9.1 User Policies Definition

System misuse is a major problem for many organisations. The main issue here is trying to identify what misuse is exactly. Certain things may be obvious examples of misuse, such as using company time and computers to search for another job, or to view forbidden websites.

However, other areas are not as clear such as an employee using his/her lunch hour to look up information about a car she is thinking to buy. Good user policies specifically outline how people may use systems and how they may not. For a policy to be effective, it needs to be very clear and quite specific. Statements such as “**computers and Internet access are only for business use”** are simply inadequate.

Every organisation must have specific policies that will be applied across the organisation. In our previous example, using a general statement of “**computers and Internet access are only for business use”** can be problematic. Assume that you have an employee who occasionally takes a few minutes to check his/her home e-mail with the company computer. You decide that this is acceptable, and choose not to apply the policy. Later on, another employee spends two to three hours per day surfing the net and you decide to fire him for violating company policy. That employee could sue the company for wrongful termination.

Other areas for potential misuse are also covered by user policies, including password sharing, copying data, leaving accounts logged on while employees go for lunch etc. All of these issues pose a significant impact on your network’s security and must be clearly spelled out within your user policies. We will now examine several areas that effective user policies must cover:

- Passwords
- Internet use
- E-mail attachments
- Software installation and removal
- Instant messaging
- Desktop configuration
- BYOD

9.1.1 Passwords

Keeping passwords secure is critical. Appropriate passwords are a part of operating system hardening. You should recall that in the past, a good password was defined as one that consisted of six to eight characters long, used numbers and special characters, and had no obvious relevance to the end user. For example, a user will use a password like “cowboys” or “godallas,” but it should always be advised to use a password like “%trEe987” or “123DoG$$”. This does not reflect the person’s personal interests and therefore will not be easily guessed.

Issues such as minimum password length, password history, and password complexity come under administrative policies, not user policies. These complexity requirements are still good recommendations. However, you should consider passwords that consist of12 characters or more. User policies dictate how the end user should behave.

However, we should always remember that no password is fully secure, regardless of how long or how complex it may be. It could also be listed on a Post-it note, stuck to the user’s computer monitor. This may seem obvious, but it is highly common to go into an office and find a password either on the monitor or in the top drawer of the desk. Any cleaner who passes by the office could potentially gain access to that password.

It is also quite common to find employees sharing passwords. For example, Bob is going to be out of town next week. He gives Alice his password so that Alice can get into his system, check e-mails and so on. The problem is that now two people have that password. What would happen if during the week Bob is absent, Alice gets ill and decides to share the password with Shelly so she can check the system while Alice is out sick? It doesn’t take very long for a password to get into the hands of so many people. This will lead to it being no longer useful from a security perspective.

Issues like minimum length of passwords, password age and password history are all issues of administrative policies. System administrators can force these requirements. However, none of this would be particularly helpful if the users do not manage their passwords in a secure fashion.

Explicit policies regarding how users secure their passwords are highly needed. Those policies should specify:

- Passwords are never to be kept in written form and in any accessible place. It is preferred that they should not be written down at all, and if they are, they should be in a secure area such as a lock box.
- Passwords must never be shared with any person for any reason.
- If an employee believes his password has been compromised, he should immediately contact the IT department so that his password can be changed in order for any logon attempts from the old password to be monitored and traced.

A recommendation is to choose a passphrase, something like ILikeCheeseBurgers, and then change the e's to 3's and use capital letters. Perhaps you should add a symbol so as to become #ILik3Ch33s3Burg3rs. This is a very secure password. It can be remembered and it has complexity as well as length.

The complexity requirements prevent dictionary attacks (using words from a dictionary) and guessing. However, you might be wondering why a long password is so important. The reason has to do with how passwords are stored. When you select a password in Windows, that password is stored in hashed format in a SAM file. Remember that a hash cannot be undone. Therefore, when you log in, Windows will hash whatever you type in and compare it to what's in the SAM file. If they match, you are in.

Hashing passwords leads to the use of an interesting hacking technique called the rainbow table. A rainbow table contains all the possible hashes of all the key combinations that might have been used in a password, up to a given size. For example, all the single-character combinations are hashed, all the two-character combinations are hashed, and so on up to some finite limit (often 8 to 10 characters). If you get the SAM file then you can search the rainbow table for any matches. If you find a match, then the associated plaintext must be the password. Tools such as OphCrack boot into Linux and then run a rainbow table against the SAM file. However, larger rainbow tables are cumbersome. No current rainbow tables can handle passphrases of 20 or more characters.

9.1.2 Internet use Policy

Most organisations provide users with some sort of Internet access. There are several reasons for this. The most obvious reason is e-mail. Apart from emailing, other reasons of having internet access within a business could be to access the web, and to even enter chat rooms. All of these can be used for legitimate purposes within any organisation but can also pose serious security problems. Appropriate policies must be in place to govern the use of these methods of communication.

The web is a wonderful resource which holds a tremendous wealth of data. The Internet is also full with useful tutorials on various technologies. However, even nontechnology-related business interests can be served via the web. Here are a few examples of legitimate business uses of the web:

- Sales staff checking competitors websites to see what products or services they offer in what areas, perhaps even getting prices
- Creditors checking a business's AM Best or Standard and Poor's rating to see how their business financial rating is doing
- Business travellers checking weather conditions and obtaining travel prices.

Of course, other web activities such as the ones below are most definitely inappropriate on a company's network:

- Using the web to search for a new job
- Any pornographic use
- Any use which violates local, state, or federal laws
- Use of the web to conduct employee's own business (i.e., an employee who is involved in another enterprise other than the company's business, such as eBay)

In addition, there are grey areas. Some activities might be acceptable to some organisations but not to others. Such activities might include:

- Online shopping during the employee's lunch or break time
- Reading news articles online during lunch or break time
- Viewing humorous websites

What one person might view as absurdly obvious might be acceptable to another. It is critical that any organisation must have crystal clear policies that specify what is and what is not acceptable during the use of the web inside working hours. Giving clear examples of what is

acceptable or not is a key factor here. You should also remember that most proxy servers and many firewalls could block certain websites. This will help prevent employees from misusing the company’s web connection.

9.1.3 Email Attachments

Most business and academic activity now occur via e-mail. As we have discussed in several previous chapters, e-mail also happens to be the primary vehicle for virus distribution. This means that e-mail security is a significant issue for any network administrator.

We cannot simply ban all e-mail attachments. However, you can establish certain guidelines for how to handle e-mail attachments. Users should open an attachment only if it meets the following criteria:

- It was expected (i.e., the user requested documents from some colleague or client).
- If it was not expected, it comes from a known source. If so, first contact that person and ask whether they sent the attachment. If so, open it.
- It appears to be a legitimate business document (that is, a spread sheet, a document, a presentation, etc.).

It should be noted that some people might find such criteria unrealistic. As the following criteria can be deemed inconvenient, these measures are actually quite sensible in preventing the prevalence of viruses, especially in email. Many people choose not to go to this level to avoid viruses, which could also be your personal preference also. Bear in mind that millions of computers are infected with some sort of virus every single year.

No one should ever open an attachment that meets any of the following criteria:

- It comes from an unknown source.
- It is some active code or executable.
- It is an animation/movie.
- The e-mail itself does not appear legitimate. (It seems to tempt you to open the attachment rather than simply being a legitimate business communication that happens to have an attachment.)

If the end user has any doubt whatsoever, they should restrain from opening the e-mail. They should contact a member of the IT department who has been assigned to handle security. That person can then either compare the e-mail subject line to known viruses or can simply ‘check out’ the e-mail personally. If appears legitimate, the user can open the attachment.

9.1.4 Software Installation and Removal

This specific matter has a very firm answer, end users should not be allowed to install anything on their machine, including wall papers, screen savers, utilities etc. The best approach is to limit their administrative privileges so as to be restricted from installing anything. However, this should be coupled with a strong policy statement prohibiting the installation of anything on users’ PCs. If they wish to install something, it should first be approved by the IT department.

This process might be cumbersome, however it is necessary. Some organisations go so far as to remove media drives (optical drive, USB, etc.) from end users’ PCs so that installations can occur from files that only the IT department has placed on the network drive. This is usually a more extreme measure than most organisations would require, but it is an option you should take into consideration.

9.1.5 Instant Messaging

Instant messaging is also widely used and abused by employees in companies and organisations. In some cases, instant messaging can be used for legitimate business purposes. However, it poses a significant security risk. There have been viruses that have propagated specifically via instant messaging. In one specific incident, the virus would copy everyone on the user’s buddy list with the contents of all conversations. Thus, a conversation that the user thought was private was being broadcasted to everyone with whom that user had messaged.

Instant messaging is also a threat from a purely informational security perspective. Without the traceability of an e-mail going through the corporate e-mail server, nothing stops an end user from instant messaging out trading secrets or other confidential information. It is recommended that instant messaging should be banned from all

computers within an organisation. If you find that your organization must use instant messaging, then it is highly necessary to outline very strict guidelines for its use, including:

- Instant messaging may be used only for business communications, no personal conversations. Now this might be a bit difficult to enforce. More common rules, such as prohibiting personal web browsing, are also quite difficult to enforce. However, it is still a good idea to have those rules in place. If you catch an employee violating them, you can refer to a company policy that prohibits such actions. However, you should be aware that in all likelihood you would not catch most violations of this rule.
- No confidential or private business information should be sent via instant messaging.

9.1.6 Desktop Configuration

Many users like to reconfigure their desktop. This means changing the background, screen saver, font size, resolution, and so on. Theoretically speaking, this should not be a security hazard. Simply changing a computer's background image cannot compromise the computer's security. However there are other issues involved.

The first issue is where the background image comes from. Frequently end users download images from the Internet, increasing your chances of catching a virus or Trojan horse, particularly one using a hidden extension (e.g., it appears to be a mypic.jpg but is really mypic.jpg.exe). There are also human resources/harassment issues if an employee uses a backdrop or screen saver that is seen offensive to other employees. Some organisations simply decide to prohibit any changes to the system configuration for this reason.

The second problem is technical. In order to give a user access to change screen savers, background images, and resolution, you must give rights that also allow to change other system settings you might not want changed. The graphical display options are not separated from all other configuration options. This means that allowing the user to change screen saver might open the door to alter other settings that would compromise security (such as the network card configuration or the Windows Internet connection firewall).

9.1.7 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) has become a significant issue for most organisations. Most or nearly all of your employees will have their own smart phones, tablets, smart watches, etc. that they will most likely carry with them into the workplace. When they connect to your wireless network, this introduces a host of new security concerns. You have no idea what networks those devices have previously been connected to, what software was installed on them, or what data might be infiltrated by these personal devices.

In highly secure environments, the answer may be to forbid personally owned devices. However, in many organisations, such a policy is impractical. A solution for this is to have a Wi-Fi network that is dedicated to BYOD and is not connected to the company's main network. Another approach, although more technologically complex, is to detect the device on connection, and if it is not a company-issued device, significantly limit its access.

There are also alternatives to BYOD. For example, Choose Your Own Device (CYOD) is a policy wherein the company allows the employee to bring their own device, but only if that device is from a list of pre-approved devices. This gives the company some control over what the user is connecting to the company network.

COPE, or Company Owned and Provided Equipment, is another option. In this scenario, the company provides the device, and has complete control over it. However, this can become an issue when the employee uses a device for both personal and professional purposes, not to mention the expense of providing employees with devices and maintaining those devices.

Whatever approach you take, you must have a policy regarding personal devices. They are already ubiquitous and spreading further. Just a few years ago, smart phones were really the only BYOD device. However in today's world we have smart watches, smart luggage, etc. It is also difficult to predict what type of devices will be coming within the next years, and how they can be regulated.