Summary

Maryland Cybersecurity Council Meeting
May 18, 2016
10:00 am – 12:00 pm
University of Maryland University College
Adelphi, Maryland

Council Members Present or Represented

Senator Susan Lee, Paul Tiao, David Engel, Anthony Lisuzzo, Shiva Azadegan, Steven Tiller, Anton Dahbura, Michael Greenberger, David Anyiwo, Sue Rogan, Jonathan Powell, Rajan Natarajan, Dr. Jonathan Katz, Belkis Leong-Hong, Joseph Morales, Howard Feldman, Clay House, Jonathan Prutow, Patrick O'Shea, Mark Augenblick, Judith Emmel, Carl Whitman

Others Present:
Amjad Ali (University of Maryland University College), Zenita Wickham Hurley (Office of the Maryland Attorney General), Robert Smolek, Randolph Staudenraus, William Pallozzi, Walter Landon, Russell Strickland, Chuck Ames, UMUC President Javier Miyares, Blair Levin, Kristin Jones Brice, Mary Ann Lisanti, Ned Carey, Dr. Cyril Draffin, Jr. and Peegan Townsend

Council Meeting

Remarks by UMUC President Javier Miyares

President Miyares emphasized the university's commitment to provide staffing and resources for the commission. He said the university already has graduated 4,000 students from its cyber programs and 8,000 are currently enrolled.

Remarks by Zenita Wickham Hurley

Ms. Hurley was sitting in as chairman of the meeting because Attorney General Brian Frosh could not attend, and neither could his backup chair, Mr. Don Fry. She said Mr. Frosh is interested in hearing from the subcommittees to preview the proposals they are planning for the May 27th report that will be going to the attorney general's office in preparation for the council's interim report to the legislature due July 1. She said Mr. Frosh is hoping for at least one substantive recommendation to send to the legislature.

She said Mr. Frosh is particularly interested in two recent cybersecurity breaches – a theft of Baltimore City personal information that led to the filing of fraudulent tax returns as well as a break in to the MedStar Health computer system that led to an encryption of important medical information and a ransom demand to get access back to that information.

She said that's why substantive recommendations are needed immediately and council members should be ready to ask questions and raise potential issues to help the subcommittees draft recommendations.

She opened the floor to any other opening remarks.

Sen. Lee introduced a member of the audience, Dr. Cyril Draffin, Jr., an expert on cybersecurity issues dealing with the grid and a past executive with Northrop Grumman and now a consultant to MIT.

Presentations

Chuck Ames

Chuck Ames, speaking for David Garcia, Maryland's Secretary of Information Technology, offered to provide information to any subcommittee that needs to know more about how the department works and how other states are dealing with cyber threats.

Between 2010 and 2014 cyber criminals figured out that they could monetize their attacks against both governments and private companies, even those with extensive cybersecurity systems. They are not doing anything different to gain access, but more people have the tools to make attempts. Tools are available on the Internet that allow relative novices to make sophisticated attacks. He said even his dentist was held up for several thousand dollars by ransomware.

He said 90 percent of attacks come through email. He displayed an example of an attempted attack against him. If he had filled out the request that appeared to come from a two-star general, he knew his system would have been compromised.

He said his subcommittee has asked the attorney general to take its findings off of the public reporting system so that what it finds is not available to cyber criminals.

He said all employees and executives must be educated as to what a fraudulent link looks like and how, especially executives, can be exploited.

The next step is an anti-virus campaign. Email inboxes usually do not have the protections to stop viruses. People use numerous platforms to access information, and all of them could be liable to attack, even if official ones are protected. Attacks can even come through heating and air conditioning systems that now are connected to the Internet. Cybersecurity requires examining all of these systems to find weaknesses and to create new firewalls.

The only way to protect yourself is to have frequent exercises with employees that get more sophisticated. Protections have to be updated routinely, and people have to understand that security creates friction that slows down a system.

Ames said Maryland is about in the middle of the states in comparing number of networks and in the size of the state budget for cybersecurity. All of the tools it has are similar to other states. But

some states, such as Virginia, have outsourced their IT. Maryland has some outsourced services and one in-sourced. Some states, such as Michigan, do a better job than Maryland, but Michigan has been working on it for 15 years and Maryland for six months.

Legislation passed in Maryland required a statewide incident response plan, which fell on his committee to accomplish. That is underway, and it is now about 60 pages, which gives a good idea of what it should look like. When it is done by July, it will give all state agencies an idea of what they should be doing.

Mr. Ames said he wants to introduce cyber exercise at the Cabinet level so that the state's leaders know how to handle the velocity with which these attacks happen.

He said that the cyber-disruption plan combines what the National Institute of Standards and Technology (NIST) requires for incident response with how the Maryland Emergency Management Administration does when it has an emergency response. MEMA would respond the same way it would for any other emergency. The plan should be completed by June or July.

The plan would be applicable just to state agencies because trying to expand it to include local governments or private entities would be too difficult at this time. No independent or individual entity within the state, other than state government, has a responsibility to respond to us. Energy providers already are working with the state on plans, but they would not extend to, say, a Gap store in downtown Annapolis.

Director Strickland said that once the plan is completed for the state, it could serve as a model for the counties.

Michael Greenberger presentation

Greenberger is Director of the Center for Health and Homeland Security at the University Of Maryland. He was joined in his presentation by Marcus Rauschecker, the center's cyber director. Greenberger said one major obstacle is that 85 percent of the critical infrastructure is in private hands, which gives policy decisions enormous consequences. Imposing government mandatory actions is proving difficult to enact while voluntary controls are inadequate. Only a major disaster would awaken people to the need for mandatory controls.

His subcommittee's first recommendation is to create a resource center in the state that would be available to all stakeholders. It would be called an educational critical infrastructure strategy, and it would be available to private companies looking for advice and guidance. Publicizing the availability of this information would lead to requests for more information. This educational infrastructure would work through lectures, workshops and discussion groups; create an online repository of lectures and presentations that would be freely available 24/7. It would help move ideas from the academic sector to the private sector.

His subcommittee's second recommendation is to identify the private sectors in need of plans and processes to protect their infrastructure. First it would have to determine how to break this down so it is meaningful to private operations. Sector-by-sector risk management plans would be required. That is made more difficult because the state cannot compel the private sector to

participate. If this cannot be implemented voluntarily, he said, legislation requiring it may have to be proposed.

Dr. Jonathan Katz presentation

He said the Education and Workforce subcommittee worked on three priorities:

The first priority is aimed at educating the general public about cybersecurity threats because most attacks exploit the behavior of regular employees, not people employed in the tech industry or people with a tech background.

The second priority is teaching the principles of building secure computer systems to all computing professionals. That's the only way to stop cyber attacks and to recover from them.

The third priority is educating dedicated cybersecurity professionals.

Speaking as a computer science professor at College Park, he is appalled that students are required to learn physics, chemistry and mathematics in high school, but the state requires no computer science. Curricula need to be developed down to the middle school because cybersecurity cannot be taught in a vacuum. This would make the general population more aware of cybersecurity needs while grooming a new generation of computer scientists.

He also encouraged contests for computer students, including one that would be Build it, Break it, Fix it, as well as summer camps run jointly by the NSA and NSF.

Finding teachers qualified to teach computer science at the middle and high-school levels is a challenge, he said, which in the long term will require increasing the number of students with bachelor's degrees or minors in computer science and in the short term training teachers to transition to the subject. Retiring computer scientists might want to teach part time.

He said the state should provide incentives for the top computer science students to stay at Maryland schools rather than heading to California or Boston as they do now. At College Park, there now are 2,700 computer science majors, up 150 percent in five years. The university has a 50 to one student/faculty ratio, the highest on campus, compared to an overall campus ratio of 18 to one.

ACES, the only undergraduate cybersecurity honors program, is understaffed and uses adjuncts. Adequate funding is needed to meet the demand at all Maryland universities. He said in Maryland higher education, the term cybersecurity is used too broadly and covers too many things.

It is important to understand from industry precisely what skills are in demand, and then tailor undergraduate education accordingly.

He said the subcommittee studied the role of community colleges in increasing the numbers of cybersecurity professionals, noting a $5 million grant from the U.S. Department of Labor to Maryland community colleges specifically for this. A path for students finishing an associates

degree is needed to transfer to a four-year university or enter the workforce.

More academic research in cybersecurity would improve security as well as help train students at the Masters and PHD levels who will be the ones who launch the next generation of cybersecurity companies and innovations.

Belkis Leong-Hong presentation

Ms. Leong-Hong said her Economic Development subcommittee is looking at cybersecurity as part of the state's economic engine. The state is the epicenter for cybersecurity with federal agencies such as NSA, DISA, CYBERCOM, among others, located here, as well as top academic institutions. Many industries that support these agencies are here.

Compared to other industries, cybersecurity is still in a young stage, which means it has high energy, entrepreneurship, innovation, initiative and excitement. It is also trying to find roots and definitions in several areas. Maryland hopes to become the Silicon Valley of cyber.

Recent attacks have not only highlighted vulnerabilities of the state's computer systems, but also some new fields that need attention, such as forensic sciences.

The state's Department of Commerce has been active in recruiting businesses, as are county and regional organizations and the Tech Council of Maryland, the Board of Trade and the Chamber of Commerce. The Innovation Marketplace in partnership with Maryland companies and the National Center for Excellence in Cybersecurity have also created excitement in the industry.

The subcommittee is examining how to ensure access to capital for these start-up companies, how to satisfy the needs of entrepreneurs, and how to assure access to leadership and to employees.

One problem is that the technology transfer rate from university research to commercial development is very low. Some academic institutions have created mentorship programs that help get ideas from the university to the marketplace. More research needs to be done on how to create an ecosystem where cybersecurity businesses can grow, including tax credits for investors, and education or apprenticeship incentives.

Among the subcommittee's recommendations is the creation of a reasonable standard of security in protecting in-state businesses from compromise. It would include using external communication channels and emerging technologies, such as artificial intelligence social media, network apps and mobile applications.

The subcommittee also proposed the creation of another cybersecurity accelerator in Maryland similar to the one based in Columbia.

Sue Rogan presentation

The Public Awareness and Community Outreach subcommittee created a timeline and action plan to increase awareness of the council's work; learn and assess the cybersecurity concerns of

individuals, families, communities and businesses; and create a repository of cybersecurity education materials.

The first priority is to design a communications plan for the Council that would include the targeted audience, what are the messages, what are the messaging venues and then implement it.

The subcommittee will look for existing surveys that assess cybersecurity concerns of individuals, families, communities and businesses, and then determine how to use them for its own survey.

The subcommittee also will do a survey of repositories of educational materials to see what already is available and what needs to be created. A quick survey on Google found plenty of available information.

Also to be determined is what agency will host this repository. Most likely the DoIT website would host it.

Susan Lee and Blair Levin presentation

Legislative and policy recommendations include:

Pushing a bill (SB-412) introduced last year to require DoIT to create a statewide information technology master plan to include a cybersecurity framework that was developed by NIST and updated in 2015.

Proposing legislation updating the Maryland Personal Information and PIPA. Lee said it has faced enormous opposition because of a lack of education and awareness of the need to update this law that applied to data breaches of personal information held by commercial entities. It would build on prior legislation to impose additional responsibilities on businesses to protect individuals' private information.

Proposing legislation that provides incentives to private parties to go after bad guys. This would require creation of a civil cause of action for remote intrusions.

Providing incentives for businesses to comply, which could be tricky because so many of the important entities are multi-state.

Since there usually is a freeze of credit when there is a breach, the question is what's the appropriate relationship between credit-reporting agencies and customers. While legislation has been proposed to prohibit a credit agency from charging a fee during a freeze, the subcommittee is trying to figure out the right balance.

The subcommittee also is working on determining whether the attorney general should issue a periodic report summarizing data breaches as part of public education. It also is discussing what constitutes reasonable security procedures, which could help immunize a company that meets those procedures from lawsuits if there is a breach.

Finally, there is a need for an entity on a state basis akin to the federal digital service corps. This would provide the talent and special skills needed in the face of an emergency. It is possible to create something with a reserve pool of talent that can be called up when necessary. The subcommittee is looking into empowering the Secretary of Information Technology to propose a plan to create something similar to a first responder cybersecurity reserve.

Ms. Hurley said the interim reports due May 27 would be circulated to council members for their feedback.

Meeting adjourned at 11:57 a.m.