



Convenience Vs. Security

© René Mente - September 23, 2000

What A Convenient World

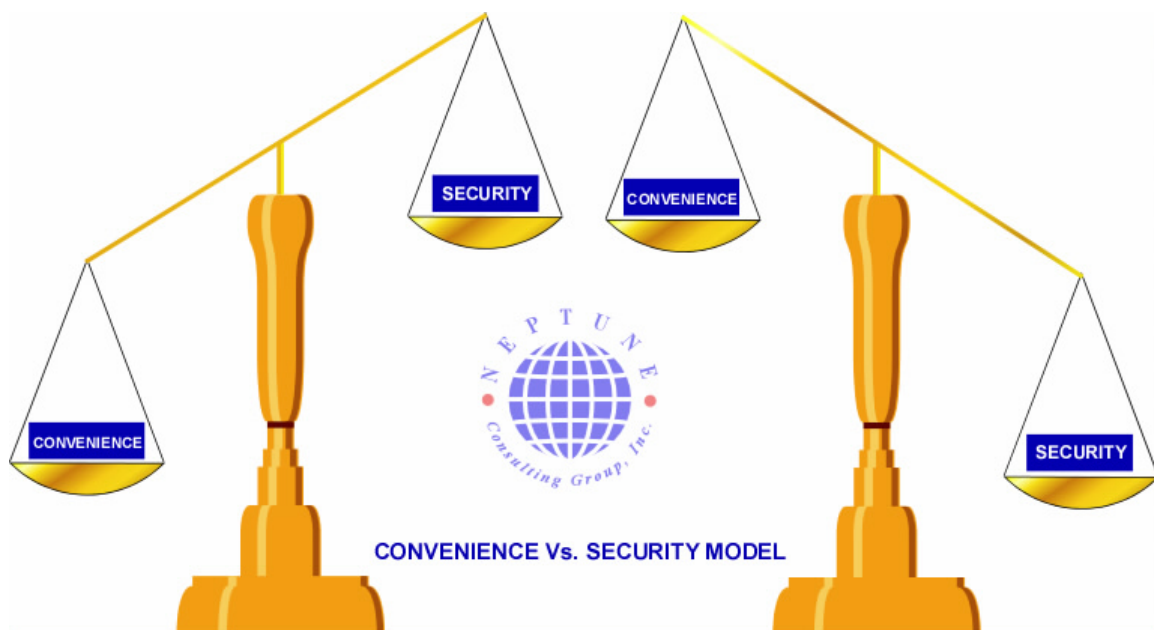
In this world of high technology and instant communications, we have come to expect each new innovation to make our lives more convenient than ever before. We demand immediate gratification in just about every aspect of our daily endeavors:

- ❑ Microwave ovens to cook our meals in a couple of minutes.
- ❑ FAX machines to transmit correspondence immediately.
- ❑ Scramjets to transport us from continent to continent in a couple of hours.
- ❑ Video-on-demand services to fulfill our desires for instant storytelling.
- ❑ Cell phones with cameras so we can share vacation pictures in real-time.
- ❑ E-commerce websites so we can shop from the comfort of our armchairs.
- ❑ And, of course, computers that enable us to be more productive than ever.

The one thing that these technologies have in common is that they are all made possible by electronics, and more specifically, computers. In fact, computers are used to design, test, and build the electronics that make these technologies possible. Computer Aided Design software is used to design the next electronic innovation; computer simulators are used to test the electronics before they get assembled, and computer-controlled robotics are used to assemble and build the next electronic invention. Can it get any more convenient than that?

Comparing Convenience and Security

We strive to make life's trials and tribulations as convenient as possible. However, making things convenient for ourselves isn't always the most secure thing that we can do. In fact, convenience is often times inversely proportional to safety and security. Imagine **convenience** as one element on a balancing scale, and **security** on the opposite side of the scale:



According to the Convenience vs. Security model above, the more convenient we tend to make things, the less secure they are; conversely, the more secure we make things, the more inconvenient it becomes.

This paradigm holds just as true in real life as it does in the computer/network security world.

Let's consider your home, for example. It would be very convenient to leave and re-enter the house if you left the front and back doors unlocked, and left the doors open all the time. However, if you leave the house to go to work in the morning with the doors wide open and unlocked, it would not be very secure.

On the other hand, you could lock all the doors, lock all the dead-bolts, set the security alarm system, and have Doberman pinchers leashed to the front and back porch. It wouldn't get any more secure than this scenario; however, it's not very convenient when you're coming back from the store with two bags of groceries in each arm.

This same simple model can be applied the world of computers and networks. Software vendors (like Microsoft, for example) make their software very easy to install, and even easier for the average computer user to start using their applications. However, in the interest of sales, sometimes they make their software a little too easy to install and use.

We can't all be network security experts. If everybody was an expert in this field, then companies like Neptune Consulting Group, Inc. wouldn't exist. We aren't suggesting that everybody should be a computer security expert before they start using computers or access the Internet; however, we are trying to make computer users and businesses aware that there are some very dangerous security risks simply by installing an operating system, leaving it in its default *wide-open* (a.k.a. – "convenient") settings, and then connecting to the Internet.

People store quite a bit of personal information on their PCs, and businesses store most of their corporate data on their servers and computers. Since this information tends to be quite valuable to their owners, and sometimes even more valuable to people with less-than-honorable intentions, there should be adequate security measures in place to protect the data stored on personal computers and corporate servers.


Common Sense to the Rescue

You don't need to be a security specialist to realize that locking the front and back door to your house is a good idea before going to work in the morning. And you don't need to be a computer genius in order to secure your workstations, servers or network. As in both cases, all you really need is a little common sense.

- Don't connect Microsoft computers directly to the Internet. Use a firewall.
- Make frequent backups of your personal and/or corporate data.
- Keep workstations and/or servers current with the latest security patches.
- Keep your personal information (such as banking passwords) private.
- Have some sort of disaster recovery plan, just in case the worst happens.

In Conclusion

Use some common sense when managing your personal or corporate data. If additional expertise is required, outsource whatever specialized functions you need to companies like Neptune Consulting Group, Inc.


René Mente
President / CEO
Neptune Consulting Group, Inc.
