Global Information Assurance Certification Paper

Latifa Ho
GIAC Security Essentials Certification (GSEC)
Practical Assignment V1.4

Security Management Framework: A New Approach based on John Zachman's Framework for Enterprise Architecture

Introduction

Because of the highly interconnected computing environment, and the shift of business practices (E-Business, E-Government) towards Internet, an open environment **[1]**, the need of central security coordination to manage business risks over information assets have drastically increased. The high profile attacks on the Internet (Nimda, Kleze worm) **[2]** and events such as the September 11 attack in U.S. have no doubt elevated corporate security or security related issues to the top of the corporate agenda. **[3]** However, government officials and security experts believed that "a critical shortage of experienced security personnel -- and not a lack of technological advancement-- is hindering the effort to secure the nation's public and private networks." **[4]** There was also projection that "the corporate world will be faced with a shortage of 500,000 to one million IT security professionals by 2003." **[5]**

Articles on the best practices of information security or ways to realign corporate security function **[6] [7] [8]** can easily be found on the Internet. There are also numerous articles on the qualifications or roles and responsibilities of an effective information security professional **[9] [10]**. Instead of giving readers yet another laundry list of Do's and Don'ts, the author of this paper would like to consolidate all the critical success factors of an effective security function and present them on a "one page" Security Management Framework based on John Zachman's Framework for Enterprise Architecture. The goal is to supply information security officers with a panoramic view of an effective information security function while at the same time give them room to further develop their practice based on their unique environment.

The "Ideal" Information Security Officer

An informal survey was done recently on several users community to gather their perception of an "ideal" information security officer. The author would like to conclude the findings with the following personality traits. They do echo what Asmuni bin Yusof presented in his paper, "Ways to Become an Effective Information Security Professional - from a GIAC Wannabe's Perspective".

Certified Information Security Professional

Certification seems to score high in users' confidence of their (ISO) Information Security Officer's ability in analyzing their security needs and delivering "appropriate, effective and timely information security services". **[10]** Only through training and certification that they are certain their ISO has acquired and maintained "an up-to-date and

significantly broad base working knowledge" on security, disaster recovery and contingency principles; methodologies; mechanisms and techniques (e.g. digital signature, encryption, access control, firewalls, authentication, virus protection, disaster planning and business resumption planning).

Policy Developer

Security Policy is the cornerstone of an information security function or the announcement of the existence of such program. Users do expect to receive this type of document but would prefer it to be clear, concise and practical. The quality of the document will reflect how much their ISO understands their business risks and be able to develop a program to mitigate those risks "within the context of their business objectives and culture". **[11]**

Certified Networking Professional

Since information protection involves creating multi-layer protective shield (also known as defense in depth), it is crucial that their ISO has broad knowledge on networking systems and protocols. It includes knowledge on system administration (Windows CE, Windows NT, Windows 2000, Windows XP and UNIX), LAN administration (Web servers, Mail servers, Hubs and Routers), Internetworking protocols (TCP/IP) and secure Extranet access (VPN services, PKI services, Token Authentication).

Certified Project Management Professional

Security implementation is very likely to be project based. The ISO is expected to manage large security and contingency projects with teams consisting of staff, vendors and business partners. The ability to effectively perform Threat Risk Assessment, Privacy Impact Assessment, Vulnerability Assessment; conduct Cost-Benefit analysis of project options; understand the complete product development life cycle; and make sure that quality is injected in the process is extremely helpful.

Pioneer

Since Information Security has long been ignored or put in the back burner, ISO is often recruited to build the security function from scratch or realign the existing security function. That means he or she has to be very innovative and resourceful and may not have competent Information Security staff to assist at early stage.

"Think like a hacker" is considered to be the best approach in capturing one. Since hackers very often indulge in finding loopholes in new technology for them to explore, the ISO will be required to stay abreast of new technology and its vulnerabilities in order to implement appropriate measures to win the Information Security Warfare.

Excellent Marketer

Communication is the key. The ISO should be busy meeting with people, understanding their needs and obtaining buy-ins from people at all levels. The challenge is to convince everybody that security is everybody's job and establish a security-aware culture.

Chief Information Officer
- Get commitment to allocate resources to combat business threats.

Chief Administrative Officer
- Obtain agreement to establish and maintain risk management programs for information resources.

Information Security Staff
- Provide leadership in implementing policies and procedures to protect IT assets.

Program Managers
- Support them in proper classification of information and data and perform Threat Risk Assessment.

IT Services
- Specify cost effective security controls and audit their implementations.

Staff
- Convey security control requirements to users and teach them to discern social engineering tactics.

Certified Auditor

It would be ideal if the ISO has a designation in IT auditing. If not, he or she is still required to have a detailed knowledge of security audit procedures and protocols and/or be able to work with IT auditors or external security auditors.

Legal Professional

In order to develop and refine the Security and Privacy architecture, he or she has to be familiar with the contents and applications of government legislation, policies, directives and guidelines related to security and confidentiality of information. Examples are the Freedom of Information and Protection of Privacy Act and the Canadian Trusted Computer Product Evaluation Criteria. He or she should also ensure that the services delivered by the Security group meet appropriate industry and international security standards (e.g. BS 7799).

Recommended Practices of Effective Information Security Function

Listed below are "The 10 Key Components of Good Information Security" from Sarah D. Scalet and Scott Berinato's perspective **[12]**.

1. Identify your risks
2. Get the CEO involved
3. Put someone in charge
4. Develop and implement a security policy
5. Educate employees and raise awareness
6. Have a security audit done
7. Incorporate physical security into the plan
8. Remember internal threats
9. Stay tuned in
10. Prepare for the worst.

The 16 recommended practices in the "Practice List for Information Security Management" at www.gao.gov/special.pubs/infosec.guide/body.htm are insightful and worth reviewing as well.

1. Recognize information resources as essential organizational assets that must be protected
2. Develop practical risk assessment procedures that link security to business needs
3. Hold program and business managers accountable
4. Manage risk on a continuing basis
5. Designate a central group to carry out key activities
6. Provide the central group ready and independent access to Senior Executives
7. Designate dedicated funding and staff
8. Enhance staff professionalism and technical skills
9. Link Policies to business risks
10. Distinguish between policies and guidelines
11. Support policies through the central security group
12. Continually educate users and others on risks and related policies
13. Use attention-getting and user-friendly techniques
14. Monitor factors that affect risk and indicate security effectiveness
15. Use Results to direct future efforts and hold managers accountable
16. Be alert to new monitoring tools and techniques

Security Management Framework

What is John Zachman's Framework for Enterprise Architecture?

John Zachman in 1987 defined Framework as "simply a logical structure for classifying and organizing the descriptive representations of an Enterprise that are significant to the management of the Enterprise as well as to the development of the Enterprise's systems." **[13]** His "Framework" is diagramed in a matrix format. The rows represent the points of view of different players in the process (Planner, Owner, Designer, Builder, Sub-Contractor, the System) while the columns represent aspects of the process (Data, Function, Network, People, Time, Motivation). This is a powerful classification scheme that enables "focused concentration on selected aspects of an object without losing a sense of contextual, or holistic, perspective."

Why use John Zachman's Framework to develop the Security Management Framework?

As Eli Primrose-Smith pointed out in her article, "Facing the new corporate security rules", "corporate security can no longer be considered a piecemeal, low-priority operation applied to discrete areas of the organization -- it should be an integrated management discipline." "Companies must take a total enterprise approach, integrating the security of myriad IT activities -- mainframes, the Internet, wireless, systems software and so forth -- into a holistic corporate security solution."

John Zachman's framework suits well with this type of initiative since it is definitely a tool for complex thinking and planning but simple, comprehensive and effective in communication. It offers a balance between the "holistic, contextual view and the pragmatic, implementation view".

Recently, John Zachman wrote an article on "Security and the Zachman Framework". **[14]** And the author of this paper took a step further to develop a comprehensive Security Management Framework based on his framework for Enterprise Architecture.

Security Management Framework

The illustration of this Framework is based on a common practice of viewing the framework in its logical representation (Why, How, What, Where, Who, When) rather than sequentially. (Diagram is displayed at page 10 of this paper.)

Control Objectives

DATA (What): Integrity, Confidentiality, and Administration
FUNCTION (How): Availability, Efficiency
NETWORK (Where): Assurance, Reliability
PEOPLE (Who): Accountability, Effectiveness
TIME (When): Authentication, Compliance
MOTIVATION (Why): Training & Awareness

Effective Communication of Well-defined Strategy (Why) (Column six)

Security Vision

- A 2 to 5 line statement to illustrate the objectives of setting up the information security function

Security Plan/Policy

- A one page statement to present service objectives, performance model and accountability definitions. It creates a boundary of what conceptually the Security Office would deliver.

Security Standards and Guidelines

- A logical explanation of the written plan to ensure compliance to government guidelines and international standards. It should cover best practices and privacy principles as well.

Security Procedures Manual

- A "cookbook" with step by step instructions on managing security incidents or business resumption related processes. Steps should include the setup of emergency response team, how to report security incident, escalation procedures, chain of commands and events documentation.

According to Micki Krause, many studies about security breaches indicate that "people are the weakest link". "Since information security is 70 percent people and process and 30 percent technology, it is essential to develop and promote a security-awareness campaign." **[15]**

Security seminars should be designed to address the needs of different client groups. There should be at least three types of security seminars.

Seminar for Senior Management

- Obtain senior executive support. Emphasize the value and benefits of embracing the security program early by incorporating security requirements (Threat Risk Assessment, Privacy Impact Assessment) in the design phase of product development.

Seminar for System Administrators

- Empower system administrators with latest tools and techniques in protecting the network infrastructure. Alert them on new security problems and fixes. Assume the role of an enabler rather than an inhibitor.

Seminar for Staff

- Keep users abreast of the business risks and reduce the vulnerability from the inside out by developing a well-trained, ethical work force. Teach staff to prevent social engineering.

Accurate Understanding of Client Needs (How)

There has been a major paradigm shift in information security function in recent years. The success of the program depends greatly on how tightly the procedures implemented linked to the business needs and what values the security group can bring to the organization at large. The security function is viewed as value added service.

The services offered by the Security Office would very likely be as follows:

Business Software Systems

- Co-ordinate and support the performance of Threat Risk Assessment and Privacy Impact Assessment.

Information Management
- Assist with Privacy Impact Assessment.

IT Services
- Provide direction on infrastructure and business support that includes business design, contingency planning and system maintenance.

Security Toolkits
- Formalize a list of tools and processes that can facilitate effective security offerings to the user community. It should cover areas such as hardware, software, physical access, servers inventory and technical handbook with recommended practices for network operation and maintenance.

In-depth Knowledge of What Need to Be Protected (What)

As Eli Primrose-Smith pointed out, "With the rise of e-business, corporate security grew more complex -- a company's most valuable property was virtual, not tangible." **[16]**

Data is ultimately what the organization needs to protect. In order to be effective, the more detailed the classification is, the better. If the control of access can be nailed down to record and document level, we know the goal has been achieved. Listed below is an example of a classification scheme in a government agency.

Published Public
Internal Unprotected
Government Internal (Business, Financial)
Government External (Business)
Business Partner
Personal Confidential

Complete Control of the Environment (Where)

Eli Primrose-Smith also observed that "there's a growing convergence between information security and the physical security of people and property… A Company's most critical corporate information isn't simply stored in computer files -- it resides in the minds of its workers. Should a large number of employees suddenly be incapacitated, the terrible human tragedy would also include thousands of years of accrued experience that even the most sophisticated business continuity and recovery plan could never fully replace." **[17]**

There is no doubt that the September 11 tragedy in U.S. redefined the scope of security protection for us. Physical environment security was elevated to the same level of attention corporations used to pay to network security only. So when we define IT Infrastructures, we need to include physical security architecture. The suggestions for categories under IT Infrastructures are:

Facilities access control
PKI infrastructure
Internetworking infrastructure
LAN infrastructure
File/Print infrastructure
Messaging infrastructure
Software development architecture

And items under network devices can be:

Firewall, DMZ, VPN
Intrusion detection system
DNS, DHCP, Proxy
Token authentication
Directory services
Hubs, servers
Workstations, printers, modems, notebooks, PDAs

Successful Establishment of Partnership Team (Who)

ISO needs a support network to assist him or her to manage the enormous security challenge. The Security Partners framework can be viewed as many inter-connected rings. Each ring is equivalent to a branch (or team) in a traditional, hierarchical organization structure. Roles and responsibilities of members in each ring should be clearly defined, and communication paths among the teams should be identified and constructed to maximize the communication opportunities. Listed below are suggestions of members that the ISO should invite to each team.

Policy and Procedures team (Architecture Core team, Security Professionals Association, Government or International Standards Organizations)
Audit and Assessment team (Internal auditors, Project Management Office)
Incident Response team (Help desk, Computer Operations, Information Protection Center, Vendors)
Business Continuity team (IT Services, Building Management)
Disaster Recovery team (IT Services, Building Management)
Education and Communication team (Training, Project Management Office, HR, and Internal Users Group)
Business Requirements team (Senior Management, Business Analysts, Business Software Development Team, and Stakeholders)

The teams will be held accountable of their performance.

An Incident Tracking Database should be set up to record and monitor all incidents. It should eventually become the knowledge base for research and education.

Realistic Management of Time Constraints (When)

Since implementing programs require funding and resources, it is logical to map the plan to the actual fiscal year.

A security calendar will allow the ISO to capture security related events and security triggers in a central location. Security events can be masked in an overlay format so that the ISO can have a 3-dimension view of these events. Items that can be found in a security calendar included security seminars, security incidents, security project milestones and deadlines, security sensitive project milestones and deadlines, compliance requirements, retention of information. Security triggers are non-scheduled events that require investigation, action and intervention.

Under Security Compliance Framework, the critical path of security initiatives should be identified and managed in order to guarantee the success of the information security program.

A formal process should be established to review the security policy and procedures, network audit and incidents pattern on a regular basis (e.g. quarterly). Detailed action plan should be developed as well.

Conclusion

The author would compare the experience of developing the Security Management Framework as peeling an onion. It definitely involved juicy and spicy excitement. She started with a strategy ("Motivation" in John Zachman's framework). Then, she identified the skin ("Time" in John Zachman's framework) of the onion which gave her the scope of this exercise. With skillful fingers (team effort of Security Partners, "People" in John Zachman's framework), she tackled the first layer of the skin ("Network" in John Zachman's framework). She was able to identify all the possible vulnerabilities through this penetration exercise and take notes for future improvement. When she got to the inner skin ("Function" or "Processes" in John Zachman's framework), she knew that the onion ("Data" in John Zachman's framework) should be at hand soon. However, she seemed to encounter more unexpected layers of protective skins (security processes) and was delighted that the Security Awareness program works. The whole team was determined to make the intruder cry.

Yes, to be an Effective Information Security Officer, you have to think like a hacker so to counter-attack each step he or she took to invade your system and steal your precious data. Sometimes, you may need to put a decoy somewhere to distract the intruder. Ultimately, to win the information warfare, you will need a solid team of Security Partners and a well-trained security-aware work force to assist you to fight at each layer. As the leader, you would need to have a comprehensive, holistic view of the information security function.

	Control Objectives	Integrity Confidentiality Administration	Availability Efficiency	Assurance Reliability	Accountability Effectiveness	Authentication Compliance	Training & Awareness
		1	2	3	4	5	6
		DATA (What)	**FUNCTION** (How)	**NETWORK** (Where)	**PEOPLE** (Who)	**TIME** (When)	**MOTIVATION** (Why)
1	**Scope**	**External Data, Internal Data**	**Threat Risk Analysis process, Privacy Impact Analysis process**	**Network Locations**	**Operation branches or departments**	**Fiscal Year**	**Security Vision**
	Planner	List of Things	List of Processes	List of Locations	List of Organizations	List of Events	List of Business Goals
2	**Enterprise Model (Conceptual)**	**Tangible Asset, Intangible Asset**	**Value Chain functional model**	**Facilities, LAN, WAN, Internet, wireless**	**Security Partners framework**	**Security Calendar**	**Security Plan**
	Owner	Semantic Model	Business Process Model	Network Logistics System	Work Flow Model	Master Schedule	Business Plan
3	**System Model (Logical)**	**Asset Classification, Access Control**	**Business Design, Contingency Planning, System Maintenance**	**Physical Environment Security, Network Management**	**Roles & Responsibilities**	**Security Compliance Framework**	**Security Standards and Guidelines (Access Control)**
	Designer	Logical Data Model	Application Architecture	Distributed System Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
4	**Technology Model (Physical)**	**Databases, documents, financial and personal data management**	**Threat Risk Assessment (TRA), Privacy Impact Assessment (PIA)**	**IT Infrastructures**	**Incidents tracking database. Team reports**	**Security Review Process**	**Security Procedures Manual, Security Awareness Strategy**
	Builder	Physical Data Model	System Design	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
5	**Detailed Representation (Out of Context)**	**Record classification, document classification**	**Security Toolkits**	**Network Devices**	**Security Contacts List. Security Performance Review**	**Action plan**	**Security Seminars**
	Sub-Contractor	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Specification
6	**Functioning**	Data	Function	Network	Organization	Schedule	Strategy

References

(1) "Data Security: Information Security and the Internet." DTI- Communications and Information Industries Directorate. URL: http://www.dti.gov.uk/cii/datasecurity/informationsecurityandtheinternet/index.shtml

(2) Clow, Julie. "CEO pokes holes at firewall 'myth'." itWorldCanada.com. 12 March, 2002. URL: http://itworld.ca/rp.cfm?v=20020660005&S=350772

(3) (16) (17) Primrose-Smith, Eli. "Facing the new corporate security rules." ZDNet. 8 March, 2002. URL: http://zdnet.com.com/2102-1107-855323.html

(4) Fisher, Dennis. "Personnel Shortage Hindering Net Security." eWeek. 13 March, 2002. URL: http://www.eweek.com/article/0,3658,s=712&a=23973,00.asp

(5) (9) bin Yusof, Asmuni. "Ways to Become an Effective Information Security Professional - from a GIAC Wannabe's Perspective." SANS Information Security Reading Room. 1 October 2001. URL: http://rr.sans.org/start/professional.php

(6) (12) Scalet, Sarah D. and Berinato, Scott. "The ABCs of Security." CIO. March, 2002. URL: http://www.cio.com/security/edit/security_abc.html

(7) (11) Tinner, Tommy. "Starting an Information Security Program and Overcoming Business Pressures." SANS Information Security Reading Room. 5 April 2001. URL: http://rr.sans.org/start/program.php

(8) "Practice List for Information Security Management." General Accounting Office, U.S. May 1998. URL: http://www.gao.gov/special.pubs/infosec.guide/body.htm

(10) (15) Krause, Micki. "Chief Security Officer (CSO) training requires range of skills." Unisys World. May 2001. URL: http://www.unisysworld.com/monthly/2001/05/cso.shtml

(13) Zachman, John. "Concepts of the Framework for Enterprise Architecture." John Zachman. 1993. URL: http://members.ozemail.com.au/~visible/papers/zachman3.htm

(14) Zachman, John. "Security and the Zachman Framework." BRCommunity.com. November 2001. URL: http://www.brcommunity.com/cgi-local/x.pl/commentary/b081.html (This site offers free membership for access. Sign up is required to access this document.)