WindowSecurity.com

Building and Implementing a Successful Information Security Policy

By Dancho Danchev
dancho.danchev@windowsecurity.com

Table of Contents

Disclaimer & Rights of Distribution

This document is provided "AS IS," with no express or implied warranties. Use the information in this document at your own risk.

This PDF document may be re-distributed without prior permission from us, provided the PDF and it's copyright notice are not changed in any way. Therefore feel free to email this document, print it to share with colleagues or post it to your website. WindowSecurity.com must be clearly acknowledged as the owners of the document and a link provided to WindowSecurity.com should you post this document to your website. Those that have done so are invited to email us at **info@windowsecurity.com** so that we may consider including a reciprocal link to your site within our own links section.

01. Overview

The purpose of this paper is to outline the strategies and managing processes behind implementing a successful Security Policy. Additionally, I will give recommendations for the creation of a Security Awareness Program, where the main objective will be to provide staff members with a better, if not much improved understanding of the issues stated in a security policy.

We will also be focusing on significantly reducing the integration period of the security policy, by way of proper explanation of all of the items pointed out in a formal security policy document.

02. Scope

This paper is by no means intended to be a complete reference on the process of building a security policy or the development of a security awareness course. Instead, it was created with the idea of providing the reader with a reliable source of advice, various recommendations and useful tips gathered from my personal experiences while building and developing security policies, as well as conducting security awareness courses.

This document will also provide you with a sample security newsletter, best practises concerning various information security threats, as well as discuss in detail some of the most common security problems which companies are facing every day (concentrating specifically on security problems endangering somehow the continuity and the proper functionality of the institution).

03. Introduction

Information security has come to play an extremely vital role in today's fast moving, but invariably technically fragile business environment. Consequently, secured communications are needed in order for both companies and customers to benefit from the advancements that the Internet is empowering us with.

The importance of this fact needs to be clearly highlighted so that adequate measures will be implemented, not only enhancing the company's daily business procedures and transactions, but also to ensure that the much needed security measures are implemented with an acceptable level of security competency.

It is sad to see that the possibility of having your company's data exposed to a malicious attacker is constantly increasing nowadays due to the high number of "security illiterate" staff also having access to sensitive, and sometimes even secret business information. Just imagine the security implications of someone in charge of sensitive company data, browsing the Internet insecurely through the company's network, receiving suspicious e-mails containing various destructive attachments, and let's not forget the significant threats posed by the constant use of any Instant Messaging (IM) or chat applications.

04. Why Have A Security Policy

As building a good security policy provides the foundations for the successful implementation of security related projects in the future, this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources.

The first step towards enhancing a company's security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of your staff into participants in the company's effort to secure its communications but also help reduce

the risk of a potential security breach through "human-factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorised sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralised document, as far as protecting Information Security Assets is concerned.

05. What Is A Security Policy

The security policy is basically a plan, outlining what the company's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems.

The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets. A good and well developed security policy should address some of these following elements:

- How sensitive information must be handled
- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and Internet connectivity in a secure manner
- How to properly use the corporate e-mail system

Basically, the main reasons behind the creation of a security policy is to set a company's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and highlight the importance of having secured communications while doing business online.

06. Getting Started

The purpose of this section is to provide you with possible strategies and some recommendations for the process of creating a security policy, and to give you a basic plan of approach while building the policy framework.

The start procedure for building a security policy requires a complete exploration of the company network, as well as every other critical asset, so that the appropriate measures can be effectively implemented. Everything starts with identifying the company's critical informational resources, a subject that is discussed in depth in the next section of the paper.

07. Risk Analysis (Identifying The Assets)

As in any other sensitive procedure, Risk Analysis and Risk Management play an essential role in the proper functionality of the process. Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality -- an important (key) process that needs to be taken very seriously. Essentially, it is the very process of defining exactly WHAT you are trying to protect, from WHOM you are trying to protect it and most importantly, HOW you are going to protect it.

In order to be able to conduct a successful Risk Analysis, you need to get well acquainted with the ways a company operates; if applicable, the ways of working and certain business procedures, which information resources are more important than others (prioritising), and identifying the devices / procedures that could lead to a possible security problem.

List everything that is essential for the proper functionality of the business processes; like key applications and systems, application servers, web servers, database servers, various business plans, projects in development, etc.

A basic approach would be:

- Identify what you're trying to protect
- Look at whom you're trying to protect it from
- Define what the potential risks are to any of your Information Assets
- Consider monitoring the process continually in order to be up to date with the latest security weaknesses

A possible list of categories to look at would be:

- Hardware: All servers, workstations, personal computers, laptops, removable media (CD's, floppies, tapes, etc.), communication lines, etc.

- Software: Identify the risks of a potential security problem due to outdated software, infrequent patches and updates to new versions, etc. Also take into account the potential issues with staff installing various file sharing apps (Kazaa, Sharereactor, E-Donkey, etc.), IM (chat) software, entertainment or freeware software coming from unknown and untrustworthy sources.

- Personnel: Those who have access to confidential information, sensitive data, those who "own", administer or in any way modify existing databases.

08. Risk Management(Identifying The Threats)

Based on the research conducted on the company's information assets, you should now be able to properly manage all the threats posed by each of your resources.

The purpose of this section is to guide you through the creation of a list outlining various potential threats, something that should also be included in the formal security policy. Each of the following elements will be discussed in depth later in the Security Awareness Program section, thus providing the staff members with a better understanding of each of the topics covered below.

- Physical/Desktop Security

System Access: best practises for password creation, passwords aging, minimum password length, characters to be included while choosing passwords, password maintenance, tips for safeguarding (any) accounting data; the dangers to each of these issues must be explained in the security awareness program;

Virus Protection: best practises for malicious code protection, how often the system should be scanned, how often, if not automatically, should Live Update of the software database be done, tips for protection against (any) malicious code(viruses/trojans/worms);

Software Installation: is freeware software forbidden, if allowed, under what conditions, how is software piracy tolerated, are entertainment/games allowed or completely prohibited as well the installation of any other program coming from unknown and untrustworthy sources;

Removable Media(CD's, floppy): "Acceptable Use" measures (perhaps by way of a AUP - Acceptable Use Policy) need to be established, the dangers of potential malicious code entering the company network or any other critical system need to be explained as well;

Encryption: explain when, how and who must encrypt any of the company's data;

System Backups: the advantage of having backups needs to be explained; who is responsible, and how often should the data be backed up;

Maintenance: the risks of a potential physical security breach need to be briefly explained;

Incident Handling: define what a suspicious event is, to whom it needs to be reported, and what further steps need to be taken;

- Internet Threats

Web Browsing: define what constitutes restricted, forbidden and potentially malicious web sites, provide staff members with brief, and well summarised tips for safer browsing, additionally let them know that their Internet usage is strictly monitored in order to protect company's internal systems;

E-mail Use: define the "acceptable use" criteria of the E-mail system, what is allowed and what is not, the company policy on using the mail system for personal messages, etc. Also briefly explain the potential threats posed by (abusing) the mail system and of the potential problems as far as spreading malicious code is concerned;

Instant Messaging (IM) Software (ICQ, AIM, MSN, etc.): whether it is allowed or completely forbidden, provide them with short examples of how an attacker might use these programs to penetrate and steal/corrupt/modify company data;

Downloading/Attachments: is downloading allowed or not, useful tips for safer downloading, explanation of trusted and untrustworthy sources, best practises for mail attachments if allowed, discussion of potential threats and dangers, use of virus scanners, etc.

These elements will later be covered in detail in a Security Awareness Program. Staff need to understand why some activities are prohibited, what the impact of certain dangers can have on the company, actions they must follow if and when a potential security problem has been suspected or discovered. By involving staff in a Security Awareness Program staff will not just broaden their knowledge on the information security field, but also learn how to act in a secure manner while using any of the company's information assets.

09. Security Policy Violation

In order to realise the importance of a security policy, staff need to be aware and fully understand the consequences of violating the policy, thereby exposing critical systems to a malicious attacker, or causing unintended damage to other companies worldwide. Violations should be handled accordingly; those who in one way or the other violate the security policy should be made aware that they may face being put through a "trial period", which involves also the limited use of some of the company information assets until they can show they are able to act in a secure manner while using the corporate systems. They should also be aware that in some (severe) cases they also may risk being fired or even prosecuted.

Whereas this may seem as overkill to some, appropriate action needs to be taken in every violation case in accordance with the terms of the AUP and the policy, with the focus on reiterating the security basics and not punishment. Otherwise there will most likely be a successful penetration, either due to human error, or misunderstanding the policy.

10. Revising The Security Policy

The purpose of this section is guide you through the process of revising your security policy, as well as to ensure its effectiveness by closely reviewing several critical factors for its lasting success.

Let us assume you have already created (or revised) the security policy, and it looks perfect to you; but how does it look to staff members? Do they understand each of the terms, devices or the applications mentioned? How clear and precise is your policy; is it maybe a little too detailed, or precise that people loose sight of what it is trying to convey. Or is it just the opposite, missing the point entirely and/or not covering any of the important issues? These are some of the critical factors that will be explored below.

In order to reduce the chance of any misunderstanding, your security policy needs to fully outline the responsibilities of each and every one of your staff members. It should clearly state what needs to be protected, how the staff should protect it, and most importantly why it needs to be protected; that way they will be able to understand the importance and distinguish between critical and less critical information assets. The policy needs to be clear, concise and approximately two pages. Don't turn your security policy into a complete security awareness course; each of the elements contained in it should be discussed in the Security Awareness Program, not in the Policy.

Define the purpose of the security policy from the very beginning; does it apply to the information assets of the whole company, or is just created to cover a particular division or department. It is a good idea to provide users with a better understanding of how important information security is to the company, pointing out why there is no such thing as 100% security, but that the risks can be tremendously reduced if everyone realises that "security is everyone's responsibility".

Each of the assets needs to be precisely described to include, among others, items such as hardware, software, personnel, acceptable Internet use, etc.

If your company has already created a security policy, don't waste valuable time and resources building a new one; just rebuild and update the current one instead, thus saving a lot of research time.

You frequently need to monitor and update your security policy as new threats and technologies appear almost every day. Try to always keep up to date with the latest security problems (and the related remedies) in order to have the information assets of your company protected to a reasonable degree.

Your policy must clearly state how the Information Security Office (ISO) can be contacted (if there is one, otherwise, a relevant contact person); staff need to know with whom they should get in touch when they have questions, doubts, or have detected any suspicious activity. You should at least have a (cell)phone and an e-mail address available for this point of contact.

11. The Implementation Of The Policy

When the security policy is all drawn up, revised, updated and agreed upon, the implementation process will follow. This is usually harder than the creation of the policy itself, due the fact that at this stage you also need to coach and educate your staff to behave in a "secure" manner, following each of the core elements pointed in the formal security policy.

The final version of the security policy must be made available to all of your employees having access to any of your information assets. The policy must be easily obtainable at any time, with a copy placed on the internal network and intranet, if applicable.

A proper implementation requires not only educating staff on each of the core elements flagged as critical in the formal Security Policy, but also changing their role in the effort to protect critical company data.

The next section will aim to guide you through the creation process of a basic Security Awareness Program, along with various innovative and interesting ways of educating your staff, using user-friendly & informal lines of communication between the Information Security Office (ISO) members and your employees.

12. What Is A Security Awareness Program

The Security Awareness Program can be defined as one of THE key factors for the successful implementation of a company-wide security policy. The main aim is to define and outline the specific role of each of the employees in the effort to secure critical company assets, as well as covering in detail each of the core elements pointed in the security policy. The program is aimed at generating an increased interest in the Information Security field in an easy to understand, yet effective way.

The Security Awareness Program is often divided into two parts, one being the 'awareness' section, the other, the 'training'. The purpose of awareness is to provide staff with a better understanding of security risks and the importance of security to the daily business procedures of the company. The training part is aimed at covering a lot of potential security problems in detail, as well as introducing a set of easy to understand (and follow) rules to reduce the risk of possible problems.

13. The Process Of Developing

This section will provide you with the various strategies of building a solid Security Awareness Program. We will discuss various methods, their advantages and disadvantages, and will also give you get a better understanding of the essential steps to building the Program.

At the beginning you must answer yourself the following questions:

- What is the Security Awareness Program supposed to accomplish, and how are you going to draw attention on that?

- Who is your audience, how "educated" they are; is it going to be necessary to divide the program into two parts, one for those who have more knowledge about computers, and one for those who are not much into computers at all?

- How are you going to reach and motivate your audience? More importantly, how are you going to get your audience interested in improving the Information Assets of the company?

- Is the Program going to rely on a formal or an informal way of communication between you and the staff members? In which way are you going to conduct and present it?

The Purpose Of The Program

First of all, you need to explain to staff what the program will be trying to accomplish, how it will aim to improve the operations of the company, and how vital the protection of Information Assets really is. You will need to explain why "Security is everyone's responsibility", and ensure everybody understands it; explain that even if the company has the latest technological improvements like firewalls, intrusion detection systems, etc., an uneducated staff member could easily endanger sensitive information, and render any technical security measure in place, completely and utterly useless.

Another common misunderstanding that you will definitely face while conducting the Program is that the majority of people often tend to think that it is not their responsibility to help improve the security of their company. Generally people are of the (wrong) opinion that only the IT department or Information Security Office(ISO) can and need to take care of issues like these, and that is where generally the buck stops.

Addressing The Audience

One major problem that I am sure you are going to be facing is the difference in the levels of computer skills (of your audience), which will sometimes force you to pay additional attention to those who are not that much into computers. On the other hand you could also choose to differentiate between those who need security education, and those who don't; the idea is to separate staff having access to any of the company information assets from those who don't (and can't endanger sensitive data in any way), as this will definitely save you a lot of time and resources. It would be a good approach to hold informal meetings with staff in order to talk on a personal level and also conduct several surveys in order to measure their skill level; this way you will know where to focus your attention to.

Measuring Their Security Awareness Level Through Surveys

Security Awareness surveys are developed with the idea of measuring the current Awareness level of your staff, but will usually also point out common mistakes and misunderstandings of your employees; which will definitely help you improve the quality of the Program, even before it starts. It is highly recommended to archive the surveys in order to evaluate the effectiveness of the Program over a period of time.

You might also want to indicate to staff members that the survey is completely anonymous, that there is no need to cheat as the main idea is to merely measure the overall security awareness level in the company, and above all that this is just a survey and not an exam. They could answer just the main question without having to answer the "Why do they think so" section, if they don't know what to give here as an answer.

Some sample Security Measuring Survey questions might be:

1. Which of the following passwords is the most secure one, and why do you think so?

- abc123456
- HerculeS
- HRE42pazoL
- $safe456TY

Why do you think so?

2. Which is the most dangerous attachment extension, and why do you think so?
- *.exe
- *.com
- *.bat
- *.vbs
- all of the above

Why do you think so?

3. Your security policy states that the Information Security Office (ISO) would never send you an update to an application, but you have just received one, what would you do next?

- as it's coming from security@company.com which is our ISO e-mail address I will just run it and have the latest version of the software.
- as stated in the Security Policy I need to scan all the attachments before running, so I will scan and run after that.
- I would call the ISO office immediately to request further information.

4. A friend of yours gave you a multimedia CD last night, which you intend to check from your workstation at work; how are you going to do it?

- he is a friend of mine, and he would never give me any destructive files like viruses, etc. I trust him/her that's why I am going to check it out right away.
- although he is a friend of mine, it is stated in the security policy that removable media is allowed but its use should be limited to the minimum; I will stick to that and would scan the CD contents and see what's inside before I do so.
- I would just check the contents of the CD from my personal PC.

5. An ISO office representative asks you (in person) for your password as they misplaced it, and would need it to implement further security measures on your workstation; what would you do?

- they can't access the workstation without my password, and as it is about improving security, I would give it to them, as they are those responsible for maintaining the security within the organisation.
- I already have the workstation properly secured so I won't give it to them.
- I won't share my password with somebody even if my manager tries to force me into telling it; I would keep it as secret as possible.

These are some sample questions covering most of the threats pointed out in the Security Policy. It is completely up to you to decide how many questions should be in the survey as well as the aspects they should cover; but it is advisable to consider issuing surveys on a regular basis in order to continuously monitor the level and the effectiveness of the Program.

Getting Their Attention

Staff already have a lot of things to think about, a lot of decisions to make, operate and run through most of the day-to-day business procedures; therefore you need to have a very good strategy to get them motivated & eager to learn how they can improve company security.

Everyone these days is interested in stories about computer security in one way or the other, especially the (high-profile) break-ins, and making use of this, your main aim will be to help understand "attendees" of the program that they are actually going to be the new "gatekeepers" of critical company data (the information assets). You will undoubtedly will get asked questions like "Yeah, it's great to contribute to company security, but what do I get in exchange", which I define as normal questions, to which you must give proper answers.

Your future "students" need to be made aware of and understand how expensive it is for a company to conduct Security Awareness Courses, and to employ security experts, in order to provide 'attainable' services to its customers. Explain to them the damages that could be inflicted to the company, to the company (brand) name, its image, etc., which will inevitably impact on them somehow in return.

On the other hand, draw their attention also to the personal benefits from the whole program and the value of all the knowledge that will be supplied to them. One good example is to mention how all that information will significantly help them increase the security level of their own personal computers at home. The information they will be provided with does not only apply for their PC's at work but applies (in full) for their home PC's as well.

Another important point to keep in mind is the different ways people learn and memorise things, or in other words, deal with information they have just been provided with. Some learn by reading the materials, while others learn more by looking at diagrams, although it is proven that a combination of these methods has maximum effect in the process of understanding the subject. Therefore, you must ensure that your presentation style is such that it appeals to a crowd of people with varying degrees of knowledge and understanding.

Everyone gets bored of reading long materials, no matter how interesting they might be; if there isn't a picture, diagram or anything that brings some sort of variety into the process, people leave it behind. Try to "visualise" every subject that you are talking about by adding plenty of pictures, diagrams, relevant artwork and cartoons.

Cartoons are especially good, as they add an element of humour; people will definitely remember a funny situation representing a far serious procedure. Cartoons are best suited for posters, and most effective when placed all over the company, with their main purpose being a friendly medium to spreading the security awareness program messages (i.e. "Lock your machine when you leave", or "don't share your ID and password with ANYONE", etc).

Humour plays an essential role in the friendly education of the staff members; consider using it as you see fit but don't turn the whole program into a big comedy where everyone laughs and just makes jokes about the word Security. The addition of a little, humourous anecdote to any of your lectures like "I've got a friend who's so paranoid about security that he burns every paper after work, but come on, don't set the fire alarms off, just shred those papers labelled confidential/secret" would do fine.

Choosing The Approach

There are several approaches that you can follow when educating staff, and this section will point out the one which I define as the best one; a combination of both formal and informal ways of education.

The advantage of the formal method is that it will help staff realise the very importance of the security issue, as they know that these presentations cost a fair amount of resources, effort and money. On the other hand it will highlight the fact that the company is taking security very serious and therefore taking very serious measures to protect its information assets by educating its staff; and all it requires from them is a little time, devotion and understanding the importance of the security issue.

Another highly beneficial point when conducting a formal Awareness Program is the fact that your message, tutorial, presentation will be spread between most, if not all of the staff members; you will reach a lot of people that way, which will save you a lot of time compared to methods like one-on-one sessions, etc.

The informal way of education consists of email reminders, discussions, posters spreading security oriented messages (that are mostly discussed at the Course), screen savers, mouse pads, mugs, stickers, etc. as Security Awareness directors keep finding new and innovative ways of educating staff members. The advantage of this method is that it doesn't push (or, oblige) people in any way, like attending a meeting, listening to lectures, etc.; it is very personalised, user friendly and highly effective due to the fact that it comes very close to their every day life and working procedures within the company (posters, mouse pads, etc.).

Informal discussions are another highly beneficial way to educate and measure the skills of staff where people ask questions, answered by a representative from the ISO; the atmosphere is usually much more informal and calm. This is a highly recommended way of communicating with employees, as it initiates a two-way conversation whereby many points can be covered.

As in many other aspects, you need to find the right balance between the formal and informal ways, as both of these methods have their various advantages and disadvantages. By closely monitoring reactions from staff to the meetings and lectures conducted, you will be able to significantly revise and continuously improve the quality of your Security Awareness Program. Always provide staff with an always-evolving way of education, thus keeping them interested, eager to know and learn, and reducing the chance of boredom, while attending any of the Program's events.

14. Security Threats Management

Once you have defined the best way for education, have your plan and strategy ready, measured the computer skills level of your staff, you should start by discussing each of the elements pointed out in the security policy, in detail.

The main purpose of this section is to explore each of these elements in detail and to discuss various threats, providing you with ready made "Best Practises" on various topics along the way. You are encouraged to include

parts of this section in your own Security Awareness Course(s), thus providing your staff with a better understanding of the issues covered below.

Physical/Desktop Threats Explained

The threats that will be discussed in this section concern the way you use your workstation, access restricted zones in the company, and the way you handle sensitive information. I will cover all the possible threats, discuss their importance in detail, and provide you various effective ways to manage them.

System Access

Staff need to be fully aware of their responsibility to keep their User ID and password as secret as possible, and it's all because this is the first line of defence within any system: the identification of the user. Explain to the user that it is completely forbidden to share his/her ID and password with ANYONE, by ANYONE you mean, anyone ranging from the representatives of the Information Security Office (ISO), to their family members. No matter how stupid this might sound to some, they must not do it; even if their manager asks them for their password, they must reject the request. This way, NO ONE can force them into revealing their ID and password, under any circumstances. I know of cases where managers have tried to force (or even, trick) their staff into giving out their passwords for some reason or other in order to evaluate their level of security awareness; to see if they comply with what is stated in the Security Policy, i.e. not to share their ID and password with ANYONE. It is always useful to provide personnel with such "live" examples of how their awareness might, and is being evaluated.

Staff are required not to write any accounting data or ID/password information on loose papers, or sticky (post-it) notes, or leave sensitive information on white boards (for example, after a meeting, white boards, and/or flip charts should be cleared off) as this could result in a potential break-in, due to the improper handling of sensitive data. No matter how safe staff might think their password is, they should not be allowed to store them on any of these bits of paper; they must do their best and memorise it instead. Another common mistake that must not be overlooked is the horrifying fact that most of the users tend to hide these notes under the keyboard, or on some "secret" place, as they call it, around their desk; another activity that should be completely forbidden due to obvious reasons. Someone could easily find the "secret" hiding place and get acquainted with vital accounting data.

You must also educate your staff in the way that strong passwords are created. The (secure) ways accounting data must be handled are outlined in the "Password Best Practises" document, which briefly summarises these two aspects. I have included a sample "Password Creation Best Practises", and a sample "Password Maintenance Best Practises" section below, which will give a overview of what must be taken into account while writing such documents.

Password Creation Best Practises

- Passwords must be made up of a mixture of lower-case (small) letters, upper case (capital) letters, numbers, and at least one special character, such as (!@#$%^&*()_+|);
- The minimum length of the password must be at least 7 characters;
- Do not use the same password on several computers and/or services as once revealed, it would compromise the security within all the others in one go.

Good Examples
- Ona327(sA
- @865DapzI
- 93Sow#-aq

All of these are examples of good passwords, because they fully comply with Password Creation Best Practises; thus containing a mixture of small letters, capital letters, as well as numbers and special characters.

Bad Examples
- aaa123bbb
- abcdefg
- 76543210

The first is a terrible one, and any properly configured cracking program will retrieve it in a matter of minutes, and let's not even mention the second and the third one. The user with the last password (76543210) obviously thought it would be an easy to remember password, as well being a secure one, as it is a long(ish) one; but what the user does not know or realise is the fact that most cracking programs will find it in a matter of seconds (as the password follows a specific numerical pattern). It might be a good idea to incorporate a little demonstration in your Awareness Course at some point providing your staff with the unique opportunity to see how a (password) cracking software operates.

Strong Passwords Creation Tips

- Use the first letters of a quote, song, etc., for example "Something takes a part of me..." would be 'Stpm'
- join two words, include a number, as well as a special character, for example 'run4life#';
- a nice strategy when memorising passwords might be the following:

Let's assume your password is Naige453$lZ; first, pronounce it several times in your mind, then ask yourself what your password is, answering this question in the following way: "My password is a mixture of the name Naigel (a foreign friend of mine), several numbers and a dollar sign; my password starts and ends with capital letters, before the last letter of the name (L) there is a dollar sign ($), and before the dollar sign, there are random numbers.

This is a very useful and helpful trick for anyone who is trying to memorise or remember their password. By repeating (almost explaining) to yourself what your password is describing it the way I suggested above, I am certain that you will not have any problems remembering sophisticated, yet strong passwords.

Password Maintenance Best Practises

The proper maintenance of sensitive data such as the User ID and password are a responsibility of every staff member. This section will briefly cover Password Maintenance Best Practises.

- Do NOT share your User ID(s) and password(s) with ANYONE, neither with an ISO representative, help desk staff, family members, nor with your manager(s). No one can force you into revealing your User ID(s) and password(s) under any circumstances, remember that. It is your responsibility to keep the data as secret as possible;

- Do NOT store your User ID(s) and password(s) on any loose bits of paper, sticky (post-it) notes, white boards, flip charts, etc.;

- Do NOT hide your User ID(s) and password(s) under the keyboard, or at any other would be "secret" hiding place. Do your best and memorise it;

- Do change your password(s) following the stated password renewal period in the security policy;

- Before entering your User ID and password, make sure no one is watching you, to avoid the so-called "shoulder surfing" technique.

- Before using your User ID and password on a third-party computer, make sure it is well protected, and free of trojans and key loggers.

Virus Protection

Based on published papers, expert's predictions, as well as drawing upon personal experiences, I can easily state that viruses will continue to be a very serious threat to critical business data, and will continue to evolve, becoming more sophisticated, dangerous and devastating.

When you start explaining what a virus is, limit it to the facts, for example like how destructive it is, what damage it can cause, the possible financial losses related to a virus outbreak, etc. Don't bother staff with the specific technical information such as ways viruses function, how they hide, and many other topics that will not be of interest to them. Instead, provide those who are most interested, with some external (internet) links to the subject.

Consider explaining what a virus/trojan/worm is, the basic functions of each of these, how to possibly recognise (the operation of) one on your system(s), the potential problems they could cause, and the devastating effects on the whole company. Provide them with live examples, briefly discuss and answer the most simple and frequent questions that come up such as "Can the data corrupted from viruses be recovered", or "What to do once infected with a virus". However, you need to clearly explain that the idea of the presentation is to prevent an infection in the first place, as once infected with a destructive virus, there is not so much you can do, especially if there are no backups of the data.

On the other hand you need to precisely explain what the personal damages would be after a virus infection; damage and/or potential loss of critical business data, documents, projects, business plans, presentations they have been working on, along with any other personal data stored on the computer will be damaged, or, more than likely, be destroyed. By getting to know the devastating effects that viruses may have, staff will be much more aware on the subject, and will more than likely understand the importance of the topic, and the risks for both their company and their home PC's.

Go through the many scenarios of how viruses can get into the company networks, how staff could be tricked into running a virus, the dangers posed by Internet downloads, problems with outdated virus signatures, etc. Also explain the fact that Anti-Virus (AV) scanners are not the best, "fool-proof" solution, and the way they rely on signatures (pattern files). Discuss how useful virus scanners are, and how the effectiveness of preventive measures that are in place depend for a large part on the awareness and vigilance of the users themselves.

Staff need to understand that our main aim is to try and prevent, not to act after we are infected; although there will definitely be infections, we can significantly reduce the risk of infection and limit potential damage by educating staff and making them aware of the dangers posed by malicious code and software (virus/trojan/worm).

The advantages of regular system scanning, as well as the potential problems of not scanning your systems need to highlighted as well; although they know that AV scanners will not detect new viruses, they will at least know that they can reduce the risk, and properly manage the danger.

Scanning the systems using outdated signature files is another common problem that need to be touched upon. Staff should update their Anti-Virus/Anti-Trojan software at least once a week, and if the software allows centralised automatic updates (most do), updates must be scheduled on a regular basis to ensure the software detects the latest viruses/trojans/worms (known to your vendor's lab).

The various ways of getting infected with malicious code should be highlighted as well; let the employees openly ask you questions: see how they react to questions like "How am I getting infected", and then provide them with a better or more complete explanation about the most common as well as specific ways of infections. Below, I have included a sample "Malicious Code Best Practises" section for your convenience ; by no means an exhaustive list, but at least you will be able get an idea of what is considered as dangerous activity.

Malicious Code Best Practises

- Do NOT run any files without first scanning them, no matter what the file extension is, i.e. (.exe, .bat, .com, .doc, etc.);
- Do NOT download any files and/or programs from unknown sources; if in doubt, contact the ISO office as soon as possible;
- Do NOT open attachments, even if they were sent by a friend or family member; verify first that indeed, he/she has sent you the file, but nevertheless scan before you open/run anything;
- Do NOT run any programs you have found on diskettes/CD's around your desk if you are not completely sure that they are yours; someone might have placed it there specially for you to "find it and check it out";
- If downloading is allowed, limit it to the minimum; if you need a specific application or something else, always contact the IT department or the ISO office for further information BEFORE you download and installing something;
- Scan (full system scan) your system at least once per week with your default AV scanner software. Be sure to update the virus signatures before you do so, and also consider automating the process by scheduling a Full System Scan for convenient regular scanning in the future;
- Update the signature files as often as possible, so to ensure that the latest malicious software patterns are detected;
- The IT department or the Information Security Office will usually NEVER mail you the latest updates of any software (unless this is preceded by a much publicised, well-advertised, company wide campaign). If you detect suspicious activity, do not delete the e-mail received and contact the Incident Handling or Help Desk team as soon as possible;
- if you have any doubts regarding malicious software (viruses/trojans/worms), contact the ISO, The Help Desk or the IT department immediately. This way you will prevent any potential devastating mishaps, due to inappropriate and erroneous handling of dangerous and harmful incidents.

Everything that is defined as forbidden must be discussed and explained; why it is forbidden or restricted, how it could harm the company or the business, etc. Play out several potential scenarios, thus helping the users grasp the topic in an easy to understand way while trying to touch base on the consequences of all of these dangerous activities.

Software Installation

Freeware, or any other type of software, obtained or downloaded from unknown or untrustworthy sources could easily affect company security, exposing critical business data and/or corrupting sensitive ones. A lot of users tend to install such programs (from screen savers to games and funny cartoons in Flash) as they put it, for various personal needs and activities; to entertain, have something nice to look at or relax themselves. At the same time, they do not realise the potential threats they are exposing the company systems and networks to, from malicious software (viruses/trojans/worms) to legal actions against the company for installing (possibly) pirated software on the company workstation(s). Thus, you need to familiarise users with the potential problems attached to each of these issues, and also explain the company policy towards installation of any (unauthorised) software on any of the company workstation(s). Files downloaded from the Internet, copied from a CD or a floppy coming from an unknown source, or anything else that has not been reviewed by the Information Security Office or not been scanned for potential malicious code (by the corporate AV systems) could actually be classified as untrustworthy, unknown and dangerous. Freeware applications, due to their nature of origin, are a significant source of threat and should be approached with caution.

Staff members need to be aware of the risks involved, and learn to think twice before they act on issues. This can be stimulated in many ways; by playing out various scenarios on how software downloaded from either the Internet or copied from any removal media could endanger the company, its business, one's privacy, or the use of company bandwidth to commit illegal actions.

It is entirely up to you to decide whether users should be allowed to download and/or install third party programs on their workstations; and implement the appropriate (security) policies and procedures that go with this decision. You will not only need to clearly state the consequences for those who violate any restrictions, but also provide the procedures for obtaining and installing new software.

It is highly recommended that users do not have the ability to install any new programs that might either expose sensitive company information, waste valuable bandwidth, or corrupt critical data. If users need new software installed for business use, they should contact their manager, the IT/IS department, the Help Desk or the ISO (depending on the procedures set out in the policy) instead of undertaking such action themselves.

Removable Media (CD's, floppies, tapes, etc.)

Removable media such as CD's (Compact Disks), floppies (Floppy Disks) and even tapes (backup/ADR/DAT/DLT tapes) can be defined as another possible entry point for dangerous and malicious files entering the company network or endangering the security of a single workstation. On the other hand, these can also be used to illegally copy sensitive data on, after which it would be easy to walk out of the premises with the stolen information.

Malicious software (viruses/trojans/worms) also use removable media to spread; some take advantage of the auto-run feature of the CD (automatically executing the auto-start file on the CD, which could be a destructive one), others still use "classic" methods like diskettes to get the workstation infected with a malicious program. For best results, removable media devices should be banned entirely (utilising floppy drive-locks, or 'CD-less' workstations; CD's can still be used via CD-Towers, for example). If you need to use removable media in your organisation, then best practises must be established, possible risks and danger scenarios discussed so to reduce malicious programs entering your networks at all points, thus protecting your company from a major disaster.

Encryption

Encryption can be defined as another "must implement" measure that will not only keep your sensitive and critical information secured against a potential attacker, but also protect you from a lot of trouble if eventually a security breach does occur. In your security policy and procedures you must clearly define the systems, files and documents that should be encrypted, by whom, and most importantly, using which algorithms. It is strongly recommended to use proven, industry standard algorithms, such as DES, IDEA, Blowfish, or RC5.

System Backups

Disaster recovery (DR) plans are essential for the continuity of the business as well as the proper functionality of the current processes. Sooner or later you will inevitably face the problem where a system crashes, no matter of the OS used, but this can be dealt with promptly, if proper backup procedures and disaster recovery plans are in place.

You will have to define the assets that must be backed up on a regular basis, the responsible individuals, best practises and procedures, as well as where the backups should be stored, i.e. a fireproof safe, vault, off-site, etc.

Maintenance

The proper maintenance of the PC/workstation is another vital issue that must not be overlooked during the course of the Security Awareness Program. Users' workstations are a significant source of threat to company security, often targeted by the so-called "insiders" snooping around, looking for unprotected workstations. Therefore, you need to educate staff on the aspect of Physical Security as well; again, this can be achieved by running through the possible scenarios, while providing tips for better overall protection.

Incident Handling

By now your staff should be able to define a potential security problem, while you should be establishing the rules for the course of action to take in case of an incident. In your policy you must clearly state what must be done in various situations; the main idea here should be to minimise and limit damage. Staff should be made aware who is responsible for handling problems, and whom they should contact as soon as they suspect a potential security problem.

Internet Threats Explained

One of the greatest security risks in the company is the Internet connectivity, and its misuse through (uneducated) employees. It is a fact that most employees will surf to sites that are strictly prohibited, and most probably will end up downloading malicious files and/or hostile code from hacker sites somehow. Any of these activities could impact the productivity of your company, especially if you think about the recovery process trying to rectify the mistakes made by staff.

Therefore, it is always a good idea to explain in detail the possible dangers of surfing the Internet; that you don't need to download anything at all to get the computer infected with a virus, trojan or even a worm but just visiting the site is enough to cause a problem. Define what constitutes a "prohibited site", and explain why it is prohibited, including the problems that could occur just by visiting it.

Web Browsing

Web browsing represents a threat to the security of the workstation, as well as to the whole organisation. Being exposed to the dangers of web browsing is very easy as hostile scripts could be downloaded, and executed automatically; all it takes for example is an outdated version of the web browser.

Staff should be able to make a distinction between sites that are classified as allowed, prohibited or potentially dangerous, and try avoid visiting prohibited ones. Java and ActiveX should be disabled by default (it will not give problems accessing pages), care must be taken with Flash movies, etc. and if ever a hint of a problem occurs, the ISO office must be contacted immediately.

There are web sites in the wild, that could attempt to scan/flood your network, just by visiting them; another variant to this (theoretical, but very possible) scenario is one of your employees using some kind of scanning service to check the security of his/her workstation, thus wasting valuable bandwidth. Something like this will invariably produce more work for the ISO office as well as their systems probably will register the usage of this service as a possible break-in attempt. Online gambling and pornographic web sites should be fully prohibited, and the web usage of staff monitored to ensure they are following the rules and regulations set forth by the Security Awareness Program.

E-mail Use

Generally the company E-mail systems are a high risk area due to their constant availability to the outside world, and the risk is often two-fold. The use of e-mail to conduct business, contact clients, and its integration in many other business related processes exposes company mail addresses and (mail) systems to potential attackers. On the other hand, this is also the number one entry point from which most of the malicious programs are entering the company. Therefore, a well-known and proven malicious code protection program is a must have on all the mail gateways, as it will detect, block and/or filter out most of the known dangerous files and hostile scripts trying to enter the company networks.

As with all aspects of IT security, company-wide security can only be improved through the proper education of staff. It is therefore highly recommended that you establish Best Practises for E-mail use, concentrating on the points below.

E-mail Use Best Practises

- If (E-mail) attachments are allowed, the attachment(s) must be scanned before opening as well as confirming with the sender (i.e. via phone) that indeed an attachment has been sent. This will also reduce the risk of running a program that has been e-mailed out automatically (unknown to the originator) via some kind of malicious application that has made use of the mail account(s) and/or mailing system of the sender. If attachments are forbidden, follow the policy and do not download/run any file(s) received as attachments;
- Java and ActiveX must be disabled while reading e-mail in order to manage the risk of auto-executing malicious programs. Just like in the internet browser, certain options of the program can usually be set and locked by way of system policies that automatically set these conditions for all users at logon;
- Do not use the company e-mail accounts for registration purposes of any kind, and do not use it while posting messages in web forums or newsgroups. You may want to create one, special (possibly aliased) account for this purpose only;
- Do not use the company e-mail system for running your own business, excessive personal mailing, sending large attachments, thus wasting valuable bandwidth;
- Do not respond to chain letters, or any other sort of spam using the company e-mail systems; if in doubt, contact the ISO office;
- Never forward any company data to external e-mail accounts (i.e. send a work document to your home email account, so to work on it further from home that evening), without first checking with your manager and/or contacting the ISO office;
- The proper use of the E-mail system should continuously be monitored and the users should be aware that they could be held liable for illegal activities, such as spamming, sending and receiving illegal ontent, etc.

Instant Messaging (IM) Applications (ICQ, AOL, MSN, etc.)

A lot of users tend to use these programs in order to communicate with friends, send and receive attachments, messages, etc as these applications often try to trick the content blocking gateway at the server level to letting content pass through. However, they do not fully realise the dangers of these programs, and the potential damages that they could cause.

A snapshot from our previous publication 'The Complete Windows Trojans Paper', available from our web site at http://www.frame4.com/publications/index.php, reviews various scenarios of getting infected with a malicious program via ICQ:

- You can never be 100 percent sure who is on the other side of the computer at that particular moment. It could be someone that hacked your friend's ICQ UIN (Unique Identification Number) and wants to spread some trojans;
- Old versions of ICQ had bugs in the WebServer feature that creates a web site on your computer with your info from the ICQ database. The bug meant that the attacker could have access to EVERY file on your machine ... and you probably realise what could happen if someone has access to your win.ini or some other system file: a trojan installed on your computer in a few minutes;
- Trojan.exe is renamed to Trojan....(150 spaces).txt.exe, the icon changed to a real .txt file; this will definitely get you infected. This bug will most probably be fixed in the newer versions.

No matter the Instant Messaging application you are using, you could always get infected or exploited; through a specific application bug you never heard about or a buggy version you never bothered updating.

When it comes to exchanging information and files no matter where, from whom or how, please be aware that there are certain dangers attached to it; realise the possible dangers of your actions and your naivety, and act accordingly.

Downloading

Downloading any data from unknown and untrustworthy sources while using company systems and networks could have a devastating effect on the business processes; you could face a situation of having your data lost, corrupted, or, in certain cases, modified. You should therefore aim to educate staff on the procedures of downloading information in a safe manner; this consists of ensuring downloadingf files only when it is absolutely necessary, scanning of the downloaded files with the corporate Anti-Virus/Anti-Trojan solution before opening it, etc.

For your convenience we have created a summarised "Internet Use Best Practises" section below; again, far from being an exhaustive list, it is aimed at giving you some basic pointers on safe Internet use.

Internet Use Best Practises

- Java and ActiveX are blocked by default. Scripts containing Java and ActiveX pose a great danger due to their insecure nature, and the resulting problems could have devastating effects on your computer, not to mention the company. Please do not block, stop or tamper with any measure (i.e. group policy) that is in place to filter out these and if you are having problems purchasing an item or visiting a trusted web site, contact the IT department, Help Desk or the ISO office for assistance;
- Do not visit inappropriate web sites with objectionable content; pornography, gambling, warez (pirated software), hacker/hacking sites, as well as those generally considered as prohibited by your security policy;
- If the use of Instant Messaging (IM) applications is allowed, do not accept any attachments no matter of the file type, extension, or originator;
- Downloading software, files or anything else is prohibited. If you need any applications for your day-to-day business, contact either the IT department, the Help Desk or the ISO office. You will more than likely need to hand in a (software) request form signed by your manager to complete the process. If you do get clearance to download a piece of software, remember to never execute it before scanning them with the corporate Anti-Virus/Anti-Trojan software;
- All internet activity should continuously be monitored and the users should be aware that they could be held liable for visiting prohibited web sites, downloading illegal files and content, as well as face a penalty of having their access to the Internet limited (until they can prove that they are fully aware of the risks created by their actions).

15. Innovative, Yet Effective Educational Methods

We have now come to understand that security can only be improved upon through the proper education of staff. However, the level of success can always be improved upon by varying the methods of education; by ensuring that you have a fresh, ever-evolving and to a certain extent, dynamic education program you will attract continued interest to your educative sessions. By keeping people continuously interested and manage to reach a large number of people you will definitely have your audience waiting impatiently for the next meeting.

Below I will review various methods, which I found to be highly successful ones and I am sure you will agree after implementing/evaluating their effectiveness.

Security Newsletter

An interesting and valuable way to reach and educate your staff is undoubtedly by way of a Security Newsletter sent via e-mail. You could also give staff the additional option of having the newsletter sent to their private (home) e-mail address as well, so even if they do not have the time to read it at work, they will have the opportunity to do so later, from home.

The main idea behind the creation of a security newsletter is to provide users with an interesting, and engaging way of understanding the points outlined in the security policy. In order to illustrate the idea more clearly, we have created a sample 'Security Newsletter' for you:

Sample Security Newsletter

<Company Name> Security Newsletter
Issue 1 - MM.DD.YYYY
http://company.com/security/
email: security@company.com
phone: 123-456-789
987-654-321 Ext. 000

01.Upcoming Events
02.Security Article
03.What is...?
04.Ask us
05.Security Resources
06.Contacts

1 - Upcoming Events

This section contains information about upcoming meetings, discussions, lecture sessions and everything regarding any forthcoming Security Awareness Program activities.

2 -Security Article

It is a good idea to provide your staff with detailed, in-depth information on a specific topic via the newsletter, thus helping them understand the subject more clearly. Let us assume that on the last Security Awareness meeting you have discussed the 'E-mail Threats' topic, so, in order to get maximum benefit out of the meeting it would be a good idea to include an article regarding this subject right after the last awareness session when everything that they have covered is still fresh in their memory.

Do not make the mistake of including a completely irrelevant article to the last security awareness meeting as this will definitely confuse staff or in the worst case scenario, turn them off the subject completely. Keep the articles brief and easy to understand; there is no need to write a complete essay on the topic, the idea here is to provide them with a dynamic way of education, as well as another informal, but precise and well summarised recap of the topics from the last meeting.

Articles that you might consider including are:

- Password Security: Discussing the importance of passwords and their crucial role in the protection of the company data, how to properly maintain User IDs and passwords, password creation and maintenance, best practises, etc.;
- Acceptable Internet Use: Discussing the possible dangers posed by Internet connectivity and things staff should be aware of while (securely) browsing the web, how to use the E-mail system in a proper manner, thus reducing the risk of spreading malicious code around the world, and in this case, around the company network;
- Why are they targeting us? An interesting topic, discussing the motivation of different attackers, which is usually highly interesting reading for everyone, providing users with a better understanding of the importance of having proper information security measures implemented within the company;
- Your role in the protection of the company: You are free to think of as many scenarios as you see fit; the idea behind these articles is to explain the most important aspects of information security in an informal yet effective way and covering social aspects combined with brief technical explanations if needed.

3 - What is...?

This section should be created with the idea of educating or informing staff, to act as an information security (IS) glossary, where various security terms are explained in a non-technical, easy to understand way.

Consider adding up to three terms in each issue, relating to the topics and articles discussed on the last (security awareness) meeting and keep them very short but yet highly informational. General security topics such as "What is a Trojan", or "What is a Worm", and "What is a Firewall" can be included, as well as many others that you define as useful and 'must-know' articles.

4 - Ask us

When it comes to educating and training users by way of a Security Newsletter, I consider this section to be the most effective and valuable one; it provides a direct and informal way of communication between the Information Security Office (ISO) and staff who in turn get the opportunity to direct their security related questions to an ISO representative.

The questions and the corresponding answers should then be included in the next issue of the newsletter, so that it will not only be a collective information source to a large group of people, but also to stimulate the asking of further questions.

To give an example:

Question: Sometimes I find myself in situations that have not been discussed in any of the Security Awareness presentations or mentioned specifically in the security policy. Following the policy I contact the IT, or the security department on what to do next, but I am worried that I might be contacting them with irrelevant or stupid questions. I do not want to bother them constantly with my problems. What should I do, and how should I proceed?

Answer: The Information Security Office (ISO) has the duty to respond to each and every e-mail concerning company security, as well as handling correspondence regarding potential security problems, etc. Their function is not only to maintain an acceptable level of company security but also to train, educate, and support users. Whether there is an incident, a problem or something you are not sure about, you are urged to call the ISO office on 123-456-789 for urgent matters, or in the case of non-urgency, drop us a line using our e-mail address, security@company.com. Remember not to do act on something you are not 100% sure about, and remember that there is no such thing as "bothering" when it comes to securing the information assets of the company.

Include up to three questions and answers in each issue; this will help a lot of people, as well as help you to analyse the effectiveness of the security policy. Gauging from the questions asked, you will be able to ascertain if something is missing or not quite right, or on the other hand it may also mean that you have got them interested and motivated them to learn and ask more questions.

5 - Security Resources

This section might consist of one or two short pieces of news covering an aspect of information security in an easy to understand manner. The idea is to help the users understand the importance of the general process called Security Awareness Training they are getting, via security news, news of latest security breaches, losses suffered by companies due to security problems, etc.

Another valuable resource you might want to include are links to external sites targeting people new to the subject (often referred to as newbies or neophytes) and well-known security forums moderated by respected security experts.

Before linking to any site, you must fully review its contents and estimate how useful (if at all) its contents would be to users wanting to get information from external sources.

6 - Contacts

Make sure to include the contact details of the ISO office at the beginning and the end of each issue so that users will know precisely whom to contact in case of a problem.

> Information Security Office Contacts:
>
> http://company.com/security/
> email: security@company.com
> phone: 123-456-789
> 987-654-321 Ext. 000

Recommendations for the Security Newsletter

This section will aim to provide you with some recommendations for the security newsletter, to help you with various topics from a successful implementation to improving its overall effectiveness.

First of all, you should archive all previous issues of the security newsletter on the company intranet so that staff will be able to get to all of the issues; you may also consider placing the archive on the external web site, but this of course depends on how sensitive the published information is to the outside.

Publish the security newsletter either weekly or twice a month depending on the frequency of Security Awareness sessions. Keep the articles short and brief and try not to give too much technical information; the key rule here is to inform and to educate, not to overload them with excess information.

Advertise; if people do not know about the existence of the newsletter, or they do not know or care about its importance, they will not read it. Broadcast the existence of the newsletter in your awareness sessions, tag information about it onto other emails, mention it in posters, incorporate it in other internal programs and campaigns within the company, advertise on the company intranet.

Always involve people; the more people feel involved or feel that they can contribute, the more interest and passion they will have in the subject. This will also help "spread the news" among staff, which may also drum up additional interest.

Ask for feedback, so that you can monitor how things are going. As mentioned earlier, this will not only help you revise the contents of the newsletter if and when necessary, but also help you gauge overall success.

Information Security Web Site

It is recommended that an Information Security Web Site is created, to act as a central starting point for everyone interested in IT security. If successfully implemented, this venture will also create a community feeling in the long run, which is an invaluable asset for company security in general.

At this stage you must decide if this web site is to be a completely separate, independent site or a sub-set or addition to an existing company intranet. In some extreme cases you may also want to consider creating two separate sites; an internal site, for staff (and accessible from the company network) only and an external site, accessible to everyone around the world, as well as by staff, for example while browsing the Internet from home. There are of course various different options and points to think over here, such as do you want it to be accessible to everyone or do you want to password protect it and/or put it on a specific server port, can the contents of the external site (extranet) be seen by or published to the outside world, maintenance of systems and content, etc. so I would recommend it to keep things as simple as possible.

The site must be clear, easy to browse, and easy to navigate; do not overload it with thousands of files and technical papers, most of which probably contain words not known to staff members. Provide them with

specific articles written by the ISO office on the most common security problems that they might face while using company systems and handling sensitive data, teach them how to identify problems, report and handle incidents. Provide them with interesting and comprehensive FAQ's (Frequently Asked Questions) on specific topics; if you cannot find suitable content for your needs, write new ones and distribute them among staff using the security web site as a distribution medium.

We have included some links to external web sites where you will be able to see several examples that will hopefully save you a considerable amount of time and research.

The 'We need YOU' Technique

This is a must-use technique, as far as changing the employees attitude towards their role in company security is concerned. Basically it provides all involved with the opportunity to actively contribute to the educational process with his or her very own advice, ideas, personal experiences, recommendations, etc.; and if the contribution(s) are good enough the employee will get the opportunity to present the topic personally at one of the lectures or discussions.

This method will motivate more or less everyone to participate in the security awareness program, while on the other hand creating a friendlier, more informal atmosphere. Having a fellow staff member addressing them with their views will significantly reduce the stress and formality of the educational process.

Everyone is free to send in suggestions and recommendations to the program as this engages staff actively in the process and will help in changing their mode of thinking. They will not see security education merely as an obligation just because they are on the payroll, but an active issue concerning the good of the whole institution. As an added bonus they will also learn how to protect their own personal PC's at home and pick up valuable tips and tricks on the way.

Educational Contests

Conducting various security related contests from time to time not only helps measuring the security awareness level of staff, but also varies and innovates the educational process.

Password cracking contests are a good example; they contestants are faced with the challenge of cracking a file that has been protected by a password chosen by a fellow contestant, with the idea of finding/eradicating weak passwords. Upon conclusion of the contest a discussion is started on how the password was cracked, what makes it a weak password (if that was the case), etc. Most staff are usually interested in such activities, and most of them will do their best to use hard to crack passwords following the recommendations on the process of creating strong passwords from the Security Awareness Course.

16. Management Summary

This section has been created mainly with the idea of answering the most common questions a manager could ask as far as Information Security is concerned. Its purpose is to explain in a brief, yet effective way why from a management point of view one would want to invest in securing the core Information Assets of the company, and the potential risks attached to cutting the Information Security budget.

A lot of businesses (still) tend to ask the question why they should invest in information security, as sensitive data is backed up every day and in the event of an intrusion, virus outbreak or data corruption, data and business processes can be restored and brought back up in a matter of minutes.

Whereas theoretically there is nothing wrong with this mode of thinking and the procedures that are in place do provide a certain degree of security, practice has shown time and time over again that the "classic" security methods such as virus scanner/backup/restore may not be enough to 'hold the fort'. People still fail to realise

that their Internet connectivity represents a big threat to the whole world if it is not properly secured; that there are hybrid code out there that will not only take out your network(s) and trash your data, but will also steal documents, passwords, etc; and that there are people out there that will try to enter your systems for whatever reason and damage your systems.

A successful intrusion with the idea of purposefully causing damage to business could damage the image of the company and the brand name to no end. It may take minutes to recover your corrupted files, but it may take years to clear a name, or image.

A simple defacement of the company web site will show the world how insecure it (and, subsequently your in-house systems) is/was, that proper security measures were not in place, and if it concerns an online shop, most of your clients will be afraid to use it anymore. Or imagine your company networks contributing to a worldwide, full-scale Distributed Denial Of Service (DDoS) attack, which will definitely get you in trouble and/or damage your reputation a lot. Just imagine being in a situation where your company systems are unknowingly attacking other businesses online, or successful penetrations in other companies are performed, using your networks!

Another common management mistake is plain and simple, smugness. How many times have you heard phrases like : "we have recently purchased a well known firewall product to protect our company network", "we have server level content blocking software as well", "our administrator is a certified security professional", or "we think we are pretty dam secure, so why should we invest in further security measures?".

Security is a never ending process that requires constant monitoring, updates, investment, research and implementation of new technologies; not forgetting the most important point: education of staff. Because no matter the amount of money you are prepared to spend, and no matter the technologies involved, the secret lies within the individual who configures your security system(s).

Internet can be a very beneficial resource to your business, however it brings certain risks with it. For the best possible results you will probably need to employ full-time specialists taking care of your (IT) security, thus ensuring you are capitalising the benefits of the Internet, while having your critical data reasonably secured.

It is to hope that by now any company manager has enough background information to be able to ask the right questions to their security products vendor, or the security consulting company building and developing their security solutions. I cannot stress enough, on the other hand, the importance of getting your company executives familiarised with all the risks posed by their Internet connectivity and other (IT) security issues; the clearer top company executives and decision makers are on the whole situation from a security point of view, the sooner and quicker an effective IT security policy/strategy will be in place!

17. Resources

Information Security Policy Papers

URL : http://www.sans.org/rr/policy
DESC : Sans Institute Security Policy Papers

URL : http://www.secinf.net/policy_and_standards/
DESC : Secinf's Policies Directory

URL : http://packetstormsecurity.org/docs/infosec/policies/
DESC : Packetstorm's Security Policies Directory

URL : http://directory.google.com/Top/Computers/Security/Policy/
DESC : Google's Security Policies Directory

URL : http://www.ietf.org/rfc/rfc2196.txt?Number=2196
DESC : Site Security Handbook

URL : http://www.utoronto.ca/security/policies.html
DESC : University of Toronto

URL : http://irm.cit.nih.gov/security/sec_policy.html
DESC : Security Policies

URL : http://www.ruskwig.com/security_policies.htm
DESC : Security Policies

URL : http://www.iwar.org.uk/comsec/resources/canada-ia/infosecawareness.htm
DESC : A comprehensive paper on the building processes of a Security Policy

URL : http://www.sun.com/software/white-papers/wp-security-devsecpolicy/
DESC : How to build a Security Policy

URL : http://www.boran.com/security/detail_toc.html
DESC : IT Security Cookbook

URL : http://eleccomm.ieee.org/email-policy.shtml
DESC : E-mail Security Policy

URL : http://www.giac.org/practical/Kerry_McConnell_GSEC.doc
DESC : How to develop Security Policies

URL : http://www.giac.org/practical/Caroline_Reyes_GSEC.doc
DESC : What makes a good Security Policy

URL : http://www.giac.org/practical/jack_albright_gsec.doc
DESC : The basics of an IT Security Policy

ISO Web Sites

http://security.vt.edu/
http://security.isu.edu/
http://www.itso.iu.edu/
http://www.ox.ac.uk/it/compsecurity/
http://www.columbia.edu/acis/security/

18. Conclusion

The aim of this paper is to explore the process of building and implementing an successful Information Security Policy in detail, as well as giving various recommendations for the development of a Security Awareness Course.

The security within any organisation starts with building a Security Policy, a centralised, evolving document defining what is allowed and what is not. Along with what I hope to be large amounts of useful information, I have provided you with some ready-made "Best Practises" sections on various security threats, as well as a sample Security Newsletter in order to save you valuable time and resources. The implementation process requires constant monitoring of Internet Threats, along with the measurement of staff knowledge and awareness levels to ensure that there is a continuous improvement in their level of knowledge and security awareness.

If you have any further questions, suggestions or recommendations please direct them to me via email at dancho.danchev@windowsecurity.com.

Part of the Frame4 Security Systems Publications Archive, this paper can be located at http://www.frame4.com/publications/index.php. Please visit the archive to get the latest updates to this paper and many other security related documents.