SANS Security Essentials (GSEC) Practical Assignment
Version 1.3

Computer Security in a Distributed Computing Environment

Charlotte Russell
February 13, 2002

Abstract

This paper will attempt to define methods in which a distributed computing environment can become more security conscious. It will describe a unique model of a computing environment, describe the security related problems inherent in working in this type of environment, and will provide solutions to promote a more unified effort to becoming proactive versus reactive while dealing with security related issues.

Working in a Distributed Environment

Managing security in a distributed environment is a monumental task. One model of a distributed computing environment is made up primarily of three significant entities: individual departments, a central computing department, and users. These three entities must work together to establish a healthy, working computing environment. In essence, it is a federated, or federal, model of computing.

"Federal: of or constituting a form of government in which power is distributed between a central authority and a number of constituent territorial units" (Leatherbury, slide 2)

Each individual department hires its own network administrator, who is given the daunting task of providing sole system management for a significant number of unique devices, operating systems, and applications for a large and varied user base. (In some cases, a single network administrator may oversee computing operations in several departments.) He or she must maintain and control the operations of these systems, and attain an appropriate level of knowledge necessary to secure them. The network administrator is supervised by a manager who may or may not be a computing professional, thus may not fully understand the responsibilities inherent in managing a network.

The central computing department houses a large number of system administrators who provide specialized, second level support for the network administrators of the individual departments. Areas of expertise include communications, mainframe, applications, programming, desktop operating systems, web support, helpdesk management, and security. The level of support given to the network administrator is determined by the amount of specialized support needed for each system. Support can range from minimal, to in-depth or hands-on. The central computing department is managed by high-level computing professionals, and also has its own network administrator who has the daunting task of providing support for each of these individual "users". The communications team manages the organization's network infrastructure. Network managers in individual departments (those not found in central computing) manage their own "subnet" of the main network.

The user base in a distributed environment varies. The definition of a user, according to an on-line, web-based dictionary is: "An individual who uses a computer. This includes expert programmers as well as novices. An end user is any individual who runs an application program." (Webopedia, URL: http://www.pcwebopaedia.com/TERM/u/user.html) A "user" in a distributed computing environment may include network administrators, system administrators who provide support in specialized areas, top level management, regular staff, management, or the novice.

Security Problems in the Distributed Environment

In a distributed environment with thousands of "users", it becomes very difficult to maintain adequate security-related controls. "Users" find creative ways to intentionally bypass security policies and other procedures that were created to protect resources. Some "users" cause problems out of ignorance (unaware of security policies). Others open the door to hackers by refusing to upgrade/update systems. In some cases, "users" don't protect the physical security of computing resources. In any case, lack of communication is most likely the catalyst for these problems which can cause confidentiality, availability, and integrity breaches.

In the distributed environment, lack of communication between departments and "users" is a problem. Network or system administrators who are responsible for their own "subnet" are generally unaware of projects and progress that other network or system administrators have achieved in other departments. They are also unaware of the problems that are encountered in other departments. Because of this lack of communication, or lack of information sharing between departments, similar problems experienced in different areas proliferate through the entire organization. These problems could be resolved if network administrators were more willing to share their experiences, problems, and achievements. The information could be invaluable to an area struggling with a similar project or problem.

Often times, the constant struggle to provide timely and efficient service becomes more of a priority than learning how to properly secure a system. There's an "us against them" attitude, i.e. network or system administrators versus one another, and, the attitude of all "users" versus the central computing security team. Security is not at the forefront of a "user's" agenda. They have deadlines and other projects that place security at a distance. The central computing security team then becomes frustrated because of the lack of cooperation, time, or interest that is shown when recommending avenues that will reduce risks. This struggle could result in breaches of confidentiality, availability and integrity.

Lack of training contributes to the inability of network or system administrators to properly configure and secure systems. Limited budgets can prevent departments from taking advantage of specialized training events. Management in the distributed area may not believe that providing a budget for security training is a priority. Limited time also prevents network or system administrators from expanding their knowledge. They may be swamped with projects and are unwilling to take the time away from work to attend training. Lack of investment in training and time could result in breaches related to availability and integrity compromises.

Awareness of security risks is also prevalent in this type of environment. Network or system administrators may not believe there is true risk involved in allowing what the security team would consider high risk. Some consider the idea of security as non-relevant- but that usually changes when there is a serious problem that involves a crashed "network" or a hacking incident.

"Many of the computer technologists who work in security are not equipped to solve…problems. They rely on their predictable computers and seem to believe that people are predictable as well. Lacking any significant contact with computer criminals, these technologists view them as people much like themselves, who think as they do and play the game by the established rules. This does not work. In addition to the technologists who can design and implement the technical aspects of computer security, information security requires the broad expertise of business, audit, and industrial security experts who can deal with the human factors and business issues. Information security experts must be knowledgeable in a range of subjects and capable of matching wits with the computer criminals." (Parker, p.18)

Another problem that is run into in a distributed environment is the typical lop-sided ratio of network or system administrators to actual systems, or machines. Typically, there is only one administrator for several systems (critical and non-critical). When that administrator is unavailable, a system that is considered critical may be left vulnerable and at a high risk for disaster unless back-up operations have been documented, and other back-up personnel are available. For example, central computing personnel who specialize in communications may be well aware of the intricacies of the infrastructure of their network. However, if a router crashes and the primary administrator is unavailable, the network will be unavailable indefinitely. Critical services must be identified, backed-up and all procedures should be documented in the event of a disaster. This type of breach would be considered an availability attack.

The over-worked network or system administrator may also be unable to support all users within their department. Some "users" require special hardware and software that may be considered "unsupportable", i.e. not on the supported items list as deemed by the network or system administrator. The "user" may feel that no assistance will be rendered and may be left to resort to their own devices, which means, a "user" who may be untrained person will begin to act as system administrator on their own behalf. Typically, the untrained user sets up a poorly configured computer on the network which will probably be hacked before patches can be installed.

Lack of funding to purchase adequate security controls prevents a department from attaining an adequate level of security. Departments in a distributed environment are typically funded using formulas based on specific criteria, leaving some departments unable to afford additional personnel, equipment, software, or physical controls. These departments continue to use old, out-dated security controls (if any exist). The department that does not have funding for adequate security controls may also be the same department that does not have funding for training. Non-existent, or out-dated physical security controls allow intruders access. Departments in distributed environments are notorious for allowing personnel claiming to be support technicians to enter computer rooms, or other areas with computers, without checking for identification or determining if the service was actually requested. The so-called support technicians are typically unsupervised while "inspecting" or "repairing" the problem. This problem could lead to confidentiality, availability, and integrity breaches.

Often, network and system administrators do not know how to define an event as an incident, and may not report it. Because they are not certain what would be classified as an incident, some administrators are not aware that an incident has even occurred. Others are not aware that procedures or personnel exist to handle security incidents, which may render them unable to respond properly. This lack of understanding could result in confidentiality, availability, and integrity breaches if an incident does occur and is handled inappropriately.

Lack of understanding of security roles in a distributed environment also plays a part in security problems. "Users" are not made aware of their responsibilities. They may not know even the basics of information security (maintaining confidentiality, availability, and integrity), and may not be aware of their role in the "big picture"- they do not know how they can help protect information. Or, they may not realize that they *should* be protecting information. Physical location plays a role in the lack of understanding. As mentioned, individual departments don't communicate well with one another. They may be physically located in different areas of an organization, or even in the different parts of a city and may be out-of-touch with the rest of the organization, i.e. unaware of issues and events). This lack of understanding and lack of communication could result in confidentiality, availability, and integrity breaches.

Failure to apply security patches or failure to follow recommended procedures leaves big holes in security. Software companies regularly notify the public when patches, fixes or upgrades to fight vulnerabilities becomes available. It's possible for the central computing security team to make information about the basics of information security available (perhaps in the form of a handbook) and checklists for methods to secure a system easily accessible on the internet. The "user" who does not accept this information or respond appropriately is the likely candidate for an infection or break in. This lack of acceptance could result in breaches of confidentiality, availability, and integrity.

Lack of security policy or a poorly publicized security policy renders an organization helpless in dealing with security problems. "Users" may not be aware that a security policy exists. Or, the policy (current or revised) is not publicized. "Users" can find themselves breaking policy (or law) without realizing that a policy forbidding the action even exists! This lack of knowledge could result in confidentiality, availability, and integrity breaches.

Other problems exist in a distributed environment, but they are typical of most environments where computing technology is in use. They include poor password management, sharing computer accounts, lack of contingency plans, not reporting suspicious activities, and many more, all of which could result in breaches of confidentiality, availability, and integrity.

Establishing a Common Ground

Computing management should oversee the smooth inter-networking of the individual departments, central computing, and users of information resources. Top level management must be made aware of the problems that could possibly occur at the lower levels, and they should also be given plausible solutions to these problems. If there are a large number of "users", individual departments, and varied levels of specialized computing knowledge, the task will not be trivial. Often, the needs of each entity vary greatly. A key to uniting these entities is to keep lines of communication open. The development and maintenance of a security plan can help minimize the number and effects of security related incidents. A successful security plan will include programs that stress the need to maintain confidentiality, availability, and integrity; provide adequate security awareness training opportunities for users, network administrators, and system administrators; establish an incident handling procedure; define critical assets and provision for defense in depth for those assets that includes: intrusion detection systems, firewalls, encryption techniques, authentication, good password management, back-up procedures, establishment of security policies and incident handling procedures, and the documentation of all elements of the security plan. Select objects of the security plan should be publicized to appropriate "users", depending on their functional role in the organization. Departments should create their own security plan.

Security Awareness

Often, "users" must be made aware that there are significant risks involved in using and administering computing resources. Educating the "user" is key to providing a stable infrastructure in any computing environment. A successful plan will include a security awareness program that will inform "users" that maintaining the confidentiality, availability, and integrity of the information entrusted to them is important.

"Awareness provides a baseline of security knowledge for all users, regardless of job duties or position." (Texas Department of Information Resources, "Practices for Protecting Information Resources", p.4)

Provide security awareness training using personnel resources from the central computing security team. This training can be conducted in a classroom or can be web-based computer training. Curriculum should be established that is easy for all "users" to understand. This might require the establishment of different course materials (basic, technical, specialized, etc.) based on the level of knowledge of the "user". And, training should occur at regular intervals.

The awareness program should teach "users" that maintaining confidentiality ensures that information deemed sensitive will not be disseminated to inappropriate entities. These entities may reside within or outside an organization's environment. Information that is deemed confidential should be clearly marked or indicated as confidential or sensitive.

The awareness program should also teach "users" that maintaining the availability of information by ensuring that adequate contingency plans are in place and documented. Perform regular back-ups and document back-up and recovery procedures. Document critical assets and the names and contact information of key personnel and vendors from which the assets were purchased. Document emergency procedures. And, document the date of the last review of the contingency plan.

The awareness program should also ensure the integrity of the information, or accuracy, of information. Information should be protected from accidental modification or erasure. Know who has access to the information and record dates when the information changed. Ensure that change control processes are in place so that only authorized individuals are allowed to modify information.

Security responsibilities should be established for all organizational personnel. Any "user" (from the administrative assistant to top level management) should be made aware of the basics of security as well as their security role in the organization. The Information Security Standards found in Texas Administrative Code identify roles for the agency head, management, staff, data owners, and data custodians, and, assigns an information security function to over see the security program. (Texas Administrative Code, "Information Resources Security Standards", URL: http://info.sos.state.tx.us/pub/plsql/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=201&rl=13)

The awareness program should make "users" aware that a security policy has been established. The purpose of the document, resources that should be protected, personnel practices (security responsibilities for "users"), physical security policies, information safeguards (password protection, etc.), incident handling procedures, and risk analysis information should be included. Also include applicable state and federal laws, as well as sanctions.

It would also be helpful to provide a security handbook in conjunction with the policy that would provide up-to-date information about specific vulnerabilities and how-to-information for "users". The handbook would be considered a living document. It would change as information about the latest vulnerabilities and risks are announced, and could also provide information specifically designed for each level of "user". It could include detailed information about password protection schemes, security risks, viruses and worms, back-up and recovery, incident handling procedures (specific instructions) and references to other security policies and applicable laws.

Security Contacts
To help keep individual departments informed about security, establish security contacts in departments who will act as liaison between the central computing security team and the department.

"Appoint distributed information security coordinators in local units and subunits. (A subunit may include all of the users of a local area network, salespersons in a local sales office, a Web site development staff, or an accounts payable staff.) The coordinators are to:

- Administer internal systems and Internet usage controls
- Identify and authenticate users for assignment of passwords
- Initiate and monitor physical and system controls such as clean desk practices and system logs
- Reports unusual events and losses to management
- Submit standards exception requests
- Provide security guides
- Arrange for training
- Convey the procedures for security from the central information security unit
- Identify by policy definitions the owners, service providers and custodians, and users and their responsibilities" (SANS Institute/National Infrastructure Protection Center, URL: http://www.sans.org/top20.htm)

For some departments, top-level management will need to provide adequate or additional resources: additional personnel, funding for training, equipment, software, and improvements in physical security. Security contacts will have to agree to cooperate with the central computing security team and agree to disseminate information and alerts to the "users" within the department.

SANS Institute, in conjunction with the National Infrastructure Protection Center, publishes the top twenty most critical internet vulnerabilities. The current list includes vulnerabilities associated with all systems, as well as those that are based solely on windows and Unix systems. A list of commonly probed attacked ports is also included. (SANS Institute/National Infrastructure Protection Center, URL: http://www.sans.org/top20.htm) Personnel from the central computing security team can disseminate alerts from software vendors and other security clearing houses (like SANS, CERT, Symantec, McAfee, etc.) to the security contacts in distributed departments. The central computing security team will act as the information filters, i.e. they will disseminate alerts and patches as appropriate to security contacts, establish incident handling procedures, provide security awareness training for security contacts and other users as requested, and respond to incidents.

Security Assessment

Conduct security system assessments. The assessment should identify critical assets, risks, threats, vulnerabilities, cost-effectiveness of security controls, and estimations of future loss and ask questions about security practices. Recommendations for improving security controls and effectiveness should also be included. Personnel involved in the assessment should include the central computing security team and all computing personnel in individual and central computing departments. The purpose of the assessment should be defined and the methodology on which the assessment is based should also be included. Participants should be made aware of what will be assessed, dates and times (if appropriate).

The shortcomings of the assessment should be made clear. Include any disclaimers or other factors that may contribute to the accuracy, or verity, of the assessment. Include questions about intrusion detection, firewalls, encryption techniques, authentication procedures, password management, back-up procedures, contingency planning, physical security controls, and other security practices. The assessment should ask questions about how departments respond to known vulnerabilities and potential risks, as well ask about security practices.

Some organizations may allow penetration and vulnerability testing. Keep in mind that written approval from the organization's top management should be received before conducting this type of testing. And, be aware that testing could distrupt network services, cause other undetermined problems, even violate organizational policies, state and/or federal laws.

Results of the assessment along with recommendations for improvement, should be disseminated to network and system administrators (as appropriate). Top level management should also review the assessment. (Some administrators prefer formal meetings to discuss the results of assessment.) Future assessments should be performed at regular intervals, as deemed appropriate by top management. Administrators and top level management should be made aware that the results of the assessment are proprietary, and should be considered confidential. The National

State Auditor's Association and the U.S. General Accounting Office have provided a "Management Planning Guide for Information Systems Security Auditing", URL: http://www.gao.gov/special.pubs/mgmtpln.pdf. Donn Parker, in his book, Fighting Computer Crime (Wiley, 1998), also provides information on conducting information security assessments.

Incident Response

Development of an incident response team that would include the central computing security team, security contacts from individual departments, and system administrators that have expertise in specialized systems. Define the group's function and core services, as well as the responsibilities of each team member. van Wyk and Forno recommend: "a team manager who is responsible for the overall administrative and personnel management of the team; a team leader/incident coordinator responsible for leading a particular incident response operation or effort; a senior information protection engineer who will provide senior technical effort for the project; an information protection analyst who will provide the core labor for the incident operation; an equipment custodian who is responsible for providing the team with all the equipment needed to conduct operations, software as well as hardware; a deployment logistics support officer who will provide the team with all the logistics and administrative support necessary for handling an incident." (van Wyk and Forno, p. 48)

To overcome confusion, define the term "incident". "Users" should understand what is deemed an incident so that they will understand that it should be reported. The CERT Coordination Center gives a general definition of an incident: "Any real or suspected adverse event in relation to the security of computer systems or computer networks -or- The act of violating an explicit or implied security policy

Examples of incidents could include activity such as:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent" (CERT Coordination Center: URL: http://www.cert.org/csirts/csirt_faq.html#2)

Incident response is described as: "…the discipline of handling situations in a manner that is: Cost effective…Business-like…Efficient…Repeatable…Predictable." (van Wyk and Forno, pp. 8-9)

Define the incident response process: create a flow chart that describes in detail the steps to be taken when handing an incident, and include steps for detection, containment, elimination, and recovery;
seek support from management (cite findings from the security assessment if necessary);
establish contact information (contact person or group, telephone number, e-mail address, etc.);
and maintain contact information for departments or groups that provide special services

(helpdesk, law enforcement, human resources, attorney, etc.). van Wyk and Forno, in Incident Response, provide information about creating an incident response team.

Training
In addition to security awareness training and other training that would be provided by security professionals within the organization, it would also be helpful to seek the advice of outside training organizations. Trainers within the organization could provide company names and contact information during training sessions, in security handbooks, or by utilizing other public arenas. "Users" could take the time to personally investigate other resources, or they could utilize the information provided by trainers. The following information provides web-based links to companies that provide security information, training, or general information about products:

Training/Publications/Information
SANS Institute. URL: http://www.sans.org/newlook/home.php (13 February 2002)
National Institute of Standards and Technology. "Federal Agency Security Practices". URL: http://csrc.nist.gov/fasp/ (12 February 2002)
Security Focus http://www.securityfocus.com/ (12 February 2002)
U.S. Department of Energy, Computer Incident Advisory Capability, "Network Security Tools", URL: http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html (12 February 2002)
National Infrastructure Protection Center. URL: http://www.nipc.gov/ (13 February 2002)
Microsoft Security. URL: http://www.microsoft.com/security/

Incident Response
SANS Institute. URL: http://www.sans.org/newlook/home.php (13 February 2002)
CERT Coordination Center: URL: http://www.cert.org/ (12 February 2002)
Security Focus http://www.securityfocus.com/ (12 February 2002)
National Infrastructure Protection Center. URL: http://www.nipc.gov/ (13 February 2002)

Malicious Code
Carnegie Mellon Software Engineering Institute, CERT Coordination Center. "Computer Virus Resources". URL: http://www.cert.org/other_sources/viruses.html (13 February 2002)
Symantec. "Security Response". URL: http://securityresponse.symantec.com/ (12 February 2002)
F-Secure. "Security Information Center". URL: http://www.europe.f-secure.com/virus-info/ (12 February 2002)
McAfee.com. "Virus Information". URL: http://www.mcafee.com/anti-virus/default.asp (12 February 2002)

Software/Applications
Red Hat.com. "Products and Services". URL: http://www.redhat.com/products/ (13 February 2002)
Microsoft. URL: http://www.microsoft.com/ (13 February 2002)
Microsoft Security. URL: http://www.microsoft.com/security/ (13 February 2002)
IBM. URL: http://www.ibm.com/ (13 February 2002)

Novell. URL: http://www.novell.com/ (13 February 2002)
Oracle. URL: http://www.oracle.com/ (13 February 2002)
Apple. URL: http://www.apple.com/ (13 February 2002)

BackUp/Recovery
Computer Associates. URL: http://www3.ca.com/Solutions/ProductFamily.asp?ID=115 (13 February 2002)
Veritas. URL: http://www.veritas.com/ (13 February 2002)
St. Bernard Software. URL: http://www.stbernard.com/default.asp (13 February 2002)
Disaster Recovery Journal. URL: http://www.drj.com/ (13 February 2002)
Disaster Recovery World. URL: http://www.disasterrecoveryworld.com/ (13 February 2002)
Federal Emergency Management Center. URL: http://www.fema.gov/ (13 February 2002)

Hardware/Networks
Cisco Systems. URL: http://www.cisco.com/ (13 February 2002)
Compaq. URL: http://www.compaq.com/ (13 February 2002)
Sun Microsystems. URL: http://www.sun.com/ (13 February 2002)
Nortel Networks. URL: http://www.nortelnetworks.com/index.html (13 February 2002)
Lucent Technologies. URL: http://www.lucent.com/ (13 February 2002)
Dell. URL: http://www.dell.com/us/en/gen/default.htm (13 February 2002)
Apple. URL: http://www.apple.com/ (13 February 2002)
Motorola. URL: http://www.motorola.com/home/ (13 February 2002)
AT&T. URL: http://www.att.com/ (13 February 2002)
Verizon. URL: http://www22.verizon.com/ (13 February 2002)
IBM. URL: http://www.ibm.com/ (13 February 2002)

Other Security Sites
Dave Dittrich http://www.washington.edu/People/dad/
Counterpane http://www.counterpane.com/

Conclusion

The solutions provided in this document are a starting point for allowing a distributed organization to develop into a more unified organization. Changes will not be immediate, i.e. changes won't take place overnight, but, cooperation, time, and patience will contribute to "turning-around" an organization that has historically resolved computing issues without considering the well being of the unit as a whole. These solutions should also improve communications and bring recovery.