To deter cyberattacks, build a public-private partnership

August 25 2014, by Phil Ciciora

The best way to combat cyberattacks may be a joint public-private partnership between government and business, says a new paper from Jay Kesan, the H. Ross

and Helen Workman Research Scholar at the University of Illinois College of Law. Credit: Jay Kesan

Cyberattacks loom as an increasingly dire threat to privacy, national security and the global economy, and the best way to blunt their impact may be a public-private partnership between government and business, researchers say. But the time to act is now, rather than in the wake of a crisis, says a University of Illinois expert in law and technology.

According to a study by Jay Kesan, the H. Ross and Helen Workman Research Scholar at the College of Law, an information-sharing framework is necessary to combat cybersecurity threats.

"Cybersecurity is a big deal, and the protection of critical network infrastructure is a matter of national security," said Kesan, who directs the Program in Intellectual Property and Technology Law at Illinois. "If nothing else, cyberattacks are very expensive, costing the global economy almost a half-trillion dollars per year, according to some estimates. For either of those reasons alone it should be given more attention."

Meaningfully improving cybersecurity and ensuring the resilience of systems will require cooperation between members of the private sector and the government, according to the paper. To that end, Kesan and co-author Carol M. Hayes, a research associate with U. of I. College of Law, propose a framework for the sharing of information about threats and solutions that they believe reconciles the competing concerns of privacy and cybersecurity, Kesan said.

"Privacy and cybersecurity are not mutually exclusive, but balancing the two interests may require cooperation and the occasional compromise,"

Kesan said. "We believe that cybersecurity can be enhanced without creating an Orwellian, Big Brother world, and encourage the development of what we call a 'Circle of Trust' that brings the public and private sectors together to resolve cybersecurity threats more effectively."

The goal is to foster trust between the private and public sectors, he said.

"When the public sector shares information with the private sector, that encourages the private sector to trust the public sector, and vice versa," Kesan said. "Our proposed framework advances this notion of trust even further by allowing both sides to preserve a degree of secrecy – for example, government secrecy for classified military activities and geopolitical information, and private-market secrecy for consumer information, including information about consumers' online activities. It functions to assure participants that overreach by either side will be limited."

Private cybersecurity researchers could benefit from information about intrusion attempts and details about vulnerabilities uncovered by government actors, and government agencies could benefit from up-to-date information about private cybersecurity innovations and the identification of vulnerabilities by private firms, the researchers say.

Although some existing laws would need to be revised to implement the proposal, "both sides could benefit from information sharing about different security measures and their rate of success," Kesan said.

To emphasize the importance of cooperation, the paper presents case studies of two recent government proposals to address cyber threats: the proposed Cyber Intelligence Sharing and Protection Act (CISPA), and the presidential executive order that outlines procedures to establish voluntary cybersecurity standards.

Both proposals would create a way for qualified members of the private sector to obtain security clearances to receive classified cyber-threat information from the government, and CISPA also would allow the private sector to share cyber-threat information with government agencies.

But according to Kesan, efforts to address cyber threats may be hindered if policymakers rely solely on voluntary compliance.

"Both CISPA and the executive order take a voluntary approach, and we argue that a purely voluntary mandate is undesirable in both contexts," Kesan said.

Under each system as currently proposed, participation by private firms is purely voluntary and there is no penalty for non-compliance.

"Voluntary programs can be effective in some situations, but they may ultimately be interpreted only as aspirational guidelines," Kesan said. "In the sensitive context of cybersecurity, aspirational guidelines for security standards could lead to low levels of compliance, the withholding of valuable information by those who do not participate, and a greater risk of overshare by those who do participate."

On the other hand, mandatory programs with effective enforcement mechanisms are likely to result in higher levels of compliance, the authors note. This may be especially true when the program concerns highly complicated subject matter, as previous research has indicated that voluntary compliance may not be as effective in those situations.

"Government intervention with the free market should be minimized, but when cybersecurity issues have implications for national security, some degree of mandatory regulation would be beneficial," Kesan said. "The Obama administration recognized this through the issuance of the

executive order on improving critical cybersecurity infrastructure, and Congress has recognized this as well."

Unfortunately, cybersecurity has proved to be a much more partisan issue than it should be, and Congress has not yet come together to take meaningful steps to protect the cyber infrastructure, Kesan said.

"Advocates for private enterprise have discouraged the imposition of meaningful cybersecurity requirements on privately owned critical infrastructure, while advocates for civil liberties and privacy invariably react with alarm to regulation that involves the collection of information about threats," he said.

Both Kesan and Hayes believe it is unlikely that Congress will pass effective cybersecurity legislation in the current session, which is scheduled to end on January 3, 2015. Although the presidential executive order and their proposed cybersecurity framework could provide some helpful first steps, the authors say that it is neither feasible nor desirable to rely solely on executive power to shore up the cyber defenses of the government and the private sector.

"Ideally, our proposed cybersecurity framework would be implemented alongside supporting legislation to ensure that cybersecurity actions and standards are subject to the checks and balances of our system of government," Kesan said. "CISPA could be easily revised to accompany our framework."

The authors also contend that it is important to ensure that this issue is subject to deliberate and careful decision-making by policymakers before a massive cyber catastrophe forces the government to act quickly and without adequate safeguards. They point to to the history of the Patriot Act, which was hastily passed in the aftermath of 9/11, and has been the target of significant criticism on civil liberties grounds over the

last thirteen years.

"It's vital that these issues are addressed soon while there is still a chance to prevent a catastrophic cyber event," Kesan said. "It would be ill-advised to rely solely on executive power or on legislation that is hastily drafted and enacted after an emergency."

More information: The paper, "Creating a 'Circle of Trust' to Further Digital Privacy and Cybersecurity Goals," is available online: papers.ssrn.com/sol3/papers.cf … ?abstract_id=2135618

Provided by University of Illinois at Urbana-Champaign