Fortifying Our Cyber Defenses

CrossTalk would like to thank the Department of Homeland Security for sponsoring this issue.

Simply stated, absent secure and resilient software at the core of our cyber defenses, the nation's critical infrastructure is at risk. Everything we do as a nation—from national defense to re-energizing the economy—depends on secure information technology systems and networks.

Increasingly, however, these software controlled and enabled systems are vulnerable to exploitation by those that seek to do our nation harm, steal our intellectual capital, or simply collect our personal information. Making critical software assets secure and resilient is a necessary part of the nation's defense-in-depth approach to cybersecurity.

The DHS, and more specifically the Office of Cybersecurity and Communications, has the lead role in securing the civilian side of those critical networks and systems. A vital component of that effort is the National Cybersecurity Division's Software Assurance Program. The program works with its partners in the federal government, private sector, and international community to reduce software vulnerabilities, minimize exploitations, and develop secure and trustworthy software products. In short, it works to protect vital networks and systems by applying sound software supply-chain risk management.

With that in mind, two points merit emphasis. First, developing secure and resilient software alone is not enough. Increasingly, our critical cyber networks and systems are vulnerable to exploitation by a variety of actors. That means that unless the systems and networks controlled by the software in question are also protected, cybersecurity will remain an elusive goal. These factors are inexorably intertwined and must remain so in order to support mission requirements across enterprises and critical infrastructures. Sound cybersecurity practices must be overlapping, integrated, and supportive. In other words, they must be a "system-of-systems" that encompass all the people, activities, processes, and technologies that together promote and define a comprehensive national cybersecurity strategy.

Second, the DHS accomplishes its mission by working closely and collaboratively with the private sector. The government is best at developing policy objectives, identifying requirements, and facilitating the achievement of those objectives. The private sector specializes in finding ways to meet those objectives and requirements through technology innovation, experimentation, and innovative product development. Working separately, we will only get half of the job done. Working together, however, we can develop the necessary products to safeguard our critical systems.

So join us in our mission and be part of the software assurance solution. Visit our Web sites <https://buildsecurityin.us-cert.gov/swa/> and <http://www.us-cert.gov/>. Learn more about the Cross Sector Cybersecurity Working Group and the Software Assurance Forum. Better yet, become part of the public-private effort and learn how to participate in these important efforts. Together we can build a trusted and resilient information and communications infrastructure based on secure and resilient software.

I hope everyone appreciates the articles in this issue of CrossTalk that explore the multifaceted dimensions of software resiliency. I thank the authors for their important contributions. More importantly, the DHS continues to seek input and feedback on collaborative efforts to advance software assurance.

MaBrown

Michael A. Brown
Rear Admiral, USN
Deputy Assistant Secretary for Cybersecurity and Communications
U.S. Department of Homeland Security