SB49__JHU__Carrigan.pdf
Uploaded by: Carrigan, Joseph
Position: FAV

SUPPORT

Joseph Carrigan
Senior Security Engineer with the Johns Hopkins University Information Security Institute

Testimony in Support of

SB 49 State Government – Department of Information Technology - Cybersecurity

Sponsor: Senator Susan C. Lee

Senate Education, Health, and Environmental Affairs, February 2, 2021, 2:00 p.m.

Mister Chair Paul Pinsky, Madam Vice Chair Cheryl Kagan, and Members of the Committee, thank you for the opportunity to speak before you today on behalf of House Bill 235 the Secretary of Information Technology and the Secretary's role in Cybersecurity.

My name is Joseph Carrigan - I am a Senior Security Engineer with the Johns Hopkins University Information Security Institute. I have been working in the technology field for over 20 years. I have worked all over the field. I started at a help desk, I have been a network administrator, a software developer, and a consultant. Throughout my tech career some part of my role included cybersecurity and since 2010, my role has been security focused. I am also the co-host of a popular security podcast produced by The Cyberwire called Hacking Humans.

When we talk about cybersecurity we are really talking about the security of our information. The security of information has three characteristics: availability, integrity, and confidentiality. Availability means that when the data is needed, we can get it. Integrity means that when the data is presented, it is correct. Confidentiality means that the data can only be accessed by people with the authorization to access it.

Over the past few years, we have seen an increasing number of ransomware attacks on governments around the country. Here in Maryland, we are not immune. We are all familiar with the Robinhood attack that crippled Baltimore City in 2019, severely degrading or shutting down government services for months. In March of 2018, Baltimore County's 911 system suffered a ransomware attack and in January 2019 the Salisbury Police Department was the victim of a ransomware attack. Late last year we saw yet another ransomware attack on the Baltimore County Public School network. Ransomware attacks are attacks on the availability of our information and in the case of Baltimore County 911 and Salisbury PD, our services. Damaging an emergency service such as the 911 system leads to increased response times for those services. This literally can be a matter of life and death.

Recently, there has been a disturbing trend among ransomware developers. They are now attacking the confidentiality of data by exfiltrating it to their custody before they encrypt it in place. The ransom demands for these strains of ransomware not only include the offer to decrypt the victim's data but also the promise to not disclose the information they have taken. Victims of ransomware who are refusing to pay the ransom, even if they can easily recover from backups, are now suffering data breaches as a result of the initial infection.

The requirement to secure our data and the systems that store, process, and transmit it is probably self-evident to everyone on this committee. It is important to understand that the protection of our systems will not be a solely technical solution. There is no one product or combination of products you can buy that will protect our data and our systems. One of the key requirements to securing our online assets is

policy. SB 49 provides the beginning of that policy by making it a requirement that the Secretary of Information Technology engage with all part of the state government, county governments, city governments, school districts, and more to develop a "consistent cybersecurity strategy" among those entities.

Years ago when someone would ask me, "Why do cybercriminals do what they do?" I would list out about 4 or 5 reasons. Now, I just respond with one word, "Money." It is important to understand that this is an economic problem. These malicious actors do what they do because they make money when they do it. They do it because it works. They will target whomever they think they can, to make **any amount of money**. You should assume that these actors are rational and will seek to maximize their profits by targeting the most information with the least amount of protection. Too often the target is a state government or a smaller local government.

These forms of governments are targets specifically because they are smaller. Smaller governments may not prioritize resources to cybersecurity, however they still have vast troves of data and systems that provide important services. Consider the amount of data that a school district necessarily keeps about its students. Consider the damage to the public trust that would occur if a malicious actor were to release the data held by a school district or even a single school.

A school district is only one example. There are many examples of data that state and smaller governments keep that is not considered public record. County and state health organizations, and social service data could be damaging if released. Often, citizens do not have an option other than trusting these the state government or smaller organizations with their data. However, they are still entitled to have that data protected and the organizations that hold this information need to have a plan to protect it.

Therefore, I support Senate Bill 49 because it assigns the responsibility of advising and overseeing the development of cybersecurity strategy across the state to the Secretary of IT. Strategy is high level thinking. A cybersecurity strategy would allow government organizations assess risk and prioritize the proper way to protect their data. An example of a strategic policy would be "Organizations will assess the risk of data destruction and data breach by assessing the likelihood and the impact of such events." The Department of Assessments and Taxation might evaluate the strategy by concluding that real estate transactions are a matter of public record. Thus, protecting them from being released would be deemed less important than protecting them from a ransomware attack that effectively destroys them. Conversely, the Prescription Drug Monitoring Program may decide that it would be more damaging to the citizens of Maryland if data were released and less damaging if it were destroyed. A unified strategy and vision for governmental bodies in the state of Maryland would be helpful to make sure that all the organizations are on the same page and know what is expected of them and would demonstrate to the citizens of Maryland that the state government takes the protection of their data seriously.

Foregoing this bill is in my opinion ill-advised. The climate of cyber-attacks is not getting better any time soon and to do nothing is to lay the groundwork for a more incidents like the one in Baltimore County last year.

To the members of this committee, thank you again for the opportunity to provide testimony here today. I encourage a favorable report of Senate Bill 49. Thank you for your consideration.

SB0049-EHE_MACo_SUP.pdf
Uploaded by: Jabin, Drew
Position: FAV

MARYLAND Association of COUNTIES

Senate Bill 49

State Government – Department of Information Technology - Cybersecurity

MACo Position: **SUPPORT**

To: Education, Health, and Environmental Affairs Committee

Date: February 2, 2021

From: Drew Jabin

The Maryland Association of Counties (MACo) **SUPPORTS** SB 49. This bill would require the Secretary of the Department of Information Technology, in consultation with the Attorney General, to develop and promote guidance on consistent cybersecurity strategies for counties, municipal corporations, school systems, and all other governmental entities.

In recent years, there has been an increasing number of ransomware attacks on governments across the United States, including within Maryland. Now, in part due to the COVID-19 pandemic, the need for increased resources to maintain cybersecurity and digital infrastructure are at an all-time high as hackers leverage the pandemic to stage cyberattacks.

SB 49 takes an important step in strengthening the relationship between the Maryland Department of Information Technology and local government information technology officials, without a state-mandated change that would preclude local input. This legislation would allow for local government entities to make the final decision on implementation of cybersecurity-related guidance, allowing counties to maintain their authority while providing a welcome resource.

MACo and county governments stand ready to work with state policy makers to develop cybersecurity strategies and appreciate the addition of language in this year's legislation to avoid putting an expensive, burdensome mandate on county IT operations. Accordingly, MACo urges the Committee to issue a **FAVORABLE** report on **SB 49**.

169 Conduit Street, Annapolis, MD 21401
410.269.0043 BALT/ANNAP ◆ 301.261.1140 WASH DC ◆ 410.268.1775 FAX
www.mdcounties.org

Lee_FAV_SB49_2021.pdf
Uploaded by: Lee, Susan
Position: FAV

Susan C. Lee
Legislative District 16
Montgomery County

Majority Whip

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

February 2, 2021

Senate Education, Health and Environmental Affairs Committee

Senate Bill 49 – State Government - Department of Information Technology - Cybersecurity

Senate Bill 49 is inspired by a recently passed North Dakota law that provides local government entities with strategic cybersecurity planning support from the State Department of Information Technology. The former Maryland Chief Information Security Officer brought up this proposal at a Cybersecurity Council meeting over the interim, and the body, composed mostly of cybersecurity experts, has endorsed the concept. We have made this easy for you this session, as this bill is amended as it passed the House last year, and would now simply require additional manuals be printed for local government entities and allow them to discover what they don't know themselves, without a mandate. Unlike the Council bill that this committee recently passed for the Department, this bill puts more tailored resources into the hands of local governments that are the top targets over the past years, from Baltimore City Police, Baltimore City, Baltimore County Public Schools, and even the local states attorney's offices. We can't neglect these institutions that are a critical part of our state tapestry of government services.

In the long run, an ounce of prevention is worth a pound of cure, as Benjamin Franklin said when referring to the need for a fire department and standardized equipment. This quote is apt today in the context of cybersecurity. with the need for a public expense to prevent a worse unmitigated situation. Today, we must prepare for and respond to the digital fires that target governmental entities with a coordinated and uniform approach that mirrors best practices and prevents worse outcomes upfront, rather than scrambling on the back end to coordinate a response amidst the chaos of a disruption and its aftermath.

Please read the fiscal note of this bill, as it has changed from last year's version. We have won the implicit support of the local school systems, MML, and are willing to work with the institutions of higher education to make sure this is a base and not a ceiling for their cybersecurity strategies. Implementing

and regulating would be in the hands of the entities themselves. DoIT would merely support the design of and sign-off on the plans.

Maryland law requires towns, school districts and counties to prepare for fires and to have adequate fire extinguishers and sprinklers in place to mitigate tragedy, but we don't adequately prepare to confront foreseeable cyber disasters. All levels of our government must be equipped with the knowledge and tools to fight and prevent digital attacks and mishaps from becoming life threatening disasters. Government has a duty to deliver services to citizens without interruption from foreseeable circumstances like cyber disruptions. Our legislative offices get the fire manuals, and our local governments should get the cybersecurity manuals, which should also be tailored to their specific needs, and limited resources.

For these reasons, I respectfully request a favorable report on SB 49.

SB49_USM_FWA_EISMEIER.pdf.pdf
Uploaded by: Eismeier, Michael
Position: FWA

Senate Education, Health, and Environmental Affairs Committee
Senate Bill 49
State Government - Department of Information Technology - Cybersecurity
February 2, 2021
Support with Amendment
Michael Eismeier
Assistant Vice Chancellor for IT and Interim CIO

Chair Pinsky, Vice Chair Kagan and committee members, thank you for the opportunity to share our thoughts on Senate Bill 49. Senate Bill 49 expands the responsibilities of the Secretary of Information Technology to include (1) advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy and (2) in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions under the control of the governing boards of the public institutions of higher education, counties, municipal corporations, school districts, and all other political subdivisions of the State.

The University System of Maryland (USM) has developed cybersecurity policies and procedures appropriate for higher education institutions that may differ considerably from the state agency environment. Although these protocols maintain a functional compatibility with state cybersecurity policies and procedures, the research-intensive environment of our institutions demand protocols that may be unfamiliar to state information technology managers.

Systemwide policies are vetted through the Board of Regents (BOR) approved Cybersecurity Standards under the advisement of the Office of Legislative Audits – the same standards against which the USM is audited. USM utilizes the same National Institute of Standards and Technology (NIST) framework that the state has used. Additionally, USM technology managers are rewriting version 5 of our standards to adopt more advanced NIST and federal practices.

Senate Bill 49 would require that USM institutions adhere to a one-size-fits-all set of policies and procedures administered by the Secretary of Information Technology. However, the USM has deployed cybersecurity best practices tailored to meet the diverse mission of each institution. Adherence to DoIT's IT Security policies and protocols will have a crippling financial impact on USM, particularly at our largest institutions like UM College Park and UM Baltimore and Regional Higher Education Centers (e.g. Universities at Shady Grove), in order to become compliant with both USM and DoIT policies. Doing so would likewise, provide no additional value to USM in terms of its cybersecurity posture. It is our desire to retain our autonomy. The USM respectfully requests an amendment to be excluded from the requirements called for under Senate Bill 49.

Thank you for allowing the USM to share these concerns regarding Senate Bill 49.