Implementing an Information Security Program

Kevin Nichols

August 22, 2001

Implementing an Information Security Program

Prepared by: Kevin L. Nichols

For: SANS GIAC Level One Course Objective
As described in
SANS Security Essentials GSEC Practical Requirements v1.2e December 2000

1.0 Introduction

Recently, there has been an increase in the awareness for the need within corporations (as well as within government agencies) to protect sensitive, proprietary and company secret information. Unauthorized modification, loss or compromise of such information could very well severely damage an organization's current operations; future or even put it out of business.

"Computer crimes of all kinds -- by insiders and outsiders -- are increasing and getting more costly, according to a recent survey of 538 companies, universities and government agencies by the San Francisco-based Computer Security Institute and the FBI. Eighty-five percent said their networks were breached in the previous year. The 186 respondents who were willing to quantify the damage they suffered put their total losses at $378 million. In last year's survey, 249 companies said they lost a total of $266 million." (1)

Computer information systems and telecommunication systems are technologies that every organization uses in their daily pursuit of business. As organizations become reliant upon such resources to conduct business, there has been a growing vulnerability.

Still, most companies or agencies are unwilling to publicly admit to such problems because such information could cause further damage to the company by damaging their reputation, possibly effecting stock prices and customer relations.

"Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems and services have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail." (2)

The ideal situation is for an organization to have built security into its computer information systems and telecommunications systems from the start. But this is not the case in many organizations. If the organization has not built in security then there may be serious vulnerabilities that exist, some of which may have already been exploited by unauthorized individuals. Groups or individuals such as hackers, organizations such as competitors or even elements of foreign governments may be taking advantage of vulnerabilities that go left unchecked.

However, the largest threat to an organization's computer information systems and the data they contain remains the trusted or authorized user. Since wide spread reports center on the threat posed by external threats, the internal threat may go relatively unnoticed or may be inadequately addressed as resources are spent countering the external threat. At the same time, many security measures that should be implemented to counter the internal threat are relatively inexpensive and also act to close up many holes that an external threat may rely on to gain and maintain unauthorized access to an organizations system and data.

A CNN article titled Downsizings leave firms open to digital attacks, dated June 27, 2001 (3), reports that "As employers pare down their payrolls to cut costs, many companies may unwittingly be leaving themselves vulnerable to hostile actions by discharged workers, including theft of confidential company information, illegal use of a company's IT resources and hidden "logic-bombs" that can destroy vital data." The article goes on to say " Common mistakes that contribute to the problem include a failure to disable the passwords and accounts of former employees, a lack of formal rules for the return of company laptops and handhelds and a failure to plug holes that make it possible for an ex-employee to exploit a former colleague's user account to gain illegal access."

Unfortunately within a large number of organizations, the IT security issue will not be addressed until that organization realizes or suffers through such an incident. However, for those IT or Security Professionals in organizations that are aware of the issue, they may have the ability to implement a viable Information Security Program to counter such threats.

Wherever the threat may be coming from the three basic tenants of information systems security are confidentiality, integrity and availability. The Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems Appendices, dated 5 June 1999 (4) defines these principals:

Confidentiality – Assurance that information is not disclosed to unauthorized entities or processes.

Integrity – Protection against unauthorized modification or destruction of information.

Availability – Timely, reliable access to data and information services for authorized users.

2.0 Implementing an Information Security Program

Once an organization's management has recognized the existence of such a threat and has directed changes to improve their posture or information security process a plan should be formulated to address the issue. The first step in implementing an Information Security Program is to assign the task to a defined work group and empower the group with the resources they require. Leaving the task solely to the IT department may not be adequate. While IT departments do acknowledge some responsibility in data security most IT organizations are content just to be able to keep their networks running, they don't always see the importance of providing security. An AP article posted on USA Today.com titled National Security Advisor sees cyberterrorist threat (5) quotes National Security Council Advisor Richard Clarke as stating "Unfortunately, most government agencies don't understand the need to improve their network security because they don't think it's their mission,". Mr. Clarke's statement is key in understanding that IT Security is not just IT's concern it's the entire organization's concern.

There are many roles that other departments within an organization should have in IT security. Departments such as Human Resources (privacy issues, inappropriate e-mail, internet abuse), Finance (protection of rates, financial standing, projections) Legal (Privacy issues, compromise of protected data) and Security (has the knowledge of security fundamentals that apply no matter what the venue and can put security first when looking at issues) all have an important role in Information Security. Incorporation of all of these departments concerns and abilities can result in cost effective and viable Information Security Program. Conversely, leaving any out of the process may leave or create vulnerabilities.

It is also important to ensure that team members have adequate training or experience within the Information Security arena. Several sources are available that provide such training. Two organizations that standout in this area are the System Administration, Networking, and Security (SANS) Institute (http://www.SANS.org) and the Carnegie Mellon Software Engineering Institute CERT Coordination Center (http://www.cert.org). These organizations provide in-depth information systems security training that can be applied to any system. Other organizations such as Aegis Research (http://www.aegisresearch.com) provide specialized training to meet specific Government requirements in information security.

Once the organization's workgroup has been established, it should baseline the organization's current systems and policies. Baseline the systems by going out and looking at what is on the network and comparing it to what the IT department says is there. Have users moved equipment or brought in and connected their own devices that could effect network performance or security? Results may be surprising. When looking at policies is there one set of IT policies addressing IT security? The workgroup may have to search through the policies of several different departments. If policies are not concise, consistent and easily accessible, no one will follow them.

Once the baseline is complete, the workgroup can begin to note where changes are required. Any changes made should be supported by approved policies - so it may help to begin there. Since policies will be the foundation of the program, there is a need to ensure that they are easy to read and understand and are complete, while allowing for changes as the technology and accepted norms within the organization change. Writing policies may be somewhat difficult. One potential resource is PentaSafe Security Technologies Inc. http://www.pentasafe.com/. PentaSafe has published "Information Security Policies Made Easy" (http://www.baselinesoft.com/ispme.html) by Charles Cresson Wood, CISA, CISP. This book is a comprehensive set of information security policies that can be easily modified to meet an organization's needs for information security policies without having to "re-invent the wheel" thus saving valuable time and resources.

A System Security Plan that ties all of the policies and procedures together, identifies key personnel, and accepted organizational standards may be a valuable tool to develop. Such a plan helps to tie things together so users do not have to search to find answers to their questions or resolve their problems. User training is also an important piece of the puzzle. An organization may have the best policies and procedures on the books but if no one makes the users aware of them they are useless and the organization is not served by having them.

An annual review of the status of the organization's systems should also be conducted. Throughout the year the workgroup or appointed individuals should track incidents and events that effect the organization's systems and the actions implemented to resolve them. Also, track the cost of clean up actions and preventative measures that result from incidents. The resulting data gives the IT Security Professional a way to quantify what is happening at their organization and can help secure resources and demonstrate the added value of the program.

The Carnegie Mellon Software Engineering Institute's CERT web site offers excellent resources intended to guide an organization through this process and then through the use of their Security Improvement Modules improve on the baseline the workgroup has established. The Carnegie Mellon Software Engineering Institute's CERT Security Improvement Modules can be found at http://www.cert.org/security-improvement .

3.0 Essential Elements of an Information Security Program

An Information Security Program can become a large and intrusive project if it's objectives are not clearly defined. Managing such a project in a way that keeps the effort in line with business objectives and as unintrusive as possible may be a tricky task but can be accomplished by beginning with the basics. Opportunities to expand and grow the program will present themselves over time and as value added can be seen by taking care of basic issues. Some of the basics to start with are outlined below. Each of these should be implemented in a manner consistent with protecting the confidentiality, integrity and availability of the organization's data as the end objective.

Access Control – Any type of Security program begins with access. The organization has something it believes needs to be protected. Access by unauthorized personnel must be denied. Most organizations understand the need for physical security measures. We all see badges and badge readers that allow entry and most of us would not think about loaning our company badge to another person. So, after an organization has put physical guards around its systems, what happens? The systems get connected to the internet and users are provided with extranet connections and dial up lines. These means of access totally bypass all of the security guards and badge readers that have been put in place. What have they been replaced with User IDs and passwords?

There are two problems with user IDs and passwords that may never disappear. User IDs tend to be pretty standard lastname_firstname (Doe_John)or lastname first intial (DoeJ) or vice versa. Second when users choose their passwords they make them easy, not too complicated, after all they have to be usable. “Hard to guess” passwords should be enforced. This means an organization may determine they need to run a password-cracking program such as Lophtcrack to see which users are complying with policy and which are not and correct any non-compliance. Users should also be advised to never give their passwords to anyone, remind them that social engineering is still a main source of information for someone attempting to break into the system.

Next, auditing and monitoring the system. Most operating systems allow for automated audit records to be kept - but is the organization using this tool? If audit logs are being kept, are they being reviewed? Auditing can not be overlooked. If the organization is not checking its system, then it may never become aware of unauthorized accounts, active accounts for employees who have departed the organization, users logging in at odd hours or remote connections being made for apparent reason. All of these could indicate that the system could be susceptible to or has been compromised.

Monitoring of the organization's networks is also important and there are tools, such as intrusion detection software, available to help automate and make this task easier and less labor intensive. An issue that will always come up when discussing system monitoring is the user's privacy. If an organization is monitoring network activities such as e-mail and internet usage, it is imperative that all users understand that while using the system their actions may be monitored. This can be documented by requiring that all authorized users sign a User Agreement acknowledging the monitoring that has been approved by the organization's legal counsel.

Computer viruses have cost companies hundreds of millions of dollars within the last couple of years. Viruses such as the "I Love You" not only caused losses in productivity but also cost additional resources in cleaning up the problem and safeguarding systems from further infections. On the opposite side of this there are many hoaxes warning of non-existent viruses or inflating the claims of potential damage done by real viruses. These are usually sent from one user to another in an earnest effort to help the intended recipient. This results in a lot of e-mail traffic for no reason - which can also be a drain on the organization resources. Organizations should ensure that they are adequately protected from computer viruses by using an anti-virus tool provided by a reputable company such as Symantech, Network Associates or any other reputable ant-virus software vendor. The organization also needs to ensure it keeps the anti-virus tool up to date. The anti-virus tool manufacturers provide updated anti-virus files for their products.

One resource for virus issues that I have found useful is: Vmyths.com. This web site is dedicated to educating people about computer virus myths, hoaxes, urban legends, hysteria**,** and the implications if you believe in them. The site also maintains a list of computer virus hoaxes. Located at: http://www.vmyths.com/ . This site is useful if questions are received from individuals within the organization about an e-mail proclaiming a new virus. Check it along with the web site of the organization's anti-virus tool provider and you can get an understanding if it's a real virus or a hoax and what needs to be done to effectively respond to it.

System Backups may be used only once in awhile but when they are needed it is critical. There are different backup schemes that can be used full, differential or incremental. The important thing is to identify which scheme works for the organization and ensure it is documented and implemented.

Further, backup tapes should be stored in a separate building or area of a building than the systems being backed up. If backup tapes are stored in a central server room and there is a fire in that room, not only will the organization lose hardware and the data its storing, it may also lose backed up data as well. If this happened, could the organization continue conducting business? A periodic check of the backups themselves should also be accomplished. If the organization cannot restore what it has backed up, it may already be in trouble. Physical access to the back up media is also a major concern. Such access should be strictly limited to prevent loss theft or other unauthorized access of such media and information.

Configuration Management is an area that most companies understand and apply to their products but never seem to fully implement over their corporate computer systems. The SANS LevelOne, Information Assurance Foundations, Core Issues and Challenges module defines Configuration Management as being "…the discipline of establishing a known baseline condition, and then managing that condition." (6) A good configuration management process will help to ensure that the organization knows what is going on in the network. Knowing what hardware and software is being used and by whom is important to be able to spot potential conflicts.

A relatively recent situation I am aware of occurred when a hardware engineer who was working in a lab connected a router that also served as a DHCP Server (assigning IP Addresses to the computers on the corporate network) corporate network. The engineer was doing his job, testing the router. The new router also became the DHCP Server for the corporate network taking control from the actual DHCP Server and giving wrong IP Addresses to the corporate computers as they were being powered on or connected. This resulted in about 500 users not being able to do their jobs for about two and a half hours until the IT department could track down the rogue DHCP Server. Had there been a configuration management process in place that the engineer was aware of the situation could have been avoided by providing a process to analyze the effects of putting the router on the network and making the appropriate changes to the device to allow the required testing. Configuration management processes can also help to track what software is used and reduce costs by ensuring everyone is using a standardized package when possible.

These are just the fundamentals of an Information Security Program. As you can guess depending on the shape the organization is currently in the task may be limited and as simple as verifying what is being done or as complex as designing a program from the ground up. Either way your organization will be better for it.

4.0 Other Available Resources

There are plenty of resources available, many of them free, that can guide an organization through the process and keep it informed of changing technologies and threats after a plan has been implemented. Some of these resources are:

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face. SANS was founded in 1989. http://www.sans.org/aboutsans.htm .

Science / Technology sections of reputable news organizations web sites such as
ABCnews http://abcnews.go.com/sections/scitech/ ,
CNN http://www.cnn.com/TECH/ and
USA Today http://www.usatoday.com/life/cyber/cyber1.htm .
These web sites usually provide good information on current events and trends.

SecurityPortal. Recognized as an objective force in the information security industry, SecurityPortal currently serves as the voice of security with its widely distributed e-newsletters and website with thousands of pages of security information.
http://securityportal.com/ .

F-Secure. F-Secure is a leading strategic provider of powerful data security solutions. Customers in nearly every industry, both private and Government, rely on our products to secure information. F-Secure supports businesses with a broad range of centrally managed and widely distributed best-of-breed data security applications built on a highly scalable management infrastructure.
http://www.f-secure.com/ .

5.0 Index of References

(1) AP, Layoffs Lead to Revenge Hacking, 19 June 2001
http://www.usatoday.com/life/cyber/tech/2001-05-31-revenge-hacking.htm

(2) International Organization for Standardization, ISO/IEC 17799:2000(E), Information Technology - Code of practice for information security management, First Edition 2000-12-01. viii

(3) IDG, Jaikumar Vijayan, Downsizings leave firms open to digital attacks, 27 June 2001
http://www.cnn.com/2001/TECH/internet/06/27/smaller.firms.vulnerable.idg/index.html

(4) Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information Within Information Systems Appendices, (05 June 1999)
Posted by the Federation of American Scientists at:
http://fas.org/irp/offdocs/6-3_20Appendices.htm

(5) AP, National Security Advisor sees cyberterrorist threat, 19 June 2001
http://www.usatoday.com/life/cyber/tech/2001-03-23-rice-cyberterrorism.htm

(6) SANS Institute, SANS LevelOne, Information Assurance Foundations, Core Issues and Challenges, 19