The new civil defense: Researchers look at public's role in national cybersecurity

February 1 2010

University of Cincinnati researchers say the nation's cybersecurity is being threatened because an important element in establishing it is not being emphasized enough - citizen awareness and participation.

In equating today's citizen role in cybersecurity to the Civil Defense efforts developed at the advent of the era of atomic weapons, UC Political Science faculty members Richard Harknett and James Stever argue that an active role for citizenry participation in security efforts is largely being overlooked. They make their case in a new paper published in the *Journal of Homeland Security and Emergency Management.*

Currently, Washington is in a period of re-examining policy towards cybersecurity. Just last week, the New York Times published an extensive story examining U.S. deficiencies in policy towards cyber attacks, and a new study of 600 computer and computer-security executives showed high levels of concern that cyber attacks at any time could compromise our energy and communication sectors.

Harknett and Stever argue that a three-pronged approach to cybersecurity is necessary: the ideas of coordination within government agencies and also between government and business interests surface in almost every discussion on the topic, but the third leg - engagement with the public about the role they can play in cybersecurity - rarely gets mentioned.

"The general population must be engaged as active security providers,

not simply beneficiaries of security policy, because their practices often create the threats to which government must respond," write Harknett and Stever. As an example, they cite the hijacking last July of up to 50,000 computers for use in a botnet denial-of-service attack on Web sites operated by the U.S. and South Korean governments.

These kinds of threats are the weakest link in our national cybersecurity, they say. The potential is there through cyber attack to, as an example, target the nation's electric grid or financial transaction records

"Any awareness campaign that remains seated in only self-interest (i.e. if you do not protect yourselves bad things will happen to you) will not establish this critical third leg of the cybersecurity triad," Harknett and Stever write. Computer users need to be made to understand that, in the networked age of the Internet, the implications of their not adhering to safe computer practices regarding passwords, security software and downloading protocols can open a door for those with much more malevolent goals than just infecting individual computers with viruses or spyware.

What Harknett and Stever are recommending is a widespread effort to remold how people view cyberspace. The current view of cyberspace as a private concern needs to be replaced with an attitude that cyberspace is a public good. As they put it, "the key reorientation of any cyber awareness plan must hinge on the notion of active participation in enhancing national security as a civic duty."

The goal would be changes in behavior by all American computer users. The effort should go so far as making secure computing practices part of what is taught to young computer users in the nation's schools.

As an example of what needs to be done, Harknett and Stever cite the onset of Civil Defense planning in the 1950s. The key difference,

though, is that Americans in the 1950s were motivated to participate because they instantly understood the perils posed by nuclear weapons. People today don't yet understand the downside risks that could come from a cyber attack.

"The ubiquity of computer technology throughout the civilian population will require full societal engagement if the national objective is a secure cyberspace. As the digital environment grows in scale and scope, so too will the need for a cyber civic culture to emerge to manage it," Harknett and Steve write. "Ironically, because the citizenry is less conscious of the cyber than the nuclear threat (as national security threat), a much greater degree of civic mobilization and understanding will be required to face this 21st Century challenge."

More information: Their paper, titled "The Cybersecurity Triad: Government, Private Sector Partners and the Engaged Cybersecurity Citizen," appears in Volume 6, Issue 1 of the Journal of Homeland Security and Emergency Management.

Provided by University of Cincinnati