World Knowledge Forum 2013

How to Secure the Cyberspace

On the morning of the second day of the 14th World Knowledge Forum, Eugene H. Spafford of Purdue University offered a dire warning on the security of cyberspace: "I'm here to tell you the situation does not look good, although it may not appear that way to you. Part of that is because you do not have the same viewpoint that I do over time."

He was joined on the panel by Cheri F. McGuire, Vice President of Global Government Affairs and Cybersecurity Policy for Symantec Corporation, Hong Sun Kim, the CEO of AhnLab, and Jeff Moss, the Chief Security Officer of ICANN. The panel of cyber security experts called for a push toward global cooperation to deal with the increasing threats to cyberspace.

"The cybercrime challenge cannot be solved by any single company or government," Ms. McGuire said. She complained that risk assessment and tolerance currently varies between industries and governments. "We need shared responsibility," she advised. She urged the industry and governments to work together in public-private partnerships.

Mr. Kim agreed while sharing his perspective on South Korea, a region he said is dogged by cyber attacks.   Mr. Kim outlined an approach to establish an international network with real-time sharing of threat information.   He insisted that although transnational cooperation is the only way to deal with serious cybercrime, regional and cultural differences present a challenge that must be respected.

"Each country has different cultures and differences in business and in banking regulations," said Mr. Kim.

Mr. Moss leaned more towards the industry to solve security problems. "If businesses can't solve this problem, if computer scientists can't solve this problem" he said, "I fear that governments will solve this problem...whatever way governments solve things. They tend to use a pretty heavy axe."

However, Mr. Moss added that there is an important role for government. "Governments are there to protect us as a society," he said,   "and I'm not seeing them doing it."

Solutions were offered by Ms. McGuire and Mr. Kim, both from cyber security companies. Ms. McGuire recommended a multi-layer system of protection and Mr. Kim described both a vertical and horizontal approach to security. He said firewalls and other approaches slow down and identify external threats to the system, but the internal sharing of information is also important to consider.

"There are a lot of things that you can do," Ms. McGuire said, momentarily turning more positive. But she and Mr. Kim admitted that a lot of the current solutions are reactionary. The focus is on containing the breach once it happens. "Attackers will come over your wall," she admitted.   "They will come under your wall, and they will come around your wall."

Dr. Spafford complained that this approach is the root of the problem.   He said that we should not be reacting to attacks, but preventing them. The industry used to know how to build machines securely, he said, but we haven't learned lessons from the past. "We should be building systems secure from the start," he said. "We have developed a culture where the belief is that patching a system afterwards or hiring someone to penetrate a system and then fixing what they find, that somehow those things are equivalent to security, and they are not."

Dr. Spafford then offered an analogy to explain.

"If you bought an automobile and the tires kept falling off or the doors kept falling off and you had to buy toolkits and bolts and staple guns to put it back together every time that happened, you wouldn't consider that safe to drive. That's how we treat our computers."

The panel also discussed how the situation became so dire in the first place. Mr. Moss offered an overview of the explosion of complexity in the system from the early days of ARPANET to our current days of cloud computing with increased virtual complexity. This increase in complexity results in an increase in vulnerability.

Nevertheless, both Mr. Moss and Dr. Spafford suggested there is a lack of interest on the part of governments, industry, and the public, to make this complex system more secure.   The industry, Dr. Spafford said, wants your information accessible for marketing purposes, and consumers want the convenience without worrying about privacy. A collective lack of will blocks obvious solutions to the problems.

"How do you measure security?" asked Mr. Spafford, "Where is the measure of privacy on anything you buy? It's not there, because the vendors don't want to offer it and consumers

don't ask for it. If I came back in fifteen or ten years, I expect I could give the same talk with different numbers because the general population does not seem to be concerned. But as leaders, we should be."