Global Information Assurance Certification Paper

olving the Security People Problem:

A University Staffing Assessment Tutorial

Sean Ensz
September 20, 2003

Table of Contents

Abstract

This report explores the processes that one should go through when attempting to convince management that more security personnel are needed in an organization. The report begins with an explanation of the problem: that there are too few security employees in most organizations—especially at universities, which are particularly vulnerable to attacks. For this reason, this report focuses largely on IT infrastructure in higher education.

After defining the problem, there is a data section that shows there is an increased level of sophistication of attacks and a shortage of security personnel to handle those attacks. The reader will then find the recommendations section, in which there is a step by step guide for existing security departments to follow if they want to convince management to add staff. It has instructions on how to write a staffing assessment based on the ten domains from the *Common Body of Knowledge*, as well as how to structure a security organization and add employees in a phased approach. The conclusion gives the reader some suggestions for submitting their ideas and staffing assessment to management in an effective manner.

Introduction

"Information security is often thought of in terms of technology – firewalls, anti-virus, code vulnerabilities and the like. However, security is fundamentally a 'people problem (Houser).'"

Most organizations lack the most important component of a comprehensive security program: people. Convincing the administration to increase IT staff can be a difficult undertaking. This is especially true in terms of the security office. Security concerns at most universities are still in the infancy stage and have not had a chance to mature to meet the overwhelming increase in security threats.

Approaches to solving security are often limited to procuring technology and using traditional — sometimes inferior — systems administrators to manage it. Securing a university's computing infrastructure involves much more than installing a firewall and intrusion detection system. Threats to computing resources are complex and the approach to mitigating them should be as well. The need for information security has finally made its way into most IT management concerns, but the proper approach is still lacking. Security is fundamentally a people problem; therefore, it takes people to solve the problem. This tutorial is meant to show the steps needed to address the acute personnel shortage plaguing most universities.

Problem Description

The Internet was born out of a collaborative effort between several universities in the late 1960's as an open research project called ARPANET (Hartley). Security was not given any consideration by those who were involved in the project. The lack of security

and the openness of the connected machines gave success to a new type of threat: the Internet worm. In 1988 a worm written by Robert Morris, Jr., a graduate student in Computer Science at Cornell, was able to infect thousands of computers in a relatively short amount of time (Winkler).

Fast-forward 30 years and look at most university networks you will find a similar picture. Higher education networks were designed to facilitate research and promote academic freedom. Universities have some of the fastest and most inherently insecure networks in the world. This is why they frequently come under attack.

Data

With the number of vulnerabilities increasing and the expertise needed to exploit them decreasing, a university network is a very hostile (Figure 1) computing environment. It wasn't until the turn of the millennium that most higher education institutions began to consider addressing the security risks. Even when these risks were examined, few institutions implemented a proper level of security to adequately protect its resources.

Attack Sophistication vs. Intruder Knowledge

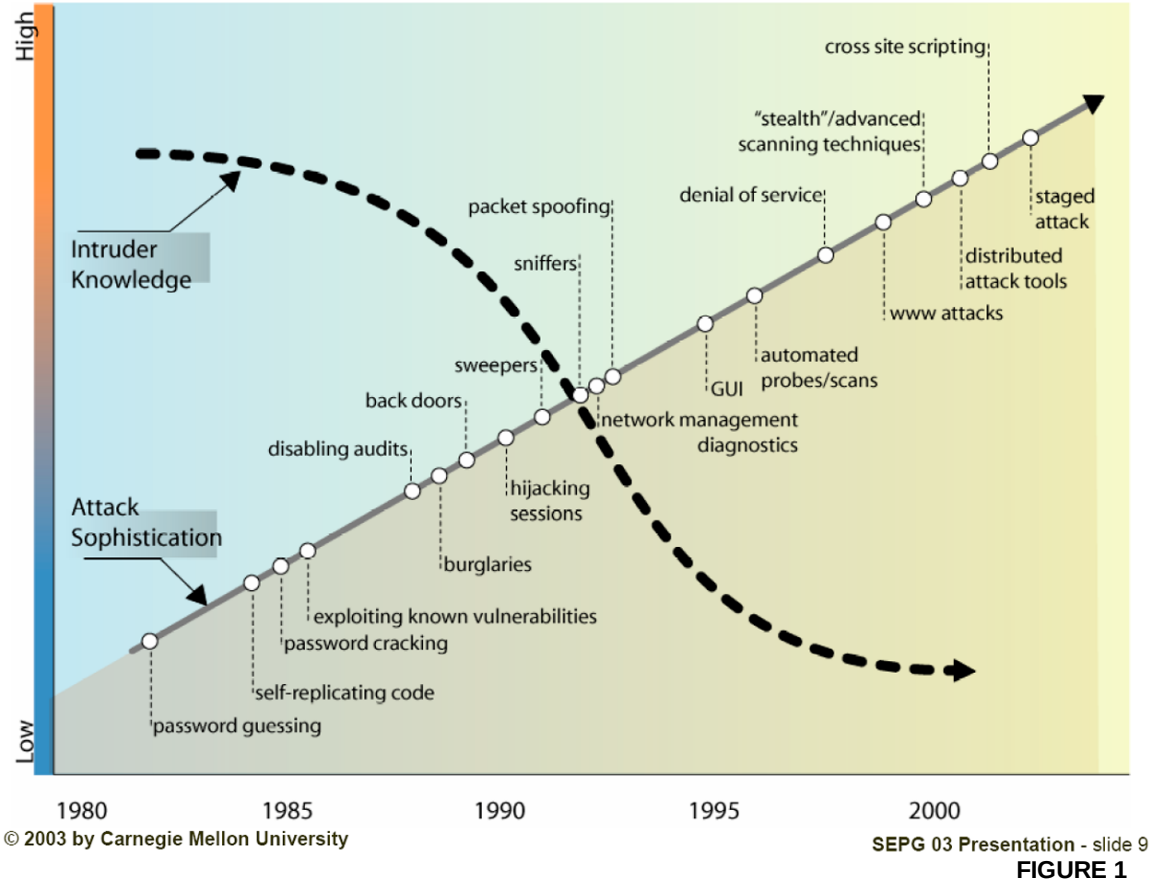


FIGURE 1

Once higher education IT departments did start taking action, they were slow to respond. Most institutions blocked a few ports on routers facing the Internet and created

acceptable computing policies, usually assigning the work to existing personnel with no security experience or training.

Many universities and some corporate organizations approach security from a technology perspective — buy more firewalls, intrusion detection systems, and antivirus software. These devices are necessary but cannot solve the problem alone. What has failed to be addressed is the number of highly trained and competent security professionals needed to do the job. Briney and Prince explain this environment very well in the 2002 ISM survey:

> Shortfalls in security budgets, management support, security staffing and end-user training conspire to create “people” problems at all levels. Making matters worse, large organizations have complex infrastructures and high exposure on the Internet, making them frequent hacker targets. Pressed by other concerns, non-security management doesn’t pay much attention to security, leaving the full-time security staff— what there is of it—to deal with what one survey respondent calls ‘ordinary, unalert, uninterested, lax, ignorant, uncaring end users.’

The risks to a university network can be high. Most higher education institutions have a decentralized approach to facilitating IT functions and therefore lack consistent standards for securing workstations and servers. In this academic environment the IT infrastructure is more likely to come under attack and requires due diligence to keep resources secure. Moreover, most system administrators are untrained faculty and staff who are given the responsibility to maintain systems that house private information and sensitive research data. This poses a large risk to the institution.

User training and standards should be of the utmost importance, but unfortunately they get little attention. User training is a facet of a comprehensive security program that requires significant staffing and publishing, and enforcing security standards across a large academic network is very time consuming. These are important issues that need to be addressed by dedicated, well trained security professionals.

Major universities generally have a large user base as well as a large number of machines to manage. In this computing environment you will find that the ratio of security staff to users and machines is significantly lower than a similarly sized organization (Figures 2 and 3). You will find that most major universities will have two or three staff persons managing security for 30,000+ users and 15,000+ machines.

2002 ISM Survey Snapshot

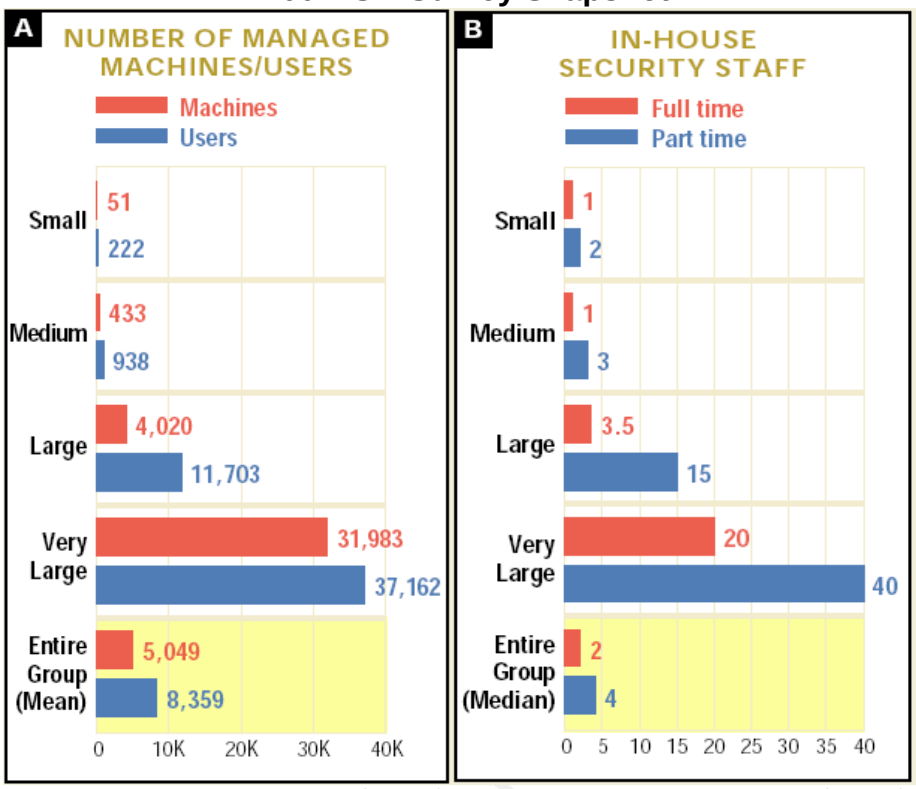


FIGURE 2 FIGURE 3

Security is only as great as its weakest link. In the *Common Body of Knowledge* we learn that there are ten domains of security and each one needs a considerable amount of time and energy dedicated to master them. If an organization fails to address one of the domains, it weakens efforts given to the remaining domains. For instance, having a strong network architecture and physical security does little good if you don't have a strong disaster recovery plan to engage when those resources are threatened. It also does little good to have acceptable computing policies if you have no one to enforce them. It is the security staff that makes the security program work. Proper security is an ongoing process. "Organizations strive for enterprise survivability as they attempt to manage risk in a more effective way. They must learn that security is not a one-time activity but a rather a continuous, risk-managed process (Nixon)."

Recommendations

This section assumes that a security program is currently established, but it has reached its limits of effectiveness because of staffing shortages. This paper gives examples of how to grow an organization, not how to create one.

The first step in increasing security staff is to gain management support. It is important that you show them that the threats are real and the university is at risk. When explaining the reasons that the organization is at risk you must be able to show them that implementing a comprehensive security plan will reduce exposure. Begin by

documenting security breaches and record the amount of time IT staff spends on each incident. You should also document failed intrusion attempts and network probes to show the frequency of attacks on your organization's resources. Once these statistics are gathered, you should compile them in a meaningful way and present them in a staffing assessment.

The staffing assessment needs to contain the following sections:

- Executive Summary
- Introduction
- Current Status
- Recommendations
- Conclusion

The assessment should be clear and concise so that your audience (management) will not lose focus.

The Executive Summary may be the only portion of your assessment that management will read; therefore, it needs to contain all the pertinent facts of your report that will grab the reader's attention. It should also contain a clear statement about the intent of the report and what your recommendations are. The Executive Summary should not be bound with the rest of your report but should instead sit on top of the report just under its cover.

The Introduction should only contain a brief description of what you intend to discuss.

The next section, Current Status, should be written as though the reader is uninformed of the department's history. This is done to give him or her a description of what has happened in regards to security up until this point. This portion can be vitally important if you are submitting it to new management to help bring them up to speed. Subsections of the Current Status section, at a minimum, need to include the following:

- when the security program began and why
- current staffing levels (with organizational chart)
- major achievements
- current level of service vs. expected level of service
- global security trends
- organizational security trends
- security asset inventory

Depending on how large and how quickly you want to grow the organization, it is probably best to approach your plan in phases. Be aware that most IT directors will be reluctant to add additional personnel because it is an expensive long term investment. If you want your assessment to be taken seriously, keep the recommendations realistic.

The Recommendations section requires some lengthy initial work to be effective. Creating appropriate roles and responsibilities for the security office is the first step. Taking into consideration the ten domains from the *Common Body of Knowledge,* you need to assign responsibilities or services to each domain. By examining the domain overviews from *Information Security Management* (Tipton and Krause), you can get a general idea of what each respective domain entails. You should try to identify the most important job functions to meet your university or organization's business requirements. The assigned responsibilities should be sufficient to accomplish the key concepts of each domain. It is possible to add more responsibilities to those domains that require special attention in your organization.

The Conclusion should be a short paragraph stating the consequence of failing to act as well as how and why the lack of proper security will place the university at risk.

According to the National Institute of Standards and Technology *Security Services Guide* (Table 1), all security services should fall into one of the following three categories: Management, Operational, or Technical. They believe that, "A comprehensive security program should include a mixture of controls from each category to provide multiple layers of protection" (Grance).

Table 1 – IT Security Categories

Management Services	Techniques and concerns normally addressed by management in the organization's computer security program. They focus on managing the computer security program and the risk within the organization.
Operational Services	Services focused on controls implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and rely on management activities and technical controls.
Technical Services	Technical services focused on security controls a computer system executes. These services are dependent on the proper function of the system for effectiveness.

Management Services can be thought of as the portion of the security organization responsible for managing the security program, policies, and risk. These services need to be carried out from a strategic perspective. Management Services is meant "to provide the management; direction; and develop, implement, and maintain information security policies and procedures; user awareness of risks, disaster recovery; and contingency planning; …" (Kovacich, p. 87).

Operational Services are those services focused on access control and compliance of IT resource users, whether they are authorized or unauthorized users. Members of the Operational Security group are considered the protectors of IT resources. Their efforts should be spent [protecting] "information systems from unauthorized access, disclosure, misuse, modification, manipulation, or destruction as well as implement and maintain appropriate information and information systems access controls… and maintain violations tracking systems" (Kovacich, p. 85).

Technical Services are centered on maintaining security hardware and software needed by the Operational Security group to carry out their job function. Primary responsibilities

include the hardware and operating system functions of devices such as firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, antivirus systems, and patch management systems. The Technical Security group will work closely with the Operational Security group to maintain proper and secure functionality of access control systems. As stated in the NIST *Security Services Guide*, "Reliance on technical resources alone will be insufficient without complementary management or operational controls" (Grance).

Once the responsibilities have been established and categorized, you can assign a position title to each category (Table 2). For our purposes, security titles can be broken down into four levels. The positions are separated into job families based on education and experience as well as job function. The following job families are loosely based on job descriptions and qualifications from Dr. Kovacich's *Information Systems Security Officer's Guide (p. 91).*

Title: Administrator

Position Summary: Provide administrative support to the security organization staff, including records management, records analysis, and policy, document, presentation material, and reports development.
Function: Administration
Education and Experience Requirements: Associate's degree, one year of security or law enforcement records experience or three years of clerical experience.

Title: Analyst

Position Summary: Identify, schedule, administer, and perform assigned technical security analyses functions to ensure that student, staff, and faculty security requirements are met.
Functions: User and systems administration and audit report analyses.
Education and Experience Requirements: Bachelor's degree in a related field or at least three years of experience.

Title: Senior Analyst

Position Summary: Act as security advisor, focal point, and leader to ensure all security functions are meeting student, staff, and faculty security requirements, as well as develop and administer applicable security programs.
Functions: User and systems administration, audit report analyses, systems security tests and evaluations, incident response, disaster recovery and contingency planning, software evaluation, security software maintenance and enhancement, and network security.
Education and Experience Requirements: Bachelor's degree in a related field and four years of related experience or a total of eight years of related experience.

Title: Engineer

Position Summary: Act as security management consultant, focal point, and project leader for security functions and programs developed to ensure that student, staff, and faculty requirements are met.

Functions: User and systems administration, audit report analyses, systems security tests and evaluation, security awareness program, incident response, disaster recovery and contingency planning, security software maintenance, enhancement, and development, network security and project leading.
Education and Experience: Bachelor's degree in related field and six years of related experience or a total of twelve years of related experience.

Table 2 – Security Roles and Responsibilities

Domain / Responsibility	Category	Position Titles
Security Management Practices		
Implement policies, procedures, standards and guidelines	Management	Security Management Engineer / Security Policy Analyst
Risk management	Management	Senior Security Management Analyst
Asset management	Management	Senior Security Management Analyst
Security awareness & communications	Management / Operational	Training & Communications Analyst / Security Management Administrator
Security management planning	Management	Security Management Engineer
Access Control		
Access rights and permissions auditing	Operational	Host Security Analyst
Access control policies/procedures/standards	Management	Security Policy Analyst
Authentication and password management	Operational	Host Security Analyst
Manual and automated removal processes	Management	Security Policy Analyst
Telecommunications and Network Security		
Firewall policy management and auditing	Technical	Network Security Analyst
Intrusion Detection management and auditing	Technical	Network Security Analyst
Network security management and monitoring	Technical	Technical Security Engineer
Intrusion response and investigations	Operational	Network Security Analyst / Senior Incident Response Analyst
Network vulnerability assessment	Technical	Network Security Analyst
Cryptography		
Application cryptographic functions	Technical	Software Security Analyst
Network-based cryptographic functions	Technical	Network Security Analyst
Storage cryptographic functions	Technical	Software Security Analyst
Hardware cryptographic functions	Operational	Host Security Analyst
Security Architecture and Models		
Security systems design and planning	Management / Technical	Security Management Engineer / All Security Analysts
Certification and accreditation	Management / Technical	Security Management Engineer /All Security Analysts
Operations Security		
Administration management	Operational	Operational Security Engineer
Resource protection	Operational	Technical / Operational Security Engineers
Security controls management	Operational	Operational Security Engineer
Threat and vulnerability analysis	Operational	Technical / Operational Security Engineers
Countermeasure management	Operational	Technical / Operational Security Engineers
Records management	Operational	Security Management Administrator
Applications and Systems Development		
Anti-virus management	Technical	Software Security Analyst
Applications vulnerability assessment	Technical	Software Security Analyst
Applications development testing	Technical	Software Security Analyst
Database security assessment	Operational	Host Security Analyst
Patch and configuration management	Operational	Software Security Analyst
Business Continuity Planning		
Planning, preparation, testing and BCP and DRP	Management	Senior Security Management Analyst
Law, Investigation and Ethics		
Law Enforcement and legal liaison	Operational	Operational Security Engineer
General investigation	Operational	Incident Response Analyst
Incident handling	Operational	Incident Response Analyst / Security Analysts

Forensic investigation	Operational	Senior Incident Response Analyst
Evidence handling	Operational	Senior Incident Response Analyst
Physical Security		
Facility security management	Operational	Physical Security Analyst
Physical threats management	Operational	Physical Security Analyst

Once the new roles and responsibilities have been established, you can prioritize them into a phased approach. Since most administrators, or the Human Resources Department, usually will not allow a large amount of staff to be hired at one time, security staff should be added slowly. Milestones should be established to determine the number of staff the organization needs by a projected date. For example, if a university currently has three Full Time Equivalents (FTE) dedicated to security and would like to increase staffing levels to seventeen, they could set two milestones. The first milestone would be to add five FTE within six months and an additional nine FTE within two years.

If a phased approach is used it is important to determine which new positions are needed first. Using the roles and responsibilities from Table 2, determine which domains are currently lacking and require urgent attention. Place a percentage of current FTE (3.00) into a matrix (Table 3) and add the needed percentage (5.00) to the lacking domain so the total is equal to 8.00 FTE. You can use the same method to add the additional nine security persons.

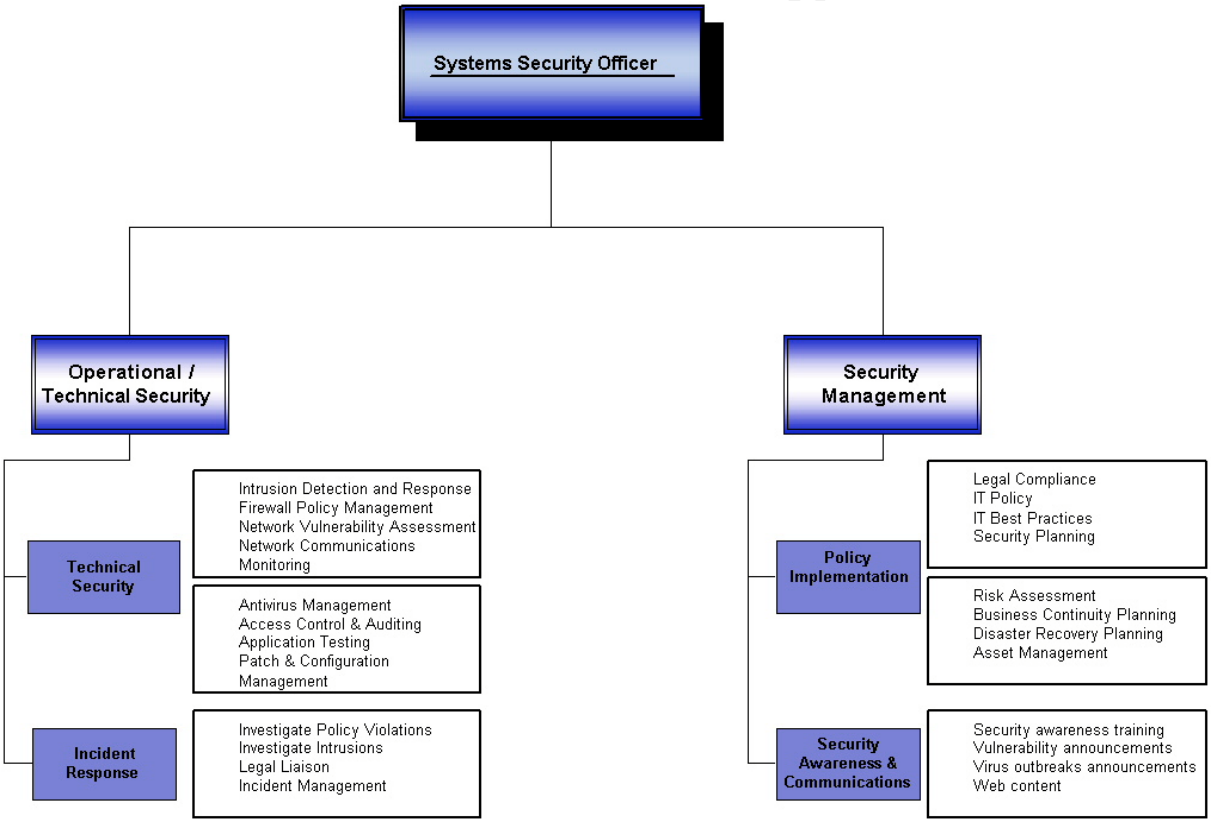
Table 3 – Recommended Personnel by Domain

Security Domain	Current FTE	Phase One		Phase Two	
		Add	*Total*	*Add*	*Total*
Access Control Systems and Methodology	0.10	0.50	0.60	1.00	1.60
Applications and Systems Development Security	0.25	0.50	0.75	1.00	1.75
Business Continuity and Disaster Recovery Planning	0.10	1.00	1.10	0.50	1.60
Cryptography	0.00	0.25	0.25	0.75	1.00
Law, Investigation, and Ethics	0.50	1.00	1.50	0.75	2.25
Operations Security	0.00	0.25	0.25	0.50	0.75
Physical Security	0.00	0.00	0.00	1.00	1.00
Security Architecture and Models	0.00	0.25	0.25	0.50	0.75
Security Management Practices	0.75	0.50	1.25	1.50	3.00
Telecommunications and Network Security	1.30	0.75	2.05	1.50	3.55
Totals	**3.00**	**5.00**	**8.00**	**9.00**	**17.00**
Current = 3 FTE					

Phase One

At this point with only eight security staff members the organizational structure will not be broad enough to have three distinct departments to meet the category structure of Management, Operational, and Technical security. The Operational and Technical security departments need to be temporarily established as one department (Figure 4). During this phase physical security is not addressed and several other domains have little dedicated effort.

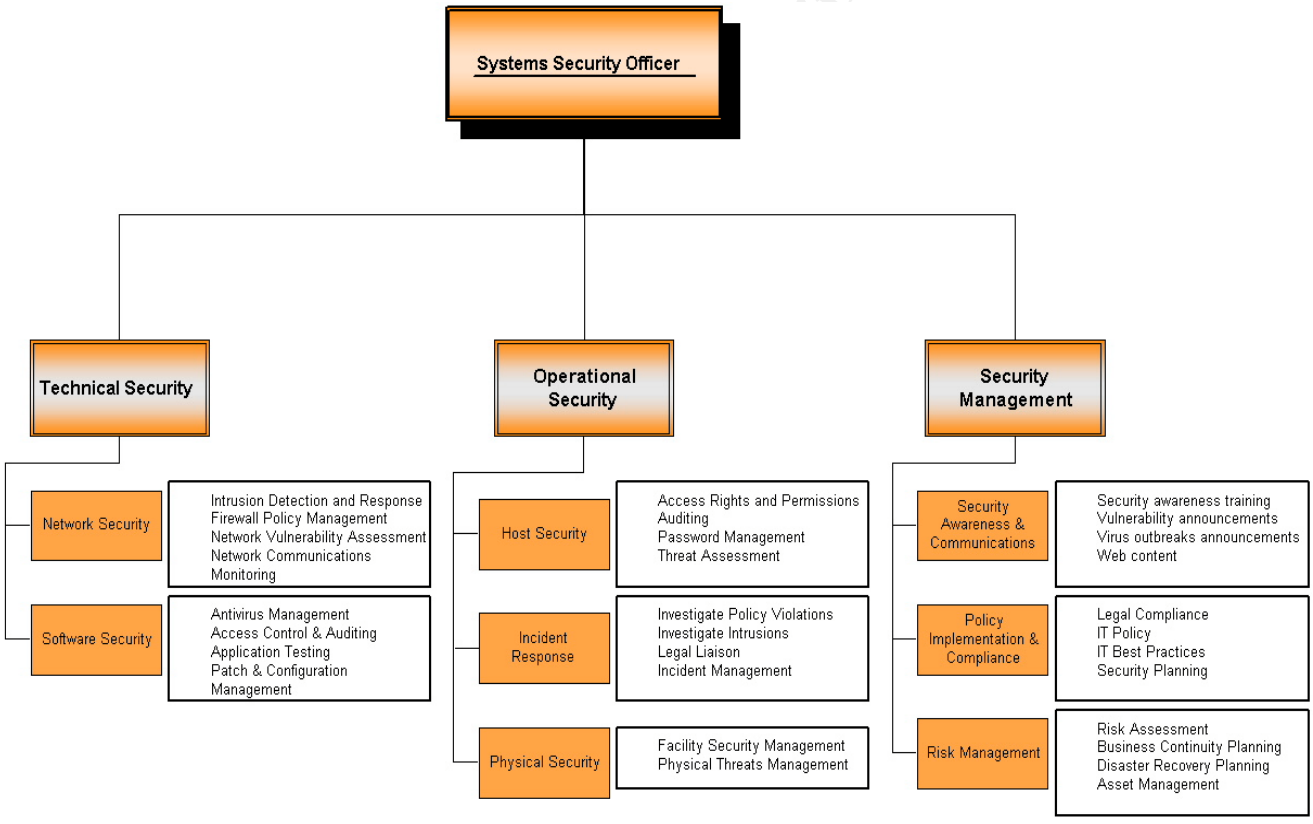
Figure 4 – Phase One Organizational Structure



Phase Two

In phase two, nine persons are added to the security office. The additional staff allows for the Operational and Technical security departments to be separated (Figure 5). Each of the domains should now be covered to meet the organizations business needs. In the example above most of the emphasis is on Security Management Practices, Network Security, and Incident Response. The areas of responsibility addressed in this phase would be host security, application security, and physical security.

Figure 5 – Phase Two Organizational Structure



Conclusion

Now that we have covered all the sections that should be included in a staffing assessment, you should be able to write one that fits your organization's needs. This report is meant to serve only as a guideline—you should always make adjustments and adapt any information to make it work for you.

Once you have finished your writing, it is time to determine the best way to present your finished work and ideas to management. These are only suggestions—you know best what tends to be effective at your organization. You will want to plan the delivery of your assessment at a time when it will be best received. Walking into the IT director's office without prompting or reason will likely be met with apathy or failure. It is best to submit your report either during a strategic planning session, after a security audit, or after a major compromise. This is when the IT management is most open to new ideas. Do not be discouraged if you see no immediate action. Personnel changes happen slowly and rarely occur unless they have to.

Keep in mind that security is a growing field, and that even if your employer does not immediately agree to add personnel, continue to be persistent. If your assessment does not convince them, the data have shown the likelihood that a high level security breech eventually will.

References

Allen, Julia. “What Is My Role in Information Survivability? Why Should I Care?”. 2003. URL: http://www.cert.org/archive/pdf/info_surv_pres040203.pdf

Briney, Andrew and Prince, Frank. “Does Size Matter?”. September 2002. URL: http://infosecuritymag.techtarget.com/2002/sep/2002survey.pdf

Grance, Tim et. al. “Guide to Information Technology Security Services”. October 2002. URL: http://csrc.nist.gov/publications/drafts/Services_PC_100802.pdf

Hartley, Steven. “History of the Internet”. May 2002. URL: http://www.orangepeel.com/en/internet/shortHistory.php

Houser, Dan. “Communicating the Language of Information Security**”.** February 2003. URL: http://www.infosecnews.com/opinion/2003/02/06_02.htm

Kocacich, Gerald. The Information Systems Security Officer’s Guide. Woburn: Butterworth-Heinemann, 1998.

Nixon, Kevin, et. al. “Common Sense Guide for Senior Managers”. Internet Security Alliance. July 2002: P. ii

Tipton, Harold and Krause, Micki. Information Security Management Handbook. 4th Edition, Volume 3. Boca Raton: CRC Press LLC, 2002.

Winkler, Ira. **“**The Morris Worm, What have we learned in a decade?”. March 3, 2000. URL: http://www.techtv.com/news/securityalert/story/0,24195,2158937,00.html