Maryland Cybersecurity Council

Initial Activities Report

July 1, 2016

Table of Contents

Higher Education:

- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland
- Jonathan Katz, PhD, Director, Maryland Cybersecurity Center and Professor, Department of Computer Science, University of Maryland, College Park
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Patrick O'Shea, PhD, Vice President and Chief Research Officer, University of Maryland, College Park
- Anton Dahbura, PhD, Executive Director, Information Security Institute, Johns Hopkis HatTT0 1 Tf 3 Tr 12 0 0 12 34pn1s1.5 0 Td [(Patrick O* (Ji>BDC /TT3 1 Tf -1.5 -

Federal Institutions:

- Judith Emmel, Associate Director, State, Local, and Community Relations, National Security Agency
- Donna Dodson, Director, National Cybersecurity Center of Excellence, National Institute of Standards and Technology

State Institutions:

- David Garcia, Secretary of Information Technology, Maryland Department of Information Technology
- Col. William Pallozzi, Secretary of of Standa8t Dodson, Director, National Cybersecurity Center

IV. Council Structure

The Maryland Cybersecurity Council is organized into the following subcommittees:

Law, Policy and Legislation Subcommittee

Subcommittee Objectives

- Examine and identify inconsistencies and gaps between State and Federal laws regarding cybersecurity; recommend any new legislation needed to address identified inconsistencies/gaps
- Recommend any legislative changes considered necessary by the Council to address cybersecurity
- Review cybercrime statutes and make recommendations for improvements thereto

Subcommittee Members

- Co-Chair: Susan C. Lee, Senator, Maryland General Assembly
- Co-Chair: Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution
- Joseph Morales, JD, Attorney, Maryland Hispanic Chamber of Commerce
- Pegeen Townsend, Vice President, Government Affairs, Medstar Health
- Howard Feldman, JD, Attorney, Whiteford, Taylor & Preston
- Ned Carey, Delegate, Maryland General Assembly
- Jonathan Prutow, Senior Associate, Aveshka, Inc.
- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland
- Paul Tiao, JD, Attorney, Hunton & Williams

Cyber Operations and Incident Response Subcommittee

Subcommittee Objectives

- Recommend best practices for monitoring and assessing cyber threats and responding to cyber attacks or other security breaches thereto
- Create or enhance shared awareness of cyber vulnerabilities, threats, and incidents within the State
- Recommend best practices for developing comprehensive state strategic plan to ensure a coordinated and quickly adaptable response to and recovery from cyber attacks and incidents[1]

[1] Senate Bill 542 lists the development of a comprehensive state strategic cyber security plan among the deliverables for the Cybersecurity Council. Md. Ann. Code, St. Gov't Art. 9-2901 (J)(6). However, the Council understands that this effort, which includes the review and analysis of highly sensitive and confidential data, has already begun under the direction of the Maryland Department of Information Technology in coordination with other State agencies. The Council will review and/or advise the Department's efforts as appropriate

- Serve as a resource for its expertise to all other subcommittees

Subcommittee Members

- Chair: David Garcia, Secretary of Information Technology, Maryland Department of Information Technology
- Mary Ann Lisanti, Delegate, Maryland General Assembly
- Walter London, Director, Governor's Office of Homeland Security
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Anthony Lisuzzo, Board Member, Army Alliance
-

- Dr. David Anyiwo, Chair, Department of Management Information Systems, Bowie

Economic Development Subcommittee

Subcommittee Objectives

- Promote cyber innovation for economic development, attracting private sector investment and job creation in cybersecurity
- Recommend strategies for increasing cybersecurity research and development funding
- Promote cybersecurity entrepreneurship in Maryland
- Recommend strategies for attracting cybersecurity companies to Maryland
  - attract venture capital
  - valuable tax incentives

Subcommittee Members

- Chair: Belkis Leong-Hong, Founder, President, and CEO, Knowledge Advantage, Inc.
- Jim Dinegar, President and CEO, Greater Washington Board of Trade
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Ken McCreedy, Director, Cyber Development, Maryland Department of Commerce
- Phil Schiff, CEO, Tech Council of Maryland
- Brian Israel, Business Development Executive, Maryland Association of Certified Public Accountants
- Steven Tiller, President, Fort Meade Alliance
- Don Fry, President and CEO, Greater Baltimore Committee
- James Foster, CEO, ZeroFox
- Henry Ahn, Program Manager, Technology Funding Programs, Maryland Technology Development Corp.

Public Awareness and Community Outreach Subcommittee

Subcommittee Objectives

- Promote the CouncilÕs objectives; spread awareness of CouncilÕs cybersecurity efforts and activities
- Learn and assess cyber concerns of businesses, community and individuals so Council can offer information that is relevant, applicable and valued
- Create a depository of cybersecurity awareness information for all, including private and public sectors as well as individuals

Subcommittee Members

- Chair: Sue Rogan, Director, Financial Education, Maryland CASH Campaign
- Catherine E. Pugh, Senator, Maryland General Assembly
- Patrick O'Shea, PhD, Vice President and Chief Research Officer, University of Maryland, College Park

- Anton Dahbura, PhD, Executive Director, Information Security Institute Johns Hopkins University
- Carl Whitman, Vice President, Instructional and Information Technology and Chief Information Officer, Montgomery College
- Jayfus Doswell, PhD, Founder, President, and CEO, The Juxtopia Group, Inc.
- Larry Letow, President and CEO, Convergence Technology Consulting

V. Recommendations

Based on observations and discussions during its first year, the Maryland Cybersecurity Council makes the following preliminary recommendations aimed at protecting the StateÕs critical infrastructure and advancing cyber innovation and jobs in Maryland:

Law, Policy and Legislation

1. Cyber First Responders Reserve

The Council recommends the creation of a cyber first responders reserve, where an appropriate state agency would coordinate with top cyber expert reservists in the event of a cyber emergency. The Maryland Emergency Management Agency (MEMA) appears to be the appropriate agency to lead and coordinate the proposed cyber first responder reserve.

The United States government recently created a digital service corps to facilitate the hiring of digital expertise that was previously difficult to hire. In addition, the federal government and the individual states have a national reserve that can be called upon in the event of a natural or other kind of disaster. Due to the growing threat cyber attacks pose to our welfare, Maryland should also have access to a reserve of digital expertise in the foreseeable event of a cyber emergency. Combining the two ideas (digital service corps and national reserve), Maryland should create a cyber first responders reserve in order to access a reserve of expertise in the event of a cyber emergency.

2. MPIPA Personal Information and Breach/Unauthorized Access Definitions & other Changes

The Maryland Personal Information Protection Act (MPIPA) was enacted t8 >8other

recommended that the ability to freeze oneÕs credit should be well advertised by relevant state government agencies and promoted as a reasonable special safeguard against the financial externalities of identity theft. The key parameters of this legislative proposal are as follows:

a. Prohibiting a consumer credit agency from charging a fee for a placement, temporary lift, or removal of a credit or security freeze when the consumer has been a victim of a data breach
b. Establishing a violation as an unfair or deceptive trade practice
c. While a credit freeze can be necessary to prevent an identity thief from exploiting access to personal information, the consumer should not have to pay the cost of lifting the freeze to be able to have access to credit for a legitimate purpose.
d. The legislative proposal would also detail the information that must be provided to a consumer in the event of a credit freeze.

5. NIST Cybersecurity Framework

The Council recommends that the Secretary of the Maryland Department of Information Technology consider the National Institute on Standards and Technology (NIST) Cybersecurity Framework and other relevant federal guidance and standards when developing or modifying the Statewide Information Technology Master Plan.

6. Maryland Data Breach Report

The Council recommends that the Office of the Attorney General issue a periodic report designed to highlight the preceding yearÕs notable events and trends in data security. The report should be a summary or ÒsnapshotÓ of data security activity and trends relevant to Marylanders to include: data breach statistics; legislative and judicial developments in the area of data security; and best practices for businesses on data breach prevention and response.

over the next year, the Council intends to gather these methods, best practices, and other resources and make them available to stakeholders.[2]

A difficult challenge for conducting risk assessments on critical infrastructure rests on the fact that the majority of critical infrastructure is privately owned. Thus, an owner of that infrastructure now has the ability to ignore government mandates pertaining to risk mitigation. The Council is optimistic, however, that carefully crafted incentives can be used to enlist the private sector in needed risk mitigation. The State should, therefore, gather tools and outline steps and best practices in performing risk assessments and provide them to critical infrastructure owner and other stakeholders.

A recommended set of tools and Òbest practicesÓ for infrastructure protection would include the use by critical infrastructure sectors of the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (the NIST Cybersecurity Framework). Use of this Framework is voluntary, but should be highly encouraged by government. NIST has also developed the ÒGuide for Conducting Risk AssessmentsÓ (SP 800-30), which is a highly valuable resource that critical infrastructure sectors may use. Private sector critical infrastructure owners should also be encouraged to make use of the Critical Infrastructure Cyber Community C Voluntary Program that supports stakeholders in their use of the NIST Framework. Furthermore, the Council recognizes that some suppliers of critical infrastructure may be compelled to adhere to alternative frameworks such as HiTRUST and ISO.

The Federal Department of Homeland Security (DHS) has published general guidance on critical infrastructure security and vulnerability assessments. This information is a good starting point to inform any effort to perform comprehensive and effective risk assessments. Moreover, the following Federal government resources can support vulnerability assessments:

- DHS National Protection and Programs Directorate to inform on internal risk management processes and to provide technical assistance
- DHS Office of Cybersecurity and Communication and its Cyber Resilience Review (CRR) process. The goal of CRR is to understand and measure key cybersecurity capabilities and provide indicators on operational resilience and the ability to manage cyber risk
- Self-evaluation tools, such as those made available through the United States Computer Emergency Readiness Team
- Infrastructure Protection Report Series, available through the Homeland Security Information Network, that identify common vulnerabilities to critical infrastructure by sector and also identify security and preparedness best practices

[2] Senate Bill 542 also requires, for critical infrastructure not covered by federal law or the Executive Order, that the Council actually conduct risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures. See 9-2901 (J)(1). Performing risk assessments, however, is a complicated and costly venture. Without funding, the Council cannot meet this mandate. The Council will focus its efforts on identifying best practices for performing risk assessments of critical infrastructure.

- Training opportunities that include courses on critical infrastructure protection and security

Education and Workforce Development

10. Basic Computer Science and Cybersecurity Education

The Council recommends that the State expand its efforts to develop a pipeline of students interested in cybersecurity by exposing students to computer science in general, and cybersecurity principles in particular, at an early age. It is unacceptable that in 2016 students are required to learn physics, chemistry, and mathematics in high school, but there are still no requirements in place for computer science.

Although cybersecurity is a broad and multidisciplinary field, it is inextricably linked with computer-science education. The State should mandate a basic level of computer-science education for all. The State should also encourage the development of curricula for computer-science education at the middle-and high-school levels, including basic cybersecurity principles. This could be done via a state-federal partnership, in consultation with industry and academia, and by getting the State's P-20 Council to focus on this issue.

Other ways to encourage middle-and high-school students to learn about cybersecurity could include State-sponsored contests focusing not only on attacks, but also on foundational principles for building secure systems in the first place. The Build-it/Break-it/Fix-it contest run by University of Maryland can serve as one possible model for this. Another possibility is to run summer camps such as the GenCyber camps run jointly by the National Security Agency and National Science Foundation in numerous states around the Country. In addition, the State could encourage mentorship opportunities with local industry or State government.

It is a challenge to find enough qualified teachers who can teach computer science at the middle- and high-school level. In the long term this problem can only be addressed by increasing the number of bachelor's degrees, and/or minors, awarded in computer science. In the near term this could be addressed by training current teachers who would be interested in transitioning to the subject, as is done as part of the GenCyber camps mentioned above. The State should also explore training retired computer science professionals to teach, and the Maryland State Department of Education should consider adding M-CERT certification in computer science at the

12. Resources for Computer Science Departments

Sufficient resources must be provided to computer-science departments within the University System of Maryland to ensure they can adequately meet student demand. Currently, demand is far outstripping the available capacity. For example, the University of Maryland, College Park, currently has over 2700 undergraduate computer science majors, a growth of about 150% over the last 5 years. If computer science and cybersecurity are to be a priority for the state of Maryland, sufficient resources must be dedicated within public universities to handle this level of interest.

13. Study of Cyber Workforce Demand and Skills

The term "cybersecurity education" is currently used to mean too many different things, both by educators and by industry, including encompassing very technical skills like penetration testing or reverse engineering to less specialized work in system administration or network management, and even extending to skills in related fields like cybersecurity law. The State should fund a study whose goal is to develop a more fine-grained understanding from industry as well as local/federal government precisely which skills are in demand, and how much demand there is for each skill. This would enable tailoring education in cybersecurity accordingly, and would also allow for better matching of students to open positions.

14. Transition Path for Community-College Graduates

Community colleges can also play an important role in increasing the number of cybersecurity professionals. Of particular note is a $5 million grant awarded by the US Department of Labor to Maryland community colleges to support cybersecurity training, certificates, and associate degrees. The State should focus on developing transition paths for community-college graduates in cybersecurity-related fields who wish to transfer to 4-year universities or the workforce.

15. Funding Academic Research

Academic research also plays an important role in cybersecurity education. Besides the benefits that accrue from the research itself, it also serves as an important component of training students at the Masters and PhD level. These graduates will not only be employed by existing cybersecurity companies, but will also be the ones to form new companies with the next generation of cybersecurity innovations. The State should consider funding academic research in cybersecurity, driven by the cybersecurity needs and challenges of State and local government.

They provide advice, mentoring, and other forms of assistance for businesses in the startup phase, but do so on a compressed timetable. The training could include, for example, advice on team building, business and marketing strategies, and addressing tax and legal concerns. Launching a statewide accelerator, perhaps even one that is a public-private partnership, would expand the number of businesses that could take advantage of the professional support and guidance provided. An accelerator program of this kind should be coupled with incentives to ensure that companies graduating the program remained in Maryland. This would promote economic growth in MarylandÕs cybersecurity industry.

Public Awareness and Community Outreach

17. Cybersecurity Repository

The Council recommends creating an online repository of cybersecurity outreach, awareness and training information available to private and public sectors as well individuals. For maximum impact, this repository should reside within a State agency that has the capacity to maintain and update the information on a regular basis. The Department of Information Technology appears to be the appropriate agency to host and maintain the repository. The key steps needed to create the repository are as follows:

1. Assess existing cyber security awareness repositories, either federal, state or local levels
2. Conduct research of existing repositories and determine how Maryland can use or leverage those resources
3. Assess, using data from the surveys, what information would be valuable
4. Determine what, if any, new materials need to be developed
5. Determine which State agency would host the repository
6. Create a master list of outreach materials/information, including the targeted audienc for the specific information
7. Work with State agency to implement the repository

The online cybersecurity repository and the proposed educational infrastructure have several overlapping goals and, therefore, could be could be a joint project. The Council would work with the selected State agency to implement the repository.

VI. Conclusion

A successful cyber attack against any of MarylandÕs critical infrastructure will almost certainly have catastrophic consequences to the StateÕs economy, vital services, and the public health and safety of its citizens. The State has a responsibility to secure its critical infrastructure as well as the data that has been entrusted to it by their citizens. In this initial report, the Council has proposed several recommendations to improve the cybersecurity of critical infrastructure entities and advance cyber innovations and jobs in Maryland. The Council looks forward to continuing its work and expanding upon these recommendations in its first full report, due to the Maryland General Assembly on July 1, 2017.