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.