Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Overview of Corporate Computer User Policy

this paper will discuss what should be covered in a corporate computer user policy that sets the overall tone of an organization's security approach. The intended audience is primarily information technology professionals.

Copyright SANS Institute
Author Retains Full Rights

AD

An Overview of Corporate Computer User Policy

Philip J. Kaleewoun, II

December 27, 2001

A corporate security policy is the gateway to a company's intellectual property. In today's world of information technology, the main threat to information security within a company is its employees. Employees are behind the firewall; furthermore, they have a username and password on the network. Therefore, a security policy should be designed to explicitly list out the dos and don'ts in your network. A security policy should serve as the company's constitution that governs how employees use the network and take care of both internal and external security issues. It should be well planned and periodically updated in order to reflect your company's ever-changing challenges and the continuous evolution in the world of technology. Having said so, this paper will discuss what should be covered in a corporate computer user policy that sets the overall tone of an organization's security approach. The intended audience is primarily information technology professionals.

Since you cannot totally eliminate vulnerabilities and threats on your network, the purpose of this policy will be to manage these vulnerabilities and threats. Your security policy will need to be clear, concise, and realistic. Clear in that it does not contain conflicting points of view, concise in that you stick to the point and discuss issues relative to your company's security well being, and realistic in that you discuss current security issues and work within the means of resources provided.

The overall program policy is usually a compilation of issue-specific policies. Issue-specific policies are used to address specific parts of your network such as Internet and email, anti-virus, data backup and recovery, and software security. These issues could either be addressed in separate documents or embedded into your security policy. The team responsible for writing this policy should work in conjunction with upper management and employ the services of a legal counsel. Upper management's involvement in the design of the policy is important because this will also help in the acceptance and implementation of the policy. Although certain parts of the policy might be confidential, most of it should be made accessible to everyone within your organization including your business partners. In fact, some business partners now require a copy of your data recovery policy in order to assure that their data is safeguarded properly.

In writing a policy there are certain aspects of network security that should be taken into consideration. These tasks involve identifying your assets, risk assessment, management of access to information, data backup and restoration, incident handling, and maintenance. This paper will discuss each of these steps in detail.

Identifying your Assets

First and foremost you will need to identify your assets and figure out the importance and value of these assets to your company. If intellectual property is the main asset of the company, then your data is your most valuable assets. For example, the data

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

on a computer may be more valuable than the computer itself. In the hands of a competitor, the losses might be even higher. Therefore, identify your assets and their vulnerabilities and take appropriate measures to safeguard them.

This section of the policy is very helpful in providing management with information relevant to decision making. Leveraging some value to each of your assets allows you to prioritize them. Remember, certain departments are more vital in the operations of the company; therefore, they should have a higher priority on the network than others.

Risk Assessment

Second, do a threat risk assessment and categorize the likelihood of these assets being destroyed or stolen. Identify the resulting damage to the organization if such an event occurred and decide if more security should be given to points of high vulnerabilities. For example, if the internet is your company's highest point of vulnerability decide whether management should prohibit employees from access to the web and email or should they be allowed to access the internet with the use of a firewall for both outgoing and incoming traffic. It is in this section that you include your anti-virus policy and state whether each user's workstation will have anti-virus software or if only the web server and mail server will have anti-virus software, also state how often it needs to be updated. Also include a laptop policy that requires the encryption of data on every mobile computer owned by your company. In most cases, data encryption is the best means of security on laptop because of the lack of physical security.

Doing the risk assessment might be one of the most difficult steps because you will have to give some financial value to what it will cost the company if the network is down for one minute in a day. This cost will be different from company to company and can mean life or death for a company. This amount for a construction company may be far less than that of an online broker. Looking at the figures, you should be able to determine where an attack is going to hurt the network the most.

There are certain costs you will have to pay for this security. Drawbacks such as monetary costs, ease of use, and network performance are far less in value when you consider the results. The increase in security will help minimize if not eliminate far greater evils such as loss of privacy (unauthorized access), and loss of services (denial of service).

Controlling Access to Information and Systems

Next, provide information and access only on a need to know basis and decide who gets access to external resources. This part of the policy is a policy within the policy because controlling access to information and systems is an interesting topic all by itself. Specify when a document is considered sensitive and confidential and therefore requires a secured method of transmission whether by encryption or the use of digital signatures to validate authentication. This section is the most important part because it deals with who has access to what and whether or not one department can view another department's files. You should spell out for what purpose can employees use network resource and that

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

worldwide web and email are not for personal use. This section of it should let employees know that they are not allowed to put any software on their PC whether for business or entertainment purposes without getting approval from the manager in charge of such activities. The software portion is important because if software is downloaded on a computer or copied off a CD the user might not have the proper license for it and this could mean a big software lawsuit on the company. Likewise, there is file-sharing software that can be downloaded off the Internet that can cause your network security to be compromised.

Physical security should be included in this section of the policy because if an intruder can walk into your building and walk out with one of your servers, the firewalls and anti-virus protection on your network are of no use. In most companies, there is only one level of physical security and that is when you enter the building, but once you're in you can go anywhere. Therefore the data center, the network operations center and all wiring closets should be locked at all times and require proper physical identification for both entry and exit. Another solution would be to put logon screen savers on each employee's computer. This section should also address the management of user passwords. The length of the password and whether or not to use special characters, letter, and numbers should be addressed. If this is decided upon, all employees should be mandated to use two of the three forms in their password and have a password length of at least eight characters. The life of passwords should also be discussed.

Remote user access is another issue in this section of the policy. The policy will have to make it clear whether or not users are allowed to dial in to the network. If remote access is allowed, everyone should be using the same secure VPN software and call back modems. If your company has a no modem policy, make sure that users don't have modems connected to their workstations.

Data Backup and Restoration

Then, create a data backup and recovery plan implement and test it periodically. The data backup and recovery plan should be an essential part of your business continuity plan. A BCP is a strategic plan used for the continuation of key business services in the event of an unexpected occurrence that seriously disrupts the business process. If such a plan exists, all personnel must not only know of its existence but also its contents and their roles and responsibilities in executing the plan. This is another reason why acceptance of the policy by both management and staff is very important to the success of the policy. Management will have to 'sell' the policy to its employees in order to ensure the success of the plan.

Your policy should include a step-by-step procedure for the restoration process that can be followed by the least technical person in your company. Keep full weekly data backups offsite as well as onsite, and specify the frequency of testing your recovery techniques, whether monthly or biannually. Your disaster recovery plan should be tied with your business recovery plan in order to swiftly put your company back on its feet after a disaster. For example, after the attacks of September 11, Deutsche Bank, which was located in the Twin Towers, made a quicker comeback than others because they had a good business continuity and disaster recovery plans[10]. Other companies that also

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

inhabited the Twin Towers but had neither a continuity plan nor a disaster recovery plan still haven't regained consciousness and probably never will.

Planning and testing your plan can be demanding, but after the recovery, it will all be worthwhile. Again the support of senior management is the most crucial determining factor as to whether an effective plan will be ultimately formulated. Also checking the quality of your tapes periodically for efficiency. This can make the difference in the time it will take to restore your data off the tapes. Remember, time is money!

Incident-Handling

As I said earlier, a policy cannot totally eliminate threats and vulnerabilities to your network; therefore, it should help minimize impact of an attack. The incident handling section should prepare you for the worst circumstances. For example, in case of a virus attack necessary measures should be taken in order to minimize the impact on your company. If the source of the attack was the Internet, it might be in your best interest to shut down your web server and isolate it from the rest of the network. This method would keep the contamination within a controlled area. If there is a laid out plan to follow in case of an intrusion or attack, things will be handled more effectively than they are in the absence of one. Although every situation is different, the plan should be as through as possible in order to take care of anything. One good thing to include in your plan is that whoever is handling the incident should take very good documentations of the step-by-step procedures taken to return the network to normal.

An advantage of doing this is that it is a proactive approach to solving your problem. From the results of the risk assessment, you will be able to evaluate your options and have better time to plan ahead. One point of caution is that never think that whatever solution you come up with is going to solve all your problems. Therefore be prepared for the worse case scenario.

Maintenance

Finally, entrust a group of people to be responsible for the enforcement of your security policy. I want to lay emphasis on a group because if there is only one person responsible, that person can still be compromised or overwhelmed. On the other hand, if it is a group of people, you will have a system of checks and balance. For example, one person should not be able to create a user account and activate on the network, this task should be divided among the members of this group. Their names and contact information should be listed in the reference section of the policy. This group should be authorized to enforce the policy. If possible, create a new department to oversee these responsibilities. Since the threats to the network reside both internally and externally, this group of enforcers should be allowed to use hacking software such as *Crack* to ensure that users on the network are adhering to the password policy. If an offender is found they should immediately be given a warning and advised of the threat they are posing to the network.

This group should also be able to run network-monitoring software on the network and scan the servers for opened ports. In addition to firewalls and antivirus software, the use of network monitoring software, port scanners, and other counter-

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

reconnaissance software will help this task force to better combat hackers both internal and external. The usage of these tools will help improve the perimeter defense on your network. Becoming familiar with these types of software will allow this group of people to know the enemies' tactics. Maintenance is a very time consuming task and can therefore be overlooked by administrators. Without checking to make sure things are how they should be the policy is of no use.

Since this group of enforcers may be authorized to carry out functions such as auditing passwords and keystrokes, and monitor email and web traffic, it would be wise to include a privacy policy that lets employees know that 'Big Brother' may be watching This would help alleviate some future legal problems.

Conclusion

Like everything else that needs planning, your security policy also has a life cycle. Once the policy has been written and implemented it should be evaluated to make sure it provides sufficient guidance, consistent and forward-looking. For example, in an effort to provide guidance, your company could make provisions for your security policy enforcers to send out pseudo email viruses to employees so that those who haven't seen an actual virus will know what one looks like. The policy should be consistent through out; there should be no discrepancy between your corporate policy and other departmental or issue-specific policies. "A security policy should also be in accordance with local, state, and federal computer crime laws"[9]. Your security policy should be opened to change in order to reflect new risks and vulnerabilities. A security policy should be independent of both hardware and software. Limit ambiguity and the use of technical jargons so that other non-technical employees will understand it, and include a glossary and reference manual at the end of the document in order to better explain certain terms. Keep in mind that this policy will need to be modified at least once a year.

In conclusion, the ideal security policy should cover all computer-related activities and practices within an organization, and make room for other unforeseen circumstances such as incident handling and disaster recovery. Implementing the proper security policy today is as important as implementing a new security patch on your network. But these policies are not given as much weight in our daily operations as they should. In fact the most difficult part after creating the policy is to get it accepted by the employees. Therefore, since most of the issues addressed in a security policy fall within the job description of the network or systems administrator he or she will need the full support of upper management in order to be successful.

The following is what I would consider a great sample policy outline because it covers most aspects of a corporate computer user policy. You could make the necessary adjustments to make it applicable to the needs of your company. It was taken from an article written by William Farnsworth of SANS Institute[2].

Sample Security Policy Outline

1. Introduction

1.1.1General Information

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1.1.2 Objectives

1.2 Responsible Organizational Structure

1.2.1.1.1 Corporate Information Services
1.2.1.1.2 Business Unit Information Services
1.2.1.1.3 International Organizations
1.2.1.1.4 Tenants

1.2.2 Security Standards

1.2.2.1.1 Confidentiality
1.2.2.1.2 Integrity
1.2.2.1.3 Authorization
1.2.2.1.4 Access
1.2.2.1.5 Appropriate Use
1.2.2.1.6 Employee Privacy

2. Domain Services

2.1.1 Authentication
2.1.2 Password Standards
2.1.3 Resident Personnel Departure

2.1.3.1.1 Friendly Terms
2.1.3.1.2 Unfriendly Terms

3. Email Systems

3.1.1 Authentication
3.1.2 Intrusion Protection
3.1.3 Physical Access
3.1.4 Backups
3.1.5 Retention Policy
3.1.6 Auditing

4. WEB Servers

4.1.1 Internal
4.1.2 External

5. Data Center

5.1.1 Authentication
5.1.2 Intrusion Protection
5.1.3 Physical Access
5.1.4 Backups
5.1.5 Retention Policy
5.1.6 Auditing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5.1.7 Disaster Recovery

6. LAN/WAN

6.1.1 Authentication
6.1.2 Intrusion Protection
6.1.3 Physical Access
6.1.3.1.1 Modems
6.1.3.1.2 Dial-in Access
6.1.3.1.3 Dial-out

6.1.4 Backups
6.1.5 Retention Policy
6.1.6 Content Filtering
6.1.7 Auditing
6.1.8 Disaster Recovery
6.1.8.1.1 Network Operations Center
6.1.8.1.2 Physical Network Layer

7. Desktop Systems

7.1.1 Authentication
7.1.2 Intrusion Protection
7.1.3 Physical Access
7.1.4 Backups
7.1.5 Auditing
7.1.6 Disaster Recovery

8. Telecommunication Systems

8.1.1 Authentication
8.1.2 Intrusion Protection
8.1.3 Physical Access
8.1.4 Auditing
8.1.5 Backups
8.1.6 Retention Policy
8.1.7 Disaster Recovery

9. Strategic Servers

9.1.1 Authentication
9.1.2 Intrusion Protection
9.1.3 Physical Access
9.1.4 Backups
9.1.5 Retention Policy
9.1.6 Auditing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

9.1.7 Disaster Recovery

10. Legacy Systems

10.1.1 Authentication
10.1.1.1.1 Password Standards

10.1.2 Intrusion Protection
10.1.3 Physical Access
10.1.4 Backups
10.1.5 Retention Policy
10.1.6 Auditing
10.1.7 Disaster Recovery

11. Security Services and Procedures

11.1 Auditing
11.2 Monitoring

12. Security Incident Handling

12.1 Preparing and Planning for Incident Handling
12.2 Notification and Points of Contact
12.3 Identifying an Incident
12.4 Handling an Incident
12.5 Aftermath of an Incident
12.6 Forensics and Legal Implications
12.7 Public Relations Contacts
12.8 Key Steps
12.8.1.1.1 Containment
12.8.1.1.2 Eradication
12.8.1.1.3 Recovery
12.8.1.1.4 Follow-Up
12.8.1.1.5 Aftermath / Lessons Learned

12.9 Responsibilities

13. Ongoing Activities

13.1.1 Incident Warnings
13.1.1.1.1 Virus warnings
13.1.1.1.2 Intrusion Vulnerabilities
13.1.1.1.3 Security Patches

14. Contacts, Mailing Lists and Other Resources
15. References

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Bibliography

1. Various. “Introduction to Risk Analysis” C&A Security Risk Analysis Group. 2001.http://www.security-risk-analysis.com/introduction.htm (December 4, 2001)
2. William Farnsworth. “What Do I Put in a Security Policy” SANS Institute. August 10, 2000. http://secinf.net/info/policy/policy.htm (December 5, 2001)
3. Various. “Case Studies: Firewall, E-mail and Internet Security” User Interface Technology. http://www.uit.co.uk/cs/cs-index.htm (December 6, 2001)
4. Fraser, B. editor. "RFC2196 Site Security Handbook." September 1997." http://www.faqs.org/rfcs/rfc2196.html. (December 10, 2001).
5. Various. “10 Tips for Creating a Network Security Policy.” Network Security Library. http://secinf.net/info/policy/10tips.htm (December 5, 2001)
6. Various. “Computer and Information Security Policy.” Network Security Library. http://secinf.net/info/policy/hk_polic.html (December 5, 2001)
7. Various. “Policy on Electronic Use of Electronic Resource.” University of Pennsylvania. September 9, 1997. http://www.upenn.edu/computing/policy/aup.html (December 11, 2001).
8. Barbara Guttman and Robert Bagwill. “Implementing Internet Firewall Security” Information Technology Laboratory Computer Security Division Policy and National Institute of Standards and Technology. April 13, 1998 http://csrc.nist.gov/publications/drafts/InternetFirewallPolicy.PDF (December 9, 2001).
9. Various. “Basic Security Policy” v.1.2a. SANS Institute. June 6, 2001.
10. Karen J. Bannan. “Be Prepared”. PC Magazine. January 15, 2002 edition.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 29th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**