Rethinking Network Security – A Three-Front War

By Dr. Fred Chang
President and CEO, SBC Technology Resources

As our nation's dependence on computing and networking technologies has skyrocketed, so too has the accessibility of our most valuable, often confidential information. Intercepting and eliminating the threat of computer-related crimes has become a top priority among leaders in the public and private sector.

So far, we've been largely unsuccessful. And it's time we explored a different approach to securing the resources that are our livelihood.

We've made great progress in equipping enterprise networks with antivirus software, firewalls, virtual private networks and advanced data encryption. Unfortunately, all of these security products have one thing in common. As useful and necessary as each may be, not one of them (or all of them combined, for that matter) constitute a total security solution.

The research tells an unsettling story. According to CERT, a major reporting center for Internet security problems, the number of newly discovered vulnerabilities reported to CERT continues to more than double each year. And, not surprisingly, the number of reported security breaches increases at nearly the same rate.

At any given time, a growing army of technically gifted delinquents is combing the reaches of cyberspace, systematically searching for weaknesses to exploit. Often the intrusions amount to minimally disruptive, albeit illegal, pranks. Other times, the criminal intent is of the worst kind, threatening the reputation and financial stability of our businesses, the privacy of our citizens, and the security of our nation.

A significant improvement in the performance of information security systems will require an evolutionary step in research and product development. The impetus will be a change of perspective.

Our view of network security, has, to this point, been somewhat narrow-minded. Currently, most security plans exist in isolation, focusing primarily on the end user or the enterprise. For example, the individual user typically approaches his computer security needs by utilizing passwords and anti-virus software on the desktop. On a larger scale, enterprises incorporate a security arsenal of cryptography, encryption, firewalls, intrusion detection and virus scanning.

Why isn't it working? Because these plans focus on protecting the figurative "neighborhoods" of the network, but can't patrol the larger information highway on which data travels. When it comes to network security, we've been locking our doors and windows, but there's no police on the streets.

It's time to start identifying and catching the criminals at large *before* they come breaking down our doors. This means viewing and protecting the network as a whole, starting at its core.

The new war of network security will be fought and won on three fronts: at the desk of the end user, at the gates of the enterprise, and soon, at the central hub of the communications network.

The burden of responsibility for securing the latter falls, in great part, on the providers of communications infrastructure – telecom carriers. The industry must invest in the development and adoption of new technologies to proactively monitor and weed out would-be cyber-criminals, policing the highways and byways of the information world.

But it can't stop there. Even the most innovative ideas will prove inadequate if created in a vacuum. Now, more than ever, government and the private sector need to work together to share information and resources toward developing comprehensive, integrated security solutions. In this case especially, the product of collaboration can truly be greater than the sum of its parts.

The Internet revolution has brought about extraordinary changes in our lives, and will continue to transform the way we see and interact with the world. But while the damage by information theft and other computer crimes continues to mount, the integrity of the Internet as a means of secure communication is slowly dissolving.

The ball is in our court.

Dr. Fred Chang is president and CEO of SBC Technology Resources, the applied research and development subsidiary of SBC Communications.