Summary
Maryland Cybersecurity Council Meeting
October 25, 2017
10:00am

The insecurity hanging over affected people has no end date since the information cannot be put back into the box. This could be more than an inconvenience for consumers—especially those on fixed incomes—who may be paying for freezes and thaws throughout their lives.

The call centers established by Equifax are inadequate and present a barrier to relief by older citizens who do not have or use computers.

2. The Governor's Executive Order on Cybersecurity. The Attorney General noted that the executive order instructs the Office of Homeland Security to create a cybersecurity plan and stated that the Council will work cooperatively with OHS to create the best possible product for Maryland.

3. The foreign interference with US elections and Maryland election security. The Attorney General observed that this of course is a concern for everyone. While he cannot judge whether the efforts made by the State Board of Elections are the right efforts, he was convinced that it understood the challenges and was making a good faith effort to address them. He indicated that SBE would make a presentation at the January meeting of the Council.

In response to the Attorney General's comments, Mr. Brian Israel remarked that a key strength of Maryland's election process is the use of the paper ballot that should be preserved.

Subcommittee Reports

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee

Senator Lee indicated that both she and her co-chair, Mr. Blair Levin, had a number of meetings with the subcommittee that produced a robust roadmap for the upcoming year:

Cyber First Responder Reserve. *July 2017 Activities Report*, (p. 10). The subcommittee will aim to complete its research on this recommendation and to offer a proposal this session or next that might be useful to the executive branch as it begins to implement the governor's recent executive order on cybersecurity.

Legislation to create a civil cause of action for unauthorized computer intrusion (p.11). The subcommittee believes that the common law remedies are not effective as indicated by court decisions in other states.

Legislation to extend the no-charge credit freeze option (p.11) in the 2017 law to minors and to eliminate the charge for corresponding thaws. Senator Lee noted that the importance of the 2017 legislation is underscored by the Equifax breach.

Legislation to encourage the adoption of the NIST Framework in the State IT Master Plan (p. 12).

Legislation that would extend breach notification requirements to the judiciary and the legislature (p. 20). This proposal would apply to the other branches a duty that already applies by law to the executive branch and to private sector entities.

Legislation to require state procurements to incorporate an independent security review and to certify an appropriate level of security prior to government acceptance (p. 20). The subcommittee recognizes that the similar legislation pertaining to procurement by the national government is likely to pass the US Congress.

Legislation that would require ISPs to have a consumer’s express consent to sell their browsing history (p. 20). The subcommittee is mindful that Minnesota already has enacted legislation to this effect, that other states are likely to follow, and that such a requirement is necessary to give consumers control over potentially very sensitive information.

Legislation that would make extortion through ransomware a crime and levy increasingly heavy penalties, depending on harm caused (p. 20).

Background research that would inform legislation requiring consumer labeling indicating the security level of IoT devices (p .21). al d6 TD(hefonati-15.84.)-qua -15.88T12 jud4(s)-10

about $3.8 million. He noted that next budget ask would be $10 million, with the normal uncertainty around the outcome. The Attorney General asked Secretary Leahy if he would welcome an endorsement from the Council of the funding levels DoIT believes it needs for cybersecurity. The Secretary indicated that such would be very helpful, adding that in looking at other states, like Arizona and Oklahoma, he thought it might be possible to ramp up quickly for less than their initial estimates.

Senator Simonaire referenced the fact that some state agencies had been holding more personal identifying information (PII) about Maryland citizens than necessary and asked Secretary Leahy what role DoIT has across the executive branch in data governance, monitoring of networks across state agencies, and training of agency staff. The Secretary stated that DoIT's mandate is to standardize data governance across all agencies and to bring agencies into a true enterprise system. To the extent that agencies do not come into that system, he emphasized that they would be held to the same baseline security required of everyone else. With respect to the security of PII in particular, he underscored the seriousness of that responsibility and that DoIT was taking active steps to address it. Finally, he answered that DoIT does offer training and that some agencies have availed themselves of it.

Mr. Levin asked Secretary Leahy, if he thought he could accomplish his goals with less than the figures suggested, then what investment would be necessary over one or two years to raise the level of state capabilities and what would be the sustainment budget in the succeeding years? The Secretary answered that a foundational investment over one or two years would be necessary. He explained that he thought the cost of that investment could be brought down by leveraging the experience of other states and consolidating the licensing of security tools used by different Maryland agencies, for example. He mentioned that timing was important and that it would be better to have the executive branch on one enterprise system so that solutions can be global and economies of scale achieved rather than taking a piecemeal approach.

The Attorney General reiterated that the question of the state's cybersecurity budget could be one on which the Council might be helpful. Understanding that the Secretary would recuse himself, the Attorney General asked whether any of the other Council members had any objection to writing a letter to the Governor recommending increased funding for the DoIT's cybersecurity budget. Hearing none, the Attorney General asked Dr. von Lehmen to draft a letter to that effect and to circulate it to the Council for comment.

Mr. McCreedy commented that he hoped due consideration would be given to the cybersecurity capabilities of Maryland firms to assist the state rather than defaulting to large out-of-state vendors. Mr. Abeles mentioned the Continuous Diagnostics and Mitigation Program (CDM) of the federal government and asked whether the state could participate in that program to access the tools that it makes available.

Council's letter to the Governor reference not only the initial investment but also the importance of sustainment funding since security tools are expensive to run.

Professor Michael Greenberger, Critical Infrastructure Subcommittee

Professor Greenberger noted that the subcommittee had executed on Recommendations 8 and 9 in the last year, as captured by the *July 2017 Report*. Specifically, it assembled an initial collection of resources and best practices for infrastructure owners (Recommendation 8) and similarly compiled the latest information about the conduct of risk assessments to be made available to critical infrastructure stakeholders to encourage risk assessment (Recommendation 9). He noted that all these materials would be hosted in a repository on the Council's website. H3(e)4(ndl)-2(s pra)4gs(a)4(ptu3)6(ha1)4(d)-9(e)4(x)-9(e)4(c)4(uted on R)6(not72-9ha)4(t 7Ar8)-4(va)4(i the)

Professor Jonathan Katz, Education and Workforce Development Subcommittee

Professor Katz provided a summary of closed items and open items from the original six recommendations of the subcommittee:

Recommendation 10 (Basic Cybersecurity Education). Professor Katz noted that there were many efforts already underway in the state and nationally that intersected with Maryland. For this reason, the item was closed in the July 2017 report as superseded by other developments.

Recommendation 11. Maryland Scholarship for Service Program. The concept is to duplicate the federal scholarship-for-service program and to fund it either by reprogramming state scholarship dollars and/or by recommending new state funding. Professor Katz stated that to advance this recommendation, a meeting with the MHEC Secretary or his staff will be planned.

Recommendation 13. Study of Cybersecurity Workforce Skills and Needs. As part of its due diligence, the subcommittee became aware of a jobs heatmap created by NIST's National Initiative on Cybersecurity Education (Cyberseek) through a grant to Burning Glass and CompTia. The site provides current and very granular information about cyber workforce needs that are keyed to the Cybersecurity Workforce Framework. This item was also closed in the 2017 Report.

Recommendations 12 (Resources for University Computer Science departments) and Recommendation 15 (Increased Funding for Academic Research). Using University of Maryland, College Park, as an example, Professor Katz noted that enrollments in computer science and cybersecurity have grown dramatically and that resources to sustain these programs has not grown accordingly. Classes at the senior level has as many as 80 to 100 students. To shed light on this issue, as well as greater support for cyber research by the state, the subcommittee is considering studies that would compare Maryland with what other states are doing.

Recommendation 14 (Transition Path for Community College Graduates). There are universities within USM that have articulations in cybersecurity with community colleges. But this does not seem to be the case for the more technical programs in the field. The subcommittee has become aware of a pilot effort to create such a pathway and is in discussion about how to support this effort.

Senator Simonaire noted the efforts of his employer, Northrop Grumman, to support K-12 cybersecurity education. He asked Dr. Katz if he knew of other firms that did this and whether there is any effort to educate younger students about how their behaviors can affect their ability to get a security clearance. The Senator noted that many cyber jobs require such clearances. Professor Katz was sure other firms are involved in supporting K-12 computer science and cybersecurity education but was not aware of a list of such firms. As someone who has held a clearance, he agreed completely with the importance of security clearances in the field. Mr.

Israel shared that a Maryland firm, LifeJourney, is a platform about cybersecurity job roles that serves many schools. It incorporates an exercise that shows students how their digital footprint

Mr. Wilson used a 2014 incident in Centerville Louisiana to illustrate that first responder cyber vulnerabilities are not hypothetical. In this case, social media and fake news were orchestrated to create a perceived local emergency and to provide false instructions to the local population. The result was general confusion and hours of effort by local authorities to bring the situation under control. He noted that the attack was traced to an adversary nation state. Given what the nation has seen more recently in disruptive DDoS attacks and major intrusions, the scenarios can be much worse.

Mr. Wilson then discussed some of the first-responder vulnerabilities and the reasons for them. The fundamental problem is that local jurisdictions do not have the staff, the expertise, or budget to keep their networks secure or to defend against an attack. The normal ways in which everyone operates create other vectors for attack. For example, responders keep names and numbers of other responders on their cell phones, which can easily be harvested for misuse in a future emergency. That emergency could be something as normal as a winter snowstorm or it could be something that is orchestrated and is much more threatening.

He suggested several steps that could improve the level of security beyond the cyber workforce development efforts already underway in the state:

Bring the issue of network and communications vulnerability into discussions with state and local responders.

Introduce failed networks into exercises that state and local responders do each year so that the vulnerability is recognized and resiliency can be practiced.

Amend Section 508 (Senator Amoss Fire Apparatus Funds) so that monies from the fund can be used for network security improvements. There are two approaches for getting better security. One is for localities to contract with one or more private vendors. The other, now being tried in some states, is to create a state-level public service network that local jurisdictions could buy into and use in lieu of their own networks.