# NETWORK SECURITY REVIEW

## THE REALITIES OF DATA NETWORKS AND SECURITY

- **Security is a process, not a solution.** You will never reach a point when you can say, "We are totally secure." New attacks and intrusions are devised every day. Your security needs today will differ from your security needs tomorrow. Security measures must be adjusted in order to address and combat new threats.
- **Security is not a single barrier, but a series of layers**. Because you want to limit access to critical resources, a layered approach to securing those resources is necessary. One deterrent may stop a few people, but the majority will try to find a way around it. Employing several deterrents creates more difficulty for people trying to access resources that they're not explicitly allowed to.
- **Given enough time and resources, any secured resource can be exploited**. This reality brings you to the cost of securing the resource as opposed to the cost of losing it. Remember, cost can mean many things: man hours, replacement time, physical assets, reputation, and so on.
- **Someone needs to be watching for security breaches.** Security will do nothing if it is not monitored properly. If no one is checking to see if the security measures are working, you will never know if you have been attacked
- **You must understand what you are securing and who you are securing it from.** If you don't know what you are trying to protect, how can you place a value on it and justify the cost of securing it? Equally, if you don't know who you are protecting it from, how will you determine who has legitimate access?

## WHAT IS SECURITY?

Security is being free from risk of loss. Security is also the measures taken to guard against espionage or sabotage, crime, attack, or escape.

When looking at data networks, these definitions of security hold true. Preventing unauthorized access to business-critical applications, data, and resources is imperative. But security comes with a price. The trick is balancing the cost of providing the security with the cost of recovery if a threat were to strike.

The only way to be completely free from the risk of loss in a data network is to never connect a machine that contains critical data to any other machine – essentially, keep it as a stand-alone. In today's world of anytime/anywhere access, this obviously isn't possible. Typically, critical data must be accessed by more than one person, so the best option is to allow access to those who are authorized and deny access to those who are not.

There is a delicate balance to security, and it is different in each case. Those who make decisions about security — whether it is the technical staff, the management team, or the CEO — must understand these concepts in order to provide the protection and security desired.

**Trusted Network Solutions can help you with this process.**

.

## THE TNS PROPOSAL

Trusted Network Solutions can assist you by performing a **Network Security Review**. We begin the process of securing your network by:

- Reviewing "acceptable use policies"
- Analyzing the network architecture
- Validating firewall rules
- Verifying users and groups
- Performing vulnerability assessments
- Identifying network access points
- Providing documentation about findings

Contact a TNS account executive for a proposal customized to fit your business needs.

TRUSTED NETWORK SOLUTIONS

406 Lawndale Drive
Salt Lake City, Utah 84115

Office: 801-484-4500
Fax: 801-484-4525

www.TrustedNetworkSolutions.com