# *Seven Good Network Security Rules*

*Note: This note was pieced together from several articles found in computer trade press magazines by Thomas Jerry Scott. It is intended to provide a good background to begin working toward better security at your worksite.*

To meet the challenges of computer and network security, it's crucial to adopt ground rules. Once they're in hand, the rest is easy.

1. ***Security and complexity are often inversely proportional.***

   Every step taken--whether it's vulnerability and risk assessment, security policy and procedure development, deployment of mechanisms or user education--should be as straightforward and simple as possible. The more cryptic the instructions and procedures, the more room for misunderstanding and misapplication.

2. ***Security and usability are often inversely proportional.***

   There is no such thing as "complete security" in a usable system. Consequently, it's important to concentrate on reducing risk, but not waste resources trying to eliminate it completely. Such a pragmatic mind-set provides a fighting chance to achieve fairly good security while still allowing productivity.

3. ***Good security now is better than perfect security never.***

   This is a corollary of the previous axiom, since perfect security doesn't exist in a usable system. Even if it were possible, a usable system is a moving target: Threats change, technologies change and business needs change. The job is never done.

   This knowledge should actually free you to shoot for "good enough." Come up with 10 things to do, but only get to four of them now, and you're probably in a better position than if you wait until it's possible to do all 10. The key is to prioritize correctly.

4. ***A false sense of security is worse than a true sense of insecurity.***

   Knowing where your enterprise is still insecure provides you with the framework for moving ahead. It's critical to know where you've left gaps, what documents and procedures are not quite right and what mechanisms need replacing.

A false sense of security does not motivate improvement--or even analysis--of an organization's security posture. It leads to false complacency, which can give rise to disaster, often accompanied by the lament, "I thought we had that covered." It's better to know where you are weak and avoid unquantifiable risks.

5. ***Your security is only as strong as your weakest link.***

   Therefore, be thorough in examinations and evaluations. For example, if there's a reason to employ VPNs (virtual private networks) to keep connections from home and remote offices to headquarters private, it may be necessary to protect that data while it resides on the notebook PCs of your mobile workforce. It may mean removing modems from desktop computers, requiring all traffic to flow through the firewall.

6. ***It is best to concentrate on known, probable threats.***

   There are imagined threats, real threats and probable threats. And there are known and unknown threats. We are most interested in real and probable threats, while we continue to expand the set of known threats.

7. ***Security is an investment, not an expense.***

   The challenge is to get this point across to upper management. Investing in computer and network security measures that meet changing business requirements and risks makes it possible to satisfy changing business requirements without hurting the business' viability. Properly secured servers let corporate information be shared with salespeople in the field and with business partners. Improperly configured systems lead to data loss or worse.

## *Conclusions*

Although it's comforting when an attack is put off, it is much better never to have to put security measures to an actual "battlefield" test. As with airbags in an automobile, it's important that they're there, but better never to have to use them. With these ground rules in mind, it's time to do the most important work in securing networks and computers: security management. Keeping the Seven Maxims in mind should help you streamline the process.