Summary

Maryland Cybersecurity Council Reception and Meeting

Thursday, February 4, 2016
11:30 am –1:00 pm
House Office Building
Room 145 (Baltimore City Delegation Room)
6 Bladen Street, Annapolis, Maryland

Council Members Present or Represented

Council Chair, Maryland Attorney General Brian Frosh, Senator Susan Lee, Senator Catherine Pugh, Delegate Ned Carey, Delegate Mary Ann Lisanti, Blair Levin, Joseph Morales, Pegeen Townsend, Howard Feldman, Jonathan Prutow, Paul Tiao, Secretary David Garcia, Walter Landon, Dr. Anupam Joshi, Anthony Lisuzzo, Robert W. Day, Sr., Kristin Jones Bryce, Judith Emmel, Clay House, Dr. David Anyiwo, Mark Augenblick, Rajan Natarajan, John M. Abeles, Zuly Gonzalez, Robert Rosenbaum, Donna Dodson, David Engel, Dr. Stewart Edelstein, Jonathan Powell, Henry Muller, Dr. Shiva Azadegan, Russell Strickland, Dr. David Wilson, Belkis Leong-Hong Jim Dinegar, Joseph Haskins, Jr., Latoya Staten,Phil Schiff, Brian Israel, Steven Tiller, Dr. Jayfus Doswell, Don Fry, James Foster, Michael Greenberger, Sue Rogan, Dr. Anton Dahbura, Larry Letow, Carl Whitman, Dr. Patrick O'Shea

Others Present:

Amjad Ali (University of Maryland University College), Zenita Wickham Hurley (Office of the Maryland Attorney General), Sachin Bhatt (Office of the Maryland Attorney General), Michael Lore (Senator Lee's Office) and Karen Morgan (Maryland Department of Legislative Services), Major Gen. Linda Singh, Major Robert Smolek

Council Reception

<u>Opening Remarks</u>

The meeting was called to order at 11:30 a.m. by Maryland Attorney General Brian Frosh who introduced UMUC President Javier Miyares.

Miyares said two weeks earlier the U.S. Department of Defense Cyber Crime Center designated UMUC as one of 13 national centers of digital forensics academic excellence.
He said the university now enrolls more than 8,000 students in cyber-related programs, and it has graduated more than 4,000 students from its cyber programs.

Miyares said UMUC will depend on the council's guidance and expertise to keep its cybersecurity programs up to date in a rapidly changing field.

Presentation by Dr. Vinton Cerf

Sen. Susan Lee introduced Dr. Cerf as one of the fathers of the Internet who has held numerous positions on corporate boards and government commissions, and was awarded the Medal of Freedom from President Obama. He is now an Internet evangelist for Google, she said.

In his remarks, Dr. Cerf warned that the war for cybersecurity is being lost and that the government must get involved in enforcing greater security measures and in creating liability for bad computer software.

"I can't think of anything more critical to our future than figuring out how do we secure ourselves in this online cyberspace environment," he said.

He said that average Internet user must accept some security practices that they find inconvenient. But it is also essential for the industry to create effective security procedures that are easier to use. If security becomes too difficult, he said, users will find ways to bypass restrictions.

He said legislators may need to pass regulations to deal with people who refuse to act responsibly. He compared it to regulations that require people to wear seatbelts while driving or restrict where people can smoke.

He said there is a need to impose a liability on providers of Internet services, equipment builders and software writers to force them to take more seriously their role in protecting against hackers.

But he admitted that even after 70 years of trying, no one is able to write software that doesn't have bugs. Writing software has become more difficult with the Internet because programmers cannot conceive all of the places their software will end up. AS they are writing software, programmers do not have the tools to tell them when they have made a mistake.

He said cloud computing is helping this problem because instead of having software distributed to untold numbers of laptops, mobiles and tablets, it is all concentrated in one place where it can be watched for bugs and updated.

Cerf proposed a "cyber fire department" that would help especially small companies that do not have the capability of responding to a cyber attack.

Providing security and international understandings on a national level are crucial to avoiding World War III, he said. If a country believes it is under attack from another country, it must be sure where that attack is coming from. A counterattack against the wrong country could easily escalate out of control.

The explosion of the "Internet of things" is also causing security problems, he said. "When we started doing this work 40 years ago, it didn't occur to us that picture frames and refrigerators would be part of the Internet." If there are a couple of hundred items in a house that have internet connections, and we know that all programs have bugs in them, he asked, then how can we protect and monitor all of the devices?

“The headline I worry about is ‘100,000 refrigerators attack Bank of America,’” he said.

Dr. Cerf raised the conundrum of privacy and security. With so many things connected to the Internet, people want to share some of that data some times but they also want to guard it at other times. How to make that possible is something for universities such as UMUC to work out.

To get more Internet security, he said, not only does government have to do more, but it also has to provide incentives for the private sector to do more. Incentives are everything, he said. If you don’t like certain behaviors, the best way to figure out what to do about it is to find out what incentive is driving that behavior and then change the incentive.

Question and Answer session

Asked about whether providing cybersecurity insurance would be a good thing, Dr. Cerf said this has become a major topic. Having insurance does not solve the problem, he said, but it could provide some leverage for insurance companies to demand certain practices to lower the cost of premiums. He said it is still difficult to figure out what a premium should be.

Another questioner said with computer literacy so low, how can the average user know that they need new software and if they get it, how to load it? Cerf said automated methods for downloading and updating software are becoming more common. Google insists on it and can force downloads on its employees. But he said there are still problems to make sure that the downloads have come from the right people and are safe. It is possible for downloads to look like they have come from Google or Microsoft, and they haven’t. But it is important to make more of this automated so the user does not have to think about it.

Another speaker asked if each person has an inalienable right to privacy, and how can that be protected and not violated.

Dr. Cerf responded that people confuse privacy with anonymity. If you live in a small town, you have no privacy because everyone knows what you are doing. In a big city, you think you have privacy, but you really only have anonymity because no one knows who you are. With the Internet, that anonymity is disappearing because so much information is available. Whether you have an inalienable right to privacy is something for the Supreme Court to decide, he said. But preserving anonymity will be hard to do today.

Another questioner asked about the difference between protection and surveillance.

Dr. Cerf said he is not in favor of building backdoors into cryptographic systems. Once you do that, the information will leak out and the bad guys will get access to it. But there must be ways to find out what people are doing, he said. Technical means of surveillance is not the only way to collect information. Some information is not encrypted and can be available through legal means. Google responds to a number of these requests. But everyone deserves the best quality crypto available to protect privacy.

Another questioner said now people in the private sector are prohibited by federal law from hacking back at attackers. Should that be changed?

Dr. Cerf said that unless you know for sure who is hacking you, then hacking back can be one of the most damaging, unhelpful actions you can take. In the financial sector, the best action to take is to shut off the money. That would be more effective than hacking back, which could come close to vigilantism.

Another questioner asked what incentives could the government put in place to promote security?

Dr. Cerf said first the government should adopt and demonstrate the best security, which it is not now doing. The attack on the federal Office of Personnel Management is a good example of how the government doesn't do it right. He said the state of Maryland is in a good position to take leadership because of its access to the high-tech community.

Beyond that, he said, the state's procurement practices can include incentives. If the state won't buy software that doesn't have high security built in, then the sellers will soon build in the security.

Another questioner asked if Dr. Cerf thought the Cybersecurity Information Act passed by Congress was adequate.

Dr. Cerf said he is not an expert on the act, but he is always leery of legislation that mandates how something in the cyber world should be organized. He said in his networking world, there is a tremendous amount of cooperation and collaboration that happens when somebody is under attack. This is not mandated by law, but by sensible engineering practices. As an example, he said a completely informal working group of private sector and government experts came together to study something called the Conflicker worm. If there had been rules in place to determine who should be in that group, it would not have been as effective.

Another questioner asked about reaching down to elementary and middle schools to teach cyber hygiene.

Dr. Cerf said absolutely. He said he was excited about the White House announcement to create cyber science for everyone from kindergarten through high school. If everyone has some knowledge about how computers work, he said, then they will avoid many of the security problems and they will be able to understand how difficult writing code is, how fragile it is and how it does not always work.

A final questioner asked if he thought that software engineers should be licensed just as civil engineers are. He replied that he thinks they should, even though he was attacked unmercifully for proposing it. If someone is putting together a major system for replacing FAA air control system, wouldn't you want to be sure the people writing that code know what they are doing? But determining how to test for a license is difficult. Tests that we give students look like they would be terrific. But when they get into the field, they flop. Figuring out how to structure the tests should be a priority.

Council Meeting

Senator Susan Lee said the legislation subcommittee is looking for what kind of legislation should be put together to update and make changes to current cybersecurity laws. Two laws were passed in 2010 to protect infrastructures such as public utilities against cyber crimes. Maryland Commission on Cybersecurity Innovation and Excellence came up with substantive recommendations, which produced legislation on data breaches.

An attempt to update the HIPAA Act dealing with personal information held by commercial entities did not pass because of lack of time. That should come up again, but not this year.

So much more needs to be done to protect personal healthcare information online that it should not be done in a piecemeal manner, she said.

Laws dealing with large-scale data breaches need to be reviewed, she said, to determine the adequacy of the centralized cyber rapid response plan and whether the Department of Information Technology needs more money to implement it.

Also past laws have exempted the state's judiciary and legislative branches from laws passed to protect the state government. That needs to be reexamined.

Blair Levin, Aspen Institute fellow and former executive director of the FCC's Omnibus Broadband Initiative, said his research found that no state has a good model for cybersecurity legislation. That gives Maryland an opportunity to create such a model that could be used by the rest of the country.

Secretary David Garcia of the Maryland Department of Information Technology, said the state should take the lead in cybersecurity because of the resources in the state, the expertise of the state's industry, and the links here to the federal government and its resources.

Belkis Leong-Hong, chair of the economic development subcommittee, said her committee will meet soon to expand on its mission. In particular, it will want to look into Dr. Cerf's suggestion about incentives for the private sector to expand the cybersecurity ecological system in the state. It also will want to look into expanding cybersecurity entrepreneurship.

The Council reception and meeting concluded at 1:00 p.m.