

# Security in a technological world

## Overview

Most companies have been compelled to adopt at least some technology in order to conduct business on a day to day basis. With this adoption, there comes the risk of the technology being used in a way that is detrimental to the company that has implemented it. It is possible to combat these threats with the proper expertise and safeguards in place.

This article will discuss the different areas of risk that exist and general strategies for minimizing their impact. Along the way we will assign a number to each area that indicates the approximate percentage of total risk. Keep in mind that focusing solely on a few high risk areas is not a valid approach. All areas must be addressed in order to provide a solid security strategy.



## The Reality of Security

Given enough time and enough resources it is possible to circumvent ANY safeguards that are put in place. Hence, it is not possible to eliminate ALL security risks when dealing with technology. The challenge of technology security is to eliminate as much risk as possible given the amount of resources that a business is willing to commit.

This may sound pretty bleak but, there is some good news. Using the resources that are available today, it is within the reach of most companies to get to an acceptable level of risk. The general idea is to eliminate the casual or opportunistic risks which actually account for a large percentage of security failures. The type of business being conducted and the level of dependency on technology are the largest factors in determining the risk tolerance and the level resources that should be allocated to eliminate risk. (i.e. A bank needs to allocate more resources than a flower shop)

## The Proactive

The following areas provide ways to eliminate threats before contamination has occurred.

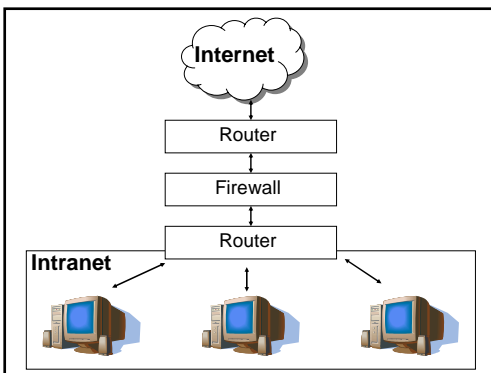
### **End-User education (35%)**

A large portion of your overall risk is determined by the behavior of your end-user community. By browsing to fringe sites, answering pop-up ads, opening malicious E-Mail attachments, etc..., end-users can circumvent even the most secure environments. The good news is you can take a proactive approach to eliminate a large portion of this risk by educating the end-users to understand they are an important piece in your security strategy.

Some businesses take the approach that network access is a privilege that must be earned by completing security training. Then on-line behavior is monitored and reviewed to ensure compliance. This may sound extreme but, as our percentages show, this one area can have the greatest impact on the success or failure of your security strategy.

### **Protect the Internet connection (20%)**

Any machine or device that is connected directly to the internet can potentially become compromised and hence allow partial or total access to your internal network. It is important to limit the type of traffic that can pass through in either direction. The



more restrictive this traffic blocking is, the fewer the number of potential vulnerabilities you are showing to the world. Be warned, it is possible to restrict the traffic flow to the point where access to the internet is no longer of value. A balance between the level of security and the usability of the connection must be established.

In recent years what these devices are called and what services they offer has become vague as the vendors have tried to put everything in one box. A Router determines when a machine on one network (the Intranet) desires access to another network (the Internet) and routes the traffic appropriately. A Firewall provides a barrier between two networks by limiting the types of network traffic that can pass through.

## The Reactive

The following areas do not eliminate risk, they control the total impact and possibly clean affected systems. These areas should be addressed so known threats do not compromise your systems.

### **Get those application updates (20%)**

The more complex a piece of software, the more likely it will have vulnerabilities that can be exploited. As a result, most security threats are related to software we use everyday to run our businesses. This is especially true when dealing with software that provides network connectivity or services. (i.e. Operating Systems, Browsers, FTP, Web Servers, etc...) Once a vulnerability is discovered, the software manufacturer will usually develop a fix to eliminate the issue. Ensuring the latest updates are in place, on a regular basis, is paramount in a complete security strategy.

A word of warning, updates of this type need to be considered very carefully. Since these systems are typically mission critical, the impact on their operational stability needs to be considered carefully.



### **Scan E-mail before it gets delivered (10%)**

The exponential growth of global E-mail usage has created an excellent avenue for the spread of malicious content. By using E-mail as the transport mechanism it is possible to get inside of an intranet and bypass most of the security precautions that have been put in place. The typical name for intrusions by E-mail is a Trojan. As the name implies, a Trojan usually comes embedded in something that does not seem like a risk and requires some type of interaction in order to activate it. Once activated the Trojan has virtually unlimited access to spread throughout your internal network.

Having all E-mail's examined for Trojans before it gets activated is critical in reducing this threat. Most E-mail providers and E-mail server software has the capability to perform this examination with no interaction, there by catching most threats before they become active.

## **Summary**

We live in a world where threats to our technology infrastructure are substantial. In order to minimize this risk, we must take an active role in ensuring we can cope with the threats that are present. Unfortunately, we have learned that for the most part we are in a reactionary mode when it comes to dealing with these threats. This means security must be important to every employee in order to minimize the greatest amount of risk. A comprehensive security strategy must address all the areas we have discussed and, possibly more areas that are specific to your business.

### **Scan for Viruses/Worms widely and often (10%)**

One of the most insidious and difficult to defend against intrusions come in the form of viruses or worms. A virus/worm is a program that utilizes a security hole in order to propagate and potentially perform malicious acts. Since they are predicated on a known security issue it is important to have a well rounded security strategy in order to minimize, if not eliminate a threat.

It is important to understand that you may not know if you are infected with a virus/worm. Some may activate on a certain date, collect information and send it back to the author, others may make your systems more susceptible to other intrusions. Just because your systems seem normal, does not mean they have not been compromised.

Scanning software looks for indications that a system has been compromised by a particular virus/worm. These indications vary based on the virus/worm being searched for and are contained in a file that can be updated by the scanning software vendor to include the latest threats. Having updated scanning software widely disbursed through out your infrastructure can help minimize the impact.

### **Let's not forget about Spy-ware (5%)**

Spy-ware is software that collects information about your computer and sends it to the originator. This can be anything from detailed information about your computer, to all of the keystrokes over a period of time. Usually this software does not damage your system directly but, it can provide the originator with information that can be used to later to compromise your system. Spy-ware is commonly used by unscrupulous vendors and advertisers to track your activity and sell that information for targeted marketing purposes.

Using the web to browse fringe sites and answering pop-up ads is the primary avenue for contamination. There are programs available that will scan for Spy-ware, and similar to Virus protection, you must keep them updated in order for them to be fully effective.