled contained in a locked garage with an alarm enabled is applying a defense in depth tactic. The car is not 100% safe but it sure would be hard and time consuming for an intruder to gain the desired access. Networks and systems must also be protected in the same manner. Determining the systems and information with the greatest risk and loss impact will dictate the applications for defense in depth. When assessing risk, impact, and establishing controls a holistic approach must be taken. If you decided to add deadbolts and alarm sensors to the doors and windows in a home but put the door key above the door and put alarm code on a Post-it® on the control panel, a holistic approach towards securing the home has not been applied. It is also imperative that a holistic approach be applied in information security starting with personnel, training, education, and security management.

II. Personnel Qualifications

To protect your assets from compromises and catch intrusions you have to think like and, in essence, become the hacker. The best police detectives are the ones that tap into the mindset and objectives of their perpetrators and are intimate with the legal system. The same principles should apply for information security. The best qualified

information security personnel are the best system and network administrators teamed with the best managers. Security administration personnel need to have mastered their disciplines in systems and network administration. The more practical experience, the better the depth of knowledge. Managers need to have a wide array of experience in infrastructure, application support and development. A manager that has been managing technical support or application development exclusively may not be a good security manager or officer. These support managers are most likely the same ones that may have taken a lackadaisical approach toward security over the past couple of decades. They need the diversity of support and development experience to understand the issues from both sides. They also need to be politically astute and socially apt to provide a convincing influence to business units, organizations, and 'C' level managers. They need to preach and sell information security in the organization and have the backing of the company executives. They need to be familiar with the influence of management structure, corporate culture, changing business models and levels of risk that affect security decisions[1]. The ability of the security manager or officer can make or break the success of an information security infrastructure.

Some Federal, US, and local government employees tend to have a tremendous amount of practical experience and training in information security. Military and intelligence divisions of the government have practiced and been trained in information security for decades and tend to have an excellent foundation for information security infrastructures. Extensive training is an essential component for information security personnel.

III. Training

Staff members play a critical role in protecting the confidentiality, integrity, and availability of information and networks. It is crucial that staff, including managers responsible for information security be trained initially and attend ongoing periodic training. Their qualifications of being the best in the administration discipline and having managerial versatility still are not enough to qualify them for information security positions. Information security requires a different mindset than that of a traditional system and network administrator. The information security team is protecting the assets from internal and external risks. They are also administrating the security systems, while improving on the best-in-class practices. They are continuously educating administrators, employees and managers. They must develop procedures and standards for all employees of diverse business units to understand and practice. They are also responsible for auditing and reporting compliance to these policies and standards. This is a tremendous amount of responsibility. And, for an industry that is in its' infancy the ability to effectively achieve this does not come naturally. It takes training and conditioning much like that of a military organization. The Computer Security Act of 1987 (Public Law 100-235)[2] established requirements for "the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." This

training provides the deep-rooted awareness and practices that are needed in today's public sector. The Computer Security Act and Special Publication 800-16 provides a frame work for results-based and role-based training. Results-based provides a progression of training starting with basic to advanced. The training curriculum is based on the job functions of individuals. By linking training to roles and responsibilities it provides a more practical and applicable curriculum. Role-based training is based on a continuum starting with awareness, building to training and into formal education. Training does not necessarily happen in sequence. Departments will evaluate the scope and needs for training and allocate future needs. This model is used to identify the knowledge, skills,
and abilities an individual needs to perform the security responsibilities that are specific to their role. The type of training needs becomes more comprehensive as individuals perform more complex multi-disciplinary activities. These are two excellent models for organizations to follow.

Training has many components and meanings. Awareness programs should educate on the directives defined in the security policy and how standards, procedures, and guidelines are developed to support the directives. New information security staff must attend awareness training. Once the staff members are fully engaged, the awareness training becomes their responsibility. Information security staff should conduct awareness training for the rest of the organization. They should focus on teaching people how to incorporate and maintain security in general rather than for a specific project. The old cliché, it is more beneficial to teach how to build clocks rather than teach how to tell time, is applicable in information security. The entire organization should undergo awareness training or activities on a regular basis to make a significant impact towards information security. The contribution of efforts to maintain security in the organization must be collaborative. Again, this training should be specific towards building knowledge and skills to facilitate security into job performance and duties.

IV. Education

Education is the capstone of the learning continuum. It creates the expertise necessary for security specialists and professionals. It takes the training and experience to the next level by integrating them with the study of concepts, issues and principals. The desired results are an educated security professional with visionary abilities, responsiveness, and effectiveness. Providing formal education is sometimes outside the responsibility of organizations. Organizations can encourage but cannot force education. Individuals that are career-oriented and strive for continued improvement, will take the initiative to complete formal education. Nevertheless, education is essential for information security specialists to be able to fulfill their roles effectively.

Formal education is becoming a key element to information security. The industry precedent of security specialists bubbling up from the ranks of computer

specialist is changing. Security responsibilities are often assigned as secondary or even tertiary duties. This only reduces the effectiveness of security efforts and creates negative attitudes. It seems that organizations are starting to recognize the complex requirements and the need for formal information security education especially for managers and executives with security responsibilities. Information security principals must be integrated into existing and new technologies. And to make matters even more complex, information security is chasing a moving target that is spawning and evolving at a rapid pace. The number of universities that are offering degrees or even certificates in information security is very small. However, it is apparent that the university systems have realized the need and are acting to meet the demand.

V. Security Management

In this section the Security Management domain will be outlined. There are ten domains of security according to the industry standard set by the International Information Systems Security Certification Consortium (ISC^2)[3]. The domains are listed in table 1.1.

1	Security Management Practices
2	Access Control Systems
3	Telecommunications and network Security
4	Cryptography
5	Security Architecture and Models
6	Operations Security
7	Applications and Systems Development
8	Business Continuity Planning and Disaster Recovery Planning
9	Law, Investigations, and Ethics
10	Physical Security

Table 1.1 – Security Domains

This section will focus mainly on the Security Management Practices domain however, some do overlap. This is not to discredit the remaining nine domains. They are all crucial to a holistic approach for information security. However, I feel that security management is the cornerstone for a successful infrastructure. Security management incorporates the identification of a company's data assets, assigns values and classifications to the assets, develops, documents and implements security policies, procedures, standards, and guidelines all aimed at providing confidentiality, integrity, and availability[4]. The first step in security management is to start developing the policy.

a. Policy

The policy is essential to and provides the framework in which to build the security program and identify the appropriate controls. It will contain many sections and sub policies. Sub policies will be targeted at specific issues. Security policies are living documents. They should be reviewed and updated on a regular schedule. Policy contents will differ for organizations according to their security needs. In December

2000 the Intentional Organization for Standardization published ISO 17799[5] – Information Technology – Code of Practice for Information Security Management. This publication provides the industry standard for Information Security and serves as a good resource for all aspects of information security initiatives including policy. Nevertheless, most policies should contain the following sections. The first section should be the purpose statement.

1. Purpose Statement

This section should state the reason the policy is being developed. There is always a driving business factor for initiatives. In this section, the purpose should be clearly stated.

2. Goal

The goal should detail the desired results of the security initiative. It should be concise and obtainable. If the goal is to simply protect a database containing financial data from unauthorized access or loss, then it should be clearly stated in this section.

3. Scope

The scope will outline the depth and breadth for the initiative. It should state what systems will and will not be applicable. This section will dictate what other specific policies should be developed to achieve the goal. It should also state the personnel and/or contractors that are expected to adhere.

4. Accountability

The policy must be accepted and sponsored by upper management. A top-down approach is required to make the program successful. This section should list the specific person accountable for the various parts of the initiative. It is a good idea to include a table of accountability that clearly identifies the tasks and responsible person or group. See table 1.2 as an example below.

Chart of Accountabilities	
Task	**Owner**
Policy Sponsorship	Chief Security Officer
Policy Education	Security Team Director and Business Unit Directors
Policy Enforcement	Security Team Director and Business Unit Directors
Policy Adherence	All employees – controlled by Security Team Director
Policy Audit	Security Audit Team
Computer Systems Baseline	Systems Admin Team Lead

Network Baseline	Network Admin Team Lead
Telephone System Baseline	PBX Admin Team Lead
Physical Environment	Current Physical Security Contractor-controlled by Security Team Director
Policy Updates	Steering Committee

Table 1.2 – Example Chart of Accountabilities

5. Document Updates

This section should outline the frequency of updates and period of submissions for updates. It should also elaborate on the steering committee set forth to approve and instate updates to the policies.

6. Data Classification

The guidelines for classifying data should be set forth in this section. Data classifications should be properly documented and controls outlined. There are many sources and examples on the Internet. The following example in table 1.4 is taken from the Hawaii Health Information Corporation concerning HIPPA[6]

Data Classifications				
	Public	**Internal**	**Confidential**	**Restricted Confidential**
Criteria	none	Unauthorized disclosure would not significantly impact company or its clients	Unauthorized disclosure could result in significant adverse impact or penalties to company or its clients	Unauthorized disclosure likely to result in significant adverse impact, embarrassment or penalties to company or its clients
Handling			Transport encryption is required when sending over a non-trusted or public network. Physical data is to be stored in locked containers.	Transport and data encryption is required when sending over a non-trusted or public network. Physical data is to be stored in locked containers with restricted access.
Release	Available to general public for distribution	Intended for use only with the organization. May be released for legitimate business needs.	Access and release limited to a need to know basis.	Access and release to only authorized persons with prior approval by managers.

Table 1.4 – Data Classification example

7. Risk Recognition

The recognition section should outline the elements that were discovered in the vulnerability or risk assessment. The details of the assessment should be kept under separate cover. But this section should provide a summary and indicate if access was gained (indicating a risk), if the risk is acceptable, and if controls are required. See table 1.3 as an example below.

Elements	NETWORK ACCESS			PHYSICAL ACCESS		
	Access	Risk Acceptable	Controls Required	Access	Risk Acceptable	Controls Required
Router	Yes	No	Yes	Yes	Yes	No
RJ45 jacks	Yes	No	Yes	Yes	Yes	No
Telephone sets	No	--	--	Yes	Yes	No
Telephone PBX	No	--	--	Yes	Yes	No
1 File Server	Yes	No	Yes	Yes	Yes	No
7 Workstations	Yes	No	Yes	Yes	Yes	No
1 Copier /printer	Yes	Yes	No	Yes	Yes	No
7 parallel printers	Yes	Yes	No	Yes	Yes	No
7 file cabinets	No	--	--	Yes	No	Yes
Office entry	No	--	--	Yes	No	Yes

DATA						Classification			
						Public	Internal	Confidential	Restricted
Client financial data – electronic	Yes	No	Yes	Yes	Yes	No				Yes
Client financial data – paper	No	--	--	Yes						Yes
Computer software storage	No	--	--	Yes				Yes		
Backup Tapes	No	--	--	Yes	No	Yes				Yes
Client statements	No	--	--	Yes	No	Yes				Yes

Table 1.3 – Risk Summary and Recognition

From this point, separate policies should be developed to provide the specifics for security in particular disciplines. These policies should be used to manage the risks associated with specific areas. The risk recognition section along with policy scope statement will provide the framework for additional policies. However, as a general guideline the following categories should have specific policies developed.

- Anti-virus
- Incident Handling

- Passwords
- Backups
- Information Handling
- Network connectivity
- Acceptable Internet usage
- Software installations
- Hardware Installations
- System Access
- Data Access
- System Administration

b. Risk Assessment & Management

Once the policy has been created, it is time to assess the vulnerabilities and assigned values. This should be done using a diverse set of tools to conduct scans and penetration tests. All findings should be documented completely and compiled to demonstrate the risks. See table 1.5 for an example.

Trophy	Access level	User ID	Method	Device	ALE
Sales projections	Administrator	johns	Weak password	10.1.1.5	$100,000
surveillance camera system shutdown	System service	rcontrol	modem	10.1.1.10 555-123-4567	$90,000
Payroll file	User	Guest	No password	10.1.1.8	$40,000

Table 1.5 – Vulnerability Findings and Values

Once risks are collected, they need to be put into perspective. The annual loss expectancy (ALE) should be calculated and documented. The ALE is comprised of an exposure factor (EF), single loss expectancy (SLE), and an annualized rate of occurrence (ARO)[7]. The next step is to set up a security infrastructure to manage the risks that have been identified.

c. Tools

The tools to achieve the control should be a mixture of standards, procedures, applications and/or appliances. When choosing applications and appliances, diversity should be exercised. By choosing different vendors to provide products, a better probability is achieved in providing a more robust solution. The products should complement each other. A mixture of open source, freeware and purchased tools

should be considered. Each product should be evaluated and tested extensively to ensure it will achieve its' intentions. For each control application or technology implemented a detailed implementation plan should be developed and tested. Documentation should be developed to include impact, maintenance, operations, security, and auditing procedures. The security tool set should be able to manage risks, provide auditing and reporting capabilities.

d. Audits

Audits are essential to provide feedback and ensure the infrastructure is operating at peak performance and keeping ahead of the curve. Audits should take place against systems and procedures. When a security baseline is established, audits should be conducted repeatedly until all baselines are in compliance. While this is being conducted, audits are the enemy for most of the staff. Once the baselines are achieved, audits should be used to report the success and accomplishments of the staff. This feedback can now be used to raise the baselines and increase the robustness of the infrastructure. It may seem like a vicious never-ending cycle because it is exactly that. In the same respect, so is the existence and creation of vulnerabilities and people that will continue to exploit them.

e. Reporting

To effectively measure the success and communicate results, reporting is crucial. The organization needs to know the value of and the success the security infrastructure provides. This can only be accomplished with reporting. The security technical control systems must produce reports on success and failure. These reports should be used to compile executive level briefings and be incorporated into security awareness sessions. They should also be used by the security staff to identify areas and systems to investigate for improvements.

VI. Conclusion

Information security is not a walk in the park. It is a very complex, multi-disciplinary, process and procedural driven industry. For some companies this may be a weak point. The government agencies and telecommunication companies are probably the best at this type of operating environment. They have been in existence for decades and even centuries. Over this time, they have learned to build clocks not just tell time. They can effectively remedy problems by adjusting or creating procedures and implementing changes. They also use this same methodology to make improvements. This type of activity lends itself to holistic approaches. As documentation and procedures are well seasoned, meaning they are well tested, reviewed, and updated, they tend to improve in depth and breadth. Information security must be approached in

this same manner. Since there are not well seasoned procedures and processes, the people involved in the creation and support must take extra time to consider breadth and depth.

VII. References

1) Unknown, "Qualifications Overview", March 2002 URL: http://www.metasecuritygroup.com/qualifications/index.html

2) National Institute of Standards Technology, "Training Requirements for Information Technology Security: An Introduction to Results-based Learning" , April 1998 URL: http://csrc.nist.gov/publications/nistbul/itl98-04.txt, March 2002

[1] Unknown, “The SOS Information Security Policies” March 2002 URL: http://www.information-security-policies-and-standards.com/infopolicies.htm

[2] Electronic Privacy Information Center, “Computer Security Act of 1987 Public Law 100-235 (H.R. 145)”, 1987, URL: http://www.epic.org/crypto/csa/csa.html, March 2002

[3] International Information Systems Security Certification Consortium, Inc. “ten domain of Information Security”, URL: http://www.isc2.org/, March 2002

[4] Krutz, Ronald & Vines, Russell Dean. CISSP Prep Guide-Mastering the Ten Domains of Computer Security. Robert Ipsen, 2001, Chapter one.

[5] International Organization for Standardizing, “IOS 17799” URL: http://www.iso.org, March 2002

[6] Hawaii Health Information Corporation,“Data Classification Matrix”,URL: http://www.hhic.org/hipaa/pdf/datamatrix.pdf , March 2002

[7] Harris, Shon. CISSP Certification –Exam Guide. Brandon A. Nordin, 2002 page 81.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event