Global Information Assurance Certification Paper

Name: Asmuni bin Yusof
Version : 1

WAYS TO BECOME AN EFFECTIVE INFORMATION SECURITY PROFESSIONAL – FROM A GIAC WANNABE PERSPECTIVES

Introduction

1. Information Security Officer (ISO) is needed in today's information driven and information dependent corporation. The position requires someone who has the education, training and experiences to lead corporation Information Assurance's (IA) activities. At a glance, the positions calls for an individual who understands systems, security, 'bad guy' behavior and corporation's business processes. Understanding risks to information and how to mitigate those risk effectively also expected out of the ISO.

2. In growing nation like Malaysia, acquiring effective ISOs is not easy. Many reasons contribute to this issues. Information Security professionals are getting scarce as clearly indicated by Mr Anthony D'Angelo of Veritect (US). [1]"There is a real scarcity of true security professionals that have a solid foundation in Information security skills right now". He notes that some recent studies support this observation, revealing that the corporate world will be faced with a shortage of 500,000 to one million IT security professionals by 2003.

AIM

3. This paper will examine the requirements to become an effective Information Security Officer.

4. At the end of this paper, one will realize that achieving Information Security proficiency and maintenance of the expertise will be a daunting task. As the saying goes; 'Learning is lifelong for Information security Professionals'. The motivating factor of me choosing this topic is the realization that people is the most important factor in Information Security. SANS clearly indicated: "Assign untrained people to maintain security and provide neither the training not the time to make it possible to do the job" as the # 1

[1] Amstrong Illena, " Back to School", SC Info Security Magazine, Sept 2001 : 12-14

management error that lead to computer security vulnerability.[2]

RESPONSIBILITIES

5. The ISO's position in a corporation varies depending on sizes and overall organization structure. The followings are some of the responsibilities of an ISO:

a. To become the principle advisor on IT Security issues for the corporation. To ensure the running of Information Security (IS) programs in the corporation. Thus ISO will be the person who is responsible for the enforcement of IS Policy.

b. To become the Security contact point for the organization.

c. To update and advise top management on security direction and issues.

d. To ensure the design and improvement in the IS Policy from time to time.

e. To perform either formal or informal Risk Assessments.

f. To conduct regular audits on IS facilities.

g. To ensure Disaster Recovery and Business Continuity Plans are in place and effective.

h. To ensure internal IS training and security awareness program are conducted to various level of users in the organization.

EDUCATION BACKGROUND

6. This section will discuss some foundations to becoming ISO. Education and training should be treated as critical success factor in achieving information assurance/security. The ISO position requires someone with education and experience in all aspects of both professions, as well as management.

a. The ISO should possess at minimum a degree in the field

[2] http://www.sans.org/newlook/resources/errors.htm

of Computer Science or Management Information System or Computer Engineering.

b. As for the professional skills, one should have a sound knowledge and skill on data communications and operating system administration. Understanding the TCP/IP and related services is paramount important.

c. One should also possess professional certification such as:

(1) Security professional certification such as Certified Information Systems Security Professional (CISSP) and/or Global Information Assurance Certification (GIAC).

(2) Networking Certification.

(3) Operating System Certification such as MCSE ,Certified Unix, etc.

EXPERIENCES

7. Education and certifications will not guarantee a successful ISO. The expertise has got to be develop through experiences while climbing up the Information Security Ladder such as administrator, Analyst, Manager, Director and so forth. Among the experiences expected are as follows:

a. 4 to 5 years of System administrator especially in web and mail servers, File Servers and Database Management System.

b. He should have enough experience in maintenance of security devices such as Firewall, VPN services and PKI services.

c. He should be able to use IS Security Audit tools either the commercial scanners or open source tools.

d. He should have knowledge and experience in handling malicious codes.

FUTURE DEVELOPMENT

8. In order to be effective, an ISO need to be equipped with advanced Information Security knowledge. ISO need to be trained in Advance Incident Handling and Security Auditing. To be able to test the strength of a corporation's security strategy, one need to be able to conduct own penetration testing. Thus, courses in ethical hacking will help develop the required skills.

ADDITIONAL REQUIREMENTS

9. To be an effective ISO, a person should have an overall view of security requirements at various level, from data to system and network requirements. The person is responsible to ensure that security in place. However, he should not be doing everything by himself. There should be a security organization in the corporation that are staffed to carry out what ever security program of the corporation. The ISO should be the head of this department and report directly to the Chief Executive Officer (CEO). The IS department is organized as follows:[3]

a. Response Team. The Response team is directly responsible for meeting any serious attack and work to assess and coordinate repair of any damage caused by the attack.

b. Forensic Team. The Forensic Team provides in-depth research and assistance to the response team. They are tasked with developing an intimate knowledge of the network they are protecting.

c. Watch Team. The Watch Team is the 24 hours eyes and ears of the security organization. In an attack situation, the Watch team is responsible for declaring an emergency and holding the fort till he Response Team and the Forensic team can take over the situation.

10. Leadership. Security program must have strong leadership and credible skills. An ISO should be able to lead and coordinate in a crisis situation such as when system under attack or being hacked. A good leader should be able to withstand pressures or Information Security 'Occupational Hazard'. As a leader, the ISO must set the example and create and foster an information protection 'consciousness' within the

[3] Wadlow, Thomas A. The Process of Network Security. Addison-Wesley 2000. P53-54

corporation[4].

11. Knowing the Legal Issues. An ISO is also expected to know legal issues that might affect the corporation. He should understand measures to protect the corporation against potential legal proceeding as a result of what emanates from the corporation's networks. How do you like this happen to your organization: "There was a case recently in London where an employee sent a known virus to a competitor with the intent of deleting information from the competitor's hard drives"[1]

12. Inter-personal Skills. Having sound technical knowledge is not enough in the endeavor of Information Security. One needs to be able to convince the top management on security issues. You are expected to convey your requirement and specifications to your security vendors if their services are needed. Within your corporation, you should be able to interact and deal with the end users of the Information System. Often times, the ISO is the middle man between the user and the vendor in filling up the gap in security.

13. Establishing Network. To survive in today's border-less society, one need to have good relationship with other entities. Maintaining contact with ISP's is a must. You should also be in communication with local CERT or at least subscribe to their mailing list. Sharing information with them will be of a great help. You should also establish network with other security professionals both in country or from abroad to share information and seek advises on certain security issues.

14. Other Traits. Some traits of an effective Information Security professional are as follows:

a. Integrity. ISOs are guardians of a great deal of sensitive and important information of the corporation. He has to be as trustworthy as possible.

b. Tactful and Self Confidence. A weaker character will not be desirable to handle incidences.

c. Flexibility. To be able to modify security program to suit ever changing threats and business processes.

[4] Kovacich, Gerald L, Establishing a Computer Security Officer Position: http/:www.shockwavewriters.com/Articles/GLK/estCSO.htm

d. Business Sense. Knowing that business objective will always take precedence if conflict occurs between the need to assure information security and to achieve business objectives.

e. Continuous Learning. Must be ever willing to update knowledge from time to time. True security professionals understand the need to make some monetary sacrifice to attain certain security knowledge.

f. Team Work. A Rambo type operation and self centered personality will not be acceptable in Information Security community.

ACQUIRING KNOWLEDGE INFORMALLY

15. Developing IS skills does not confined to formal education and training alone. There are people out there who are ever willing to share their knowledge and to discuss security matter. The followings are some of the sources of information that could be optimized:

a. Special Interest Group. The group either meet physically or virtually, discussing subjects of common interest. The most recent malicious code such as 'Code Red' and 'Nimda' are among the hottest topics discussed currently.

b. Product User Groups. Users of a particular security product or network devices (such as routers) formed up a group to discuss the strength and weakness of a particular product. Hence, enhancing the knowledge in handling the product.

c. Professional Associations. The ISO should become a member and take part in one or more of several associations related to IS. Good examples are the Computer Security Institute (CSI) and Information System Security Association (ISSA) and National Computer Security Association. Several of the associations also sponsor annual, international conferences. The conferences give the ISO opportunity to meet other IS professionals and share problems and solutions on an international scale.

d. Trade Journal. and Magazine. Such publications contain

articles about the latest technologies, problems with this of that software; and more and more contain IS related articles. All this information will help you stay abreast of the technology and the related security issues.

e. Government. A number of government agencies, become good source of security information. US Department of Energy Website and National Institute of Standards and Technology (NIST) are excellent source of information.

f. Other Sources. The followings could provide good source of information:

(1) Conferences.

(2) Seminars.

(3) 'Old Boy Network'

(4) Consultant.

(5) Vendors.

(6) In-house expert.

g. The Internet. A rapidly growing source of IS information is the Internet. Those sites provide information which can help you learn IS positions, problems, solutions to those problems , etc.

CONCLUSIONS

16. Information Security Officer will remain important in a corporation. Producing a really effective ISO will be a difficult but not impossible. One need to undergo both computing and business management to be on the ball. With the ever changing of computing technologies and threats, one will not cease to acquire new knowledge in Information Security.

References:

[4] Amstrong Illena, " Back to School", SC Info Security Magazine, Sept 2001 : 12-14

[2] http://www.sans.org/newlook/resources/errors.htm
[3] Wadlow, Thomas A. The Process of Network Security. Addison-Wesley 2000. P53-54
[4] Kovacich, Gerald L, Establishing a Computer Security Officer Position: http://www.shockwavewriters.com/Articles/GLK/estCSO.htm

---

[5]Amstrong Illena, "Liability Worries" http://www.westcoast.com/asiapacific/articles/2001_08/feature/specialfeature.html

QUIZ QUESTIONS

Multiple Choices

Q1 - Name 2 of the most sought after Information Security Certification today:

A - CISSP

B - GIAC

C - CCNA

D - MCSE

The answer should be A and B for obvious reason.

Q2 - For future development of a security professional, one should pursue the following knowledge except:

A- Advance Incident Handling

B - Advance Security Auditing

C - Configuring and Maintenance of Firewall

D - Ethical Hacking

The answer should be C i.e. Configuring and Maintenance of Firewall

Q3 - The Information Security Organization is organized with the following Teams:

A - Response Team

B - Forensic Team

C - Training Team

D - Watch Team

The answer should be A, C and D. Training Team should come from general MIS department.

Q4 - There are many sources of information that may help develop an effective Information Security Officer. Choose the less appropriate sources of the list below:

A - Conferences

B - Old Boy Networking

C - Television

D - Internet

The answer is television

Q5 - An Information Security Officer should possess the following experience in order to become an effective ISO

A - He should have knowledge on cryptography code breaking

B - He should have enough experience in maintenance security devices

C - He should have knowledge in handling malicious code

D - 4-5 years of system administrator

Answer should be A as code breaking capability would be very tough to achieve. Knowledge on cryptography is suffice.

<u>True/False Quiz</u>

Q1- Acquiring knowledge of Information Security cease when one has achieved certain level of standard/qualification

Answer is False. Learning is lifelong for Info Security professional. This is due the ever changing threats and advancement of Information communication technology (ICT)

Q2- The ISO must always shows his mastery in Information Security by trying to solve all security problem alone.

Answer is False. He must work in a team and together develop the team.

Q3 - The minimum entry for Information Security professional is Master Science in Computer or MBA.

Answer is False. MSc and MBA is a bit too high of the education back ground expected out of him.

Q4- Information Security professional should establish networking to improve his professionalism

Answer is True. He should establish the networking to share experience, knowledge and problem and seek help from each other.

Q5 - Business Objective will always take precedence against Information Security Requirement.

Answer is True. Business objective will always have higher precedence if choice has to be made between those 2 requirements.