Evolving Cybersecurity Faces a New Dawn

Over the last two years, we have been inundated with bad news about the state of cybersecurity. The list of concerns is growing and endless: rampant cybercrime, increasing identity theft, sophisticated social engineering techniques, relentless intrusions into government networks, and widespread vulnerabilities continuously exploited by a variety of entities ranging from criminal organizations and entrepreneurial hackers to well-resourced espionage actors. We also are facing the implications of cyberwarfare in light of last year's cyber attacks against Estonia. In a recent speech on cybersecurity, U.S. Department of Homeland Security Secretary Michael Chertoff warned, "We've entered an era of new threats and vulnerabilities," and the consequences of failure are exponentially greater.

The stark reality is that the bad guys are winning and our nation is at risk. Given these difficult times, it is easy to feel overwhelmed and believe the situation is hopeless. However, I believe we are on the verge of a new dawn for cybersecurity, and in the coming months we will achieve significant progress in securing our critical networks. We have been on a four-stage journey that began in the late 1990s.

The first stage was ignorance. For the most part, up until 1998 we were clueless as to the vulnerable nature of our networks and the implications of interconnected systems. With the growth of the Internet and increasing dependence of military forces on networked systems as early as the 1991 Gulf War, we have rapidly leveraged the promise of net-centric capabilities. However, our understanding of the need for robust security mechanisms in this new environment was slow to catch up. As information technology boomed in the past two decades, the best young minds flocked to developing the latest and greatest systems—not to protecting data and corporate networks. But then, we entered stage two of the journey.

That second stage constituted awareness. It is no secret now that the Defense Department and other intelligence community members first became dramatically aware of our collective network vulnerabilities based on a series of exercises and actual events that occurred in the late 1990s. These events highlighted significant shortfalls in our cybersecurity posture that ultimately resulted in forerunners of today's Joint Task Force-Global Network Operations (JTF-GNO), under the authority of U.S. Strategic Command. There is no doubt that JTF-GNO's experiences in dealing with rampant cyber intrusions over the past three to four years have contributed greatly to focusing senior leadership attention throughout the federal government on this serious issue.

We now are entering phase three of the journey, which is actualization. We understand the nature of the threat and the implications for our nation, and there is a growing sense of urgency. Resources are being mobilized and focused on tackling a problem of global proportions. The President's Comprehensive National Cybersecurity Initiative (CNCI) is on the table. It is not perfect, but it is a good package of efforts that will bear fruit over time. Also, the president just signed new cybercrime legislation—the Identity Theft Enforcement and Restitution Act—that makes it easier for prosecutors to go after cybercriminals. There's also the Commission on Cyber Security for the 44th Presidency, which soon will publish sweeping recommendations including the need for a comprehensive National Strategy to Secure Cyberspace.

Congress actively is involved in cybersecurity as well. Representatives Jim Langevin (D-RI) and Michael McCaul (R-TX) recently announced the creation of the first House Cybersecurity Caucus, which will seek to raise awareness and provide a forum to discuss cybersecurity challenges. Legislation making its way through Congress would overhaul the original Federal Information Security Management Act, making information technology security more operationally relevant. Also, a House subcommittee recently began working on legislation that would expand the Federal Energy Regulatory Commission's authority to deal with cyberthreats against the nation's electric power grid. Finally, research and development efforts are being focused to seek leap-ahead cybersecurity technologies. While actions are slowly moving in the right direction, we still are a long way from the last stage.

This fourth stage is the cyber mindset. In this stage, we reach a level of transformation where government, business and individuals are keenly aware of information security mechanisms. Cybersecurity becomes institutionalized and paramount in a rapidly changing information technology environment. In this new cyberculture, the concept of "service-oriented enterprise architectures" will help organizations understand their business environments better while supporting improved information sharing between the public and private sectors. Also, we will have sufficient, but not overburdening, legislation to improve the security of the global networked environment and enable operational resilience to cyberthreats. Strong identity management and authentication capabilities will become more tightly integrated into online transactions involving banking, collaboration and sharing of personal information.

Yet, while all this progress is occurring, cybercriminals, terrorist organizations and espionage forces will continue to focus on countering our best efforts. Obviously, the fourth stage never will reach steady state, but we will achieve a much higher state of effectiveness than today. Good efforts already are underway, and our collective sense of urgency is increasing daily. We certainly are on the verge of a new dawn for cybersecurity as a national priority.

Lt. Gen. Harry D. Raduege Jr., USAF (Ret.), is chairman of the Deloitte Center for Network Innovation.