

The Washington Times

Commentary

LANGEVIN, ET AL.: Public-private collaboration

James R. Langevin, Mark Gerencser and Charles G. Boyd

Attacks against U.S. computer networks - most of them privately owned - are increasing in number and severity. Let's hope the new administration moves decisively to foster collaboration between the public and private sector so America can become cyberresilient.

The reasons for doing so are manifest. In 2007 alone (the last year for which records are fully tabulated), the Department of Homeland Security tracked more than 37,000 cyber-attacks - a more than 800 percent increase over 2005. The Defense Department's computers are probed hundreds of thousands of times every day, and in 2007, hackers believed to be backed by the Chinese military took down the unclassified e-mail system in the Office of the Secretary of Defense for more than a week.

Meanwhile, U.S. companies lost more than \$1 trillion worth of intellectual property last year because of cyber-intrusions. The energy sector is particularly vulnerable, with global utility operations hit by an estimated 1,000 hackers annually. A major cyber-attack could result in weeks-long power outages or cause even more damage to the national economy - a prospect we can hardly afford.

In December, a cyber-attack simulation conducted by the nonpartisan Business Executives for National Security, headquartered in the District, highlighted America's vulnerability and the need for a comprehensive, national approach to cybersecurity. Over two days, more than 230 senior leaders from industry, government, Congress, academia and the military tried to respond to a simulated cyber-attack that decimated telecommunications in the Eastern United States and damaged financial institutions and other targets.

At nearly every turn, the participants encountered difficulty restoring normal operations. Their failure to plan for the attack - and the difficulty they experienced communicating with one another when the simulated attack was under way - prolonged recovery time to the point of major system failures.

The simulation revealed that while parts of the federal government and some private companies are doing a lot to strengthen their own cyberdefenses, the United States is only addressing pieces - and not the whole - of

cybersecurity. This approach will fail because cybersecurity is, like a chain, only as strong as its weakest link.

Focusing cybersecurity efforts solely on one's own organization robs attention from the bigger picture. Whether they realize it or not, companies, government agencies and other organizations are part of an interconnected system that cannot absorb a major attack. Narrow-point solutions such as firewalls, anti-virus software and intrusion-detection technology help, but they don't suffice.

True protection requires cyberresilience. That can be achieved only through collective action and cooperation on a scale rarely witnessed before: a national effort involving business, government and society - similar to the way "Y2" - the apprehension about what would occur with the advent of the year 2000 - was approached, but designed for the long haul and not just one event.

No single organization has the capacity to build this resilience. We need to work as a large and inclusive community across government, industry and nonprofit organizations - a megacommunity of sorts.

Melissa Hathaway, recently named by President Obama to review the nation's cybersecurity policies, was chosen in part for her ability to foster collaboration within government to deal with cyberthreats. We hope her report urges collaboration beyond government - involving business and society as a whole - so America can become cyberresilient.

Resilience is different from risk avoidance (working to ensure nothing happens) or even risk management (choosing what to protect and what not to protect). Resilience assumes bad things will happen and requires advance planning and preparation. "We will need to end a culture where we ignore problems until they become full-blown crises," Mr. Obama said recently when discussing the economy. This is also true of cybersecurity.

A lot is at risk: financial systems, power grids, air traffic control and more. A major cyber-attack will happen, and it will affect more than we think. The question is: Will we be ready - and resilient?

Rep. James R. Langevin, Rhode Island Democrat, is co-chairman of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Mark Gerencser is a senior vice president at Booz Allen Hamilton. Charles G. Boyd is president and chief executive officer of Business Executives for National Security.