Global Information Assurance Certification Paper

Information Security Program:
The First 12 Months

Tim Cheung

GSEC Practical Requirements (v1.4b) Option 1

Submitted: October 10, 2003

TABLE OF CONTENTS

Summary

For most companies, the Information Security (InfoSec) Program is viewed as an expense. Often, companies find it hard to see the Return On Investment (ROI) with an InfoSec program. In addition, the person responsible for Information Security (InfoSec) usually reports to someone within the Information Technology (IT) Department. According to the META Group, an InfoSec program takes 3 years to establish value. Meanwhile, the average CIO/Director/Management of Information Department (IT) changes every 18 months. The success of an InfoSec program will depend on whether it can prove its value to the business of the company.

This paper will outline a practical plan for the first 12 months of a successful InfoSec Program. The somewhat controversial issue of InfoSec governance will be addressed. The paper will then discuss the things that need to be done in the first 6 months of the year, the last 6 months of the year, plus a plan of attack for the InfoSec program. The paper will end with a discussion on the next steps. 12 months is not nearly enough time to complete an InfoSec program. But, the first twelve months of the program, in most cases, will determine whether a program will succeed or not.

Introduction

There is a wealth of information available on the Internet that will deal with different parts of the Information Security (InfoSec) Program. In fact, there is so much information that it is hard to know where to start. Without a proper strategy and plan in place, InfoSec professionals will find themselves running around in reactive mode, being busy and quickly getting nowhere.

In a field where a job well done is when nothing happens (i.e. no problematic incidents occur), the InfoSec professional must have a strategy and a plan that will show value to the company on a regular basis.

Organize for Success

The person responsible for Information Security has many names. They have been called Security Director, Security Manager, Information Security Officer, Chief Security Officer, Chief Information Security Officer, and so on. For the purpose of this paper, I will use the name Chief Information Security Officer (CISO). The title, CISO, clearly defines a person who has the ultimate responsibility for Information Security.

Security Governance

The location of the CISO in an organizational structure is crucial to the effectiveness of the InfoSec program. Since InfoSec affects all areas of the company, the CISO needs to be in a position where he or she can have the most impact. In the last year or two, there have been many articles regarding this issue. So where should the InfoSec Position reside? And who should the person in this position report to?

Though common wisdom states that the CISO should not be part of the IT department, in April 2003, a survey from the *Information Security* magazine showed that 40% of the CISO still reports to management within IT (Saita). Early efforts of large corporations to have executive level CISOs have failed. High profiles CISOs in Fortune 500 companies have resigned or their positions have been reorganized out of the organizations. So, why is there such a high failure rate?

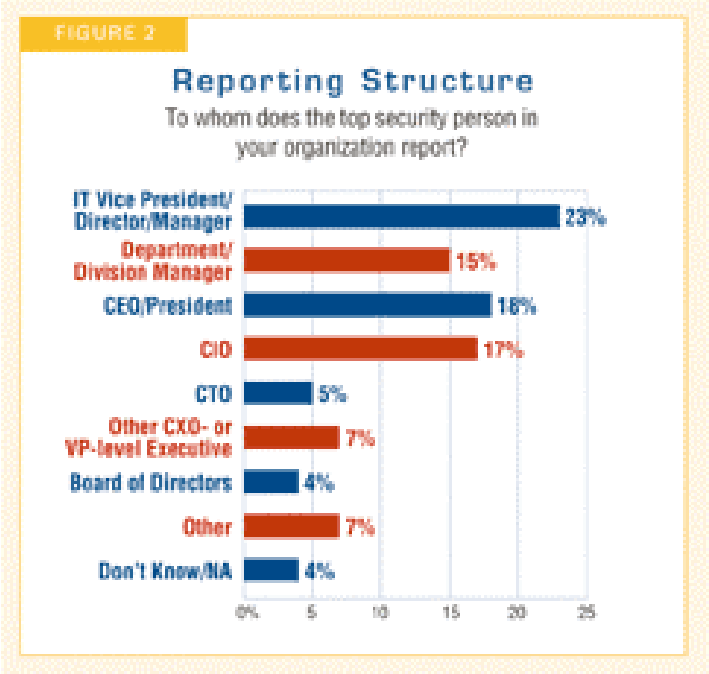

Figure 1 SOURCE: *Information Security* (Magazine) survey of 880 IT Security professionals, April 2003. (Saita).

Most corporations know that a need for information security exists, but are unsure of what it entails. Without having a clear understanding of the need, corporations react in one of two ways: (i) some hire a director or executive level CISO to design a paper InfoSec program; (ii) while others hire a technical CISO within the IT department who installs the latest security products.

In the first case, the executive CISO is located in upper management; the InfoSec program includes a little more than a creating a set of policies and trying to enforcement them. With the unpopular role of enforcing policies, the CISO is viewed as the “Big Brother,” watching everything from above and putting a stop to things that are not within the policies. The executive CISO role is viewed as being counter productive to the business of the organization. As a result, conflicts and stress are created between the CIO and the CISO. Since most of the InfoSec issues involve the IT department, full cooperation between the CISO and CIO is critical to the success of the InfoSec program.

The second way that companies react to the issue of InfoSec is to hire a technical CISO. The technical CISO, usually located within the IT department, proceeds to install all the latest InfoSec products: intrusion detection system, firewall, VPN, PKI, etc. These IT centric technical solutions are also viewed as being counter-productive to the business community. Such solutions are usually driven by a CISO who does not have a good understanding of the business and how to communicate to it. They usually run into a brick wall when they are called to account for the money that they have spent. Not knowing how to speak the business language is usually the nail on the coffin for the technical CISO.

The CISO needs to have a combination of business and technical skills. An InfoSec program affects people, and the technology in all areas of the corporation. The program would include the writing of Information Security policies, which is a set of policies that will govern different data, system access methods, and technologies within IT. Since InfoSec issues are not purely technical, the CISO will also need to develop an InfoSec Awareness program to educate users on Information Security. Lastly, the CISO will need to build an InfoSec Architecture, which will include the policies, standards, procedures, and technology; that is, new software on existing systems and new hardware.

For the InfoSec program to succeed, none of these things can be done in a vacuum. Namely, the CISO must establish and maintain a constant level of communication with all areas of the business.

Although an executive level CISO is ideal, the majority of business will not need to begin with the CISO at the executive level to start. In fact, having the roots of an InfoSec program in IT will give the program a head start. As previously mentioned, since most InfoSec issues will involve IT, having the CISO report to either the CIO or an executive responsible for IT will ensure a working relationship between the two parties. As the InfoSec program grows and proves its value to the corporation, then it might make sense to move the CISO to an executive level. But, this will depend on how dynamic the executives are and how open they are to changes.

Responsibility and Authority

No matter where the CISO is on the organizational chart, the InfoSec program must have the support and backing from the management and executives. Along with the responsibility of securing all information in a corporation, the CISO must also be given the authority to enforce the InfoSec program when violation occurs.

Otherwise, the users will come to realize that there are no consequences to violating InfoSec policies. The CISO and the InfoSec program will loose credibility.

If the CISO has the responsibility but not the authority for the InfoSec Program, the results would echo what consultant Thornton May once said, “[CISOs] haven't made their enterprises more secure-they've just centralized blame," effectively giving the CEO one neck to choke, no matter what kind of breach has occurred." (Slater).

An InfoSec program without the proper authority is doom to failure.

The First 3-6 Months

With the proper authority and organizational structure, the CISO needs to start developing the Information Security Program. The program usually includes:

- Developing and managing policies, standards and procedures, and guidelines

- Testing, recommending, and implementing security hardware and software
- Performing assessments and audits on information systems
- Responding to incidents
- Designing and testing Disaster Recovery Program
- Developing a Corporate InfoSec Awareness Program

The CISO will also need an overall plan and strategy on how to implement the InfoSec Program. Although the average InfoSec program takes 3 years to establish, there are things that can be done within the first 12 months to show immediate value to the organization. In the first three to six months, there are three basic things that can be done:

1. Assess the current state of InfoSec
2. Write and implement Initial Policies
3. Get involve in new and upgrade projects

1. Assess the Current State of Information Security

The first three months of the program should be spent identifying the current state of information security. If CISO does not know what they have, and where they are as far as InfoSec is concerned, they will not be able to tell if their program has made any security improvements or not. The CISO might have a general idea, or a gut feeling, but personal impressions do not count for much to the people who are paying their salary.

The information gathered in the first three months will give the CISO an idea of the size of the challenge(s) ahead. This exercise will also allow the CISO to start communication with the IT department and other business units. The process will also reveal other security concerns that may not have been considered by the CISO.

Inventory of Systems / Issues (First 3 months)

Document, document, document; the CISO will be THE Document King. The CISO will know every system and every department within the organization, and will know how the company is structured and every key person in the organization.

The first task in creating an inventory of the systems is to identify all the applications that the company has, the servers that they are on, the owners of the applications, and the people supporting the systems. All infrastructure devices will also need to identify their physical and logical locations, plus the people responsible for them. Most of the information will likely be available from different groups. The CISO will need to gather the information and put it all in one place. This inventory list will be a living document and will need to be updated regularly.

Prioritize (First 3 months)

After all systems have been inventoried, executives or the senior management team will need to prioritize the list based on their importance to the business of the company. This is another critical step in the InfoSec program. The process will identify the key systems of the corporation as determined by the business. This will give the CISO a starting place for securing what is most important to the company.

The priority list will be used for the following purposes:

- InfoSec Program: identifies which systems are analyzed and secured first
- Disaster Recovery Plan: determines which systems are restored first in case of a disaster
- Patch Management Program: to priorities which systems are patched first

Risk Analysis

Begin the risk analysis process based on the information that have been collected. Identify the risk for each system, the options and costs to mitigate the risks. The role of the CISO is one of risk management. The CISO completes a risk analysis for each system and presents it to the business unit. From there, the business unit either accepts the risk, or approves the measures being recommended by the CISO. In order to do their job effectively, the CISO must be able to report the risks and present the solutions clearly. Failure to do so may result in a wrong business decision.

Metrics, Metrics, Metrics

Identify and start collecting metrics. Metrics will become the key performance indicators of your InfoSec program. The editor of the CSO printed a letter from a reader about using the *Fear, Uncertainty, and Doubt* approach to an InfoSec program. The reader wrote, "*Don't tell me about possibilities, show me probabilities – with data to back them up*" (McGrath). Metrics will help quantify the current condition of InfoSec in the company, and it will help identify any hot spots that need to be addressed first. By collecting metrics, the CISO will have a baseline to compare the effects of the InfoSec program.

The hardest part of metrics is figuring out what needs to be measured and recorded. A standard list of metrics may include:

- Number of password reset requests
- Number of failed logons
- Number of Stolen notebooks, computers, etc
- Number of Virus Detected
- Number of users with admin access to various systems
- Number of system compromises thwarted

- Number of employees attending awareness training
- Number of systems compromised
- Percentage of security patched applied within 24 hours

2. Create and Implement Initial Policies

The foundation of the InfoSec program is policies. All other parts of the program will be based on these policies. The technology, training, monitoring and enforcement will all be according to the InfoSec policies. Effective policies take time to develop and they will evolve as new technologies and systems are implemented in the organization. Along with these policies, there needs to be ways to monitor policy compliance. Compliance to policies will also become one of the measurements of the effectiveness of the InfoSec program.

There are two policies that need to be in place within the first three months of the program:

Audit and Risk Assessment Policy	This policy will give the InfoSec group the authority to perform audits and risk assessments on any system on the corporate network. This policy must be in place prior to any InfoSec activity relating to corporate systems.
Acceptable Use Policy	A general acceptable use policy outlining the proper use of company computer systems and resources.

In addition to these, the following policies will need to be developed within the first 6 months of the program:

VPN Policy	Defines the requirements for systems that are using Virtual Private Network (VPN) connections to the corporate network.
Dial-in Security Policy	Defines the requirements for people who are using dial-in access to the corporate network.
Wireless Policy	Outlines the corporate standards for wireless AP and devices on the network. Even if there is no corporate wireless solution, there should be a policy that states, "no wireless devices are permitted to be connected to the corporate network."
Third Party Connection Policy	Defines the requirements for people outside the corporation who require access to the corporate network. This would include business partners, vendors, and consultants.

Sample policies and templates are available from the SANS website at www.sans.org.

3. Get Involved in New/Upgrade Projects

Get started with security now. The best time to look at security in an application life cycle is right at the beginning of the project. Do it right from the start; check that the security of the application is set up according to the policies and standards that have been developed, or that will be developed. The CISO should meet regularly with the Application Development and support team to find out what projects they are working on.

The CISO needs to get to know the applications group intimately. These are the people who support the applications and deals with the business units on a regular basis. The CISO does not know everything that needs to be done and they will not know everything that is going on. The application group will be the eyes and ears of the CISO, alerting the CISO of any changes that may affect InfoSec.

Month 7 – 12

For the rest of the year, the CISO needs to focus on building the InfoSec architecture to support the policies that have been developed. Hardware and software systems should be installed to monitor policy compliance and secure the enterprise. If more money is required, the CISO needs to start building the business cases to support the extra funding required for the next fiscal year's budget.

Continue to develop policies as needed and as changes occur. As of March 2003, "*over 1,400 individual policy statements have been defined for use within an organization. Most organizations, however, require only about 200. Identifying the correct policy set is essential to the success of an InfoSec program*" (Schreider). The company may not need 200 policies, but they will need more than what has been developed within the first 6 months.

The CISO needs not to worry about running out of things to do, as one can continue Risk assessment of the systems on the prioritized system list.

Plan of Attack

InfoSec Program Plan

The InfoSec plan should align to the business plan. "*Included in plans should be infosecurity's mission and how it fits the enterprise's vision and business plan.*" (Saita). The plan should be viewed as a business enabler, a way of reducing the risks of doing business and not reducing business.

In order to show value, the CISO should include in the overall plan, things that need to be done in the next quarter, as well as in the next year. The CISO should have a quarterly review of the InfoSec program plan and revise the overall plan if required. The CISO needs to write quarterly InfoSec reports for the supervisor, executives, and IT management. The report should include the following:

- Report on what was accomplished in the last quarter
- Report on metrics for the quarter
- Report on what will be done in the next quarter.
- Updated InfoSec Program Plan if there are any changes

"Pluck the Low-Hanging Fruit"

The CISO needs to tackle the things that adds value to the business first. A quick look over of all the systems will usually reveal one or two "*gaping holes in corporate security architecture and policy. Fix them right away, and make a big deal out of it.*" (Berinato). Do this on a regular basis to keep InfoSec on the minds of the whole corporation.

Develop an Incident Respond Procedure

As incidents occur, document and record the details of each incident. Record the systems that were affected, how IT responded, and how the incidents occurred. Analyze the incidents to see if there are things that can be done to prevent similar incidents from happening in the future. The SANS web site has a number of Incident Handling forms (www.sans.org/incidentforms/) that can help the document process, which may be downloaded and modified according to each company's need(s).

Develop an Information Security Awareness Program

Informal InfoSec Awareness training can happen at any time. Training and teaching may be done through a various media, such as e-mail, IT newsletters, or on the internal web portal. In the last quarter of the first year, the CISO should start developing the InfoSec Awareness program. By this time, the CISO should have a good idea of where the security challenges are in the company. There should be enough metrics collected to be able to start addressing the training requirements for their company.

What's Next?

Using the metrics that have been collected in the first year, the CISO can review the effectiveness of the InfoSec Program. Depending on how much has been accomplished, the CISO can choose to have an independent audit performed on the overall program, on key systems, or have a penetration test of the perimeter. This will give a good indication of what still needs to be done. The independent audit report will also form the baseline to compare with for the next year.

The CISO should continue to produce quarterly updates for the supervisor, the executives, and IT management. The InfoSec program needs to continue to show value to the company. Guy Turner, the Information Security Manager of West Tennessee Health Care says, "*I take every opportunity to portray information security as supporting the organization's mission and enabling the*

safe and efficient use of information. Over time, I think it has sunk in that security means making things more efficient." (Briney). The days of Fear, Uncertainty, Doubt tactics are gone. There is no more unlimited budget to install the latest security toy because "the sky might fall." Instead, the CISO needs to justify the expenses of an InfoSec program. The CISO would also need to successfully show that the implemented program is having a positive effect to the overall information security of the company. The CISO that can continue to show the value to the corporation needs not worry about being "reorg'd" out of the corporation.

References

Radcliff, Deborah. “Chief (in)security officer.” June 10, 2002. http://www.computerworld.com/printthis/2002/0,4814,71866,00.html

Saita, Anne. “Turnover at the Top.” June 2003. http://infosecuritymag.techtarget.com/2003/jun/turnover.shtml

McGrath, Kevin. “The FUD Hit Home.” June 2003. http://www.csoonline.com/read/060103/letters.html

Slater, Derek. “Identity Crisis.” The CIO Role. June 2003. http://www.csoonline.com/read/060103/crisis.html

Berinato, Scott. “Bob Moore Knows How Not to Get Fired.” June 2003. http://www.csoonline.com/read/060103/fired.html

Schreider, Tari. “InfoSec 101 for BC Pros.” March 2003. http://www.contingencyplanning.com/PastIssues/mar2003/1.cfm

Vijayan, Jaikumar. “IT managers see need for risk metrics.” June 9, 2003. http://www.computerworld.com/securitytopics/security/story/0,10801,81897,00.html

The SANS Institute. “The SANS Security Policy Project.” http://www.sans.org/resources/policies/

Briney, Andrew. “Proving Ground.” September 2002. http://infosecuritymag.techtarget.com/2002/ciso/aug/ciso-roundtable.shtml