NEW
AMERICA

May 2018

Cybersecurity for the States: Lessons from Across America

Natasha Cohen ZLWK FRQWULEXWLQJ DXWKRU %ULDQ 1XVVEDXP

Cybersecurity Initiative

Last edited on May 29, 2018 at 1:03 p.m. EDT

Acknowledgements

The authors would like to thank Robert Morgus, Ian Wallace, and David Weinstein for their assistance with the formation and development of this project. We would also like to thank all the experts we interviewed for this project and the reviewers who provided us with feedback, who are too numerous to name.

This paper was produced as part of the Florida International University - New America Cybersecurity Capacity Building Partnership (C2B Partnership). This innovative collaboration brings together two cutting edge institutions to address one of the biggest issues of our day: cybersecurity. Find out more at newamerica.org/cybersecurity-initiative/c2b

About the Author(s)

Natasha Cohen is a fellow in New America's Cybersecurity Initiative. She is also the Director for Compliance and Information Security Risk at BlueVoyant, where she directs BV's internal compliance and risk efforts and leads a team of cyber professionals to help clients to assess,address, and integrate cybersecurity across their business enterprise and risk management frameworks.

%ULDQ 1XVVEDXP is a fellow in New America's Cybersecurity Initiative. He is also an assistant professor in the College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC) at the University at Albany, an DIILliate scholar with Stanford's Center for Internet and Society (CIS), and a former intelligence analyst.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

Contents Cont'd

Executive Summary

This study examines states' efforts to advance cybersecurity efforts, enumerating lessons learned from an in-depth focus on three case studies of states that have seen demonstrable successes.

State programs are all unique and heavily dependent on the organization of local government, but across all structures, the key lesson is that effective and lasting programs institutionalize cybersecurity efforts in several areas:

- Formalization of a trust-based relationship with the private sector. Leadership, interest, and involvement from partners can enable timely and actionable information sharing and mitigate risk across the ecosystem.
- Codified roles, responsibilities, and authorities in law and/or executive order. Such action is a clear indication of leadership support for cybersecurity efforts and helps to reduce friction and confusion.
- Cross-bureaucratic agreements or structures. Cybersecurity is a topic that crosses the responsibilities of multiple existing institutions, which should all be involved as stakeholders. Bureaucratic superstructures or supra-bureaucratic coordinators help to break down stovepiping and align all of state initiatives.

While this report focuses on state efforts, the federal government has a role to play in helping states develop their programs. Priority efforts should include:

- Designating specific cybersecurity funding that is linked to national priorities. Such funding mechanisms could provide guidance to state and local policymakers and help streamline the national ecosystem. While cybersecurity remains a line item in other funding mechanisms, it necessarily remains more generic and less supportive of current policy and strategic initiatives.
- Deconflicting and streamlining federal incident response, guidance, and assistance programs. Current stovepiped structures create conflicting guidelines in many areas such as incident reporting and regulatory requirements.
- Prioritizing and institutionalizing the expansion of formal localized assistance programs, particularly from DHS and DoD. State, Local, Tribal, and Territorial (SLTT) efforts rely heavily on personal connections, for which the existing programs are currently underresourced and/or immature nationally.

Chapter 1: Introduction

This report focuses on state-level cybersecurity because of its critical place in the cybersecurity ecosystem within the United States, particularly in three key areas: responding to cyber incidents, protecting critical infrastructure, and supporting the development of a cyber workforce.

Today’s cyber threat environment features a proliferation of cybercrime and attacks from nation-state, nonstate, and nation-state-sponsored actors on both public and private sector systems, along with global “contagions” that can affect large swaths of digital infrastructure simultaneously.[1] To address these challenges to America’s security, we need to have a national cybersecurity program that is e concerted SLTT action. From elementary STEM education, to community colleges and vocational training, to universities and research institutions, to workforce development and retraining initiatives—these are programs and challenges that are overwhelmingly built and run by states and localities.

States also have the advantage of local relationships informing the provision of services e

Chapter 2: Three Approaches

The following three approaches demonstrate how proper leadership, organization, governance, and prioritization can succeed in fostering information sharing, improving defensive efforts across the entire ecosystem, streamlining incident response processes, and supporting workforce development programs.

While these are not the only valid means of solving the problems and threats described above, it is worth delving deeply into the selected case studies to analyze the specific factors enabling their success. As we detangle the skeins of cross-sector solutions, we can thereby tease out the threads of lessons learned regarding the dependencies for that success, and form a greater understanding of the challenges faced by policymakers and operators using each model. This section provides a summary of each case study; a full analysis for each is provided in Appendices IIII.

Part I: The Community Approach (Arizona)

Timely, actionable information sharing is a pervasive challenge throughout the cybersecurity community. The 24 Information Sharing and Analysis Centers (ISACs) and numerous Information Sharing and Analysis Organizations (ISAOs) provide information sharing capabilities and services to widely varying degrees of comprehensiveness, but few take a cross-sectoral approach and even fewer provide regularly valuable and dependable information to their members.

BOX 2

ISACs and ISAOs

Information Sharing and Analysis Centers (ISACs) were first introduced in 1999 pursuant to the Presidential Decision Directive-63 (PDD-63) signed in 1998. These sector-specific organizations, linked to each of the established Critical Infrastructure Key Resource (CI/KR) sectors, are established by the owners and operators of that sector to provide sector-based threat analysis and information sharing.[8]

Executive Order (EO) 13691, signed in 2015, set forth the concept of the Information Sharing and Analysis Organizations (ISAOs) as communities for disseminating information across a specific region or in response to a specific threat. ISAOs often are cross-sector organizations and can expand beyond the

New Jersey has been able to increase the breadth and quality of its monitoring services, expand its information sharing and educational initiatives to reach organizations and individuals across multiple sectors, and increase its efficiency across developing cybersecurity priorities. Especially important to this consolidation and coordination is offering state and external partners a single point of contact for cyber concerns.

The NJCCIC serves as the central coordinating, and in some cases, also the operational arm of cybersecurity within New Jersey. Its four branches provide monitoring and incident response services across the executive branch, cyber threat analysis and dissemination, risk and compliance assessments, and external services. The NJCCIC works with internal and external stakeholders already existing within the state, but also provides a new suite of services that operate across relevant agencies and sectors. One of the keys to the NJCCIC's success is its brand and recognition—it has become the locus for external stakeholders to report incidents and disseminate information to organizations within New Jersey and for entities seeking updated information.

However, operating such an organization is heavily resource dependent, and like many other states, New Jersey faces challenges with recruiting talent. Furthermore, this public-sector driven approach does not engender the kind of effusive two-way sharing that the ACTRA model does, although it provides a reliable system for dissemination to the private sector and improved coordinated defense to New Jersey's executive branch agencies. This trade between centralized public sector coordination and control, and more diffuse cross-sector governance models highlights important concessions that come with any particular model of administrative structure.

Placing the CISO under the aegis of the Homeland Security Office in New Jersey sends a strong message that cybersecurity is not just an IT problem, and gives the state CISO a mandate to expand cybersecurity planning across state agencies. However, funding gaps and/or a mismatch in strategy from the state's information technology apparatus can challenge eand ant hd(within5(h ancylia)10(b6)6(e s)5se)11(tw) /T1_(

(CIO) in the Washington Technology Solutions department (WaTech) and through the O

Chapter 3: Lessons for State Policymakers

Every state and territory is different, and the unique laws, structures, and priorities that each state's policymakers inherit tend to impact their decision-making on cybersecurity efforts. That being said, there are some common lessons that policymakers can keep in mind as they design and move their programs forward.

Lesson I: Proactive Leadership Matters

Each of the actions described in this report require strong leadership from the top. Cybersecurity is, and should be, an executive-level issue. Gubernatorial support lends legitimacy to the efforts of the operational-level employees executing on the plans, and helps tie together disparate elements of state bureaucracy.

Effective cybersecurity programs will necessarily have to extend beyond a single term, however, and will likely cross parties and administrations. Current governors should strive to form long-term strategies that will come to fruition beyond their administration, developing enduring models and effective means of implementation. This process should include pushing programs down to the staff level so that they can survive political transitions and institutionalizing programs through legislation.

BOX 3

The Texas Cybersecurity Act

The Texas Cybersecurity Act (House Bill 8), signed into law in 2017, is one of the most comprehensive pieces of legislation regarding cybersecurity at the state level. Among other things, the bill establishes requirements for agencies to follow related to cybersecurity and a 48-hour breach notification requirement, prioritizes narrowing the workforce gap, and sets clear direction for the state's Cybersecurity council.

It also requires the Department of Information Resources (DIR) to support the creation of an ISAO to be run under the state's cybersecurity coordinator. This organization will be focused on solving the workforce problem and helping to spread cybersecurity expertise to the various political subdivisions (local

Lesson II. Institutionalization Aids in Sustainability

nationwide mean that, much as states often have fewer resources and specialized personnel than their federal counterparts, many localities have weaker capabilities or less specialized workforces than their state counterparts. Thus, the need for states to offer support to these jurisdictions is often much higher than the states have capacity for.

Lesson V. A Comprehensive Program is a Centralized Multistakeholder Approach

To create a comprehensive program, there needs to be significant engagement in cybersecurity programs from multiple parts of government, not only IT. As described above, external involvement helps to increase buy-in. But separating cybersecurity from IT can be critical to strategic planning and prioritization. Security and technology have similar components while harboring distinct goals and challenges with regard to growth and risk; having a CISO who reports to the CIO can, in some cases, create a conflict of interest. It can also impede efforts to integrate cybersecurity into the rest of the security and response processes in a state. If separating the CISO from the CIO isn't possible, having significant parts of the program led by other departments can help to achieve those aims. It is clear, however, that segmenting responsibilities for cybersecurity among various government entities presents its own set of bureaucratic challenges.

A cybersecurity superstructure or a cybersecurity coordinator or advisor that sits on top of existing agencies to set priorities and coordinate and/or run cybersecurity efforts throughout the state can be a solution to this problem. It is unlikely that a state would choose to countermand the legal authorities of specis

legislative branch, where there are several pending bills concerning cybersecurity efforts at the federal level.

Within DHS itself there is additional work to be done to streamline the process for working with SLTT actors. Voices from various parts of the department or affiliated entities (SECIR, FEMA, NCCIC, MS ISAC, CERT, CSAs, PSAs, etc.) have their own outreach programs that suffer from a lack of central coordination. While each organization may be doing great work, such success can be tempered by competing communications. There should be department-wide priorities for SLTT efforts that are tied to speci which the National Guard cyber teams are trained and funded to conduct domestic operations in support of DHS, in an agreement similar to that between the DoD and the National Science Foundation (NSF) for the NSF's Polar Program.[15]

Appendix I: Methodology

This report seeks to answer three questions:

- What has been achieved in managing cybersecurity needs at the state level?
- What are the challenges states face in doing so?
- What are the dependencies that have supported those successes?

In order to examine each case in detail and gain a deep understanding of the specific needs and environments affecting each set of choices, the authors have focused on three states: Arizona, New Jersey, and Washington. These states were chosen for their diversity of approach, maturity (demonstrated success over time), and scalability (capacity for duplication in other states seeking to improve or begin cybersecurity program(s).

Representatives from ACTRA sit in the ACTIC, Arizona's "all-hazards" Fusion Center that serves as Arizona's analytic and dissemination organization statewide. ACTRA's president also sits on the ACTIC's executive board representing private sector, as a bridge to law enforcement and intelligence. The Fusion Center processes various threat and information feeds and communicates critical information to state/local/tribal entities, critical infrastructure operators, and nontraditional organizations. Structurally, the ACTIC sits within Arizona's Department of Homeland Security, although the chief information security officer for the state reports directly to the Arizona CIO, who resides in the Arizona Department of Administration.

Arizona also runs several other initiatives, some of which are run in concert with or are supported by ACTRA. These include various exercises that span across the private and public sectors, including federal and state partners, including regional cybersecurity workshops that reached over 750 people in the latter half of 2017, mostly in underserved areas. The State CISO and the ACTRA's CEO, communicating directly with a U.S. government agency, and have greater confidence in the anonymization of the information sharing.[21] If the government needs or desires to identify the originator of the intelligence, they can route the request through ACTRA.[22]

The need to share and deliver accurate information is manifested in efforts to align the self-interest of all key stakeholders, and drives ACTRA's National Security/Risk Management Value Proposition. ACTRA's goal is to "deliver a timely, cost effective, actionable individual and/or collective response to protect individual critical sector corporate assets, and improve our national security through adopting a unique collaborative structure."[23] In order to do so, ACTRA and its members place a heavy emphasis on the quality and value of the intelligence it shares. For its direct or manual information sharing mechanisms, ACTRA strongly suggests that intelligence shared be limited to new or unusual tactics, techniques, and procedures (TTPs), and/or vulnerabilities.[24]

Specific information sharing initiatives include email alerts sent directly by members to other vetted member touchpoints, specialized sharing per industry (e.g. supplier threats to an industry), disseminating information via a shared threat intelligence system that includes STIX/TAXII feeds and a plug-in for most SIEM platforms, and both unclassified and classified ACTRA FBI Tear Sheet Exchanges held at the Arizona Fusion Center, that include FBI and other agency briefs. The latter briefings, facilitated by the FBI and DHS agencies, are held monthly (classified briefings being held quarterly,) and are open to all members and key agency stakeholders under Chatham House Rules and legal protection. The briefings are essential to developing a working relationship and inter-reliance between private and public-sector individuals and cyber professionals, and agency stakeholders within the state of Arizona. If the government stakeholders share real actionable information, private institutions are more likely to share information back. The discussions that stem from these briefings are also useful both for the private sector representatives in attendance and for the government briefers, as they often go further into detail and impact than a one-directional briefing could achieve.[25] Regular C-Level roundtables coordinated by Arizona's CISO Mike Lettman also aid in this ongoing effort.

BOX 4

The Threat Unit Fellow (TUF) Program

ACTRA's information sharing efforts are facilitated by the Threat Unit Fellow (TUF) Program. The ACTRA Cybersecurity Academy (ACA) runs a 300-hour apprenticeship/training program with a robust cyber threat analysis curriculum, and real-world experience across all ACTRA organizations. Upon graduation from this program, TUF members become a part of the ACTRA Virtual SME[26] Response TUFTeam (VSRT) and serve as analysts in ACTRA and at their own organizations, where they can feed information to the Threat Intelligence Platform and provide a vrm4Tela9t19(a)13( )-m4Te 9(vr)0(P)24s, wt on curriculum sets that would institutionalize some of the training elements and make it more aligned with prospective employers.

ACTRA and its members also work with the Phoenix Chamber of Commerce, which has a cyber workforce collaborative initiative directed by Jennifer Mellor. One initiative, which utilizes the SkillBridge[31] and Career Skills Program (CSP)[32], both offered by the U.S. Department of Defense, provides government sponsored six-month apprenticeships in public and private organizations for service members leaving the military. Once that period is completed, companies who take part in the program providing internships can then hire the trained individual at their own discretion. This program was discovered by an ACTRA member company as part of their relationship with southern Arizona military facilities and has now expanded as a pilot to other members and to other military installations in Arizona.[33] In turn, ACTRA just announced that the program will be rolled out across all of Arizona shortly through a rapid deployment methodology developed during the ACTRA pilot in cooperation with the ACTRA Member Organization serving as the Team Lead.

Cyber Defense

ACTRA is written directly into the Cyber Annex to Arizona's emergency response plan.[34] Per this plagr(x t)5(er Anne[(o)-10(d b50)5(ad.)]T0This pr)11(ogr)16(am w)5nmh theoed b5hme exposure to national efforts and related activities performed in other areas of the country.[39]

Local engagement creates further challenges for member firms with professionals in multiple areas. ACTRA training is only available at its designated facilities; if an organization has its security staff employed in a distant location, they must front the cost for travel and accommodation for portions of the training. Finally, some ACTRA information may be duplicative with that received by employees from other areas, adding a step of deconfliction with already reported or differing intelligence.[43]

Member Limitations

Although ACTRA's fees for service and participation in the organization and its programs are a fraction of the cost of membership for most Information Sharing and Analysis Centers (ISACs), there is some barrier to entry created by such dues and charges. Non-members do not receive direct benefits beyond the formal RFI advisories, although they further profit from the improvements to the ecosystem. Smaller companies may also not have the in-house expertise to be properly analyze and act on the information they receive.[44] This is proactively addressed through the availability of automation where possible and in the future, and special MSP relationships.

Larger ACTRA members and outside stakeholders voluntarily donate additional funds, thereby keeping the general membership costs low, and chosen stakeholders offer discounts for services provided to members.[45] Even beyond the cost factor, other limitations present ongoing obstacles to full private sector market penetration. Procuring buy-in from corporate executive and legal teams has proven to not be an impediment given ACTRA's formula, including the information sharing initiatives. That said, both policymakers and lawyers need to be educated at times, particularly around information sharing. ACTRA's board includes senior legal representatives from fortune 50 member companies, facilitating informed stakeholders proactively supporting the mission.[46]

Information Sharing

Although some machine-to-machine interface progress has been achieved toward automating the information sharing process, much of ACTRA's dissemination process remains manual as a result of the ubiquity of certain existing tools and norms. If an organization does not have a compatible SIEM platform, or if the internal security structure does not allow such a connection, all information sharing and receiving methods must be manual and can be relegated to e-mail and other communication platforms, resulting in delays in delivery. Uniform display of information beyond the Threat Intelligence Platform—dashboarding—is also a work in progress.[47]

Facilitating detailed information release back to U.S. government agencies in a non-anonymized manner involves information requests being manually routed back to the company of origin for clearance unless the authorize the sharing on submission. This process can take a prolonged period of time, resulting in deferred delivery and supplementary resources required to complete the task.[48] That said, the consensus of those interviewed is that ACTRA's information sharing occurs exceptionally quickly due to the flat responsive network, compared to other solutions.

Dependencies

Leadership

Founder Frank Grimmelmann has been the face of ACTRA since its inception. His relationships with cyber professionals, business and government agencies around the state, the region, and the country have brought in new members, encouraged others to participate, and opened a multitude of doors. Frank provides the vision and is the face of the organization, both internally and to those outside ACTRA, a critical element that continues to align the various interests of the individuals and organizations involved.

In the various interviews conducted for this study, multiple stakeholders drew attention to the strength of Frank's leadership and his role in keeping a consistent voice as an advocate for strengthening the ecosystem. The member organizations also trust Frank and the operational systems/processes in place to be their anonymizing proxy, enabling the efficient and effective involvement of the private sector in state and federal cybersecurity initiatives in Arizona.

However essential Frank has been to ACTRA, the concept has proven to extend beyond Arizona and Frank's direct involvement. WICTRA, the Wisconsin Cyber Threat Response Alliance, led by Jerry Eastman, is well on its way to demonstrating that localized versions of the ACTRA model are replicable and scalable.

Trust

This trust now extends beyond Frank to and among the members of the organization itself. Because ACTRA is operated independently and outside the government agencies with which it is involved (receiving no federal funding or grants), and as it continues to be built on a framework of personal and professional relationships, member organizations are more likely to share information back through ACTRA. Its proven system of anonymity instills

physical security, that have helped bring in new members.[52] This convergence of the physical and cyber worlds is being further leveraged through the FBI InfraGard program and relationships.

State Leadership

Having strong leadership at the state level, particularly by the CISO (who is an ACTRA Board Member, with the State of Arizona as a member organization) and the Arizona Department of Homeland Security, has dramatically increased the effectiveness of ACTRA's programs. The state and its representatives conduct multiple exercises that include ACTRA member organizations, hold networking and information sharing events, and exhibit a willingness to participate in ACTRA's programs.[53] Efforts such as state-offered training and contract negotiation (available to public entities only), which has enabled local governments to take advantage of state pricing opportunities in this sector, have further enriched the cyber ecosystem as a whole.

Community

The local community of information security professionals in Phoenix is a particularly active and collaborative one, built on working relationship and trust engendered over time. There are multiple sporting venues, which attract population densities for events and create a need for frequent and regular exercises, preparation, workforce and economic development collaboration, and information sharing between a range of public and private sector entities. Arizona is also large enough to have institutes of higher education fostering a large talent pool, and a vibrant and growing roster of companies across a broad range of industry; the region, however, is home to few Fortune 500 companies, which could dominate any conversation and present significant proprietary barriers to entry and participation, however in practice this has not proven to be the case even among fortune 50 companies. This combination of local interest and engagement has created a more collaborative community and one that is increasingly informed and enthusiastic about the ACTRA mission.[54]

Appendix III: New Jersey & The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC): The Bureaucratic Superstructure Approach

Overview

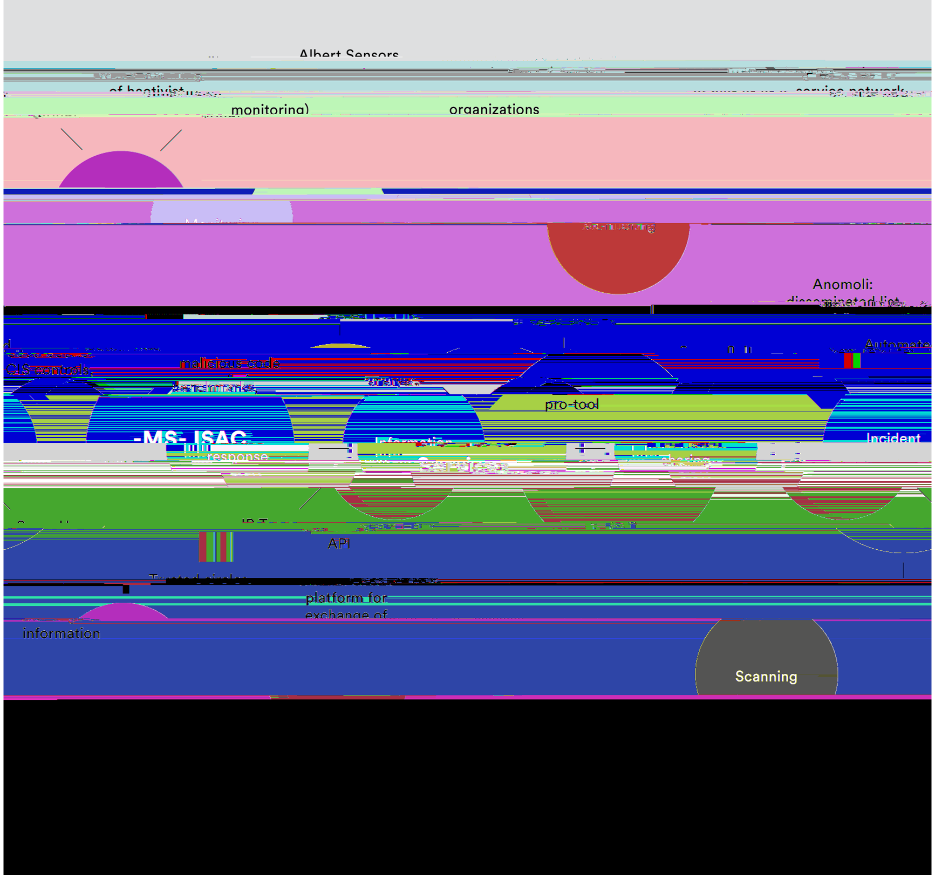
In 2016, the responsibility for cybersecurity strategy and oversight for the executive branch of NJ State Government was transitioned from the NJ Office of Information Technology (OIT) to the NJ Office of Homeland Security and Preparedness. The Division of Cybersecurity is responsible for the strategic development and implementation of an enterprise information security program to ensure the confidentiality, integrity, and availability of the State of New Jersey Executive Branch's information resources, systems, and services while promoting and protecting privacy. It focuses on identifying threats to state systems and assisting departments and agencies in managing risk to acceptable levels.

A component organization within the Division of Cybersecurity is the NJ Cybersecurity and Communications Integration Cell (NJCCIC), the first of its kind, state-level information sharing and analysis organization in the United States. Established by Executive Order #178 (Christie – May 2015) the NJCCIC acts as the state's one-stop shop for coordinating cybersecurity information sharing and incident reporting, performing cybersecurity threat analysis, and promoting shared and realtime situational awareness between and among the public and private sectors.

The NJCCIC was founded as an effort to integrate cybersecurity into the New Jersey State Fusion Center. It has expanded into a multifunction organization serving as an enterprise monitoring apparatus for the executive branch (Security Engineering and Cyber Operations Branch – SECOPS), a threat analysis organization (Cyber Threat & Analysis Branch – CTIA), center for risk management (Governance, Risk, and Compliance Bureau – GRC), and vehicle for outreach and services (Partnerships Branch). The Partnerships Branch also hosts the Incident Response Team, which provides services to some executive agencies, but mostly does triage on events to refer the affected to a private entity, the MS ISAC, or law enforcement for response.

New Jersey operates on a shared services model, for information technology infrastructure. The state chief technology officer (CTO) leads the state Office of Information Technology (OIT), which is responsible for providing and maintaining the information technology infrastructure of the executive branch of Sstate gGovernment, including all ancillary departments and agencies. The CTO

Figure 1 | MS-ISAC Services



Successes

Monitoring

Through its SECOPS branch, NJCCIC has a robust monitoring service for New Jersey's executive branch agencies. It provides both network and endpoint monitoring services and centralizes logs and alerts through a SIEM and log aggregation solution. Over the last two years, NJCCIC has increased sources to the SIEM by an order of magnitude and has been able to integrate feeds from SIEM solutions deployed to other agencies.[59] The NJCCIC will continue to add visibility across all departments and agencies of the executive branch. To support this increase in data, SECOPS personnel have focused a substantial amount of time on increasing efficiency, creating custom analytics, and decreasing false positives.

New Jersey has also deployed multiple Albert sensors from the MSAC to cover the executive branch agencies and the election systems that run on separate infrastructure.[60]

Information Sharing

The CTIA branch utilizes the information coming into SECOPS along with reporting from NJCCIC members, liaison relationships, and open source research to provide an intelligence and analysis functions for New Jersey and its citizens. CTIA disseminates multiple products, including cyber advisories, formal intelligence products, and a weekly bulletin, in addition to publicly

Outreach and Services

NJCCIC has over 6,200 members from approximately 3,000 organizations, which span across multiple industries, public and private sectors, and have expanded to reach 43 out of 50 states and members in 18 countries.[65] There are also multiple trade groups and sector working groups among the membership, which help to funnel information to multiple smaller organizations.

The cyber liaison officers in the Partnerships Branch and the analysts from CTIA provide regular threat briefings and trainings. These events, which are free to members, provide instruction on best practices and serve as a resource, particularly for small and medium businesses (SMBs) and municipal governments and organizations who would find it difficult to gather the kind of large scale threat trend information that the NJCCIC has.

The NJCCIC also runs incident response table top exercises and simulations for executive leaders and cabinet officials on a yearly basis, and has started performing risk assessments on behalf of federal partners leveraging federal resources. These activities have helped to raise awareness and increase preparedness across the state, particularly among the senior leadership.[66]

Efficiency

The OIT-driven shared services model was completed in 2017. This initiative moved control of infrastructure assets and the people who managed them out of the individual executive agencies and to the centralized control of OIT. This e 11(t)5(e)10(,CI)1-w(e inst thior)10(se)5(g9(erv)15(ie)5(s. Th c(e)5(a)10(t tr)d in 2a(entr)15(aliz)-9(ed c)5(

NJCCIC uses a mixed model of state employees and contractors. It also regularly employs interns who are hired as part time contractors while in school and then converted to full time state employees upon graduation; this program has been a robust pipeline for the NJCCIC and augments traditional recruiting methods. New Jersey is also exploring some scholarship programs in order to further leverage those individuals who are looking to enter the workforce.

Reciprocal Information Sharing

Although NJCCIC has been able to share out information, it still has work to do in developing robust bidirectional threat intelligence sharing, especially with private sector organizations. Recent changes in the law require regulated

- Providing security metrics to track the performance of the information security program; and
- Developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:
- Coordinating and conducting compliance and risk assessments of agencies and their information assets;
- Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;
- Conducting penetration tests of agency networks, applications, databases, and systems; and
- Conducting information security risk assessments of third parties with access to state of New Jersey information assets.

Since the CISO has oversight only over the executive branch of New Jersey government, there also remains a hole in centralizing security over the other branches of government, as well as for municipal or independent public sector institutions such as schools and election systems. There continues to be some shadow IT in operation that is not coordinated with the OIT or the CISO.[68] Funding gaps in IT and a lengthy procurement process further challenge efforts to update legacy systems and implement new security tools.

Integrating cybersecurity with physical security also remains a challenge, with strong support from state executives but far from complete adoption or understanding among those around the state.

Dependencies

Executive Support and Buy-in from Stakeholders

New Jersey benefited extensively from executive support and sponsorship from the governor and his cabinet. The administration set expectations up front that this would be a long term, essential project that deserved attention at the executive level. Accordingly, the director for NJCCIC and the CISO were set up to report directly to the director of Homeland Security, a cabinet-level position in New Jersey.

Also essential in building a sustainable project has been the understanding that the cybersecurity initiatives and programs started under this administration, if successful, would necessarily continue well into the next governor's administration and hopefully beyond. The acceptance and support of this long term viewpoint from the top of the administration helped to pave the way for stakeholder buy-in across the bureaucracy and with external partners.

Emphasis on Collaboration

A key factor in the success and widespread nature of the NJCCIC's partnership program is its ethos around collaboration. The NJCCIC leadership defines the organization as a service provider, with customers and partners across multiple sectors. This consistent engagement and emphasis on empowerment of mission has built successful relationships with the executive agencies, state police, FBI, DHS, and others.[69]

Funding

The NJCCIC is supported both by direct state services and grant funding, which has paid for personnel and next generation tools. Being well funded enabled the NJCCIC to focus on recruiting qualified and competitive candidates, which further helped to lend credibility to the organization's work.

Appendix IV: Washington State: The Multidisciplinary Approach

Overview

Numerous observers have commented on the strength, or perceived strength, of Washington State's cybersecurity efforts. The Hewlett Foundation noted that Washington is "…considered by many to be a leader in advancing cyber policy for prevention, incident response and technology."[70] The Pell Center at Salve Regina says that Washington has "…been at the forefront of cybersecurity protection and preparedness."[71] These are among many outside commentators who have noted the interesting decisions that Washington has made.

A few key points characterize Washington's approach. The first is a multi disciplinary approach that combines expertise and focus around cybersecurity in both information technology (where cyber vulnerabilities appear) and emergency management and risk management (where consequence management is often conducted). Secondly, Washington has taken numerous steps organizationally that are seen as forward-leaning—from early adoption of the National Guard as a tool for cybersecurity, to a large-scale reorganization of their technology agency to focus on security in addition to traditional operational imperatives. Third is the relative maturity of its capabilities and structures. While some structures, like the cyber planner position of the Emergency Management Division, are small and not heavily resourced, they exist structurally and have already begun to build strong relationships and processes.

While the idea that cybersecurity is everyone's problem, not just an IT problem, has become widespread in the world of security, the same cannot necessarily be said for the more structured and routinized world of state government bureaucracies. The structure of Washington's cybersecurity efforts shows that the state has, in fact, recognized this issue. Washington's early cybersecurity efforts were not focused around a center of gravity in the Office of the Chief Information Officer (CIO), but rather initially in their emergency management office (the state Emergency Management Division (EMD), a part of the Washington State Military Department, Washington's office of National Guard).

Starting in 2012, efforts to address cybersecurity were largely based in the state Emergency Management Division, and has since included the hiring of a cybersecurity manager and the creation of a Cyber Emergency Response Annex ("the Washington Significant Cyber Security Incident Annex" or WSCIA) to supplement the state's existing Comprehensive Emergency Management Plan or CEMP.[72]

Subsequent efforts have focused more on the IT and IT security components of cybersecurity, as opposed to the management components focused at EMD within the Washington State Military Department. In 2015, the state legislature approved the creation of an Office of Cybersecurity headed by the state chief information security officer (CISO) who would report to the CIO.[73] Subsequent efforts also added a chief privacy officer who also reports to the state chief information officer and expanded efforts to provide centralized IT services through Washington Technology Solutions, known as WaTech, which is led by a director co-hatted as the CIO.[74] The following year, 2016, the governor of Washington signed an executive order creating a new Office of Privacy and Data Protection within the Office of Cybersecurity, an office that intends improve information sharing about standards, best practices and other training for both state agencies and the general public.[75]

Successes

Protection of Critical Infrastructure

Washington has done a number of things that are seen as forward leaning. Perhaps at the top of the list is its early adoption of its National Guard assets for cybersecurity purposes. Through extensive work from lawyers on all sides, and with the support of the governor's legal advisers,[76] the state has managed to create legal processes to enable National Guard teams to engage state agencies and critical infrastructure partners. While early versions often took almost a year to sort out, the fact that these processes now exist and are understood more widely, serve as a starting point for the possibility of growing such cooperative efforts.

With the introduction of the Office of Cybersecurity, which is exclusively focused on the defense of state networks, the National Guard has been able to focus on its private sector partners.[77] The Washington National Guard now conducts an average of two penetration tests per year on critical infrastructure partners' systems. Its efforts going forward are to "train the experts"; while penetration tests are useful, there are multiple sources for such expertise. Given the Washington Guard's extensive experience with SCADA systems and with the assumption that a persistent attacker will likely be able to penetrate these systems over time, program leadership is turning to conducting hunt operations and providing instruction on how to do the same to critical infrastructure operators.[78] The state has also been able to sponsor clearances for critical infrastructure operators so that they can receive classified briefings.[79]

These engagements serve three functions: First, they increase the defensive posture of critical infrastructure; second, they enable Guard units to gain experience on real, operating systems; and third, they provide critical touchpoints between the National Guard and their critical infrastructure partners before an incident occurs. By testing these systems, the Guard units also become familiar with networks and tools they may one day need to defend and build critical relationships that can support incident response efforts.

Well-Exercised Capability

While many states have cyber units or plans, there is always some delta between the capabilities that exist in theory, and those that are actually deployable in the case of an incident. Washington State has embraced the fact that the only way to understand the gap between expectation and reality is to test those capabilities, relationships, and people. As such, the state engages in at least four cyber exercises annually.[80] These exercises, are importantly, designed to test various provide assistance to local governments or other branches of government upon request.[83]

Part of Washington's incident response protocol is to activate the Cyber Unified Coordination Group (UCG), which includes personnel from government agencies at the local, state and federal levels, as well as the private sector and academia, that can assist in response by "…providing additional resources, authorities, and information." [84] Although this group has never been activated in response to an actual incident, the group is brought together during the annual exercises so that its usage is well understood and members can build the relationships that will help facilitate response in the case of an emergency.

Centralization and Management of Statewide IT Resources

Washington's cybersecurity strategy includes substantial investment in centralizing the security program through the Office of Cybersecurity and providing common resources through WaTech. Doing so enables the state CISO, Agnes Kirk, to set state-wide policies and standards and provides resources for operators in the various agencies beyond what they would be able to purchase or do for themselves. Particularly successful has been a program to institute centralized review of changes and configurations to improve compliance, security, and visibility across the enterprise for the network providers.[85]

Partnerships

Partnerships are key to the Washington model, across disciplines, across sectors, and across geographic boundaries. Perhaps the most pronounced partnerships—and the area in which many other states are still struggling—are the cross-sector ones. The private sector is deeply involved in Washington's cyber efforts. Perhaps most importantly, the Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) enables information sharing among trusted partners in government, academia, and the private sector. This group, which is similar in construct to an informal ISAO, has both public and private co-chairs, and wide involvement from private sector partners.[86] While currently relatively informal, there have been discussions of using more formal tools—like non-disclosure agreements—to structure CIRCAS, and there is a partnership with the University of Washington to develop a secure technical portal for information sharing (as opposed to sharing by phone and email).[87]

&KDOOHQJHV

Authorities

Like many states, Washington has different agencies that are tasked with different components of cybersecurity and have differing legal authorities for responding to them.[88] In Washington, WaTech is legally responsible for protecting state networks in Washington, the Washington State Patrol is legally responsible for statewide law enforcement, and the adjutant general is legally responsible for emergency management and for most homeland security roles in the state. While each of these roles, and the legal authorities that underpin them, make sense, these roles are not as integrated as they could be. Certain episodes, like the WannaCry ransomware explosion, have pointed out the limitations of not having a single state cyber point-of-contact or information hub.[89] Although there has been a memorandum of agreement drafted to delineate responsibilities between the EMD and WaTech, it has yet to be signed.[90]

This bureaucratic challenge is common in many states, and results from the vulnerabilities and consequences of cybersecurity being spread across many domains and the perception that cybersecurity programs might bring in resources. The reality, however, is that such programs often come with few additional resources that then must be spread out between the different agencies, complicating matters further.

Communications

Related to the conflict over authorities, the lack of a single voice on cybersecurity has created challenges for the State in disseminating and gathering information. Because there are many voices at the State level, federal and private sector partners alike sometimes do not know where to go for information; likewise, State organizations wishing to send information out to their private sector partners must work through a myriad of partners themselves.

Desire for Broader Access to Federal Resources

While Washington has a good relationship with many federal partners, the state also recognizes that they (ityRl)102,T* [(ha)15lve102,rs t1Twhe concnizeeerte ing in

Washington’s leadership has also advocated for an expansion of Computer Emergency Response Teams (CERTs) to deploy one to every FEMA region and an increase in the number of Cybersecurity Advisors (CSAs)[92] currently deployed regionally.[93] Although Washington has regular contact with the Protective Security Advisors (PSAs) and CSAs in the region, such an increase in both programs would enable more interaction and better localized planning coordinated nationally.

Competition for Talent

Although most states struggle to compete with the private sector for cybersecurity talent, Washington’s competition is particularly steep given the number of large technology and defense industrial base companies operating in the area. Providing access to training, a wide variety of opportunities across the enterprise, and a clear mission goes a long way, but as Washington’s CISO remarked, “there is a clear need to develop new on ramps for people wanting to enter the space.”[94] To further this goal, the Office of Cybersecurity is partnering with the National Security Agency (NSA) and DHS Centers of Academic Excellence for Cybersecurity 10(bl)6(ad)65oCyb5) and DblS(c)r1(ecur)5t(0g s6ther)11(e isx e(c)5cf0() and D

Outreach

Despite the fact that many areas of government in Washington have clearly put a level of prioritization on cybersecurity issues, it is not surprising that the function is still not as well-resourced as some might hope for. Few resources are harder to come by in state government than additional personnel, and so many agencies are forced to try and do as much as is possible with limited numbers of people. In this regard, Washington deserves much credit. By leveraging outreach—the connecting of government agency efforts with those of organizations and institutions outside of government, they've been able to have impacts outsized to the personnel devoted to the issue. For example, despite there being a single cyber coordinator at the EMD within the Washington State Military Department, he has been able to connect the EMD with many public and private sector partners across numerous activities[97]—exercises, information sharing serves a “Super TAG” who is triple hatted with duties also as the head of the State Emergency Management Division and the State Homeland Security Advisor. Because the TAG has direct reports in all of these areas, he is able to coordinate resources between them all, helping to reduce some bureaucratic friction.

Appendix V: Full List of Interviews

Chuck Ames, Maryland Director of Cybersecurity

Major General Courtney Carr, The Adjutant General, Indiana

Dave Christensen, NJ IT Sector Chief

Kawana Cohen-Hopkins, Section Chief, FEMA

Major General Bret Daugherty, The Adjutant General, Washington

Tom Duffy, Vice President of Operations, MSISAC

Jerry Eastman, CEO, Wisconsin Cyber Threat Response Alliance

Christine Figueroa, Protective Security Advisor for Arizona, Department of Homeland Security

John Forte, Deputy Executive for Homeland Protection Mission Area, Johns Hopkins University Applied Physics Laboratory

Michael Geraghty, New Jersey Chief Information Security Officer and Director, NJCCIC

Daniel Gerstein, Senior Policy Researcher, RAND

Frank Grimmelmann, CEO, Arizona Cyber Threat Response Alliance

Dave Halla, Senior Advisor, Johns Hopkins University Applied Physics Laboratory

Matthew Hartman, Director, Strategy Coordination & Management (SCM), Department of Homeland Security

Martin Hellmer, SSA Phoenix Cyber, Phoenix FBI Field Office

Blair Hyde, Preparedness Analysis and Planning Specialist, FEMA Region III National Preparedness

Juliette Kayyem, National Security Analyst for CNN and Faculty Director of the Homeland Security Project at Harvard’s Kennedy School of Government

Todd Kimbriel, Chief Information Officer, Texas

Agnes Kirk, Chief Information Security Officer, Washington

Robert Lang, Cybersecurity Manager, Washington State Military Department

Notes

[1] Meyer, C. (2017, 7 1). Deciphering an Evolving Threat Environment: An Interview with Frank Cilluffo. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/88113-deciphering-an-evolving-threat-environment; Manfra, J. (2017, 10 3). Written testimony of NPPD Office Cybersecurity and Communications Assistant Secretary Jeanette Manfra for a House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection hearing. Retrieved from US Department of Homeland Security: https://www.dhs.gov/news/2017/10/03/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-and

[2]

Cyber%20Incident%20Reporting%20United%20Message.pdf

13 RAND has a study forthcoming regarding FEMA's role in cybersecur14(l)-pd

NEW
AMERICA