

# Better Safe Than Sorry

*First Appeared in  
The Bandwidth Desk,  
September 14, 2001.*

**T**uesday morning's savage attacks on the World Trade Center and the Pentagon and the plane crash in Pennsylvania have taken an enormous toll in lost and broken lives, with profound and enduring consequences beyond our comprehension.

The strike against America and against free people everywhere will alter our political, economic, educational, social and cultural institutions and even our beliefs, our psyches and our behavior.

In these sad and terrible days, those who have been struck directly and personally by this inhuman attack and those nearest to them are coming to know its full and terrible effects, but we are all struggling with difficult and troubling thoughts and emotions. Safety and security are much on our minds. We feel vulnerable, even defenseless against unknown forces willing and able to commit such far-reaching evil. As in all such times, we seek strength and comfort with family and friends and we take for granted the security and reliability of basic services in our society, telecommunications among them.

Like so many others, I got a fast-busy signal over and over again when I tried to reach my daughter in Manhattan on Tuesday morning and, when I heard from her later in the day, and from my younger daughter, other family and friends, we shared similar stories about difficulties in getting our calls through. We did get through to one another that day, as did most callers, according to news reports. The main problem was not a disruption of facilities but twice-normal call volume. Call failures were still high through much of Wednesday. Cellular phone users had par-

ticular difficulty on Tuesday because, according to a report in The New York Times, ten wireless centers serving lower Manhattan had been destroyed by the attack. And, not incidentally, several local television stations with antennas atop the World Trade Center were knocked off the air as well. Email messaging slowed considerably on Tuesday morning as Internet traffic increased sharply, but traffic and congestion eased later in the day.

We can take some comfort that there was no evident major telecommunications outage last Tuesday. More than that, there is considerable reason to rejoice because cell phones enabled some victims of the attacks, on the planes and in the stricken buildings, to share final words with loved ones or leave parting messages for them, to call out to rescuers for help, or to let friends or family know that they were safe and tell them their whereabouts. Still, this week's horrifying events must give all of us pause regarding the security and reliability of the communications and information infrastructure, nationally and internationally.

In 1998, TTI conducted an extensive study of the safety and security of the U.S. communications and information infrastructure and concluded, "The U.S. has the most advanced communications and information infrastructure in the world, with high-quality, ordinarily reliable services. These services are essential to national defense, our economy and the infrastructures that support our society and each of us personally, and we take for granted that they will remain secure. But, in fact, our communications and information infrastructure is vulnerable to physical and cyber attacks that could harm national security and the economy and endanger human lives. The



**RICHARD THAYER, PH.D.**  
President & CEO

7018 Beechwood Drive  
Chevy Chase, MD 20815

T: 301.913.2883  
F: 301.913.2884

Email: [info.tti@verizon.net](mailto:info.tti@verizon.net)  
<http://www.ttinetwork.com>

list of vulnerabilities is long. There are divergent views on their seriousness, and there is no consensus on what to do. These are serious concerns for all of us. The federal government, equipment and service providers, and customers must work together to improve infrastructure surety.”

While last Tuesday was not an instance of cyber terrorism, such terrorism is a continuing concern for countries and peoples throughout the world. Many positive steps have been taken to improve the security of the U.S. communications infrastructure in recent years, including the prevention of cyber attacks, but more must be done. Little more than a week ago, at a conference in Washington, DC, experts once again called attention to the dangers that cyber terrorism poses to governmental, financial, economic and social institutions, to freedom and to human life. Sensitive communications, voice and data, attendees were told, remain vulnerable to eavesdroppers and hackers engaged in mischief, espionage or sabotage, and to terrorists determined to disrupt or destroy vital communications links.

Telecommunications systems designers, engineers and manufacturers and telecommunications service

providers employ sophisticated software and advanced technologies to assure the reliability of our communications infrastructure, with great success. But the challenge remains formidable.

Roger Cox, who specializes in communications security at Sandia National Laboratories in Albuquerque, New Mexico, summarizes the situation this way. “Over the course of the last 15-20 years, communications networks have become much more complex and tightly integrated. From the advent of digital switches to today’s mix of packet and circuit transport over a variety of protocols and media, including wireless, under sophisticated software control, service networks have become increasingly complex. The sheer number of interacting technology options, including those stimulated by unbundling, has taken service-level complexity to a whole new level, where no customer, individual carrier or equipment vendor has ultimate management responsibility.”

“With digital software control of communications networks,” Cox continues, “the rise in complexity in communications systems has grown to mirror the complexity that has been implicitly present in large soft-

ware codes. At the same time, the cycle times, from concept to service availability, have been dramatically reduced, and there are fewer technical staff with purely speculative oversight roles to catch subtle problems before they arise.”

“The bottom line,” says Cox, “is that every new service architecture can be expected to suffer from at least one major service collapse event after it enters production, or upon any major architecture change. For some customers, once is too often.”

As we consider the threat of terrorism and more broadly the safety and security of air travel, our cities’ subways, access to our workplaces and their very structure, and more, those of us in the communications and information industry have our own responsibilities cut out for us.

Richard Thayer is President & CEO of Telecommunications & Technologies, International, Inc. ([www.ttinetwork.com](http://www.ttinetwork.com)), a telecom and IT consulting firm located in Chevy Chase, MD. Contact by email: [rthayer.tti@verizon.net](mailto:rthayer.tti@verizon.net), or phone: 877.913.2883.

*Copyright 2001, Richard Thayer and Scudder Publishing Group, LLC. [www.scudderpublishing.com](http://www.scudderpublishing.com)  
Reprinted with the permission of the publisher.*