

*Special Report:*

## **Computer Security**



### **Basic Security Awareness for Your Business Computer Network:**

As you probably are aware you will indeed encounter new security issues when linking a computer to other computers. The following information is tailored to heighten your awareness concerning network security in the work place perspective.

- Recognizing security concerns outside and internally to the company.
- Understand the need to develop a detailed security policy before setting up a security system.
- Identify details that should be covered in a security policy.
- Identify security features that are built both into the software and hardware of your company's network.
- List several ways to allow and restrict access permission using the built-in features.

Network security "is" the whole system of hardware, software, and of course the procedures that most importantly protect your data, hardware devices, and network software. Here are a few questions to ask yourself:

- What are the threats to your network?
  - a) Threats from within Employee carelessness
  - b) Employees with bad intention
  - c) Temptation and Distractions
  - d) Strangers in the building
  - e) Attacks from outside unauthorized Dial-in
  - f) Misuse of a Wide Area Network – (WAN Access)
  - g) Internet Access

*Special Report:*

## **Computer Security**



### **Basic Security Awareness for Your Business Computer Network:**

- What kind of protection is available for a network?
  - a) A security policy
  - b) Simply obvious precautions
  - c) Options in your networks hardware and software components
  - d) Firewalls
  
- What kind of protection do you need for "your" network?

Assessing the right amount of security for your network might take some time and consideration.

- a) What is your data worth?
- b) Are you connected to the Internet?
- c) Do you use an email server in house? ( MS Exchange server )
- d) Do employees have the ability to connect to the company network remotely?
- e) What kind of resources "ARE" available over the network?

A business can do several things to insure that security is routine. They can:

- Limit access to the building or office area
- Insist that employees follow certain rules for virus protection and passwords
- Develop and implement a security policy ( essential )
- Use security options that are available in software applications and network routers

Ok, what is a Security Policy?

A security policy is the document that outlines your company's security needs and procedures. It identifies what you need to protect and assigns priority to the items. Without a policy you may run the risk of protecting unimportant data while leaving the really important data exposed.

*Special Report:*

## **Computer Security**



### **Basic Security Awareness for Your Business Computer Network:**

This next section will be brief but most certainly is the most important element, "creating a security policy." You will need to take the time to consider the unique security needs of your business "the kind of sensitive data you have." You might have data that requires extreme precautions. Other data might only require reasonable degree of caution.

Here are a few main steps in formulating the security policy.

- Assess Risk
- Determine vulnerability
- Analyze budget
- Write the security policy
- Implement the security policy
- Continually audit security

Here are a few additional questions you may ask yourself in writing the security policy:

- Do I have proprietary information that gives you a competitive edge in the market?
- Do I have client information that my company is legally bound to protect?
- Employee information
- Critical business records
- Payroll data

The security policy also helps you justify the cost of security.

The cost may or may not be high but will undoubtedly be worth it.

We hope this article was informative and makes you aware of some security issues that are evident in the workplace.