2022

“Cyberstate” of Washington Localities

- Priyanka Menon
- Kiran Bondalakunta
- Perry Maybrown

University of Washington School of Law Technology Law and Public Policy Clinic

Contents

Abstract

Washington is poised to implement the federal cybersecurity grant program included in the recent federal Infrastructure Investment and Jobs Act, which would allocate1.9 billion dollars to the nation's cybersecurity. From that sum, the federal government has earmarked 1 billion dollars to create a grant program dedicated to helping state, local, tribal and territorial governments better prepare for cyberattacks. Data from numerous research agencies indicate that local governments are prime targets for cybercriminals because of the infrastructure and operational gaps in local jurisdictions security program. Like many other governments in the nation, local governments in Washington operate under significant resource constraints. Currently, the State government does not have a formal or cohesive approach to assisting local jurisdictions. However, in 2021 Washington passed SB 5432 which appointed the Office of Cybersecurity as a resource for local, municipal, and tribal governments. The state is now well situated to implement impactful and reliable programs to assist local governments in their cybersecurity efforts and improve the whole state's cybersecurity posture.

I. Overview

This paper is the result of the research conducted by the ransomware team within the University of Washington School of Law's Technology Law and Public Policy Clinic. The study's overarching goal was to analyze the cybersecurity preparedness of the State of Washington (the "State"). The research and this report focus specifically on the issues encountered by Washington local governments in their cybersecurity planning and preparedness efforts. Washington's first-tier government agencies include 39 counties, 281 cities and towns, more than 80 different special purpose districts, and 29 federally recognized tribal governments. Local jurisdictions face numerous cybersecurity planning and preparedness challenges. This report explores how Washington's current cybersecurity governance approach impacts local governments. It also investigates how the local IT governance and management structure might also contribute to the challenges. The cyberstate of local jurisdictions is important because a state cannot fully prepare for a cybersecurity incident without considering the interest of its local government partners.

While preparing this report, we relied on scholarly articles, news reports, government publications, data collected from anonymous polls conducted during the Association of County and City Information Systems' (ACCIS) 2022 spring conference, and interviews with federal, state, city, and county officials in Washington State.

II. Introduction

Local governments play a vital role in providing basic needs like water, electricity, roads, etc., to their citizens. Governments at all levels, including cities and counties, increasingly rely on technology to provide these essential services. Providing these basic necessities require that the government store such key information as names, addresses, driver's license numbers, credit

card numbers, social security numbers, and other personal information. This reliance on technology to house such sensitive information makes local governments particularly vulnerable to cyber-attacks.

Cyber-attacks are unwanted attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems[1]. Attacks that involve breaking into a computer system could be accomplished through malware, hacking, or acquiring stolen login credentials. Malware, or malicious software, is perhaps the most significant security risk to an organization. Of all the different types of malware that could threaten an organization, ransomware has gained tremendous media attention recently. Ransomware is a malware criminals employ to lock data on a victim's computer, typically through encryption. Once the data is locked, the criminal demands payment before the criminals decrypting and returning access to the ransomed data.[2] As per the sixth annual data breach report released by the Washington State Attorney General, data breaches skyrocketed from 78 in 2020 to 280 incidents in 2021.[3] Out of the 280 reported incidents, 150 were related to ransomware—which was 5% more than 2020. The following three recent attacks on local Washington governmental agencies show how local the issue of cybersecurity has become.

In 2021, the Clover Park school district in Pierce County experienced a ransomware incident that disrupted the functioning of school computer systems.[4] Malware installed on the computer systems caused the disruption, and some confidential files related to the school district were subsequently found on the dark web. While this incident was under investigation, King

[1] https://www.ibm.com/topics/cyber-attack
[2] William Stallings, Information Privacy Engineering and Privacy by Design, 148 (Mark Taub ed., 1st ed. 2019).
[3] https://www.atg.wa.gov/news/news-releases/ag-data-breach-report-2021-sets-new-record-number-data-breaches-and-ransomware
[4] https://www.kiro7.com/news/local/clover-park-school-district-investigating-possible-ransomware-attack/J7ZJQSJGBRARJE5IEM3CMJVV2M/

County public hospital district No.2 d/b/a Evergreen health hospital system reported a data breach that affected 22,579 Washingtonians.[5] However, this time the culprit was not ransomware but hacking.

As a public hospital district, the law requires Evergreen Health to undergo annual audits by the State Auditor's Office. In 2019, Evergreen submitted data related to patient payments to State Auditor's Office (SAO) using the file transfer service provided by the company Accellion. The incident occurred when hackers breached Accellion's computer system. Investigation revealed that attackers hacked into Accellion's 20-year-old file-sharing product, ultimately impacting over 100 organizations, including Evergreen Health.

More Washingtonian's health records were compromised when the Chelan-Douglas County health district in East Wenatchee fell victim to a cyber-attack in July 2021.[6] The breach occurred when cybercriminals accessed the district's network with an unauthorized login. Attackers stole personally identifiable data like names, social security numbers, dates of birth/death, financial account information, treatment information, diagnosis information, medical record/ patient numbers, and health insurance policy information.

Washington's struggle with cybersecurity is not a unique one. Data from numerous research agencies indicate that local governments are prime targets for cybercriminals because of their infrastructure and operations gaps. A recent report published by the Center for Internet Security investigating the cybersecurity preparedness of the United States' 90,000 plus local government entities states that nearly one-third of the local governments would be unable to tell if they were under cyber-attack.[7] Since the pandemic, the cyber-attacks on local governments

[5] https://compliancy-group.com/2021-july-healthcare-breaches/
[6] https://www.hipaajournal.com/patient-data-stolen-in-july-2021-cyberattack-on-chelan-douglas-health-district/
[7] https://cyberlaw.stanford.edu/blog/2022/03/local-governments-are-attractive-targets-hackers-and-are-ill-prepared

have increased drastically due to a lack of efficient security tools and people working from home with an unsecured network. The malware injected into the network from an unsecured network is undetectable until the cyber-criminal takes control of the network. Even sharing a sensitive document via email in a compromised network will have severe repercussions.

Cybersecurity should be a concern for both big and small organizations. In the past, experts believed that larger organizations presented significant risk profiles and were thus more likely to be the targets of cybercrimes than smaller organizations. However, a recent report published by Managed Security Service Providers[8] explains that bad actors are more likely to prey on smaller and medium sized organizations because attacks on larger organizations brings greater scrutiny from law enforcement. This means that cybersecurity should be a concern for all governmental organizations, not just larger counties like King and Spokane.

III. Discussion

A. Local decision-making environment

The core challenge public sector cybersecurity professionals face today is one of governance.[9] Cybersecurity governance is the process by which organizations analyze security risks, prioritize resources, and establish procedures to manage security incidents.[10] Because cyber threats are dynamic, achieving perfect security is beyond the capabilities of any organizations. Thus, cyber governance focuses on developing programs to reduce risk to a tolerable level.[11] The process consists of policy and law making which sets the plan of action for an institution and which depends on the efficiency of the enterprise's organizational and

[8] https://www.msspalert.com/cybersecurity-research/why-ransomware-attacks-prefer-small-business-targets-rather-than-rich-enterprises/
[9] Michael Garcia et al., Beyond the Network: A Holistic Perspective of State Cybersecurity Governance, 96 Neb. L. Rev. 251, 253 (2017) (Introduction).
[10] Autumn C. Pylant, Initiating a Collaborative Cybersecurity Governance at the State Level (Spring 2020), (Ph. D. dissertation, West Chester University Doctoral Projects. 59).
[11] Ibid.

operational structures that executes the plan.[12] So then, who is responsible for this task in the public sector?

The United States has a decentralized federalist form of government. In decentralized federalism, planning and decision-making are delegated away from central authority, with the states and local governments handling issues of local concerns. Federalism supports an institutional structure that values the principles of local self-determination and autonomy—two values fundamental to local governments. The practical effect of this institutional structure is that federal, state, and local governments are responsible for their own issues, and cybersecurity is no exception. [13] Thus, governments at each level are responsible for developing policies and procuring resources to manage their IT assets and security.

At the federal and State level, each has adopted laws that establish the principles under which they secure their IT equipment and networks. For example, the Federal Information Security Modernization Act and the National Institute of Standards and Technology's standards ensure federal network and infrastructure security. Similarly, in Washington, RCW 43.105 outlines the roles and responsibilities that ensure the security of state IT assets. The state delegates a majority of cybersecurity responsibilities to the Office of Chief Information Officer (OCIO) and Office of Cybersecurity (OCS). To protect the State IT assets, the OCIO has adopted Standard No. 141.10, which defines the specific steps State agencies must take to secure their IT to ensure privacy, confidentiality, integrity, and availability of systems and data. However, at the city and county levels in Washington, there is currently no standardized network and infrastructure security approach.

[12] https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020
[13] Michael Garcia et al., Beyond the Network: A Holistic Perspective of State Cybersecurity Governance, 96 Neb. L. Rev. 251, 253 (2017) (Introduction).

The State extends the security mandates under Standard No. 141.10 to local governments through data sharing agreements where applicable. Beyond these ad hoc arrangements, local IT infrastructure security remains primarily the responsibility of local jurisdictions. Some local governments attempt to conform to the State standard voluntarily, while others follow private industry standards to varying degrees.

Beyond establishing policies and standards that define the tasks organizations need to accomplish to keep their IT systems secure, the local leaders are also responsible for gathering the necessary resources to attain their security objectives. In this regard, some elected Washington officials and practitioners we interviewed felt financing cybersecurity efforts at the state and local levels is a federal responsibility. In recent years, there has been a surge in federal involvement, specifically to secure elections and critical infrastructure owned by states and localities.[14] However, ensuring the security of local IT infrastructure should not wholly be a federal responsibility, for a multitude of practical reasons.

Generally, the distributed nature of the internet presents unique challenges to cybersecurity. Nation-state actors who are beyond the reach of local law enforcement often perpetrate cyber incidents. Thus, the scope and scale of cyber incidents may appear beyond the capabilities of cities and counties. However, incident response is just one aspect of cybersecurity. As the adage goes, prevention is better than cure. Efficient planning and preparedness are critical to cybersecurity, starting with securing the IT systems. With or without assistance from federal/state governments, cities and counties are responsible for securing their IT assets. Localities must be willing to tackle the attendant responsibilities as autonomous political bodies.

[14] https://www.cisa.gov/election-security

Counties and cities rely on technology to run government functions. As a result, they store citizen data in their systems just like any organization. Further, during the global pandemic, many local governments moved to telework, [15] heightening the need for setting up secured IT environments for their employees to carry out their day-to-day functions. In addition to cities and counties, many special purpose districts in Washington are responsible for delivering critical functions. These are limited purpose local governments separate from cities and counties responsible for operating airports, ports, and providing local irrigation, transportation, emergency medical, and fire control services. Expecting the federal government to tackle these monumental tasks nationally is imprudent and counter to federalism principles. However, this does not mean that cybersecurity is exclusively a local concern.

Cybersecurity is generally framed as a collective issue rather than an individual problem.[16] Local governments operate in a complex socio-political ecosystem that involves many obstacles and a collection of independent actors with divergent political values. First, because cyber-incidents like ransomware sometimes involve nation-state actors, local governments do need federal and state assistance to apprehend criminals and respond to cybercrimes. Further, due to the limited local opportunities for raising revenue[17], local governments need intragovernmental aid to prepare for cyber-incidents. However, these local needs are in constant tension with the local desire to maintain independence and autonomy. Managing these issues requires deliberate actions and thoughtful efforts by local governments. However, many Washington local

[15] https://kingcounty.gov/audience/employees/employee-transportation-program/Telework.aspx
[16] Jacqueline Eggenschwiler, A Typology of Cybersecurity Governance Models, 13 St. Antony's International Review 64, 71 (2018) (Types of Cybersecurity Governance).
[17] https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2021/07/local-tax-limitations-can-hamper-fiscal-stability-of-cities-and-counties; https://www.q13fox.com/news/washington-senator-introduces-bill-to-allow-for-state-income-tax; https://www.cbpp.org/research/state-budget-and-tax/states-grappling-with-hit-to-tax-collections

governments have not realized these goals either because of a lack of experience or not possessing the savvy necessary to meet these challenges.

B. Local cybersecurity challenges

Among the local city and county officials we interviewed and polled, none identified the unavailability of technology as a hindrance to developing a cybersecurity program. The core concern appears to be *access* to available resources, technical and human, caused by lack of funding, strategic governance, and day-to-day management. The local officials discussed the following specific issues:

Human resource and staffing – 91% of the local officials polled were concerned about the quantity and quality of human resources. Numerous organizations are understaffed, and some indicated talent acquisition as a problem. Further, smaller local Washington governments do not have a cybersecurity focus. The organization's IT staff is responsible for everything IT, from setting up employee workstations to cyber planning and preparedness. Further, 13% of the poll participants indicated a lack of cyber-awareness among the leadership as a debilitating factor.

Some also face operational challenges in the form of third-party risk management. Third-party risk management is the process of assessing and controlling cyber and information security risks presented by an organization's relationships with third parties.[18] The interviewees were concerned about non-responsiveness from smaller vendors to notifications regarding vulnerabilities in their system. Further, some interviewees were concerned that releases and patches from vendors are obtuse, and it is hard to prioritize between critical and non-critical matters.

[18] Gregory C. Rasner, Cybersecurity & Third-party risk, 109, (Narendra Patlolla ed., 1st ed. 2021).

Limited funding – nearly all local officials interviewed identified limited funding as an impediment to local cyber preparedness. These officials believe lack of funding is a chokehold that adversely impacts all downstream business decisions. The problem is compounded for smaller jurisdictions as they usually do not have access to federal or state emergency management funds because of their small size. Issues concerning the affordability of insurance also came up during some interviews. Because of limited financial resources, some local organizations have not implemented basic technical measures like dual factors authentication and data backup that are required by insurance companies if they are to offer coverage at a reasonable rate.

Weak ties with the State government – many local officials interviewed were dissatisfied with the Washington State's level of participation and assistance. Currently, the state government provides ad hoc assistance to local jurisdictions. Though interview responses from the Office of Cybersecurity (OCS) alluded to it "working to strengthen connections with local governments," the local officials remain skeptical about forthcoming State assistance primarily because of the high attrition rate among C-level State employees responsible for cybersecurity.

C. Factors Contributing to local cybersecurity challenges

i. The Organizational and operational structure

Local governments' organizational and operational structures indicate how organizations prioritize different aspects of cybersecurity. These structures define how activities such as task allocation and supervision are directed toward achieving organizational aims. Currently, Washington localities lack a cyber-focus. 85% of the poll participants responded that the number of employees supporting cybersecurity efforts is not proportional to the local government population. For an organization to effectively manage the flood of information and activities

related to cybersecurity, staffing must be proportional to the locality's population. Further, the lack of human resources prevents organizations from taking on beneficial projects. For example, 70% of the poll participants indicated that they do not apply for federal or State grants related to cybersecurity because they do not have the human resources to handle the paperwork.

Though a little more than half of the organizations that participated in the poll seem to have a c-level employee directing their cybersecurity efforts, the IT analyst is responsible for providing strategic vision and direction in many organizations. For instance, 52% of the poll participants had a c-level official in charge of cybersecurity, and 48% indicated their cybersecurity efforts are managed and led by IT analysts. An analyst could perform the entire gamut of IT services-- from providing support services to setting cybersecurity policy for the whole enterprise. However, dedicated security professionals offer organizations subject matter expertise and can efficiently handle the flood of information organizations usually receive about cybersecurity risks and threats. For instance, numerous Information Sharing and Analysis Centers (ISACs) help local organizations protect their infrastructure from cyber threats by disseminating actionable threat information. However, the provided information is useless unless there is an adequate knowledgeable staff who can understand, interpret and act on the information.

Further, concerning the organization's reporting structure, 15% of the local officials indicated they report to their chief information or technology officers, 32% to their IT department managers, and 38% to their mayor or city/county administrator. There are many benefits to having cybersecurity managers' report directly to the city/county manager or an administrator as this kind of structure could raise the importance of cybersecurity throughout the organization. However, it could also be a liability if these officials fail to appreciate the urgency and seriousness of the problem and provide the support needed to build a robust cybersecurity

program. This is especially important because 59% of the poll participants indicated that city/county managers or administrators make funding decisions related to cybersecurity. Some were concerned about the leadership's apathy towards cybersecurity. If the leadership does not grasp the importance of cybersecurity, then it will be hard to gather financial support for cybersecurity efforts.

a. Budgeting and acquisition

The cascade of local problems starts with limited funding. The biggest obstacle to developing a cybersecurity program for counties and cities is dollars. Local governments appear to rely primarily on local revenue for cybersecurity and, in some instances, on state and federal grants. There is a confluence of issues here. As mentioned *supra*, sometimes the organizational structure itself is a hindrance—it could limit the local government's access to intragovernmental aids, or the leadership's indifference to cybersecurity could make garnering much-needed support for cybersecurity difficult. Further, when stacked against the other looming socio-economic issues relevant to the community, local governments frequently are required to place the issue of cybersecurity on hold.

Additionally, not all local organizations have established processes that could inform budgetary decisions. Some State officials wehen interviewed indicated that the State is less likely to provide financial aid to those organizations that are unclear on their cybersecurity goals. Thus, organizations must first have a way to access the cyber risks, which will help them understand the areas that need funding. Establishing these processes becomes critical for the local governments as the State implements the federal cybersecurity grant program included in the recent federal infrastructure bill.

ii. Weak ties with the State government

In Washington, there is a disconnect between State behavior and the expectations at the local level. The State currently does not have a concrete plan to plug local governments into the regular flow of business. Washington has what some scholars call a "multi-stakeholder" or "multidisciplinary" cyber governance approach.[19] The multi-stakeholder is a type of governance that seeks to bring together in an informal fashion different stakeholders to deliberate and implement solutions to collective problems.[20] This governance model has the advantage of reduced transaction costs and access to specialized skills in a complex setting. Under this approach, the State collaborates with private, local, and federal partners on cybersecurity issues on a need to basis (Washington's cybersecurity structure is discussed in detail under section D.*ii*.c. *infra*). In the absence of a formal structure, the State extends assistance to the local governments on an ad hoc basis. This ad hoc approach theoretically provides flexibility and increases the efficiency of the State's multi-stakeholder operations. However, some of the local issues result from this governance model. Because in the absence of formal structures and commitments localities depend on the State's willingness to provide help.

D. Improving the cybersecurity posture of localities

Overcoming the above-identified challenges requires local savviness. As sovereign bodies, local governments have the primary responsibility for their cybersecurity. These issues can be resolved only through self-initiated efforts of local governments supplemented with reliable support from the State.

[19] Natasha Cohen, Cybersecurity for the States: Lessons from Across America, 14-15, https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/

[20] Jacqueline Eggenschwiler, A Typology of Cybersecurity Governance Models, 13 St. Antony's International Review 64 (2018) (Abstract).

i. What can localities do?

It goes without saying that when people collectively work towards a common goal, the results are more impactful than when they operate in separate silos. Instead of each county/city attempting to resolve their cybersecurity issues individually, they should collaborate with professional consortiums, especially established ones like ACCIS. ACCIS is an organization whose members include chief information officers of the cities, counties, state agencies, and some special purpose districts in Washington. ACCIS offers opportunities not just for professional development for local government IT professionals, and they also represent the issues and interests of local jurisdictions to the State. Further, professional organizations are uniquely positioned to effectuate some of the collective purchase programs that could help local governments build their cybersecurity infrastructure cost-effectively.

Further, local governments should take positive steps toward elevating the importance of cybersecurity in their organizations. The county managers or board of directors who make strategic decisions for local organizations might find it difficult to provide oversight in a highly technical area like cybersecurity. Helping decision-makers understand why cybersecurity matter is a critical step in gaining support. This can be accomplished through a regular exchange of information between IT and leadership or by bringing in an outside facilitator. This external facilitator could be a local educational institution or a professional consortium like ACCIS.

However, these suggestions do not imply that local governments must tackle cybersecurity issues alone. Due to the limited local opportunities for raising revenue, local governments need intragovernmental aid to prepare for cyber-incidents. Despite the challenges inherent in a multi-stakeholder approach, the best option available currently to local governments

is to foster a strong partnership with the State. In turn, the State should abandon its "ad hoc" approach and move toward formalizing its relationships with local governments.

ii. What should the State do?

Local governments have myriad challenges in addressing cybersecurity. A policy initiative that has gained momentum since 2019 among state legislators to address local cybersecurity challenges is the whole-of-state approach.[21] The whole-of-state encourages state governments to look beyond the state assets to the interest and concerns of the local jurisdictions. The approach likely grew out of England's "joined-up government" approach prevalent in 1998[22] and was used there to successfully provide aid to weaker states.[23] In practice, the whole-of-state appears to be an offshoot of the multi-stakeholder governance approach. It builds on and refines the fundamental tent of "collaboration" in the multi-stakeholder approach and brings in a formal framework for implementing some of the partnership objectives of a collaborative undertaking. Both North Carolina and North Dakota have taken positive steps toward resolving cybersecurity challenges from a whole-of-state perspective.

a. North Carolina[24]

North Carolina's whole-of-state addresses three key areas of cybersecurity: information sharing, incident response, and incident reporting. Though local governments are not required to use state resources to address their cybersecurity issues, the state government actively engages with local governments to raise awareness of the resources and services that are available to them. NC has created a state-specific Information Sharing, and Analysis Center called the NC-ISAC. NC-ISAC provides a central resource for gathering information on cyber threats to

[21] https://statescoop.com/whole-of-state-approach-on-cybersecurity-growing-in-popularity/
[22] http://news.bbc.co.uk/2/hi/special_report/1998/11/98/e-cyclopedia/211553.stm
[23] https://www.cgdev.org/sites/default/files/archive/doc/weakstates/Fragile_States.pdf
[24] NC's Whole of State Approach to Cybersecurity: Working across the state to Prepare, Prevent and Support.

critical infrastructure and enables two-way information sharing between state agencies and local NC governments.

NC also created a Joint Cybersecurity Task Force that provides incident response assistance to *any* government entity in NC, including county governments and school districts. The focus of this task force is to remediate and recover infrastructure and data compromised during an attack and provide training that can help prevent future cybersecurity incidents. When an entity reports an incident, the state offers subject matter experts, resources, and assistance ranging from incident coordination, resource support, technical assistance, and on-scene incident recovery and deployment of the NC Joint Cyber Security Task Force to assist if needed.

In 2019, the NC General Assembly passed N.C.G.S. 143B-1379, which requires all local government entities to report cyber incidents. Further, to reduce the likelihood of repeat attacks, NC is also considering legislation that would prevent NC governmental agencies from paying ransom in response to a ransomware incident.

b. North Dakota

In North Dakota, the state government has the power to oversee cybersecurity for all levels of government, including counties, towns, courts, and schools. It is the first state in the nation to provide network services to all government agencies, including the counties, cities, and school districts. ND Senate Bill 2110 defines network services as equipment, software, and services necessary to transmit voice, data, or video. The state runs a secured central network that the local governments can join if desired. Further, under SB 2110,[25] ND Information Technology Department can centrally "advise and oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the state board of

[25] https://legiscan.com/ND/text/2110/id/1892250

higher education, counties, cities, school districts, or other political subdivision."

c. Washington

The current governance approach in Washington incorporates some of the features found in North Carolina. The State has implemented mandatory breach reporting requirements, which obligates any entity, including local governments, to report security incidents affecting 500+ people. Additionally, the State through the Washington Auditor's Office provides some services like penetration testing for free. However, there is a waiting list of over five years to access these services. Though there was once talk of creating a local ISAC like in North Carolina, the idea seems to have been abandoned. However, many local officials expressed an interest in having a Washington-specific ISAC to provide localized information.

(ii) Cybersecurity governance currently in Washington

The primary agency responsible for coordinating IT services efforts in Washington is the Consolidated Technology Services Agency (WaTech). Organized under WaTech is the Office of Chief Information Officer (OCIO), which provides governance direction for statewide enterprise architecture and standards. An oversight body called the Technology Services Board advises the CIO about cybersecurity investments, risks, and policy changes. Following a significant security breach that exposed about 1.6 million Washingtonians' personal information, in 2021, the State passed Senate Bill 5432, establishing a separate Office of Cybersecurity (OCS). The OCS is responsible for identifying risk to the State's network, and the Washington Military Department focuses on the risk that impacts critical infrastructure.

The State responds to "significant" cyber events in a "whole of government, the whole of community" fashion.[26] A "significant" cyber incident is one that is likely to cause, or is causing,

[26] WA Significant Cyber Incident Annex

harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture of the State.[27] The State also coordinates its incident response efforts with non-state agencies. For this purpose, the State has set up a Cyber Unified Coordination Group (Cyber UCG), which consists of representatives from federal, state, local governmental, academia, as well as private and critical infrastructure sectors. The composition of the Cyber UCG changes based on the nature and scope of the cyber incident. The Governor can also utilize the National Guard to help with incident response.

If a "significant" incident impacts local governments, the State will likely step in and aid. However, the State's cyber-incident response plan requires the local governments to plan their own response and recovery process. But 36% of the polled local officials indicated that they do not have an incident response plan. Currently, most local governments appear to rely on the incident response services of their insurance companies.

(iii) Is Washington moving towards "whole of state"?

In addition to setting up a separate Office of Cybersecurity, the 2021 Senate Bill 5432 also assigns OCS the responsibility to serve as a cybersecurity resource for Washington local, municipal and tribal governments and develop a catalog of cybersecurity services for local partners. In 2021, Washington was also selected to work with the National Governor's Association on policies to advance its whole-of-state cybersecurity posture. Accordingly, the State appears to have embraced a whole-of-state attitude toward cybersecurity. However, what

[27] Ibid.

whole-of-state means to Washington is currently unknown.[28] Perhaps SB 5432 will take on some of the whole of state objectives.

Based on the tenor of Senate Bill 5432 and our conversations with the state and local officials, it is doubtful that "serv[ing] as a cybersecurity resource" would include creating and maintaining a secured network for the local governments' use like in North Dakota. However, the State is interested in providing shared services to its local partners.

The local cybersecurity officials welcomed Washington's offer to provide a catalog of cybersecurity services. 74% of the poll participants indicated they are willing to pay a small fee to access the services. In addition to developing a catalog of cybersecurity services for local governments, the State should utilize the federal cybersecurity grant money to implement some of the following collaborative programs designed by other states and provide them free of cost to local governments.

Training - Delaware currently offers voluntary statewide training to state and local government employees. [29] With the federal infrastructure grant, Washington should establish training centers in collaboration with the University of Washington that provide free cybersecurity awareness courses to local government employees. The University of Washington is uniquely positioned to take on this task because it houses the Information School that already provides educational programs on cybersecurity.

Free assessment tool – Michigan collaborated with five of its counties to develop an assessment tool called CySAFE. [30] It is a free security assessment tool to help small and mid-sized organizations assess, understand, and prioritize their basic IT security needs. Assessment

[28] The OCS did not respond to this question during interview.
[29] Christiana K. McFarland, State and Local Partnership for Cybersecurity: A State by State Analysis, 7-14, https://www.nlc.org/resource/state-and-local-partnerships-for-cybersecurity/
[30] Ibid.

tools like CySAFE are critical for those small Washington governments without a risk assessment process. A risk assessment process that could inform and support cybersecurity budgeting efforts is essential to obtaining intra-governmental aid through grants.

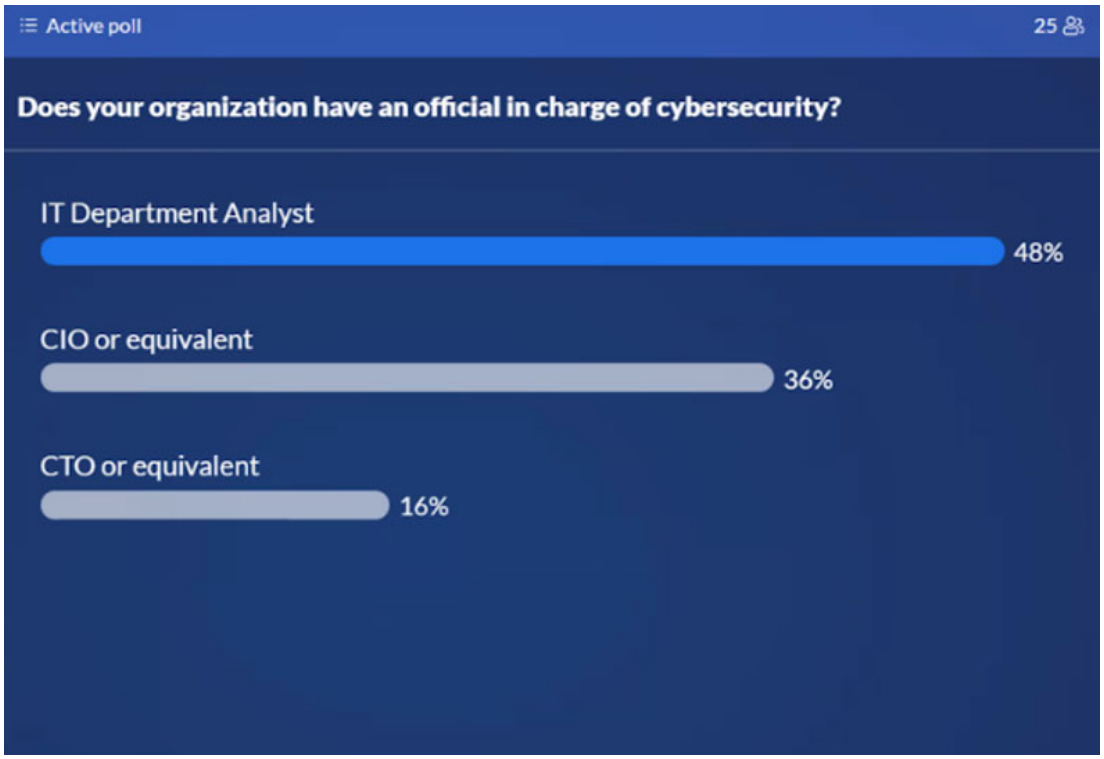
Cybersecurity working groups - Many states have established working groups to incorporate local interests.[31] For example, in Massachusetts's Cyber Resilient Working Group connects various levels of government. Some states establish them for a limited time to achieve a specific goal or to conduct research or produce reports. Others are permanent organizations set up to address present and future issues. Washington currently has a working group called Cyber UCG that comes together in an ad hoc manner in the event of a cyber incident. Washington should establish a permanent cybersecurity council under the OCS exclusively for local jurisdictions. The council will be a venue for the local governments to bring present and future cybersecurity concerns to the State.

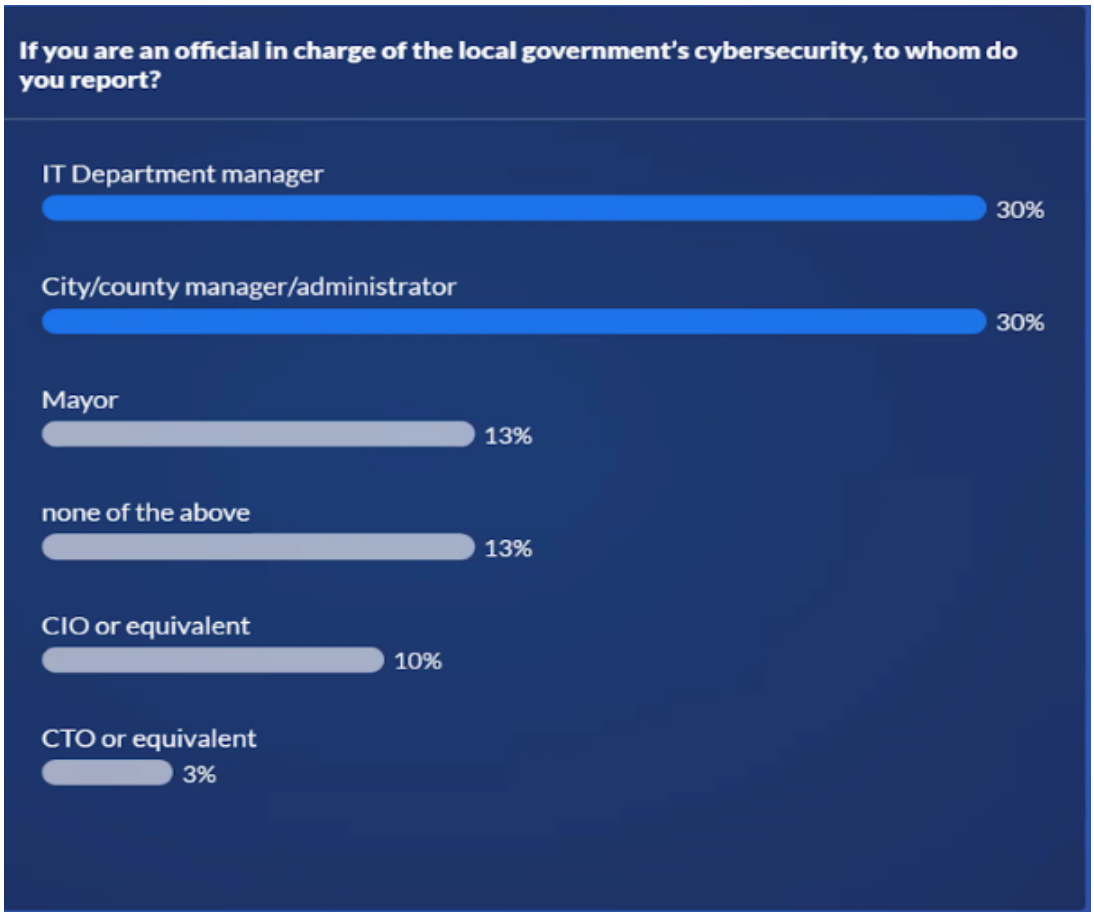
IV. Conclusion

Washington is uniquely positioned to address the cyber issues of its local governments. The State is better equipped to facilitate collective action because of its proximity to local issues and interests. However, it must take steps to formalize its relationships and commitments to better serve these small communities. These steps will hopefully provide local governments in Washington a reliable partner to help shoulder the burden, and better protect themselves against future cyberattacks.

[31] Ibid.

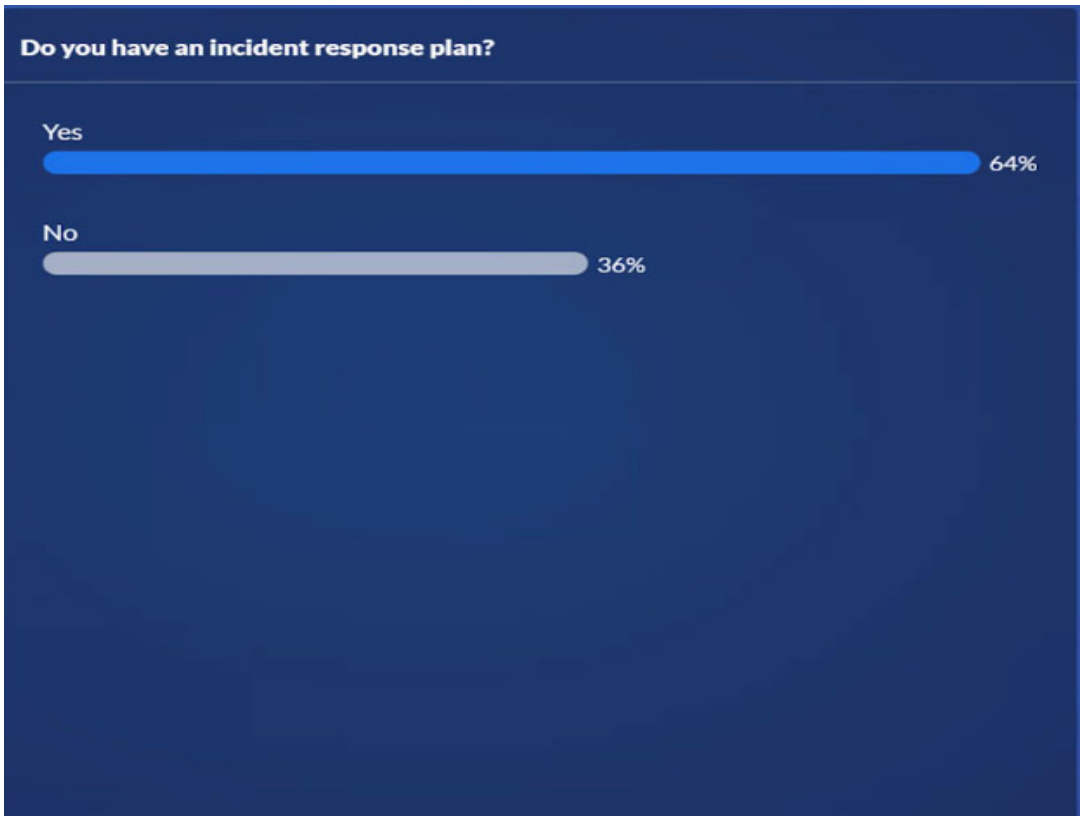
Appendix A - Poll results from ACCIS 2022 Spring conference


Active poll
25
Does your organization have an official in charge of cybersecurity?
IT Department Analyst
48%
CIO or equivalent
36%
CTO or equivalent
16%


If you are an official in charge of the local government's cybersecurity, to whom do you report?
IT Department manager
30%
City/county manager/administrator
30%
Mayor
13%
none of the above
13%
CIO or equivalent
10%
CTO or equivalent
3%


Who makes the funding decisions in your organization for cybersecurity?
City/county manager/administrator
59%
IT Department
31%
CIO or equivalent
9%
CTO or equivalent
0%
Mayor
0%


Do you rely on any state or federal grants for cybersecurity?
We lack the manpower to apply for grants.
73%
Federal grants
20%
State grants
7%


Do you have an incident response plan?
Yes
64%
No
36%


Should there be a fee attached to the services in the catalog?
We don't mind paying a small fee.
74%
No.
26%

Appendix B – List of Interviewees

1. City, county, multipurpose district officials at the 2022 Spring ACCIS Conference.
2. Washington State Office of Cyber Security
3. Zack Hudgins, Washington Office of the Chief Information Officer
4. Dan Mann, Office of the Washington State Auditor
5. Alisha King, Washington State Cybersecurity & Critical Infrastructure Manager
6. Ian Moore, Cybersecurity State Coordinator/Advisor, CISA Region 10 (WA)
7. Mike Almvig, Skagit County Information Services
8. J.D. Braathen, Snohomish County Department of Information Technology
9. David Olsen, Jefferson County Information Services
10. Josh Booy, Lewis County Information Services
11. Jesse Moore, Office of the CISO, University of Washington
12. Cooper Smith, Washington State Office of the Attorney General
13. Ryan Davis, Chief Information Security Officer NS1