Cybersecurity Threat Reduction

Cybersecurity threats to businesses, government agencies and citizens are increasing drastically. Software security companies like Symantec have detected an average of 9,000 new malicious websites daily (63 percent are infected legitimate sites). They have found more than 400 million new variants of malware. Over 1 in every 250 emails is malicious, and an increasing number are targeted at businesses, specifically upper management and research and development.

Thefts of personal information, credit card numbers and identity have also increased. Cyber-criminals steal billions of dollars' worth of intellectual property from U.S. companies and sell it to the highest bidder overseas. They are installing software onto tens of thousands of computers, establishing large networks from which they can launch criminal attacks.

The proliferation of cyber-criminal activity is a drain on national productivity. The average worker and consumer spend time fighting identity theft and struggling with infected computers. Our businesses spend increasing resources defending against and recovering from cyber-attacks.

A cyber-secure vision for Idaho

Under the leadership of the University of Idaho's Center for Secure and Dependable Systems, industries in the state of Idaho will have access to training to enable them to cost-effectively secure their corporate networks, protecting corporate and customer data.

Idaho industry will be known as a reliable and innovative source of high-quality security software, developed by businesses using best practices, and employing highly qualified software engineers trained in the latest software security technologies.

Idaho citizens will have access to high-quality software products that protect their computer systems from cyber-attacks.

The importance of cybersecurity

Idaho businesses are vulnerable to cyber-attacks for a number of reasons, including:

- Inadequate training and support: Modern computer systems are complex and cannot be adequately configured and safeguarded by lay citizens. Small businesses cannot afford full-time staff to manage and maintain computing system security.

- Incorrect mental models: Computer software is sophisticated. An average small business can develop a website, providing itself with an online presence, but it does not have an accurate mental model of how the system works in conjunction with the underlying hardware, network, and operating system and over 2.8 billion other users on the internet. Even trained software developers misunderstand how systems work.
- Insufficient numbers of professionals: The U.S. educational system is not graduating enough computer science and IT professionals to keep up with demand. Student enrollments dropped after the dot-com bust, and have not returned in sufficient numbers. There is an incorrect belief among students and parents that good jobs are all overseas.

Importance of increased funding

The National Science Foundation Cybercorps program and the National Security Agency/Department of Homeland Security Center of Academic Excellence program are two successful programs that support cybersecurity education at universities. The NSA/DHS program could use substantially more funding to support the building of education capacity at designated universities.

The federal government must support the concept of regional software-quality testing labs (an academic and private partnership) that work with industry to provide training and resources to enhance the security of their networks and increase the quality of software developed and used by that industry. These labs also provide software security testing and analysis consulting services to area industry, similar to pharmaceutical and ground water testing facilities based at universities.

Research focused on technology innovations and on understanding the human element in the use of complex computer systems is vital, as is the development of tools, technologies and processes that enhance software security and quality through better training, software testing and software development.

For more information, please contact:

John K. “Jack” McIver, Vice President for Research and Economic Development
vpresearch@uidaho.edu | 208.885.6689 | www.uidaho.edu/research/federal-relations