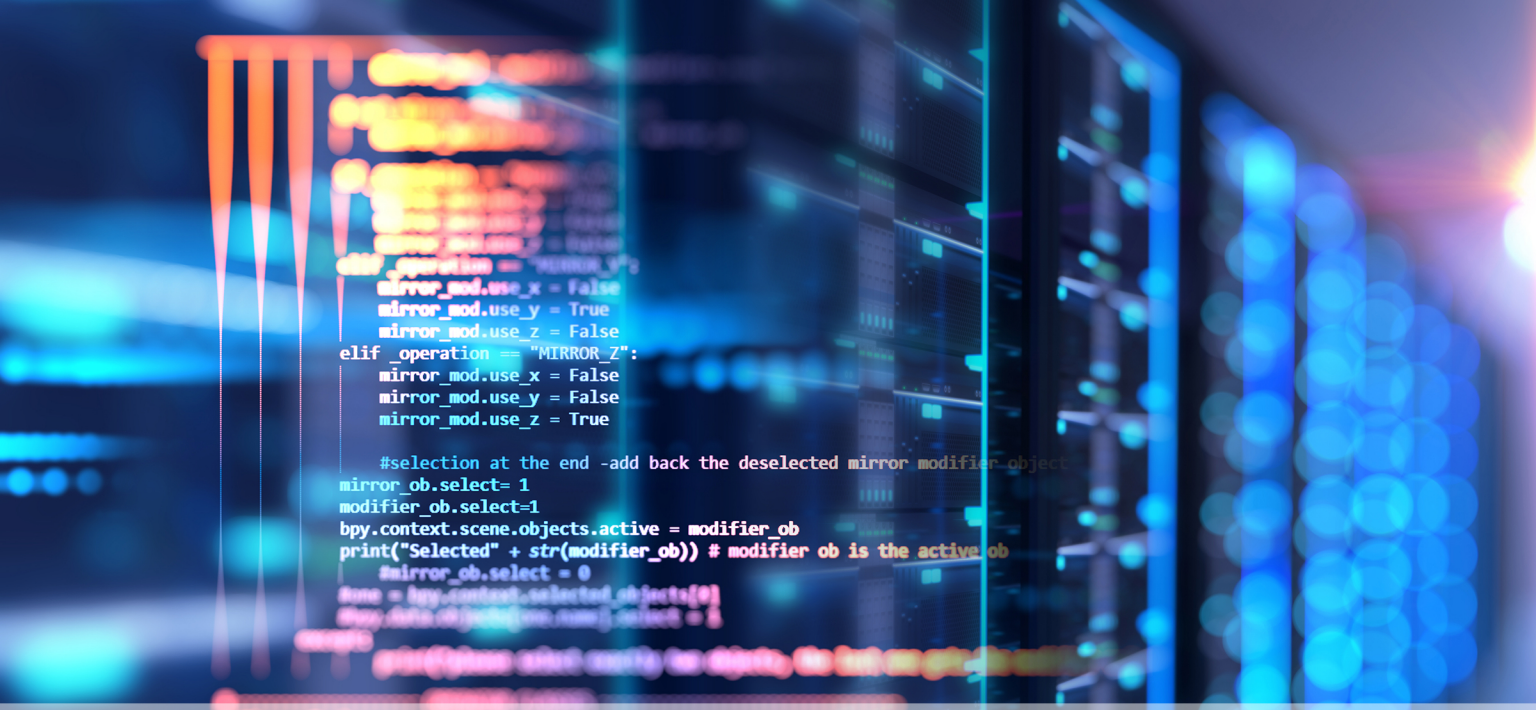

MARYLAND CYBERSECURITY COUNCIL ACTIVITIES REPORT

2021-2023

CONTENTS

Statutory Requirement

This is the fourth biennial activities report of the Maryland Cybersecurity Council covering FYs 2022 and 2023. The report is required by SB 542 (2015). Md. Ann. Code, St. Gov't Art. § 9-2901 Section 3.[1] All Council reports, the Council's membership, its plenary and subcommittee meeting minutes, and various cybersecurity resources for consumers and small- and medium-size businesses may be found on the Council's website at https://www.umgc.edu/mdcybersecuritycouncil.

[1] Section K states that "beginning July 1, 2017, and every two years thereafter, the Council shall submit a report of its activities to the General Assembly in accordance with § 2–1246 of this article".

Executive Summary

We can build a more secure, resilient, privacy-preserving, and equitable ecosystem through strategic investments, and coordinated, collaborative efforts.

--National Cybersecurity Strategy[2]

Cybersecurity risk is a shared challenge involving the private sector, federal, state, and local jurisdictions, and individual consumers. The risk is shared not simply as a common experience, like credit card fraud, that has affected so many individuals. Rather, it is shared as a mutual dependency. A breach of one organization can expose many individuals to identity theft, extortion, or other related harms. The cascading effects of a successful critical infrastructure breach can disrupt an entire nation. Shared risk means that each participant has a stake in the other's cybersecurity.

The Maryland Cybersecurity Council collaborates on cybersecurity issues, sponsors research, and recommends cyber-related policies for legislative consideration, among other outcomes. Established by statute and chaired by the Attorney General, the Council's membership is broadly representative of Maryland government and civil society—business, education, nonprofits, and consumer interests. By design, it instantiates the recognition that reducing cybersecurity risk shared across sectors in Maryland is best served by convening a broadly representative stakeholder group to address the challenges.

Cybersecurity Risk & The Council's Activities for the Biennial Period

Over the last two years, the Council has focused on cybersecurity risk as pertaining to Maryland consumers, state and local government, critical infrastructure, and workforce development. The Council has played a role—sometimes a significant one—in identifying policy recommendations to reduce risk, and its members have been active in supporting efforts to implement these in law. The Council's efforts have also extended to other activities. All of these, legislative and otherwise, are highlighted below.

Consumers. For context, according to one of the most comprehensive datasets that tracks cybersecurity events,[3] there were well over 1,200 reported breaches of organizations in the US since July 1, 2021. For the 2022 calendar year, the Federal Bureau of Investigation reported that Maryland residents and businesses ranked 13th in the nation with internet-related crime losses topping $213 million.[4] These losses include the cost of recovering from data breaches, business email compromise, and identify theft, among others.

---

[2] The White House. (2023*). National cybersecurity strategy*. (p. 23). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[3] University of Maryland CISSM Cyber-attacks Database. Accessed June 15, 2023. https://cissm.liquifiedapps.com/.
[4] Federal Bureau of Investigation. (2023). Internet crime report. (p. 26). https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

- *In 2022, SB 643/HB 962 (Commercial Law – Maryland Personal Information Protection Act – Revisions)*[5] became law. The bill was proposed by two Council members, then-Senator Susan Lee and then-Delegate Ned Carey. It was consistent with a Council recommendation, shaped by input from Council members, and actively supported by them during the legislative session. The bill enhances the ability of consumers to be proactive in protecting themselves after a breach. It expands the number of personal information categories for which a breach notification must be made under law and shortens the notification period, among other changes.

- *House Bill 807/Senate Bill 698 (Online and Biometric Data Privacy)*[6] was a significant 2023 bill that would have accomplished two major objectives. It would have greatly expanded consumer control over the collection and use of "sensitive information" collected about them and their children by commercial entities. It would also have established a task force to make further privacy-related recommendations to address a range of questions, including the knowledge standard applicable to social media platforms in enforcing their user age restrictions. While the bill remained within committee this year, some version will likely be proposed in 2024. Noteworthy is that the bill was supported by five convenings by the Council's Ad Hoc Subcommittee on Consumer and Child Privacy during the summer of 2022 and the resultant staff report. The Subcommittee was chaired by then-Senator Lee, and the bill was proposed by Senator Malcolm Augustine and Delegate Sara Love. Representatives from the Office of the Attorney General, Ad Hoc Subcommittee members, and the Council staff provided favorable testimony during the legislative committee hearings.

- The Council sponsored two open webinars to raise consumer awareness of cybercrime and the remedies available for victims. Supported by the CASH Campaign, a Council member, these webinars ran on October 24, 2022, and November 14, 2022, and included then-Attorney General Brian Frosh and Joe Carrigan, Senior Security Engineer, Johns Hopkins University Information Security Institute.

State and Local Government. During the last two years, Maryland state and local jurisdictions have been targeted by malicious cyber actors. Widely reported and the focus of hearings by the General Assembly, the Maryland Department of Health suffered a significant ransomware attack in December 2021, severely impacting the capacity of both the agency and its 24 local partners to provide services.[7] In November 2022, Washington County reported a "disruption to certain computer systems, including the county's website and some services" and noted that the "disruption was affecting some capabilities at the Emergency Communications Center".[8]

---

[5] Ch. 503, Acts of 2022 (SB 643/962). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0643/?ys=2022rS.

[6] 2023 Reg Sess. at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0807.

[7] Gaskill, H., & DePuyt, B. (2022, January 12). A Month after cyberattack, health officers and lawmakers detail continued outages. Maryland Matters. https://www.marylandmatters.org/2022/01/12/a-month-after-cyberattack-health-officers-and-lawmakers-detail-continued-outages/.

[8] Cyber Attack Archive. Cybersecurity incident' disrupts Washington County website, some services. *Seculore Solutions*. Retrieved May 16, 2023, from https://www.seculore.com/resources/cyber-attack-archive/maryland.

Similarly, during the period of this report, compromises with varying impacts were announced by Prince George's County,[9] Worchester County,[10] the Baltimore City State's Attorney Office,[11] and Leonardtown.[12]

Three bills were proposed as a package by Senator Hester and then-Delegate Pat Young in the 2022 session to address cybersecurity challenges across Maryland state and local government. All three bills were passed by the General Assembly and signed into law by Governor Wes Moore. These bills were *SB 812/HB 1346 (State Government - Cybersecurity - Coordination and Governance),*[13] *SB 754/HB 1202 (Local Government Cybersecurity Coordination and Operations (Local Cybersecurity Support Act of 2022*)),[14] and *SB 811/HB 1205 (State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022*).[15] These bills embodied most of the recommendations of an ad hoc committee co-chaired by Senator Hester and Ben Yelin, Program Director for Public Policy and External Affairs at the University of Maryland Center for Health and Homeland Security.

Governor Moore included funding for cybersecurity in response to this legislative package as part of the Administration's strong mandate to rebuild Maryland's government to full capacity. Specifically, the 2024 budget included $152 million for continued support of cybersecurity assessments and remediation and to support the implementation of major cybersecurity legislation passed during the 2022 session. Other investments in the FY2023 budget include "$17 million for the Local Cybersecurity Support Fund administered by the Maryland Department of Emergency Management and $4 million and 20 positions in the Department of Information Technology to support the implementation of the cybersecurity legislation."[16]

The bills are as follows:[17]

- *SB 812/HB 1346 (State Government - Cybersecurity - Coordination and Governance)* significantly enhances the capacity of state government to (a) manage its IT infrastructure

[9] Chasen, R. (2021, December 14). Prince George's government affected by ransomware attack. *Washington Post*. https://www.washingtonpost.com/dc-md-va/2021/12/14/prince-georges-ransomware-attack/.
[10]Kinnally, K. (2022, May 4). Worcester implements new safety measures after cyber breach. *Conduit Street*. https://conduitstreet.mdcounties.org/2022/05/04/worcester-implements-new-safety-measures-after-cyber-breach/.
[11] Mann, A. (2022, February 25). Baltimore state's attorney has twitter account hacked, recovered. *Baltimore Sun*. https://www.govtech.com/security/baltimore-states-attorney-has-twitter-account-hacked-recovered.
[12] Velazco, C., & Ler, R. (2021, July 8). Shut down everything': Global ransomware attack takes a small Maryland town offline. *Washington Post*. https://www.washingtonpost.com/technology/2021/07/08/kaseya-ransomware-attack-leonardtown-maryland/.
[13] Ch. 242, Acts of 2022 (SB 812/Hb 1346). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0812/?ys=2022rs.
[14] Ch. 241, Acts of 2022 (SB 754/HB 1202). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0754?ys=2022RS&search=True.
[15] Ch. 243, Acts of 2022 (SB 811/HB1205). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB1205?ys=2022RS&search=True
[16] Maryland Department of Management and Budget. (2023). *Budget Highlights: Fiscal Year 2024*. (Page 25). https://dbm.maryland.gov/budget/Documents/operbudget/2024/proposed/FY2024MarylandStateBudgetHighlights.pdf.
[17] The summary that follows is drawn from Department of Legislative Services (2022*), 90 day report* (A-19, C-31-33; C-29, C-33, D-1: C-20, C-31, C-33-34). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.

and cybersecurity risk by moving the Executive Branch toward a centralized cybersecurity model, and (b) assist local units of government improve their cybersecurity posture and resiliency. Among other things, the bill codifies and expands the Maryland Cyber Defense Initiative,[18] establishes reporting requirements of state agencies and local governments, mandates that each unit of state government complete an external assessment at least biennially, and requires the Office of Security Management (OSM) within the Department of Information Technology (DoIT) to assist each unit in remediating any findings.

- *SB 754/HB 1202 (Local Government Cybersecurity – Coordination and Operations (Local Cybersecurity Support Act of 2022))* confirms and enhances the role of the Maryland Department of Emergency Management (MDEM) in working with DoIT to strengthen the cybersecurity of local units of government. It establishes the Cybersecurity Preparedness Unit (CPU) in MDEM and the Information Sharing and Analysis Center in DoIT. It also requires local governments (other than municipalities) to, in a manner and frequency established by DoIT, create cybersecurity preparedness plans, complete assessments, and report local cybersecurity incidents. Units of local government that use the state-operated broadband network are also required to certify to DoIT their compliance with the Department's established minimum standards.

- *SB 811/ HB 1205 (State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)* provides for the development of a strategic investment plan to replace large, vulnerable Executive Branch legacy systems serving state agencies and citizens and includes requirements for enhanced cybersecurity practices of certain public water systems. Specifically, the bill establishes an independent Modernize Maryland Oversight Commission to make "periodic recommendations on investments in State IT structures" and "advise the Secretary on a strategic roadmap with a timeline and budget that will (a) require the updates and investments of critical IT and cybersecurity systems to be completed by December 31, 2025, and (b) require all updates and investments of IT and cybersecurity to be made by December 31, 2030." In addition, the bill provides for "the Local Cybersecurity Support Fund to support local government cybersecurity preparedness" and "assist local governments applying for federal cybersecurity preparedness grants." By December 1, 2023, each water and sewer system that serves more than 10,000 users and receives financial assistance from the state must assess its vulnerability to cyber-attacks, develop a cybersecurity plan if one is appropriate, and report statutory recommendations to the General Assembly.

Critical infrastructure. In February of this year, the FBI arrested two individuals on charges of conspiracy to physically disable power substations in the Baltimore area. Similar attacks or planned attacks have occurred in other states. These attacks and others like them "should serve as a harsh reminder of not only the need to increase preventative measures against physical attacks

[18] Executive Order 01.01.2019.07.

on the U.S. grid, but also to remind that the grid remains vulnerable to cyber-attacks".[19] The national government has responded vigorously in recent years with efforts aimed at utilities—electric, pipelines, and water—to enhance their cybersecurity.[20] Nonetheless, significant responsibility remains with the states through their regulatory agencies. Last year, in fact, the Maryland Public Service Commission for the first time issued cybersecurity regulations for utilities serving the state.[21]

- The Council heavily influenced a key statute that was enacted in 2023 that enhances the capacity of the Public Service Commission to engage utilities about their cybersecurity. *The bill was SB 800/HB 969 (Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023*))[22] sponsored by Senator Hester and Delegate Lily Qi. As enacted, it stipulates cybersecurity as a regulatory goal of the Commission, provides for additional staff with expertise in the field, provides for the establishment of minimum cybersecurity standards for covered utilities, increases the frequency of cybersecurity external audits of utilities, and requires the sharing of audit information with the Commission, among other provisions. The bill was informed by: 1) a year-long study of the electric utilities serving Maryland by an NSA employee working in the Office of the Attorney General under the NSA's fellowship program; and 2) a small working group, comprised of members from the Council, with expertise in cybersecurity and the energy sector.

- Apart from its involvement in legislation, the Council has continued to fulfill its responsibilities under SB 339 (Public Safety – 911 Emergency Telephone System) with the Emergency Number System Board (ENSB). The statute requires the ENSB to consult with the Council on cybersecurity standards for the state's NextGen 911 system.[23] The Council's subcommittee has met three times with representatives of the ENSB Standards Committee to understand the NextGen 911 project, to receive updates on the committee's work, and to provide feedback.[24] The Council's role was preserved in SB 633 (Public Safety – 9–1–1

---

[19] Scheffel, P. (2023, March 27). The thwarted Baltimore grid attack is a wake-up call on U.S. grid cybersecurity. *CHHS News & Events*. https://www.mdchhs.com/2023/03/27/the-thwarted-baltimore-grid-attack-is-a-wake-up-call-on-u-s-grid-cybersecurity/.

[20] Easterly, J., & Fanning, T. (2023, May 7). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. *Cybersecurity and Infrastructure Security Agency Blog*. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[21] MD Code Reg 20.06.01.01 - .05 at https://dsd.maryland.gov/Pages/COMARSearch.aspx#Default=%7B%22k%22%3A%2220.06.01.01%22%2C%22r%22%3A%5B%7B%22n%22%3A%22dsdFullTitleName%22%2C%22t%22%3A%5B%22%5C%22%C7%82%C7%82737472696e673b233230202d205075626c6963205365727669636520436f6d6d697373696f6e%5C%22%22%5D%2C%22o%22%3A%22and%22%2C%22k%22%3Afalse%2C%22m%22%3Anull%7D%5D%2C%22l%22%3A1033%7D.

[22] Ch. 499, Acts of 2023 (HB 969). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0969?ys=2023RS..

[23] Md. Code Ann., Pub Safety Art, § 1-309.1 (A), at https://mgaleg.maryland.gov/2019RS/chapters_noln/Ch_302_sb0339E.pdf.

[24] See subcommittee meeting minutes for October 4, 2021 at https://www.umgc.edu/content/dam/umgc/documents/upload/Minutes%20for%20October%204%202021_A.pdf, June 1, 2022 at https://www.umgc.edu/content/dam/umgc/documents/upload/minutes-for-june-1-2022.pdf , and

Emergency Telephone System – Alterations) which became law in 2022.[25] It requires the annual reporting of each county's public service answering point to describe its progress in complying with cybersecurity standards. Where counties are not in compliance, they must submit a remediation plan. For counties that do not comply with the remediation plan, the ENSB may withhold funds.

Risk and the Cybersecurity Talent Gap. The inability of organizations to staff cybersecurity positions contributes to cyber risk in obvious ways. Not only do positions go unfilled, but existing staff experience higher levels of burnout. It also hampers the growth of the cyber sector of Maryland's economy. As with the nation as a whole, the state's public and private sectors have a persistent shortfall in talent needed to fill cybersecurity roles. Maryland employs over 52,700 people in cybersecurity. It is estimated that these employees met only 68% of the state's workforce need.[26]

- In 2023, *SB 801/HB 1189 (Economic Development – Cybersecurity – Cyber Maryland Program)*[27] was enacted. The bill was proposed by Senator Hester and Delegate Catherine Forbes. Consistent with a 2021 Council recommendation,[28] this bill was informed by extensive fact-finding within the Council's Subcommittee on Workforce Development that included presentations by representatives of the US Chamber of Commerce, the Kentucky Chamber of Commerce, Cyber Florida, and the Georgia Cyber Center. In essence, the bill implements the US Chamber's Talent Pipeline Management Model for expanding the cyber workforce in the state. Central to the model is inviting industry with education and training providers to define the skills needed, to develop the training programs to provide those skills, and as practicable, to target training on groups traditionally underrepresented in cybersecurity. The bill assigns administrative responsibility for the program to TEDCO, establishes a CyberMaryland Advisory Board charged with creating a strategic plan, and creates a CyberMaryland Fund from which to support training and education efforts.

- In 2022, *SB 4/HB 24 (Cybersecurity Scholarship Program – Alterations)*[29] likewise became law. Sponsored by Senator Hester and then-Delegate Eric Luedtke, the bill extended the Maryland Cybersecurity Scholarship for Service Program that was established in 2018.[30] In line with an earlier Council recommendation,[31] the purpose of the program is to help Maryland public entities recruit cybersecurity talent. The 2018 bill restricted the service options to cybersecurity-related work roles in units of state government and to teaching positions in public high schools. The 2022 bill expands the eligibility of the Scholarship for Service Program to part-time students. The bill also increases the number and types of public

---

May 5, 2023 at https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees/maryland-cybersecurity-council.

[25] Ch. 349, Acts of 2022 (SB 633).

[26] *Cyberseek (2023). Cybersecurity supply/demand heatmap*. Accessed June 20, 2023. https://www.cyberseek.org/heatmap.html.

[27] Ch. 578, Acts of 2023 (SB 801). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0801.

[28] See Appendix A, 2021 Recommendation 5.

[29] Ch. 208, Acts of 2022 (SB 4/HB 24). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0004/?ys=2022rs.

[30] Ch. 415, Acts of 2018 (SB 204). The bill was sponsored by Senator Bryan Simonaire and then-Senator Lee.

[31] See Appendix A, 2016 Recommendation 11.

entities that can participate in the program as venues where the service requirement can be met.

Looking Ahead

The Council will continue these core activities that it undertakes from year to year: conduct research, engage with the General Assembly to realize Council recommendations of record, and perform public outreach. As part of its research program, Council subcommittees have committed to two particular projects in the next two fiscal years. One of these is focused on the cybersecurity of another critical infrastructure sector (water utilities); the other on consumer cybersecurity hygiene and operational security. Finally, and more generally, the Council has begun to explore the intersection between its charter and emerging issues concerning artificial intelligence (AI) and quantum computing (QC). With the other activities, these are discussed in more detail below.

Introduction

The Council's statutory charge includes both specific responsibilities and a broad mandate to consider emerging cybersecurity issues affecting the state and its residents. The Council is to assess the cybersecurity risk of critical infrastructure in Maryland, assist critical infrastructure entities not covered by Federal Executive Order 13636 to meet federal cybersecurity guidance, encourage and assist private sector firms to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework, identify regulatory inconsistencies between state and federal cybersecurity law that may complicate compliance by Maryland businesses, support the creation of a cybersecurity resiliency plan for the state, and recommend any other legislation to address cybersecurity issues.[32] In pursuing its charge, the Council makes policy recommendations to inform legislation, provides expertise to the General Assembly, undertakes educational and other public outreach initiatives, and fulfills duties required by other statutes.

The Council is particularly fitted for its purposes for several reasons:

- *Its size and stakeholder diversity enable it to capture a broad array of cybersecurity issues affecting Maryland residents.* The Council is based on the "whole of community" approach to cybersecurity. It includes representation from the Governor's cabinet, the State Board of Elections, the General Assembly, critical infrastructure, academia, advocacy groups, and the cybersecurity industry, among other sectors.
- *The Council functions as a convener of expertise to shape its recommendations.* This role is sometimes exercised through the Council's standing subcommittees and more recently through ad hoc subcommittees and working groups. This expertise has come from the Council membership itself, from the organizations it represents, from outside policy groups, and from out-of-state partners willing to share information about their successful initiatives and models. The results have been captured not only in meeting minutes and other documents but in the Council's substantive reports.
- *The inclusion of members of the General Assembly creates a direct bridge for the Council's recommendations into the legislative process*. For most of this biennial period, these members were then-Senator Susan Lee (District 16, Montgomery County), Senator Katie Fry Hester (District 9, Howard and Montgomery Counties), Senator Bryan Simonaire (District 31 Anne Arundel County), then-Delegate Ned Carey (District 31A, Anne Arundel County) and then-Delegate MaryAnn Lisanti (District 34A, Harford County).
- *The Council is able, in various ways, to help shape and support bills that realize its recommendations.* Council members provide subject matter expertise to sponsors and drafters. The Council uses subcommittees and working groups convene stakeholders with a particular interest in bills to collect their input. Finally, individual Council members provide favorable legislative testimony for those bills and recruit others in their networks to do so.

[32] Md. Ann. Code Ann, St. Gov't Art. § 9-2901 (J).

The Council's Organization, Membership, & Staffing

By statute, the Council is chaired by the Maryland Attorney General or the Attorney General's designee(s).[33] It has included 55 other members organized into six subcommittees. The Council's composition reflects a "whole of community" approach to addressing cybersecurity issues.[34] The membership is a mix of statutorily designated and discretionary seats, with appointments reserved for the Attorney General, the President of the Senate, and the Speaker of the House.

Key federal agencies, state departments and agencies, including the Board of Elections,[35] state legislators, and various sectors of the state are represented on the Council: critical infrastructure, higher education, the cybersecurity services sector, small businesses, statewide business and technology associations, and nonprofits. In addition to its appointed members, the Council engages 'contributors' to its work, viz. individuals who are not appointed members but who are willing to offer their time, expertise, and perspective.

The Council typically meets in plenary session three times per year. As part of its ongoing discovery, it dedicates half of its business meetings to presentations by subject matter experts on cybersecurity-related issues. During this biennial period, presenters included:

- Mathew Scholl, Chief, Division of Computer Security, National Institute of Standards and Technology ('The Next Cybersecurity Horizon: The Risks of Quantum Computing and Quantum Resistant Cryptography')
- Shoshana Zuboff, Professor Emerita, Harvard Business School ('The Market and Consumer Privacy')
- The Honorable J. Michael McConnell, former Director of the National Security Agency and Director of National Intelligence ('The National Threat Environment and the Urgency of Cybersecurity Talent Pipeline Development')
- Marcus Sachs, Deputy Director for Research, McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University ('Cybersecurity and the Grid')

During the period of this report, the Council's six permanent and three ad hoc subcommittees met a total of 26 times in public session. As discussed below, their meetings served as a forum for broader stakeholder input informing recommendations and particular bill provisions. As an example, the Ad Hoc Subcommittee on Consumer and Child Privacy used its public sessions to collect input from various presenters over five convenings to inform a staff report that supported legislation proposed in the 2023 session.[36] Likewise, through its subcommittees, the Council has

[33] Ibid, §9-2901 (G).
[34] Ibid, §9-2901 (C) – (F).
[35] SB 281. MD. Ann Code, St. Gov't Art. §9-2901, at https://mgaleg.maryland.gov/2018RS/chapters_noln/Ch_151_sb0281T.pdf.
[36] The presenters included Rob Bonta (California Attorney General), Andrew Kingman (State Privacy and Security Coalition), Irene Ly (Policy Counsel, Common Sense Media), Haley Hinkle (Policy Counsel, Fairplay), Phyllis Marcus (Partner, Hunton Andrews Kurth LLP), Amy Gajda (The Class of 1937 Professor of Law, Tulane University), Bethan Corbin (Senior Counsel, Nixon Gwilt Law), Maureen Mahoney (Director of Policy and Legislation (California Privacy Protection Agency), and Quinn Laking and Nikita Vozenilek (third-year law students at the University of Maryland School of Law).

organized events, such as the consumer-directed webinars, and secured funding to sponsor the original research discussed below.[37]

The subcommittees, their objectives, and their appointed members during all or most of this report period are included in Appendix C.[38]

By statute, the University of Maryland Global Campus is the permanent staffing agency for the Maryland Cybersecurity Council. The university has been designated as a National Center of Academic Excellence in Information Assurance and Cyber Defense Education by the National Security Agency and the Department of Homeland Security, and as a National Center of Digital Forensics Academic Excellence by the Defense Cyber Crime Center Academic Cyber Curriculum.

The Council staff was augmented during the period of this report by an NSA employee who joined the Office of the Attorney General on a full-time basis for one year. Under the scope of work, this employee completed a research report for the Council with recommendations concerning the electric utilities serving Maryland.[39] This arrangement with the NSA was under an external fellowship program that the Agency offers its workforce.

The Council's Activities in Detail

During the period of this report, the Council focused on cybersecurity risk to Maryland consumers, state and local government, critical infrastructure, and workforce development. Most of the Council's work—its recommendations and the supportive activity of its members—was in connection with cybersecurity legislation proposed and largely successful during the 2022 and 2023 sessions. A foundation for this work was accomplished through several research efforts that were sponsored by the Council. It is useful to first highlight those efforts.

Developing Policy Recommendations

During FY 2022 and 2023, more than 80 cyber-related policy recommendations emerged from the Council's subcommittees, working groups, and research reports that the Council sponsored or co-sponsored. As a matter of routine, these activities are briefed out to the plenary Council by the subcommittee chairs at its triannual meetings. These recommendations were in addition to 35 others already on record by the Council as of the last biennial report.[40]

---

[37] The National Cryptologic Foundation and Johns Hopkins University provided grants that funded a cyber hygiene survey of Maryland adults. The survey was conducted under the sponsorship of the Council's Subcommittee on Public and Community Affairs to provide a baseline for public policy discussions within the Council and to inform both its webinar programming and the cyber-related education outreach of the Foundation. The survey implementation was concluded in early 2023 with preliminary analysis reviewed in the subcommittee in May.

[38] With the elections last fall and the change in administrations, a number of members have left the Council to be replaced by new members.

[39] See Corcoran, L. (December 2021) at https://www.umgc.edu/content/dam/umgc/documents/upload/cybersecurity-and-the-maryland-electric-grid.pdf

[40] See Appendix A.

Two Council reports were responsible for two-thirds of the new recommendations and had a significant impact on the particular provisions of bills that became law. These were *Cybersecurity and the Maryland Electric Grid – Findings and Recommendations (December 2021)*[41] *and Maryland State and Local Government Cybersecurity – Analysis and Recommendations (December 22, 2021).*[42] A third work product, *Report of the Ad Hoc Subcommittee on Consumer Privacy (December 19, 2022),*[43] supported a major consumer bill that was unsuccessful in 2023, but will likely be proposed in some form in 2024.

For this research, the Council relied on its existing staff (the December 19, 2022 report), secured additional staff (an NSA Fellow who prepared the December 2021 report), and leveraged its own staff in combination with staff time donated by the Council's member organizations (the December 22, 2021 report).

Informing & Supporting Legislation Consistent with Policy Recommendations

The nexus between the Council and the General Assembly through the Council's legislative members was instrumental in the enactment of seven bills in the last two years that realized policy recommendations the Council produced. An eighth major bill that was staged and supported by a Council ad hoc committee was not enacted but will likely be proposed in some form in 2024. Not only the recommendations but provisions of the bills themselves were often shaped to some degree through discussions within the Council's subcommittees, ad hoc committees, and working groups as reservoirs of expertise. Further, as part of the legislative process itself, individual Council members, other subject matter experts that they recruited, and the Council staff provided briefings to legislators, testimony before committees, and answered questions of legislative committee staff.[44]

The eight bills are summarized below.

Consumer Cybersecurity

The Maryland Personal Information Protection Act (MPIPA) provides in part for notification to consumers in cases when a business confirms a breach of covered personal information that is unencrypted. The notification alerts consumers so that they can increase their operational security. For personal information not included in the statute, there is no legal obligation for a business to provide notice. This can provide gaps in a consumer's awareness of sensitive data

[41] See Corcoran, L., Cybersecurity and the Maryland Electric Grid: Findings and Recommendations for the Office of the Attorney General and the Maryland Cybersecurity Council (December 2021) at https://www.umgc.edu/content/dam/umgc/documents/upload/cybersecurity-and-the-maryland-electric-grid.pdf.
[42] See von Lehmen, G., Stewart, C, and Yelin, B. (December 22, 2022) at https://www.umgc.edu/content/dam/umgc/documents/upload/maryland-state-and-local-government-cybersecurity-analysis-and-recommendations.pdf.
[43] See von Lehmen, G. (December 2022) at https://www.umgc.edu/content/dam/umgc/documents/upload/12192022consumer-digital-privacy-recommendations.pdf.
[44] During this period, the following Council members provided testimony within committee in support of bills incorporating council recommendations: John Abeles, Tasha Cornish, Cyril Draffin, Terri Jo Hayes, and Markus Rauschecker. Report authors Laura Corcoran and Dr. Greg von Lehmen also provided favorable testimony for selected bills.

that is breached. Because technology permits increasing collection and use of sensitive personal information, the Council has an open-ended recommendation on record to update MPIPA as appropriate.[45]

In 2022, Senator Lee and Delegate Carey proposed *SB 643/HB 962 (Commercial Law - Maryland Personal Information Protection Act – Revisions)*[46] which passed the General Assembly and the Governor signed into law. It continued a line of bills over the years that have strengthened MPIPA and the ability of consumers to manage their cybersecurity risk. It adds genetic information to covered personal information for which notification of a breach must be given, shortens the notification period for certain businesses, and expands the types of businesses that must maintain reasonable cybersecurity procedures and practices, among other provisions.[47] The Council's Subcommittee on Law, Policy, and Legislation, co-chaired by then-Senator Lee offered inputs that helped shape the bill.[48]

In 2023, *HB 807/SB 698 (Online and Biometric Data Privacy)*[49] was a major Council-related consumer bill that remained within committee and was not enacted. It would have greatly expanded consumers' control over sensitive information collected about them and their children by commercial entities and would have established a task force to make other privacy-related recommendations, including recommendations to address some of the shortcomings of the federal Child Online Privacy Protection Act (COPPA). The bill was supported by a series of five convenings by the Council's Ad Hoc Subcommittee on Consumer and Child Privacy during the summer of 2022 and the resultant staff report. The Subcommittee was chaired by then-Senator Lee, and the bill was proposed by Senator Malcolm Augustine and Delegate Sara Love. The Office of the Attorney General, Council members,[50] and the Council staff provided favorable testimony during the legislative committee hearings. Some version of the bill is likely to be proposed in 2024.

State and Local Government Cybersecurity

Three bills were proposed as a package by Senator Hester and then-Delegate Pat Young in the 2022 session to address cybersecurity challenges across Maryland state and local government. All three bills were passed by the General Assembly and signed into law by the Governor. These bills were *SB 812/HB 1346 (State Government - Cybersecurity - Coordination and Governance),*[51] *SB 754/HB 1202 (Local Government Cybersecurity Coordination and*

[45] See Appendix A, 2016 Recommendation 2.
[46] 2022 Reg. Sess. at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0643?ys=2022RS&search=True.
[47] Department of Legislative Services (2022), *90 day report* (p. I-3). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.
[48] See the subcommittee's meeting minutes for November 11, 2021 at https://www.umgc.edu/content/dam/umgc/documents/upload/Minutes%20for%20November%2011%202021_A.pdf
[49] 2023 Reg Sess. at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0807.
[50] Markus Rauschecker as a Council member and Robyn McKinney for the CASH Campaign of Maryland, a Council member organization.
[51] Ch. 242, Acts of 2022 (SB 812/HB 1346). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0812/?ys=2022rs.

Operations (Local Cybersecurity Support Act of 2022)),[52] and *SB 811/HB 1205 (State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022*).[53]

These bills were decisively shaped by the Council's aforementioned study, *Maryland State and Local Government Cybersecurity – Analysis and Recommendations (December 22, 2021).* This study was conducted by an ad hoc Council committee approved by then-Attorney General Brian Frosh as Council chair at the request of Senator Hester and then-Delegate Young, co-chairs of the General Assembly's Joint Committee on Cybersecurity, Information Technology, and Biotechnology. In parallel, the Joint Committee staged a series of hearings on cybersecurity during the summer and fall of 2021. The immediate impetus for this effort was the near passage of SB 69 (Cybersecurity Coordination and Operations – Establishment and Reporting) in the 2021 session and an amendment to the bill, proposed in the final moments of the session, that called for a formal study of the state's cybersecurity posture to inform future legislation.

The study addressed three sets of questions posed by the President of the Maryland Senate, Bill Ferguson, and Speaker of the House, Adrienne Jones, concerning state and local cybersecurity. The questions covered governance, Executive Branch agencies, and local jurisdictions. Altogether, the study included 35 recommendations, most of which were included in the three bills and codified into law. To stage the bills prior to session, Senator Hester and Delegate Young arranged for the study and its recommendations to be briefed by the study cochairs and lead authors to the House Appropriations Committee, [54] the House Health and Government Operations Committee,[55] and the Senate Education, Health, and Environmental Affairs Committee.[56] The study cochairs and lead authors also provided testimony during the bills' hearings and participated on subsequent working groups during session that were concerned with the bills.[57]

Governor Moore included funding for cybersecurity in response to this legislative package as part of the Administration's strong mandate to rebuild Maryland's government to full capacity. Specifically, as part of this the 2024 budget included: $152 million for continued support of cybersecurity assessments and remediation and to support the implementation of major cybersecurity legislation passed during the 2022 session. Other investments in the FY2023 budget include: "$17 million for the Local Cybersecurity Support Fund, administered by the Maryland Department of Emergency Management, and $4 million and 20 positions in the

[52] Ch. 241, Acts of 2022 (SB 754/HB 1202). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0754?ys=2022RS&search=True.
[53] Ch. 243, Acts of 2022 (SB 811/HB 1205). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB1205?ys=2022RS&search=True.
[54] January 21, 2022.
[55] January 25, 2022.
[56] January 27, 2022.
[57] The House Health and Government Operations Committee held hearings on February 2, 2022, and the Senate Education, Health, and Environmental Affairs Committee on March 3, 2022. Joint working groups were convened on March 9 and March 17, 2022.

Department of Information Technology to support the implementation of the cybersecurity legislation."[58]

As enacted, the bills are summarized below.

SB 812/HB 1346 (State Government - Cybersecurity - Coordination and Governance) significantly enhances the capacity of state government (a) to manage its IT infrastructure and cybersecurity risk by moving the Executive Branch toward a centralized model, and (b) to assist local units of government improve their cybersecurity posture and resiliency. Among other things, the bill codifies and expands the Maryland Cyber Defense Initiative,[59] establishes reporting requirements of state agencies and local governments, mandates that each unit of state government complete an external assessment at least biennially, and requires the Office of Security Management (OSM) within the Department of Information Technology (DoIT) to assist each unit to remediate any findings.

Independent audits are required of specified units within the Legislative and Judicial branches, the Office of the Attorney General, the Office of the Comptroller, and the Office of the State Treasurer for compliance with specified cybersecurity standards. With the exception of municipal governments, local government entities must consult with their local emergency manager to create or update a cybersecurity preparedness and response plan and complete a cybersecurity preparedness assessment as established by DoIT.

Significantly, the bill provides that the statewide cybersecurity strategy must be funded via appropriations that the Governor must include in the annual budget. This replaces the charge-back model for cybersecurity services provided to state and local government. Following the practice of the federal government, the bill also requires that the Executive Branch publish the ratio of cybersecurity spending to total IT spending as an accountability metric.

DoIT's responsibilities are also expanded "to include (1) centralizing the management and direction of information technology (IT) policy within the Executive Branch under the control of DoIT; (2) ensuring the statewide IT master plan allows a state agency to maintain its own IT unit; (3) developing a statewide cybersecurity strategy; and (4) developing and requiring basic security requirements to be included in state contracts. DoIT is further required to develop a centralization transition strategy and conduct a performance and capacity assessment."[60]

SB 754/HB 1202 (Local Government Cybersecurity - Coordination and Operations (Local Cybersecurity Support Act of 2022))[61] confirms and enhances the role of the Maryland Department of Emergency Management in working with DoIT to strengthen the cybersecurity of local units of government. It establishes the Cybersecurity Preparedness Unit (CPU) in the

---

[58] Maryland Department of Management and Budget. (2023). *Budget Highlights: Fiscal Year 2024*. (Page 25). https://dbm.maryland.gov/budget/Documents/operbudget/2024/proposed/FY2024MarylandStateBudgetHighlights.pdf.

[59] Executive Order 01.01.2019.07.

[60] Department of Legislative Services (2022*), 90 day report* (pp. A-19 and C-31-33). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.

[61] 2022 Reg. Sess. at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0754?ys=2022RS&search=True.

Maryland Department of Emergency Management and the Information Sharing and Analysis Center in DoIT. It also requires local governments (other than municipalities) to, in a manner and frequency established by DoIT, create cybersecurity preparedness plans, complete assessments, and report local cybersecurity incidents. Units of local government that use the state-operated broadband network are also required to certify to DoIT their compliance with the Department's established minimum standards.

Under the bill, the Office of Security Management must provide an annual report to the Governor and specified committees of the General Assembly, which includes OSM's activities and accomplishments from the previous 12 months and a compilation and analysis of the data and information contained in cybersecurity reports received from state and local agencies, as specified.[62]

HB 1205/SB 811 (State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)[63] provides for the development of a strategic investment plan to replace large, vulnerable Executive Branch legacy systems serving state agencies and citizens and includes requirements for enhanced cybersecurity practices of certain public water systems. Specifically, the bill establishes an independent Modernize Maryland Oversight Commission to make "periodic recommendations on investments in state IT structures" and "advise the Secretary on a strategic roadmap with a timeline and budget that will (a) require the updates and investments of critical IT and cybersecurity systems to be completed by December 31, 2025, and (b) require all updates and investments of IT and cybersecurity to be made by December 31, 2030." In addition, the bill provides for "the Local Cybersecurity Support Fund to support local government cybersecurity preparedness" and "assist local governments applying for federal cybersecurity preparedness grants." By December 1, 2023, each water and sewer system that serves more than 10,000 users and receives financial assistance from the state must assess its vulnerability to cyber-attacks, develop a cybersecurity plan if one is appropriate, and report statutory recommendations to the General Assembly.[64]

Critical Infrastructure Cybersecurity

In 2023, Governor Wes Moore signed into law *SB 800/HB 969 (Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)).*[65] The bill was sponsored by Senator Hester and Delegate Qi. Similar to the state and local government cybersecurity bills, this bill was shaped in decisive ways by a Council-sponsored study and a small working group[66] from the Council's Subcommittee on Critical Infrastructure.

---

[62] Department of Legislative Services (2022), *90 day report* (C-29, C-33, and D-1). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.
[63] 2022 Reg. Sess. at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB1205?ys=2022RS&search=True.
[64] Department of Legislative Services (2022*), 90 day report* (pp. C-20, C-31, and C-33-34). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.
[65] Ch. 499, Acts of 2023 (HB 969). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0969?ys=2023RS.
[66] The working group consisted of Council members John Abeles, Cyril Draffin, and Terri Jo Hayes.

The report, *Cybersecurity and the Maryland Electric Grid – Findings and Recommendations (December 2021),* was completed by an NSA Fellow who worked full-time for one year within the Office of the Maryland Attorney General on grid security for the Council. The report made 29 recommendations. The report and its recommendations were shared with the Maryland Public Service Commission (PSC) which had already moved to issue its first cybersecurity regulations effective July 25, 2022.[67] These regulations were previewed to the Council's Subcommittee on Critical Infrastructure at its June 2022 public meeting.[68] The working group of the subcommittee was formed at Senator Hester's request to review the regulations, identify recommendations of the December report that were still relevant, and make other recommendations as needed. Other related Council activity included working group discussion of questions with the Subcommittee on Critical Infrastructure at its October 2022 meeting,[69] participation of Council staff and working group members at a meeting with PSC staff in January 2023,[70] and testimony by working group members and the report author at the legislative committee hearings on the bill.[71] The Council as a whole was apprised of the working group's activity at its October 2022 meeting.[72]

SB 800/HB 969 embodies selected recommendations of the December 2021 report and proposals of the working group, accomplishing a number of things. It makes cybersecurity an explicit regulatory focus for the PSC, requires appointment of staff with cybersecurity expertise, and details various cybersecurity-related requirements for public service companies not including common carriers and telephone companies. Among those requirements, which also apply to municipal electric utility and member-regulated cooperatives, are third party technology assessments to be conducted each year beginning after July 2025. The bill requires the PSC to collect certifications from the assessed entities regarding their compliance with assessment standards and to compile a report for the State Chief Information/Security Officer (CISO). Finally, the bill establishes certain reporting requirements for public service companies for cybersecurity incidents.[73]

Cybersecurity Workforce Development

Senate Bill 801/House Bill 1189 (Economic Development – Cybersecurity – Cyber Maryland Program)[74] was likewise enacted in the 2023 session and signed into law by the Governor. The

[67] Md. Code Regs. 20.06.01.01 – 05 at https://dsd.maryland.gov/Pages/COMARSearch.aspx#k=20.06.01#l=1033.
[68] See the minutes of the June 1, 2022, meeting at https://www.umgc.edu/content/dam/umgc/documents/upload/minutes-for-june-1-2022.pdf
[69] See the minutes for October 20, 2022, at https://www.umgc.edu/content/dam/umgc/documents/upload/recording-of-the-meeting-on-october-20-2022-sci.pdf.
[70] The meeting was held via Zoom on January 6, 2023.
[71] See the March 7, 2023, hearing of the Senate Education, Health, and Environmental Affairs Committee at https://mgaleg.maryland.gov/mgawebsite/Committees/Details?cmte=eee&ys=2023RS&activeTab=divMain and the March 9, 2023, hearing of the House Economic Matters Committee at https://mgaleg.maryland.gov/mgawebsite/Committees/Details?cmte=ecm&ys=2023RS&activeTab=divMain.
[72] See the minutes for October 26, 2022, at https://www.umgc.edu/content/dam/umgc/documents/upload/draft-minutes-for-october-26-2022_.pdf.
[73] Department of Legislative Services (2023), *90 day report* (pp. C-27 and H-10). https://dls.maryland.gov/pubs/prod/RecurRpt/23rs_90_Day_Report.pdf.
[74] Ch. 578, Acts of 2023 (SB 801). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0801?ys=2023RS.

bill was sponsored by Senator Hester and Delegate Forbes. Consistent with a 2021 Council recommendation,[75] SB 801/HB 1189 was informed by extensive fact-finding within the Council's Subcommittee on Education and Workforce Development, chaired by Senator Hester. This fact-finding included presentations by the US Chamber of Commerce about its Talent Pipeline Development Model, the Kentucky Chamber about its experience implementing that model in several sectors of its state's economy, and by CyberFlorida and the Georgia Cyber Center about the workforce development strategies in their states.[76]

The new law provides for the establishment of a cybersecurity workforce development hub in the Maryland Technology Development Corporation (TEDCO), the creation of a "Cyber Maryland Board" to advise on a cybersecurity workforce strategic plan for the state, engagement with industry to identify workforce needs, and the creation of a "Cyber Maryland Fund" for grants to encourage the development of training consistent with the strategic plan. Beginning in FY 2025, the Governor must include in the annual budget bill an appropriation sufficient to support staff at TEDCO to administer the program and may include $250,000 for the Fund.[77]

As is the case with the public sector nationally, Maryland state and local jurisdictions find it difficult to recruit and retain the cybersecurity talent that they need. In 2022, Maryland's existing cybersecurity scholarship for service program was expanded by the enactment of *SB 4/HB 24 (Cybersecurity Scholarship for Service Program – Revisions)*,[78] proposed by Senator Hester and then-Delegate Eric Luedtke. The original program was established in 2018 through legislation proposed by two legislative members of the Council to implement a 2016 Council recommendation.[79] The 2022 changes open eligibility to part-time students to apply for the program under specified circumstances. The revision also increases the number of different public sector positions that can meet the service obligation. Specifically, it adds cybersecurity-related staff roles in county and city governments, law enforcement agencies, public high schools, and community colleges, and cybersecurity teaching positions in community colleges.[80]

Cybersecurity Risk & Other Council Activities

In addition to its legislation-related activities, the Council engaged in other efforts related to consumer risk and critical infrastructure risk.

- The Council's Subcommittee on Public and Community Outreach organized two webinars in the 2021 – 2023 period to raise consumer awareness about cyber crime, highlight risk

[75] See Appendix A, 2021 Recommendation 5.
[76] See subcommittee meeting recording for June 28, 2022; August 25, 2022 at https://www.umgc.edu/content/dam/umgc/documents/upload/8252022-recording-meeting-education-workforce-development.pdf, and October 3, 2022 at https://www.umgc.edu/content/dam/umgc/documents/upload/recording-of-the-meeting-on-october-3-2022.pdf.
[77] Department of Legislative Services (2022). *90 day report* (pp. C-28 and H 19). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf.
[78] Ch. 208, Acts of 2022 (SB 4/HB 24). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0004/?ys=2022rs.
[79] See Appendix A, 2016 Council Recommendation 11. The bill was SB 204 proposed by then-Senator Lee and Senator Simonaire.
[80] Department of Legislative Services (2022). *90 day report* (p. L-20). https://mgaleg.maryland.gov/Pubs/LegisLegal/2022rs-90-day-report.pdf

reduction strategies, and identify where to get help when affected. The webinars were 'Cyber Criminals Are Looking for You' (October 24, 2022) and 'Consumers Lose Millions in Cyber Scams: Don't Be One of Them' (November 14, 2022). These webinars were hosted as a public service by The CASH Campaign. Presenters included then-Attorney General Brian Frosh and Joseph Carrigan, Senior Security Engineer, Johns Hopkins University Information Security Institute.

- As required by a 2019 statute,[81] the Council continued to provide consultation to Emergency Number Systems Board (ENSB) in regard to the cybersecurity standards for the NextGen 911 system. The Council's subcommittee met twice with representatives of the ENSB cybersecurity standards committee to understand the NextGen 911 project, to receive updates on the committee's work, and to provide feedback.[82] The Council's role was preserved in SB 633 (Public Safety – 9–1–1 Emergency Telephone System – Alterations) enacted in 2022.[83] It requires the annual reporting of each county public service answering point to describe the progress in complying with cybersecurity standards. Where counties are not in compliance, they must submit a remediation plan. For counties that do not comply with the remediation plan, the ENSB may withhold funds.

The Next Two Years

The Council will continue the core activities that it undertakes from year to year. It will conduct additional fact-finding, engage the General Assembly to realize its recommendations of record, and perform public outreach. To inform these activities in part, Council subcommittees have committed to two particular projects in the next biennial period. More generally, the Council will consider the intersection between its charter and the technologies of AI and quantum computing.

Of the particular projects, one continues the focus on critical infrastructure. The Council's enabling statute is especially concerned with critical infrastructure "damage or unauthorized cyber access" which could threaten life on a large scale, cause "catastrophic economic damage" or "severe degradation of State or National security".[84] The Cybersecurity and Infrastructure Security Agency (CISA) and others have warned about the targeting of water utilities across the nation.[85] Various reports, including by the utilities' own Water Sector Coordinating Council,

[81] Md. Code Ann., Pub Safety Art, § 1-309.1 (A). https://mgaleg.maryland.gov/2019RS/chapters_noln/Ch_302_sb0339E.pdf

[82] See subcommittee meeting minutes for October 4, 2021 at https://www.umgc.edu/content/dam/umgc/documents/upload/Minutes%20for%20October%204%202021_A.pdf, June 1, 2022 at https://www.umgc.edu/content/dam/umgc/documents/upload/minutes-for-june-1-2022.pdf , and May 5, 2023 at https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees/maryland-cybersecurity-council

[83] Ch. 349, Acts of 2022 (SB 633). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0633/?ys=2022rs

[84] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 Section (J)(2).

[85] See Cybersecurity and Infrastructure Security Agency. (2021). *Ongoing cyber threats to U.S. water and wastewater systems.* (Cybersecurity Advisory No. AA21-287A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a and more recently Woolf, K., & Livingston, B. (2023). Dragos analyzes Russian programs threatening critical civilian infrastructure. *Dragos*. https://www.dragos.com/resource/threat-intelligence-brief-russian-software-programs-threatening-critical-civilian-infrastructure/.

point to the cybersecurity challenges faced by water service providers and the range of cybersecurity preparedness among them.[86] Maryland has suffered at least one ransomware attack on a water utility.[87] Supporting the interest in water service cybersecurity by the Subcommittee on Critical Infrastructure, the Office of the Attorney General has initiated an application for an NSA Fellow to staff a Council report that would provide: (a) insights into the challenges faced by the utilities serving the state, and (b) recommendations practicable within federal regulations and recent state legislation.

The other project focuses on consumer risk. Specifically, it will entail conducting a statewide survey of the cyber hygiene of Maryland adults as an initiative of the Subcommittee on Public and Community Outreach. This is both to inform the subcommittee's program of public outreach and potential policy recommendations by the Council as a whole for enhancing this awareness. While the survey was begun late in this biennial period and a preliminary analysis of the data has been completed and briefed to the Council,[88] the fruit of this research will come in the next two years as the Council more fully digests the results. The survey is supported by grants from Johns Hopkins University and the National Cryptologic Foundation.

The threat landscape is rapidly changing. While AI will produce many benefits, it unfortunately will also be leveraged to more efficiently compromise consumers and enterprises at scale and to create other forms of social disruption. Quantum computing in the not-to-distant future will be able to break current encryption measures putting at risk data held by governments and companies and the security of operational technology. The Council is just beginning to grapple with the impacts of these accelerating technologies on Maryland residents.

Conclusion

By statute, the Maryland Cybersecurity Council embodies a "whole of community" approach to cybersecurity issues affecting the state. Its membership cuts across the public and private sectors. This breadth keeps the Council focused on a range of cybersecurity-related issues important to the state and its residents. These issues concern consumer protection, state and local government cybersecurity, criminal law, cyber education and workforce development, and the economic development of the state's cybersecurity sector. The Council's contribution includes recommendations that inform legislation; public education, outreach, and support activities; and participation in studies that yield insight into ways to further enhance the cybersecurity and resiliency of the state. The Council's meetings are public, and it invites the participation of everyone who has an interest in cybersecurity issues.

---

[86] See Water Sector Coordinating Council. (2021). *Water and wastewater systems: Cybersecurity 2021 state of the sector.* https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf and Montgomery, M., & Logan, T. (2021). *Poor cybersecurity makes water a weak link in critical infrastructure*. FDD (Center on Cyber and Technology Innovation). https://www.fdd.org/wp-content/uploads/2021/11/fdd-memo-poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure.pdf.

[87] WSSC Water 2021, June 15). *WSSC Water investigating ransomware cyberattack*. [Press release]. https://www.wsscwater.com/news/2021/june/wssc-water-investigating-ransomware-cyberattack.

[88] See Appendix B. The preliminary results were briefed to the Council at is June 15, 2023, plenary meeting at https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees/maryland-cybersecurity-council.

More Information

Questions about the report may be addressed to:

University of Maryland Global Campus
ATTN Maryland Cybersecurity Council Staff
3501 University Boulevard East
Adelphi, Maryland 20783
Marylandcybersecuritycouncil@umgc.edu[89]

[89]This report originated in a draft by the University of Maryland Global Campus, the Council's staffing entity, that (a) incorporated comments of Council members and (b) was subsequently edited and approved for publication by the Office of the Maryland Attorney General.

APPENDIX A

Recommendations of the Maryland Cybersecurity Council

2016 - 2023

Recommendations in the 2016 Interim Report		Originating Subcommittee
1.	Creation of Cyber First Responder Reserve	Law, Policy, Legislation
2.	Updates to the Maryland Personal Information Protection Act	
3.	Civil Cause of Action for Remote Unauthorized Intrusions	
4.	Facilitating Use of the No-charge Credit Freeze Option	
5.	Inclusion of NIST Cybersecurity Framework in the state IT Master Plan	
6.	Publication of a Maryland Data Breach Report	
7.	Integrated Cyber Approach for Mid-Atlantic Region	Cyber Operations & Incident Response
8.	Educational Resources for Critical Infrastructure Owners and Operators	Critical Infrastructure
9.	Identify Maryland Critical Infrastructure and Risk Assessments	
10.	Basic Computer Science and Cybersecurity Education	Education & Workforce Development
11.	Maryland Cybersecurity Scholarship for Service	
12.	Resources for University Computer Science Departments	
13.	Study of Cyber Workforce Demand and Skills	
14.	Transition Path for Community College Graduates	
15.	Increased Funding for Academic Research	
16.	Cybersecurity Business Accelerators	Economic Development
17.	Cybersecurity Repository	Public Awareness & Outreach

Recommendations in the 2017 Biennial Report		Originating Subcommittee
1.	Update the state's Executive Branch breach law and extend personal information privacy protections and breach reporting requirements to the judicial and legislative branches.	Law, Policy, and Legislation
2.	Legislative or policy changes that would require state IT procurements to resource and include an independent security verification of device or code readiness and/or system security readiness prior to government acceptance. The Council is sensitive to the recommendation's potential impact on Maryland's business sector and on the cost of goods and services to the state. The Council intends that these considerations weigh into a discussion of a regime that would contribute to the cybersecurity of the state.	
3.	Legislation requiring express consumer consent for internet service providers (ISPs) to sell or transfer consumer internet browser history. (Replaced 2021 Recommendation 2).	

	Recommendations in the 2017 Biennial Report (Continued)	Originating Subcommittee
4.	Inclusion of a ransomware definition in the Maryland's extortion statute or a new code section with increased penalties for extortion levels below the general extortion statute threshold.	Law, Policy, and Legislation
5.	Legislation to create the right of civil action against former employees in the event of a breach due to intentional conduct that was the proximate cause of actual damages or mitigation costs, with punitive damages available when plaintiff can prove malice.	
6.	Legislation that would require IoT devices to include consumer labelling about the security features the devices incorporate. (Replaced by 2021 Recommendation 3).	
7.	Legislation to ensure the transparency to consumers of data held by data brokers about them, the right of consumers to inspect and correct wrong data, and the right to opt out of the sale of their data by brokers for marketing or people search purposes.	
8.	Maryland develop the capability for sharing cybersecurity information and providing outreach support. (Replaced by 2019 Recommendation 4).	Critical Infrastructure Subcommittee & Incident Response and Cyber Operations Subcommittees (Joint Recommendation)
9.	The implementation of a comprehensive Computer Network Defense (CND) program to provide robust protection to state assets, business information, and citizen data across all agencies. Clearly, the 2017 and 2019 Executive Orders have driven significant changes that will enhance the cybersecurity posture of the state's Executive Branch. To be commended too is the increase in funding for new initiatives of the Office of Security Management. Nonetheless, the Council believes that investments at the much higher levels it recommended must follow by one means or another to fully realize the promise of these important Executive Orders.	Cyber Operations and Incident Response Subcommittee

Recommendations in the 2019 Biennial Report		Originating Subcommittee
1.	The state should address the security vulnerabilities of its absentee balloting system as soon as possible.	Joint Recommendation of Law, Policy, Legislation Subcommittee and Critical Infrastructure Subcommittee
2.	North Dakota Senate Bill 2110 should be considered in conjunction with all interested stakeholders to understand to what extent it could serve as a model for Maryland.	Law, Policy, and Legislation
3.	The state should act to support the cybersecurity of the electric utilities serving Maryland. Noted in this connection are actions taken by California, Michigan, and other states in consultation with their utility stakeholders.	Critical Infrastructure Subcommittee
4	Information Sharing and Analysis Organization (ISAO). The state should establish or facilitate an information sharing and analysis organization especially targeted on small and medium-size businesses in Maryland. Such an organization would enable small and medium-size businesses to better protect themselves against breaches by receiving timely threat information, breach mitigation assistance, advice on steps to take to protect themselves, and proactive training. There are different models that state policymakers can consult for this purpose. (Replaces 2017 Recommendation 8).	Joint Recommendation of the Critical Infrastructure Subcommittee and the Economic Development Subcommittee
5.	Cybersecurity Workforce Development. The state consider the following: a) raising the cap for employer reimbursement of wages paid to technical interns and apprentices in cybersecurity to a level approaching a greater percentage of the actual wage paid, and b) scholarship forgiveness program for cybersecurity graduates that remain in state for some stipulated number of years. The latter would mirror the program currently offered to life science graduates.	Economic Development
6.	Support for IP Start-ups. Institution of an R/D tax credit against employer-paid state and local taxes and filing fees for qualifying cybersecurity product start-ups.	
7.	Implementing a tax credit analysis in coordination with the Maryland Department of Commerce to review existing tax credits. The objective is to do the following: consolidate existing tax credits, eliminate redundant or obsolete credits, and streamline the application and award process for receiving available tax credits. Mindful of the competing demands on the state, but with an eye to supporting growth in the state's business base, the Council further recommends that so much as possible relevant existing tax credits be extended to provide longer availability and available funds for existing tax credits be increased.	

Recommendations in the 2021 Biennial Report		Originating Subcommittee
1.	That the state consider incentives for businesses to assess their cybersecurity posture and to invest more, if necessary, to create a cybersecurity program consistent with recognized standards and frameworks.	Law, Policy, Legislation
2.	That the state consider appropriate legislation to ensure the transparency to consumers of the information held by entities about them and how it is used, the right of consumers to inspect, correct and delete such data, and their right to opt out of the sale of data to third parties. (Replaces 2017 Recommendation 3)	
3.	That the state consider legislation to enhance the security of Internet of Things (IoT) devices. (Replaces 2017 Recommendation 6)	
4.	That there be transparency with the state by critical infrastructure providers about compromises that interfere with operations.	
5.	That the state consider a strategic partnership a) to engage business and industry in identifying gaps in IT/cybersecurity workforce development and in defining training requirements; b) to leverage the postsecondary sector and other training and education providers to offer needed training; c) to coordinate upskilling opportunities for the unemployed or underemployed; and d) to provide enhanced funding for a variety of pathways to the cybersecurity profession, including apprenticeships and career and technical education.	Cybersecurity Education and Workforce Development

	Recommendations from Sponsored Research 2021 - 2023	Originating Subcommittee
	See Appendix B in Cybersecurity and the Maryland Electric Grid – Findings and Recommendations. https://www.umgc.edu/content/dam/umgc/documents/upload/cybersecurity-and-the-maryland-electric-grid.pdf	Critical Infrastructure
	See Appendix B in State and Local Government Cybersecurity – Analysis and Recommendations. https://www.umgc.edu/content/dam/umgc/documents/upload/maryland-state-and-local-government-cybersecurity-analysis-and-recommendations.pdf	Ad Hoc Subcommittee on State and Local Government Cybersecurity
	See Executive Summary in Report of the Ad Hoc Subcommittee on Consumer and Child Privacy. https://www.umgc.edu/content/dam/umgc/documents/upload/12192022consumer-digital-privacy-recommendations.pdf	Ad Hoc Subcommittee on Consumer and Child Privacy

APPENDIX B

Preliminary Analysis of Adult Cybersecurity Hygiene Survey

Johns Hopkins University

Information Security Institute

Maryland Resident Cybersecurity Awareness and Practices PILOT Survey: A Summary of Preliminary Findings

Anton Dahbura, Joseph Carrigan, Jamie Stelnik and Mohammed Khalid

The complete 75-page report may be found at https://1drv.ms/b/s!AjqEqIxJkAfagekxqw3xnSybYEuGrw?e=4VHsdt or by contacting Anton.Dahbura@jhu.edu

Abstract: We conducted a pilot survey on the cybersecurity habits and knowledge of Maryland residents using Amazon's MTurk service. We collected over 500 valid responses from MTurk workers in Maryland and analyzed the results. Key findings include the following: A large proportion of Marylanders have been the victims of online scams where they experienced a financial loss. Marylanders seem overconfident in their cybersecurity knowledge. One in five Marylanders admit to using the same password for most of their online accounts. In this report we discuss the survey and its methods, analyze the compiled results of the survey, and recommend further, more rigorous research in this area.

Funding for this work was provided by the National Cryptologic Foundation and the Johns Hopkins University Information Security Institute.

June 20, 2023

Acknowledgements

The Maryland Resident Cybersecurity Awareness and Practices survey would not have been possible without the work and guidance of many individuals from across the Johns Hopkins and Maryland community. We would like to thank each of them for their input, guidance, and commitment to inclusive excellence at The Johns Hopkins University Information Security Institute.

Introduction

Background

The Maryland Resident Cybersecurity Awareness and Practices Survey was conducted by members of the Johns Hopkins University Information Security Institute (ISI) in order to become more informed about Maryland residents' general knowledge of cybersecurity, their cybersecurity practices, and the impact of cyber scams on their lives. The survey allows participants to respond regarding their personal practices or their practices at their work, without distinguishing between the two.

Objectives

The primary objective of this pilot survey is to perform a preliminary assessment of the cybersecurity knowledge and habits of Maryland residents. The results of this survey are intended to guide the direction of future research into the topic area. Future surveys should be more formal and use the lessons learned in this survey to focus more on areas that emerge as interesting to future researchers while still, more importantly, pertinent to Maryland residents.

Methodology

The Amazon Mechanical Turk (MTurk) platform was used to recruit participants, conduct the survey, and gather results. MTurk is a 'crowdsourcing' website with which businesses can hire remotely located "crowdworkers" to perform discrete on-demand tasks. Employers (known as requesters) post jobs known as Human Intelligence Tasks (HITs), such as identifying specific content in an image or video, writing product descriptions, or answering survey questions. Workers, colloquially known as Turkers or crowdworkers, browse among existing jobs and complete them in exchange for a fee set by the employer. [Wikipedia]

The survey was conducted on MTurk from October 2022 through February 2023. 549 participants completed the survey and were paid $5 each. The survey was listed as "Survey About Your Cybersecurity Habits" and participants were told that the survey would require approximately 10 minutes to complete. Funding for the survey fees were provided by the National Cryptologic Foundation and ISI.

The participants were asked to answer 31 questions as seen at the end of this summary.

Census Data

2020 Maryland Census Data was used in order to gain census demographic information pertaining to Maryland Counties by United States Census Bureau (2023) and Maryland Department of Planning (2022).

Analysis of Data

The survey data was analyzed using Python through Jupyter Notebook. Both graphs and tables were created with the survey data and census data. The data was visualized through bar graphs and crosstabs. Crosstabs visualize the frequency distribution of two different survey questions. One-dimensional bar graphs were created to visualize how many participants chose each answer for a question. Dual-axis bar graphs were used to compare these survey ratios to the census data ratios. Finally, crosstabs were used to create two-dimensional tables, comparing each question to each other by seeing how many participants answered each combination of answers.

Discussion, Conclusions, and Future Work

Overconfidence In Cybersecurity Knowledge

Our group of participants is highly-educated compared to the general population of Maryland. Over 47% of participants have a bachelor's degree and over 29% have a graduate degree. On average in the state of Maryland, only around 23% of residents have a bachelor's degree and less than 20% have a graduate degree. Further, 89.61% of survey participants self-assessed as confident with their computer skills and 74.5% of participants self-assessed as knowledgeable about cybersecurity. These questions were the final two questions asked on the survey, meaning that after participants answered the security questions at least partially incorrectly and stated that almost one in four had been scammed, they still believed that they were very knowledgeable about cybersecurity and had good computer skills.

Even with survey participants being highly educated and self-assessing as knowledgeable about computers and cybersecurity, not a single person out of 549 participants was able to correctly answer all four of the multiple-choice security questions, and 12.11% of participants did not answer any of the questions correctly.

This is concerning because even though these participants have gone through years of schooling to get their degrees and believe that they are knowledgeable on the questioned subjects, there is clearly much more for the average Maryland resident to learn. This shows a need for more computer and cybersecurity training in the state of Maryland, even for people who truly believe that they are prepared. If security training is as common for Maryland residents as it is for the survey participants, where around 62% of participants

have had security training within the past year, then clearly something needs to change in the way that we are currently training our residents.

High Victim Rate of Online Scams

We were surprised by the results of the questions pertaining to on-line scams. Nearly 1 in 4 respondents (23.32%) said they have lost money to an online scam. Additionally, we were surprised by the amounts reported lost. The median loss for those who lost money was $200.00 which was higher than we expected. The average loss was $3,320. This average includes two respondents who reported losing $100,000 each. If we eliminate these 2 responses as outliers, the average loss drops to $1,522. It is important to note that losses in the hundreds of thousands of dollars are not unheard of in online scams.

If we use the numbers above and assume that 23% of Maryland Residents (1.4 Million of Maryland's 6.1 million residents) have lost money to online scams, and that the average loss was $1,522, we arrive, albeit naively, at a loss of $2.1 Billion for Maryland residents. In 2022, the federal Bureau of Investigation's Internet Crime Report listed reported losses of nearly $218 million for 11,644 victims, an average loss of $18,711. While our survey asks if people have *ever* been scammed and the FBI report is for a single year, we are convinced that this data shows that online scams are under-reported, particularly when the dollar values are low. We believe that further research in this area would be of value to the state of Maryland.

Password Reuse

There were five possible answers for the survey question 'How do you choose a password for your online accounts?' They follow as:

- I use passwords that are similar but different for all of my accounts
- I use a unique complex password for my accounts
- I use the same password for most of my accounts
- I use personal information as all or part of my password
- I use the same password for all of my accounts

10% of participants use the same password for all of their accounts and over 20% use the same password for most of their accounts. If nearly 1 in 4 participants has been hacked before and over 30% of participants use the same password for most or all of their accounts, 6% of participants have both been hacked and have the same password for most or all of their accounts. The hackers would then be able to easily hack many more of their accounts. While 6% is not a high percentage, that is almost 33 people in this survey alone.

Further, we asked participants how they managed their passwords, and almost 41% of participants said they remembered their passwords. If over 200 people can remember all of their passwords that easily, they must be very similar across accounts. This further emphasizes our finding from before: that many people are not only susceptible to being hacked once, but across all of their accounts if they share the same or a similar password.

We believe that this data about passwords shows how weak people truly secure most of their accounts and how if someone gets scammed once, they are much more likely to be scammed again.

Ignorance About Data Breaches

Over 45% of people stated that their personal information has been disclosed to unauthorized people. This is almost 250 participants. If we use this data and assume that 45% of Maryland's adult residents have also had personal information disclosed to unauthorized people, that would mean over 2.7 million people have had their personal information breached.

However, we were surprised by this low response rate of 'yes.' We believe that almost everyone's data has been breached before, whether they know it has or not. We believe that the 'no' response rate of almost 38% is extraordinarily high, especially coming from a group of people where almost 1 in 4 have been hacked. Further, we were similarly surprised that over 17% of the participants did not even know whether their personal information had ever been disclosed.

Significance of the Findings

We believe that our findings show that the state of Maryland needs to invest more in cybersecurity awareness and training for all of its residents. Further, we hope that this effort will be a partnership with the private sector and also become a standard part of the educational process for all students in Maryland.

Limitations

We understand that there were many limitations in our survey and decisions we would change in the future. These include:

- Obtain more respondents, so more statistical analysis can be performed on the raw data
- Add interviews with participants to obtain more accurate answers about how, where, and when they were scammed
- Partner with an organization that specializes in survey taking and survey analysis
- Collect gender data in our demographics
- Compare our survey to those done in other states

- Ask respondents who have been scammed out of money if they reported the crime to law enforcement. This would be helpful in determining the rate at which cybercrime goes unreported.
- Ask respondents who have received a phishing email claiming to be from a financial institution if they are customers of the institution being impersonated. This would provide insight into the rate at which phishers ”get it right.”
- Build a regional or national alliance for cybersecurity awareness and training Partner with financial institutions, who would be very interested to see the survey results as they would want an idea of how much money people are losing.

References

Maryland Department of Planning (2022). Maryland counties socioeconomic characteristics. Accessed April 6, 2023.

United States Census Bureau (2023). Annual county and puerto rico municipal resident population estimates by selected age groups and sex: April 1, 2020 to July 1, 2021 (cc-est2021-agesex). Accessed April 6, 2023.

Survey Questions

Demographic Questions: Questions 1-4
Backup Behavior Questions: Questions 5-7
Security Awareness Questions: Questions 8-11
Security Hygiene Questions: Questions 12, 15-18
History Questions: Questions 19-21, 24-28 Final
Questions: Questions 29, 31

1. Age (select one):
    - 18–24
    - 25–34
    - 35–44
    - 45–54
    - 55–64
    - 65–75
    - 75 years or older
2. Please select the jurisdiction of your primary residence:
    - Allegany County
    - Anne Arundel County
    - Baltimore City
    - Baltimore County
    - Calvert County
    - Caroline County
    - Carroll County
    - Cecil County
    - Charles County
    - Dorchester County
    - Frederick County
    - Garrett County
    - Harford County
    - Howard County
    - Kent County

- Montgomery County
- Prince George's County
- Queen Anne's County
- St. Mary's County
- Somerset County
- Talbot County
- Washington County
- Wicomico County
- Worcester County
- I don't know

3. Education Level (Select One):
    - Do not have a HS Diploma or GED
    - High School Diploma or GED
    - Some College
    - Associate's Degree
    - Bachelor's Degree
    - Graduate Degree
    - I don't know
4. What year were you born? (Integer field)
5. How do you backup your data (Check All that apply)
    - I use a cloud service (e.g., Microsoft OneDrive, Carbonite, Google Drive)
    - I use removable storage that I keep in my house
    - I use removable storage that I keep in a location other than my house
    - I keep multiple copies of my files on my computer
    - I do not back up my data
    - I don't know
6. How often do you back up your data? (Check all that apply)
    - Continuously
    - Daily
    - Weekly

- Monthly
- Less often than monthly but at least once a year
- Once a year or less frequently
- I do not back up my data
- I don't know

7. When was the last time you made sure your backups were valid?

- Within a day
- Within a week
- Within a month
- Within a year
- More than a year ago
- I do not back up my data
- I don't know

8. What is Social Engineering in an information security context?

- Any action in which someone tries to convince another person to take an action which may not be in their best interests
- Actively trying to circumvent or get around security safeguards by finding weaknesses in a system that can be exploited without personal interaction
- Attempting to inform people about the use of proper security policies, processes, and procedures
- When a company makes a public announcement about something positive that has happened or is going to happen
- I don't know

9. What is Spear Phishing?

• When someone fraudulently sends a specifically crafted message to a person to convince them to take an action which may harm them

- Targeted marketing emails sent to a specific person by a company based on their buying history or web browsing habits
- When someone sends an email specifically designed to belittle the recipient
- When someone in a business setting sends an email to a coworker inappropriately delegating their work to the recipient
- I don't know

10. What is Phishing?

• When someone fraudulently sends emails to people to convince them to take an action which may harm them

- When companies or individuals send out emails to promote or sell their products
- When someone you know sends an email that was forwarded to you encouraging you to forward that message on to everyone in your address book
- When someone sends an email to a large group of people and one of the recipients replies with a personal response to all recipients of the original email
- I don't know

11. What is Multifactor Authentication?

• An additional piece of information beyond username and password which someone must provide to gain access to a system (e.g., website)

- The Frequent changing of a password so it is harder for an attacker to guess
- Adding different numbers to the ends of a username so a user never has the same username on multiple sites
- When someone uses a different password for each website they access
- I don't know

12. Where do you use multifactor authentication? (Select one) (Grouped with other multifactor questions)

- I do not use multifactor authentication.
- I use multifactor authentication on my important online accounts.
- I use multifactor authentication on most of my online accounts.
- I use multifactor authentication wherever it is offered to me.
- I don't know.

15. What form of multifactor authentication do you use? (Check all that apply) (Grouped with other multifactor questions)

- I do not use multifactor authentication
- Messages sent to my phone that contain a code
- An application on my phone that verifies I am logging in
- An application that generates a one-time code • A hardware security token (e.g., YubiKey or Google Titan)

- I don't know.

16. How do you choose a password for your online accounts? (Check all that apply)

    - I use the same password for all of my accounts
    - I use the same password for most of my accounts
    - I use passwords that are similar but different for all of my accounts
    - I use personal information (names of pets, children, or friends) as all or part of my password
    - I use a unique complex password for my accounts
    - I don't know

17. How do you manage the passwords for your online accounts? (Check all that apply)

    - I remember my passwords
    - I write my passwords down
    - I use a password manager
    - I don't know

18. When have you ever received security awareness training at your place of employment or through other means such as a community organization or an advocacy group?

    - I have never received security awareness training.
    - I have received security awareness training within the past month
    - I have received security awareness training within the past 6 months
    - I have received security awareness training within the past year
    - I have received security awareness training a year or more ago
    - I don't know.

19. Have you ever been the victim of ransomware? (Yes/No/I don't know)

20. To your knowledge, has your personal information been disclosed to unauthorized people,
    e.g., via a data breach? (Yes/No/I don't know)

21. Have you ever been the victim of an online scam where you lost any amount of money? (Yes/No/I don't know)

24. If so, about how much money did you lose as a victim of this scam (enter 0 if you have not lost any money)? Integer

25. Have you ever been targeted by a scammer who called you directly on the phone? (Yes/No/I don't know)
26. Have you ever lost access to any of your online accounts due to someone else taking it over? (Yes/No/I don't know)
27. Have you ever received an email claiming to be from a financial institution you use that asks you to log in to that account to resolve some issue? (Yes/No/I don't know)
28. How likely do you think you are to be targeted by a malicious actor (Hacker) at some time in the future? (5 point scale + I don't know)
29. I am very confident with my computer skills. (5 point Agree/Disagree scale)
30. I am knowledgeable about cybersecurity. (5 point Agree/Disagree scale)

Appendix C

Council Subcommittees, Objectives and Appointed Members

Fiscal Year 2022 – 2023

Subcommittee on Law, Policy, and Legislation
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, District 16, Maryland General Assembly[90]
- Co-chair: Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution
- Ned Carey, Delegate, District 31A, Maryland General Assembly[91]
- Howard Feldman, Esq., Attorney, Whiteford, Taylor & Preston
- Michael Greenberger, Director, Center for Health and Homeland Security, University of Maryland, and Professor, Francis Carey School of Law, University of Maryland, Baltimore
- Joseph Morales, Esq., The Morales Law Firm
- Jonathan Prutow, Project Manager, eGlobal Tech
- Markus Rauschecker, Cybersecurity Program Director, University of Maryland Center for Health and Homeland Security
- Paul Tiao, Esq., Attorney, Hunton & Williams[92]
- Pegeen Townsend, Vice President, Government Affairs, Medstar Health

Subcommittee on Cyber Operations and Incident Response
Subcommittee Objectives

- Recommend best practices for monitoring and assessing cyber threats and responding to cyber-attacks or other security breaches
- Create or enhance shared awareness of cyber vulnerabilities, threats, and incidents within the state
- Recommend best practices for developing a comprehensive state strategic plan to ensure a coordinated and quickly adaptable response to and recovery from cyber-attacks and incidents
- Serve as a resource for its expertise to all other subcommittees

Subcommittee Members

- Chair: Michael Leahy, Secretary, Department of Information Technology (DoIT)[93]
- Barry Boseman, Director, State and Local Affairs, National Security Agency, Liaison to the Council

[90] Susan Lee left the Council in spring 2023 with her appointment as Maryland Secretary of State.
[91] Mr. Carey did not run for re-election in 2022 and vacated his seat on the Council as of January 1, 2023.
[92] Mr. Tiao resigned his Council seat in the fall 2022 with his appointment to a position within the White House Office of the National Cybersecurity Director.
[93] With the change in administrations, Secretary Katie Savage now leads DoIT.

- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System
- Robert W. Day Sr., Senior Project Manager, Howard University
- Linda Lamone, State Administrator, State Board of Elections[94]
- Walter "Pete" Landon, Director, Governor's Office of Homeland Security[95]
- Mary Ann Lisanti, Delegate, District 34A, Maryland General Assembly[96]
- Anthony Lisuzzo, Board Member, Army Alliance
- Major General Timothy E. Gowen, Adjutant General, Maryland Military Department[97]
- Colonel William Pallozzi, Maryland Secretary of State Police[98]
- Russell Strickland, Secretary, Maryland Department of Emergency Management

Subcommittee on Critical Infrastructure and Cybersecurity
Subcommittee Objectives

- For critical infrastructure not covered by federal law or Executive Order 13636 of the President of the United States, identify best practices in conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber-attacks and need the most enhanced cybersecurity measures
- Use federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber-attacks to the infrastructure could reasonably result in catastrophic consequences
- Assist infrastructure entities that are not covered by the Executive Order in complying with federal cybersecurity guidance
- Assist private sector cybersecurity businesses in adopting, adapting, and implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Assist State of Maryland government entities, as well as educational entities, in adopting, adapting, and implementing the NIST Cybersecurity Framework
- Recommend strategies for strengthening public and private partnerships necessary to secure the state's critical information infrastructure

Subcommittee Members

- Chair: Markus Rauschecker, Cybersecurity Program Director, University of Maryland Center for Health and Homeland Security
- John Abeles, President and CEO, System 1, Inc.
- Dr. David Anyiwo, Chair, Department of Management Information Systems, Bowie State University
- Cyril Draffin, Project Advisor to the Massachusetts Institute of Technology (MIT) Energy Initiative
- David Engel, Director, Maryland Coordination and Analysis Center

[94] Ms. Lamone will retire September 1, 2023, with her seat filled by her successor.
[95] Mr. Landon left the Council as an outgoing member of the last administration.
[96] Ms. Lisanti did not run for reelection in 2022 and vacated her seat on the Council on January 1, 2023.
[97] Brigadier General Janeen L. Birckhead was appointed Adjutant General by Governor Wes Moore in April to replace outgoing Major General Timothy Gowen.
[98] Lt. Colonel Roland Butler has been appointed Secretary of State Police in the new administration.

- Zuly Gonzalez, Co-Founder and CEO, Lightpoint Security
- Michael Greenberger, Director, Center for Health and Homeland Security, University of Maryland, and Professor, Carey School of Law, University of Maryland, Baltimore
- Terri Jo Hayes, Executive Consultant, Mfusion, Inc.
- Fred Hoover, Esq., Counsel, Maryland People's Counsel[99]
- Clay House, Vice President, Architecture, Planning, and Security, CareFirst

Subcommittee on Education and Workforce Development
Subcommittee Objectives

- Identify opportunities to enhance and support cyber workforce training and education in Maryland, including:
  - Recommendations for enhancing student interest in pursuing cybersecurity education
  - Recommendations for developing programs for students and professionals entering the cybersecurity field
  - Recommendations for attracting teachers and faculty qualified to teach cybersecurity courses in high school and beyond
  - Recommendations for developing and modifying high school and higher education curricula to enhance cybersecurity skills and talent; recommendations for developing fundamental skills necessary for cybersecurity students and professionals
- Promote cyber research and development (R&D) in higher education, including recommendations on funding, incentivizing, or fostering collaboration in R&D
- Recommendations on improving pathways to employment in the cybersecurity field

Subcommittee Members

- Chair: Katie Fry Hester, Senator, District 9, Maryland General Assembly
- Tasha Cornish, Executive Director, Cybersecurity Association of Maryland (CAMI)
- Dr. Michel Cukier, Associate Professor and Director, ACES, University of Maryland
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Miheer Khona, CEO Rising Sun Advisors
- Kevin Kornegay for David Wilson, EdD, President, Morgan State University
- Kimberly Mentzel, Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- Henry J. Muller, Director, Communications-Electronics Research, Development and Engineering Center, U.S. Army, Aberdeen Proving Ground
- Laura Nelson, President/CEO, National Cryptologic Foundation
- Rodney Petersen, Director, National Initiative for Cybersecurity Education, National Institute of Standards and Technology, Liaison to the Council

[99] Mr. Hoover resigned his Council seat in spring 2023 with his nomination (later confirmed) as chair of the Maryland Public Service Commission.

- Jonathan Powell, U.S. Department of the Navy
- Bryan Simonaire, Senator, District 31, Maryland General Assembly

Subcommittee on Economic Development
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, such as attracting venture capital and offering tax incentives

Subcommittee Members

- Chair: Belkis Leong-Hong, Founder, President, and CEO, Knowledge Advantage, Inc.
- Tasha Cornish, Executive Director, Cybersecurity Association of Maryland (CAMI)
- James Foster, CEO, Zerofox
- Don Fry, President and CEO, Greater Baltimore Committee[100]
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank[101]
- Mary Kane, CEO, Maryland Chamber of Commerce
- Brian Israel, Business Development, Strategy, Corporate Finance, Forvis
- Mathew Lee, CEO, Fastech
- Kimberly Mentzel, Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- Steve Pennington, Vice President, Technology and Innovation, Maryland Tech Council
- Troy Stoval, CEO/Executive Director, Maryland Technology Development Corporation (TEDCO)
- Steven Tiller, Board Member, Fort Meade Alliance

Subcommittee on Public Awareness and Community Outreach
Subcommittee Objectives

- Promote the Council's objectives and spread awareness of Council's 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, CASH Campaign of Maryland

[100] Mr. Fry retired in 2022. The Greater Baltimore Committee has undergone a reorganization and a new representative will be invited.
[101] Mr. Haskins retired in April of this year.

- Anton Dahbura, PhD, Executive Director, Information Security Institute, Johns Hopkins University
- Jayfus Doswell, PhD, Founder, President, and CEO, The Juxtopia Group, Inc

Larry Letow, President, US Region, CyberCX