NEW AMERICA

May 2018

Cybersecurity for the States: Lessons from Across America

Natasha Cohen, with contributing author Brian Nussbaum

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.

Brian Nussbaum 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 affiliate 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.

About FIU-New America C2B Partnership

The Cybersecurity Capacity Building (C2B) Partnership is a partnership between Florida International University and New America designed to develop knowledge and policies aimed at building the cybersecurity capacity in the workforce, at the state and local level, within the U.S. government and industry, and internationally.

Contents

Executive Summary

Chapter 1: Introduction

Chapter 2: Three Approaches

- Part I: The Community Approach (Arizona)
- Part II: The Bureaucratic Superstructure Approach (New Jersey)
- Part III: The Multidisciplinary Approach (Washington)

Chapter 3: Lessons for State Policymakers

- Lesson I: Proactive Leadership Matters
- Lesson II. Institutionalization Aids in Sustainability
- Lesson III. The Private Sector is a Vital Part of the Ecosystem
- Lesson IV. Focusing on Local Priorities Can Fill a Void
- Lesson V. A Comprehensive Program is a Centralized Multistakeholder Approach

Chapter 4: Recommendations for the Federal Government

- Recommendation I: Dedicate Specific Funding Mechanisms for Cybersecurity Tied to Federal Priorities
- Recommendation II: Synchronize Federal Responsibilities and Authorities
- Recommendation III: Prioritize the Expansion of Localized Assistance Programs

Contents Cont'd

Appendix I: Methodology

Appendix II: Arizona and the Arizona Cyber Threat Response Alliance (ACTRA): The Community Approach

- Overview
- Successes
- Challenges
- Dependencies

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

- Overview
- Successes
- Challenges
- Dependencies

Appendix IV: Washington State: The Multidisciplinary Approach

- Overview
- Successes
- Challenges
- Dependencies

Appendix V: Full List of Interviews

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 effective at all levels: national, state, local, and across various private sector industries. The federal nature of our government, and the resultant division in its structure and authorities, demand that state governments take an active and proactive role in responding to threats to their citizens and the organizations located in their jurisdiction.

States maintain citizen databases and provide a range of services to their residents. Protecting the integrity and confidentiality of that data and ensuring the availability of those critical services is essential to offering efficient and effective government to the citizenry. Furthermore, state agencies are on the front lines of communication and response whenever there is an incident. While historically this role has sometimes expanded to federal agencies for cybersecurity, with the prevalence of threats and their widespread impact, this primary role shifts back towards state action in most cases. States also play a role that the federal government typically does not, (except in unique circumstances or when state resources are exhausted) which is supporting localities and municipalities as they deal with crises and manage the consequences of such events. In this sense, even when states are not on the front lines of cyber incidents, they often are expected to support other jurisdictions; all this despite the fact that many states are in nascent or flux states in terms of their own cybersecurity.

Mapping and defending critical infrastructure is highly connected to state governance, due to the close relationship between regulatory agencies and their geographic sectors, as well as areas of responsibility that are under the direction of state officials, such as election security. Sectors or industries that are often regulated at the state level—like electricity, water and wastewater, and telecommunications—are areas in which states have serious cyber equities, because they are expected to manage the consequences of failures or incidents. In a similar vein, educational institutions and curricula are also shaped or controlled at the state and local level. To address the shortage of a trained cybersecurity workforce in the United States, curricula needs to be laser-focused on information technology and cybersecurity. That change will only happen with

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 effectively targeted and marketed toward their citizens. Public-private partnerships can flourish in these environments. For example, cyber ranges in Michigan and Arizona are run through partnerships between universities, the private sector, and the public sector. In Indiana, the state runs CritEx, an annual exercise exploring the ramifications and consequences of a cyber incident that affects one sector or one critical infrastructure organization.[2] Missouri's Office of Cybersecurity runs a program to identify "vulnerable internet-connected systems belonging to organizations from various industries. The program identifies high-risk systems that, if left insecure, could lead to disruptions within critical infrastructure or significant data loss, and contacts the owners of the impacted systems to mitigate risks."[3] Programs like this that embrace and rely on constellations of local and regional partners are not likely to result from one-size-fits-all federal programs, but from the efforts of the states—what justice Louis Brandeis termed "the laboratory of democracy."[4]

The answers to technical questions about how to secure networks are largely public knowledge; the challenges we face in cybersecurity often result from questions of process and people. The difficulty, as described by policy advisors from the National Governors Association in their 2017 report *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*,[5] lies in organizational structure and governance. Our own report focuses on three case studies in which states have shown success in addressing these challenges, and from which we can form conclusions that can be beneficially applied across various state structures.

While the breadth, scope, and scale of state cyber efforts varies widely, several states have effective, mature cybersecurity programs. The most commented on include programs in California, Michigan, New Jersey, New York, Texas, Virginia, and the state of Washington, to name a few. For the purpose of demonstrating different stylistic and fundamental approaches toward achieving a common goal, this report will examine state cybersecurity programs with substantive success in specific key areas. No state has all the answers yet, but this report highlights three that have made particular progress: (1) Arizona, (2) New Jersey, and (3) Washington.

Each of these states has demonstrated certain capabilities or approaches that have the potential to inform other states' efforts. The lessons learned from this study form a guide for state and local policymakers, strengthening their ability to ensure that their own cybersecurity program is as comprehensive and effective as possible. It is important to note that the approaches of these states are not mutually exclusive. In fact, elements of each model have already been adopted

by the other states highlighted in this report, and their programs are the better for it. Every state faces a unique set of challenges, draws on its own comparative advantages, and has its own political, organizational, or legacy IT environments that shape their cyber efforts. So while no model will be ideal in all contexts, individual successful programs and approaches can collectively constitute a menu of options from which states can pick and choose those methods and techniques that fit their needs.

Alongside the conclusions we might draw to help inform action for individual states, this report also offers several recommendations for the federal government. There is a similar level of urgency for the federal government to facilitate the development unifying structures, serve the needs of state governments and their constituents, and better utilize and coordinate resources from mature and effective state programs for national defense objectives. States have been clear that they are interested in federal support, not just in terms of financial resources, but in terms of expertise and organizational support.

- First, the federal government should designate specific cybersecurity funding that is linked to national priorities, namely making sure states have done baseline risk and capability assessments, the development of mature response capability for incidents across multiple sectors, and the development of an interdisciplinary approach.
- Second, federal incident response, guidance, and assistance programs should be deconflicted and streamlined to create a cross agency solution.
- Third, the Department of Homeland Security (DHS) and the Department of Defense (DoD) should prioritize the expansion and institutionalization of localized assistance programs.

→ BOX 1

DHS' CSA Program

DHS' Cybersecurity Advisors (CSA) program currently employs 11 professionals nationally with deep backgrounds in information security to cover the 10 FEMA regions. These advisors are tasked with the following:

- Providing guidance and information to SLTT organizations by participating in cybersecurity councils/teams that report to the governor, assisting with state-level planning and information sharing initiatives;

- Connecting SLTT organizations to federal resources at the MS-ISAC, NCCIC, and other parts of DHS, such as the teams that provide technical assessment services;
- Increasing awareness of federal cybersecurity policy, executive orders, and information-sharing programs by conducting one-on-one or group meetings, providing briefings, and attending conferences and symposia; and
- Conducting assessments of SLTT organizations' strategic and tactical cybersecurity risk exposures and capabilities.

With only 11 CSAs deployed across America, these advisors can sometimes be challenged to connect with and provide services to all entities under their purview. While this team is still being rolled out, the Protective Security Advisors (PSAs)[6], of which there is one designated for each state, can utilize their existing networks to do some of the initial groundwork, identifying points of contact for the CSAs and introducing SLTT organizations to the services provided by the new CSAs and their federal partners. The CSA program is expected to increase to 24 members by the end of 2018, and the existing roadmap has up to 93 advisors planned, with 44 currently approved in the upcoming proposed budget.[7]

Even if the program meets its ambitious target to triple by next year, it will still be limited in its capacity to reach the critical infrastructure and public sector entities it is designed to support across the country. Consistent contact and relationship-driven action is key; the current program simply does not have the resources to achieve its stated goals. Even then, its stated goals may not be sufficient. There are 50 states, numerous territories and tribal governments, dozens of major cities, and hundreds of localities in need of assistance. Many states will not be able to help their sub-jurisdictions until they've built much more substantial capacities of their own. The current effort, while valuable and appreciated by those who benefit from it, is not up to the scale of the challenge.

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 I-III.

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

critical infrastructure designated industries. Many are not-for-profits, but they do not need to be. ISAO structure is designed to be flexible to fit the tailored needs of each constituent group.[9]

Both ISACs and ISAOs can diverge in size and scope, with some organizations providing sophisticated services such as near real-time analysis and monitoring, training, or briefings, and others less capable of doing so.

The State of Arizona and the Arizona Cyber Threat Response Alliance (ACTRA) have formed a successful partnership that has achieved notable success in facilitating, supporting, and encouraging the sharing of real, actionable information on cyber threats and vulnerabilities. This relationship has been built over time and is based on a foundation of trust, essential for facilitating information sharing efforts. Additionally, ACTRA runs its own workforce development programs, underpinning such efforts across the state in cooperation with the Chamber of Commerce, and by pairing knowledge of need with capability of risk reduction and response, helping to provide critical resources to cybersecurity defensive efforts in both the public and private sectors.

There are challenges with using a private sector-driven and local approach: fostering a collaborative environment focused on the common good, adequately reaching and serving organizations outside of the core area, and overcoming members' resource limitations [funding] and self-interest. To create a mutually beneficial environment and encourage participation from across the private and public sectors, strong leadership from both sides is needed. Furthermore, members must trust that they have anonymity when desired, and also that their counterparts in other organizations and across the government are sharing back into the system just as they are. Such a scenario requires a reliable partnership with state entities, participation from the federal government, and the development of a cybersecurity community that reaches across sectors. ACTRA, which serves as an interface between its private sector members and its public sector partners, provides a buffer that engenders faith in the anonymity and effective dissemination of information.

Part II: The Bureaucratic Superstructure Approach (New Jersey)

Legacy bureaucratic structure, based on long past legislative authorities or historical agency mission statements, which are often heavily sector-specific, segments responsibility for cybersecurity between multiple agencies and state officials. By standing up the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and consolidating services through a shared model,

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 tradeoff 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 efforts to update legacy systems and implement new security tools.

Achieving cybersecurity goals by creating an extra-bureaucratic structure is dependent on executive support from the governor and cabinet across successive administrations, consistent funding sources, and a protracted willingness to collaborate with partners and customers across multiple sectors—factors that all introduce a certain risk of inconsistency over time.

Part III: The Multidisciplinary Approach (Washington)

The state of Washington has taken the shared services model to its full maturity, with IT services centralized through the Office of the Chief Information Officer

(CIO) in the Washington Technology Solutions department (WaTech) and through the Office of the Chief Information Security Officer, who reports directly to the CIO. Washington is also notable for its multidisciplinary approach to cybersecurity, extending responsibility outside of the information technology community to the emergency management and military departments of the state bureaucracy.

Institutionalized mechanisms for cooperation between departments increase the longevity of a cybersecurity program and increase efficiency for multistakeholder operations. Such an approach in Washington has enabled a substantial cybersecurity exercise program that reaches across stakeholders, sectors, and partnerships, improving pre-incident planning and information sharing initiatives. Washington has taken the lead nationally in its use of the National Guard to increase the defensive posture of critical infrastructure partners across the state, provide Guard units a way to gain experience with live state and private sector systems, and create an avenue for communications prior to an incident. This kind of capacity building is valuable for developing competencies within these units, but also has the potential to offer benefits in the case of an incident response that requires these units to support the owners of these networks.

Washington's shared services model has improved compliance, security, and visibility across the executive branch of government. The bifurcation between the office of the CIO and the Departments of Emergency Management and Military Affairs, however, has created occasional friction resulting from conflicting priorities and authorities. Related to this challenge, the lack of a single voice on cybersecurity has created challenges for the State in disseminating and gathering information.

Still, the achievements of this model are substantial, and have been supported by strong state leadership and legislative efforts to canonize the new organizations and authorities. Washington has thereby created an ingrained structure and platform from which to engage with stakeholders across public and private sectors and take advantage of available talent and partnerships.

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 governments) in the state through several regional centers of excellence.[10]

Lesson II. Institutionalization Aids in Sustainability

The institutional approach should span across the various different agencies and branches of state government. Engaging the various stakeholders in the planning and operation of a cybersecurity program helps to institutionalize the initiatives and bridge leadership transitions between CIOs, CISOs, and state administrations. Cybersecurity is a whole of government problem; involving parts of government outside of the IT department creates buy-in from across the state enterprise. In addition to institutionalization of positions and agencies, secure and consistent funding sources or human resources structures (civil service job titles or training programs) are also enablers of successful and sustainable programs.

Lesson III. The Private Sector is a Vital Part of the Ecosystem

Likewise, engaging private sector leadership and independent researchers is an integral component in fostering a cybersecurity ecosystem within the state, and can add vital expertise and perspectives to planning, defense, and response efforts. Enabling the private sector to play a significant role also makes them a stakeholder in the states' program and aids sustainability efforts. As these relationships mature, they support the development of trust, which is essential for effective information sharing. Additionally, the technology industry and educational institutions of a state can play an important role in shaping a vibrant and successful cybersecurity talent pool, which can have a catalytic enabling effect on state and local cyber efforts.

On the flip side, the private sector should also actively reach out to state governments to start and/or increase these efforts. Just as the private sector needs an open and supportive state government, state officials need an engaged and open community to work with.

Lesson IV. Focusing on Local Priorities Can Fill a Void

By focusing on the local environment, states can also ensure that they better serve their own communities. National-level exercises are, as they should be, geared towards situations that would have a whole-of-country impact. States can be more granular, focusing on specific scenarios that are likely to affect their citizens, and forming the relationships needed to respond to those kinds of events. State-municipality relationships are sometimes as fractured as—or more so than—federal-state ones. The challenges of federalism extend all the way through the U.S. system; states need to focus downward as much as they do upward. In this regard, the sorry state of municipal financing and budgets

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 specific agencies that manage key parts of the cybersecurity eco-system, but having a single voice and strategy on cybersecurity is essential for efficiency and effectiveness. These super-bureaucratic entities also help to bring a strategic element to the cybersecurity effort by running across the various elements of state government. Such an organization and its leadership should help develop a state-level cybersecurity strategy, align economic priorities with the security needs of the state, and facilitate public-private cooperation.

Chapter 4: Recommendations for the Federal Government

Recommendation I: Dedicate Specific Funding Mechanisms for Cybersecurity Tied to Federal Priorities

There is a widespread and acknowledged requirement for increased cybersecurity-related funding for states and cities. Existing federal funding mechanisms, such as those designated for emergency services and counterterrorism, allow funding to be spent for cybersecurity, but are not specifically designed to fund those efforts. Typically the grant recipients are in disciplines like law enforcement and emergency management, and as a result little of the eligible money has in fact flowed to cybersecurity-related projects or agencies.

Creating cybersecurity-specific funding mechanisms tied to national priorities could provide guidance to state and local policymakers and help to align SLTT programs with federal objectives and other SLTT programs to help streamline the ecosystem. When cybersecurity remains a line item in other funding mechanisms, it necessarily remains more generic and less supportive of current policy and strategic initiatives.[11]

Recommendation II: Synchronize Federal Responsibilities and Authorities

To make incident response more efficient and effective, whether for large or small incidents, the United States should prioritize deconflicting efforts, authorities, and responsibilities across the various agencies. The existing incident reporting guidance lists several points of contact that depend on the nature of the incident, which may or may not be known until well after the event. [12] Furthermore, in many cases, verbal guidance provided to SLTT representatives from various federal agencies on how to report an incident has been conflicting.

Local representatives from relevant federal agencies can address these concerns from a regional perspective, but a national approach driven from the policy level is needed. To adequately mark and resolve conflicting issues, there may need to be a single point of contact for the federal government, perhaps located at each FEMA region, to coordinate federal government response. There are additional studies forthcoming that examine the challenges of deconflicting in greater detail.[13] This issue clearly requires more study and prioritization from the agencies involved, and should be taken into account by policymakers in the

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 specific, deconflicted initiatives across different departments and functionalities. Because states have fewer specialized and focused cyber workforces than federal partners, a small number of cyber "generalists" at the state level are often expected to consistently interact with a half-dozen or more federal agencies or partners, often leaving these state agencies or organizations confused or overwhelmed.

Recommendation III: Prioritize the Expansion of Localized Assistance Programs

To better coordinate its SLTT efforts, the Department of Homeland Security (DHS) should further expand its localized assistance programs. The Cybersecurity Advisor (CSA) Program, designed to provide direct coordination, outreach, and regional support to private industry and SLTT governments has only 11 active advisors, who are roughly aligned with the 10 FEMA regions. Even if DHS reaches its targets for ramping up the CSA roster, which is by no means assured, it will still be limited in its capacity to reach the numerous critical infrastructure and public sector entities it is designed to support. Consistent contact and relationship-driven action is essential to the development of SLTT-level engagement, both with public and private entities. The current program simply does not have sufficient resources to achieve its stated goals; and arguably its current stated goals are insufficient given the scale and scope of the cybersecurity challenges facing SLTT partners.

There is additional work to be done to establish requirements and work through the authorization of DoD elements aiding the domestic mission. Such forces could come from U.S. Cyber Command through a domestic/homeland defense Mission Essential Task List as part of the Title 10 wartime mission or through the National Guard under Title 10 or Title 32 to defend critical infrastructure deemed essential for conducting or supporting military operations. So far each state has been left largely alone to develop the legal authority for activating the National Guard in the case of an emergency; guidance and additional authorizations from Congress and the NGB would help to streamline these efforts and help states build effective programs, like those in Washington State and North Carolina[14], among others. DoD and DHS might also consider habitual relationship with an underlying set of principles and a memorandum of understanding (MOU) by

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).

Appendix II: Arizona and the Arizona Cyber Threat Response Alliance (ACTRA): The Community Approach

Overview

To tackle the cybersecurity challenges facing the state, Arizona has created a "team of teams."[16] One of these teams, the Arizona Cyber Threat Response Alliance (ACTRA), is an Information Sharing and Analysis Organization (ISAO) formed in 2013. Its stated mission is to serve as the "hub for collaborative cyber information sharing in a neutral environment of trust where partners from industry, academia, law enforcement and intelligence come together, leveraging cross-sector resources to more effectively analyze critical, real time intelligence and respond to emerging cyber threats to Arizona's Critical Infrastructure and Key Resources."[17]

ACTRA has its roots in the Arizona InfraGard[18] and remains wholly independent of, but closely aligned to that organization as its "operational cyber arm" by agreement. In 2012, the AZ InfraGard initiated a planning effort, led by current ACTRA CEO Frank Grimmelmann, to understand and respond to barriers to effective bi-directional communication and information sharing between private and public sector organizations. Although this effort was led by members of the private sector, there was active involvement from the local Federal Bureau of Investigation (FBI) and U.S. Department of Homeland Security (DHS) offices and the Arizona Counter Terrorism Information Center (ACTIC). The study found a need for a separate but affiliated non-profit entity that could serve as the "self-governed private sector controlled hub for cyber information exchange and response."[19]

This arrangement allows ACTRA to focus only on cybersecurity information sharing and communication needs, and creates an effective, independent conduit (or buffer) between its private sector and public sector Member Organizations, and the agencies nationally. This separation engenders trust in the anonymization of data shared with government agencies, and helps to coordinate the efficient flow of communication. Rather than place the burden on public sector agencies to choose which private sector entities to inform and involve in specific cybersecurity efforts, ACTRA serves as the point of contact for its private and public sector Members, engaging the various members as needed. Its affiliation with InfraGard—all direct member touchpoints of ACTRA must also be InfraGard members—allows ACTRA to pre-vet its members without additional expenditure of resources.

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, Frank Grimmelmann, co-chair the new Arizona Cybersecurity Team (ACT), an executive level initiative launched in 2018 by Governor Doug Ducey to coordinate the various groups around Arizona working on cyber issues. The ACT includes representatives from federal, state (legislative and executive branches), and local government, the private sector, and higher education.[20] These members represent the various groups with a stake in cybersecurity in the state; given Arizona's established strategy of working through a team of teams, this organization will help to formalize this structure.

The following section describes the successes and challenges of having strong private sector leadership and widespread involvement in a state's cybersecurity program, and the factors that have enabled this model to flourish in Arizona.

Successes

Information Sharing

Fusing Member Organization policymakers, legal representatives and technical professionals, ACTRA's information sharing initiatives are diverse and highly dependent on the culture of trust established throughout the organization and its members. This sense of assurance is established first at the personal level, and subsequently empowers organizational dealings at every level. All ACTRA members sign an NDA, which prevents them from discussing any details about ACTRA or its member companies without explicit permission to do so. "Chatham House Rules" are also mandated for every ACTRA event. Because the information shared and the platform on which data is shared are owned by the member organizations themselves, members don't feel as though they are

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 virtual watch center service. This is further complemented by a physical Watch Center that triages incidents among VSRT TUFTeam members. These physical ACTRA trained TUFTeam VSRT members are employed by a MSP stakeholder, and have dedicated hours and bifurcated systems so that they can monitor the ACTRA systems and their own client systems simultaneously. However, ACTRA information is fed only back to those customers who are members of ACTRA.[27] Additionally, ACTRA distributes formal non-attributed advisories as requests for information (RFI) across the InfraGard and ACTIC networks. By exception approved by a Member Organizations, these can be shared with attribution with these external networks or a subset of them under the control of the member.

The TUFTeam Training is available to ACTRA Member professionals across the private and public sector and serves to build relationships between individual organizations and across sectors. Thus far, private sector, state, federal and local analysts have gone through the training; law enforcement officials and National Guard service members are scheduled to attend a session in the second quarter of 2018, while keeping the lanes in the road separate to align diverse stakeholder's self-interests.

Workforce Development

In addition to the TUFTeam/VSRT programs, ACTRA has several collaborative volunteer-driven Cyber Warfare Ranges "in the wild" for community leveraging community outreach and workforce development. One range is physically located at Grand Canyon University (but not a university resource), and the second range is located in the City of Mesa's Arizona Labs also operating independently through an identical structure. These ranges "enable penalty-free offensive and defensive exercises, and real-world operations that provide knowledge and forensic insight into how to better defend infrastructure by getting into the head of the adversary."[28] They also enable security professionals to test defensive infrastructure without risking actual organizational data.[29]

These collaborative endeavors also serve as a training ground for any individuals who may want to gain practical expertise in the field. A headhunter volunteers at the range to help place individuals who have gained experience on the range with companies needing security professionals.[30] Volunteers at the ranges are working

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 plan, in the case of an incident, ACTRA is tasked along with bidirectional communications to:

- provide resources to the Arizona Department of Administration and all Arizona state government agencies upon request;
- assist the FBI with managing and facilitate the state's role in critical infrastructure protection; and
- communicate and report information on observed cyber security incidents.

Since its inception, ACTRA has yet to be called upon for such a coordinated incident response, but after news broke about Russian targeting of the Arizona election system in 2016[35], state officials received offers for aid from several members of ACTRA.[36] ACTIC and ACTRA have also held multiple exercises to coordinate efforts in the case of an incident.[37] Additionally, ACTRA VSRT Members have been stood up alongside agencies in the Multi-Agency Coordination Center (MACC) during a major event and expect to during other major Arizona events in the future.

ACTRA also facilitates participation in regional and national table top and live exercises run by DHS, DoD, and other organizations.[38] Representatives from public and private member organizations regularly participate in these exercises, which further increases the personal ties in the cyber ecosystem and provides

exposure to national efforts and related activities performed in other areas of the country.[39]

ACTRA has three additional programs designed to increase the capabilities of cyber defense within its purview. The first such program is the ACTRA Think Tank, an invitation-only brain trust of experts who can translate the challenges experienced by members and threats observed on the ranges to solutions for the market. The think tanks drill down into particular issues and sometimes uses a member organization's infrastructure (with member approval) to test solutions. The ACTRA Special Operations Group then operationalizes those findings. These two teams have made progress in efforts to increase reliable automation by connecting various SIEM platforms with ACTRA's Threat Intelligence system, and to leverage resources in the development of additional solutions available across ACTRA.

The third program is channeled through a local university and enables students to perform open source cyber intelligence collection. In large part because of ACTRA's imprimatur (or engagement), the Phoenix FBI, DHS and other agency stakeholders supports the program, and agency stakeholders provide briefings to the students on how to remain legal in their activities.[40] With its deep network, ACTRA also serves as a point of contact for technology transfer programs within universities and chosen vendor stakeholders, when they might be looking for potential pilot sites or feedback on new cyber technologies.[41]

Challenges

Locality

The ACTRA model depends heavily on the relationships built within its community. At its core, ACTRA is a grass roots organization conceived and constructed by its constituency for its members, both organizational and individual/professional. For entities outside of the Phoenix area, attending regular and frequently scheduled meetings is an onerous investment of time and travel, especially given the demands on the types of senior executives that should be participating.[42] Although some members have advocated for virtual meetings, which now occur monthly and quarterly, the experience is not as rich as participating personally; there are also significant roadblocks to conducting the classified briefings remotely through secure video telecommunications. ACTRA is also expanding its efforts using out of state Member Organizations as the catalyst for collaborative but individual grass roots initiatives in other areas of the country, driven by the local leadership to reflect the unique aspects of the community but have the ACTRA model as a foundation for building capacity.

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

confidence, and its focus on the value proposition encourages strong participation.

→ BOX 5

WICTRA

The Wisconsin Cyber Threat Response Alliance (WICTRA) is an organization built on the ACTRA model and adapted for the needs, challenges, and realities for member organizations in Wisconsin. While WICTRA is maturing, members receive dual membership in both WICTRA and ACTRA so that they can take advantage of the information and training available to ACTRA members while participating in the local meetings in Wisconsin. Eventually, each organization will be "independent," yet maintain a very close collaborative, peer-to-peer relationship.[49]

Jerry Eastman, the CEO of WICTRA, envisions services very similar to those offered to ACTRA members, but likely more virtualized given the wide geographical spread of members. WICTRA also faces some additional challenges in working with the State of Wisconsin government, which unlike Arizona has individual CIOs and CISOs for each of the 30+ executive agencies. Although there is a state CIO and CISO, each of the agency officers play a large role. Wisconsin is a "Home Rule" state, thus each county government reports unto itself, thus the 72 counties, cities, villages, and tribal entities typically have their own IT structure, such as CIOs and CISOs. IT (especially for cyber) Resources (personnel and funding) are scarce at the local level of government. Like Arizona, Wisconsin has a State Fusion Center, the WI Statewide Intelligence Center (WSIC). WICTRA members are already serving in shifts in the center multiple days a week to help connect WSIC with the private sector and provide intelligence and context when possible.[50]

USG Participation

The willingness to share by U.S. government entities in the area (FBI, DHS, TSA, and others) fosters greater participation, as members feel that they are getting a return on their investment of time, funding, information and resources.[51] These public sector institutions have strong relationships in other areas, such as

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 real-time 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

provides vision and leadership for OIT and is responsible for coordinating and conducting all executive branch technology operations. The CTO directs the planning, implementation, and governance of enterprise Information Technology systems in support of the executive branch of state government's business objectives and operations, to improve cost-effectiveness, service quality, and mission development.

→ BOX 6

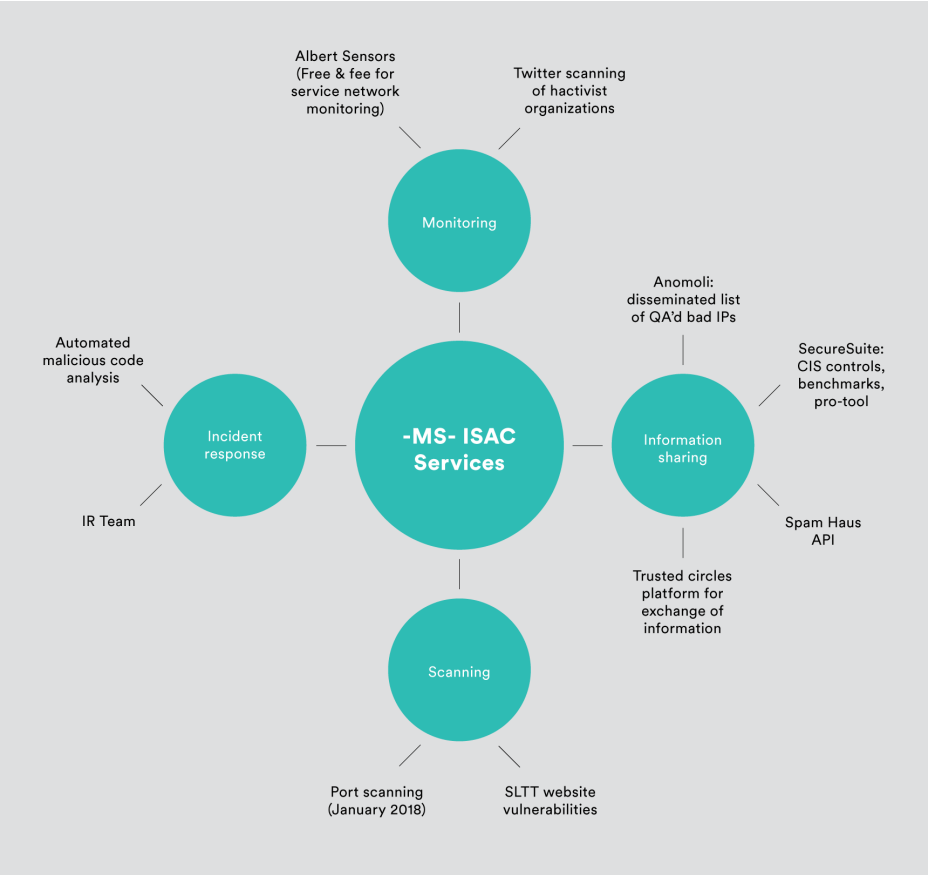
The MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) was formed in 2003 and in 2010, joined the Center for Internet Security (CIS), a nonprofit entity working to "harness the power of a global IT community to safeguard private and public organizations against cyber threat."[55] The MS-ISAC has a cooperative agreement with DHS to coordinate cybersecurity activities among SLTT governments. Originally, the MS-ISAC worked through the state CISO or other designated point of contact for all SLTT efforts, but in 2010 opened membership to local and tribal governments and began interacting with them directly in 2011. Since that time, the MS-ISAC has grown to over 2,000 members, with representation from all states and territories, 78 of 79 state fusion centers, tribal and local governments, mass transit authorities, airports, public universities, K-12 institutions, election directors, and more.[56]

The MS-ISAC provides monitoring and incident response services, runs information sharing programs and platforms, and performs scans on SLTT infrastructure. A graphic showing the various initiatives currently offered to SLTT organizations is shown in Figure 1. In addition to services performed for its members, the MS-ISAC also passes information back and forth with DHS through the NCCIC, the ISACs and ISAOs, and the national and international CERTs (to get information to international partners).[57]

Key to the MS-ISAC's success has been its focus on feedback and engagement. The center conducts annual surveys of its members, performs an annual self-assessment, and sends out post-incident surveys. As with any survey program, feedback is spotty, but augmented by the MS-ISACs outreach program, the center's staff has been able to make concrete improvements based on this feedback.[58]

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 agencies to its centralized monitoring service until the Center has total network

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 MS-ISAC 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 accessible resources hosted on the NJCCIC website. One of the most successful analysis and information sharing initiatives orchestrated by CTIA was in response to the proliferation of ransomware incidents in 2017. The analysts built out dozens of ransomware profiles for each variant discovered through its monitoring services, reported in the media, or reported directly into the NJCCIC. These profiles (of which there are now over 200) were published on the website along with recommendations for end users and IT departments. This service was also used extensively by local police departments serving as the first line of response to many infections in New Jersey.[61]

CTIA provides SECOPS with vetted IOCs found through the monitoring services or those that are reported to NJCCIC from other sources which are then distributed to partner organizations via the NJCCIC's automated indicator sharing platform, New Jersey Cyber Threat Intelligence eXchange (NJCTIX). Each IOC is vetted and confirmed as legitimate and actionable prior to distribution, with the understanding that quality over quantity helps to engender trust from its members and liaison services.

NJCCIC has built substantial liaison relationships with federal and state agencies through a consistent focus on collaboration.[62] NJCCIC serves as a clearing house for representatives from those agencies, who can use the NJCCIC as a dissemination tool to get information out to citizens and organizations within New Jersey.[63] These liaison services also serve as source of information for the CTIA analysts, who have built up effective processes and regular points of contact to exchange information in support of ongoing investigations.[64]

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 effort, along with NJCCIC's state-wide monitoring services created a centralized point of contact for cybersecurity and helped set statewide standards to increase efficiency and create an effective baseline for security.[67]

Challenges

Human Capital

Like many other public sector institutions, New Jersey struggles to recruit talent. The six- to eight-month onboarding process often discourages even those interested individuals from applying or delays their arrival so long that they take a competing offer. However, the NJCCIC has been relatively successful in maintaining the employees it has, due in part to a robust focus on mission and ensuring that its employees are allowed to push the envelope to continue to innovate and work on sophisticated programs.

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 companies in New Jersey to report cybersecurity incidents to the NJCCIC.

Governance and Cross-Bureaucratic Funding

Given the relatively recent transition of cybersecurity responsibility to the Office of Homeland Security and Preparedness, and is not rooted in any legislative mandate, executive branch departments and agencies are still adjusting to this change. Without codification in law, the recent gubernatorial changeover also adds a certain amount of uncertainty in its longevity. The State CISO reports to the Director of NJOHSP and serves as head of NJOHSP's Division of Cybersecurity. The state CISO establishes and manages an 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 and safety. The state CISO has overall responsibility for the development, implementation, and performance of the information security program by:

- Setting strategic information security planning across the executive branch of state government;
- Publishing the Statewide Information Security Manual's policies and standards;
- Developing, managing, and executing the statewide Information Security Incident Response Plan;
- Identifying security requirements to limit the risks associated with identified executive branch business objectives as defined by the governor and the heads of state agencies;
- Developing, maintaining, and interpreting the Statewide Information Security Manual's policies and standards;
- Providing information security subject matter expertise to state agencies;
- Drafting and implementing an information security awareness and training program to be used by all state agencies;

- 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 components and elements of the state cyber response. One is typically a cabinet level executive exercise, to enable better understanding of cross-disciplinary and agency interaction at the leadership level of the state. A second annual cyber exercise typically focuses on partnership with a county in the state and related infrastructure partners. As counties in Washington vary hugely in their cyber sophistication[81]—from very high-end capabilities in some counties home to high-tech giants, to less well funded and staffed counties—this set of exercises is designed to highlight and nurture relationships with local partners. Another is typically an internal state focused exercise, designed to illuminate processes and relationships below the state executive level, testing more operational and tactical incident response capabilities. Finally, there is typically at least one exercise that is designed as a prelude to a large regional or national exercise like Cyber Shield, enabling the state to assess regional and national level connections, as well as state level processes. This mix of exercises—a mix of scale, scope, focus—and their consistent annual nature leaves Washington very well exercised in the cyber arena.

These exercises are guided by cybersecurity annex to the state's Comprehensive Emergency Management Plan (CEMP).[82] Updated regularly based on exercise results, organizational changes, or alterations in the threat landscape, the annex provides a framework for response to a cyber incident and details responsibilities across the state.

Incident Response and Monitoring

Washington has a robust incident response system within the Office of the Cybersecurity. The statewide Security Operations Center provides external monitoring services, and the Cyber Incident Response team, which provides incident response services to agencies within the executive branch and can also

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]

Challenges

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 would benefit from further federal support in the cyber realm. In particular, Washington State leaders have been particularly vocal in their support for a centralized and specifically targeted grant program for cybersecurity efforts and the pending legislation (H.R. 3712) to create Cyber Civil Support Teams (CSTs). These "Cyber CSTs" would be comprised of National Guard soldiers and airmen under the authority of the Governor but with direct connection to the Department of Homeland Security (USCERT) and the Department of Defense.[91]

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 in the state, NIST, and private companies.

Dependencies

Support of State Leadership

Governor Inslee, who was first elected in 2013, defines the Washington State approach to cybersecurity as "Community Cybersecurity."[95] Specifically, the governor identifies five pillars:

- Regional collaboration between public, private and tribal partners
- Resilience of networked systems for public safety and commerce
- Promoting research, analysis, and sharing of cybersecurity information and best practices across private, public and tribal sectors
- Unity of effort for the protection of critical infrastructure, and,
- Dedication to workforce development to strengthen our economy and enhance our cybersecurity posture.

Leadership across Washington's cybersecurity programs point to the support of the Washington State Governor and his office, particularly in tackling legal hurdles and dedicating time and resources to exercises and events, as key to the progress made in multiple areas.[96]

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 partnerships, planning efforts, as well as to help facilitate these partners access to federal resources through the DHS PSAs and the regional DHS CSA.[98] This outreach and good will is a testament to the kind of good work state government employees can do, however the limited staffing and time-intensive nature of the relationship building components of this work suggest that there could be a certain fragility in depending on it being done by just one or two people.

Access to IT Talent and Infrastructure

Washington State's unique workforce provides it with a unique advantage: access to wide-ranging IT and cyber talent. The state—and its cyber efforts—have benefited from the broad availability of IT expertise in several ways. First, it provides skilled cyber operators and analysts, both for state agencies and for the National Guard. The National Guard has been able to build on this base of skills to create teams with deep expertise in ICS and SCADA systems.[99] Second, close contact with members of the private sector that serve as the foundation for IT infrastructure enables collaboration in the case of an incident. This expertise permeates into the local level as well in areas of high tech density, such as Pierce County.[100] Third, partnerships with universities, buoyed by their private sector partnerships, have increased access to IT and cyber talent pipeline for the public sector as well.

The Triple Hat

The Revised Code of Washington, RCW 38-52 gives the task of comprehensive emergency management to mitigate, prepare for, respond to, and recover from emergencies and disasters caused by all hazards, whether natural, technological, or human cause to the adjutant general.[101] In Washington, the adjutant general

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, MS-ISAC

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

Bryan Langley, Executive Director, Indiana Department of Homeland Security

Andrew Lauland, Senior International/Defense Researcher, RAND

John Leo, Director, PwC

Mike Lettman, Chief Information Security Officer, Arizona

Richard Licht, Chief Administrative Officer, Center for Internet Security

Josh Liss, Former Analyst, NJCCIC

Victor Macias, CYBERCOM

Jennifer Mellor, Vice President of Economic Development, Phoenix Chamber of Commerce

Chetrice Mosley, Cybersecurity Director, Indiana Department of Homeland Security

Dewand Neely, Chief Information Officer, Indiana

Chad Payeur, Exercise Program Specialist, FEMA

Nancy Rainosek, Chief Information Security Officer, Texas

David Roberts, Chief Innovation Officer, Indiana Economic Development Corporation

Michael Rolling, Chief Information Security Officer, Missouri

Clayton Romans, Deputy Director, Strategy Coordination & Management (SCM), Department of Homeland Security

Bob Rose

Major Jonathan Rupel, Information Security, Indiana Army and Air National Guard

Dr. Paolo Shakarian, Fulton Entrepeneurial Professor, Arizona State University

Francesca Spidalieri, Senior Fellow, Pell Center

Sri Sridharan, Director, Florida Center for Cybersecurity

Tad Stahl, Indiana Army and Air National Guard

Roisin Suver, MS-ISAC representative to the NCCIC

David Tygart, Chief J36 Defensive Cyber Programs, Indiana Army and Air National Guard

Guy Walsh, Strategic Initiatives, CYBERCOM

Dave Weinstein, Former Cybersecurity Advisor, New Jersey Department of Homeland Security and New America Cybersecurity Fellow

Bradford Wilke, Chief, CSA Field Operations, Department of Homeland Security

The authors also interviewed several members of ACTRA who due to privacy considerations remain anonymous.

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 Indiana Guard training site helps state, feds protect infrastructure. (2016, 5 26). Retrieved from US Army: https://www.army.mil/article/168580/indiana_guard_training_site_helps_state_feds_protect_infrastructure

3 The SANS Institute. (2017, 12 5). SANS Announces 2017 Difference Makers Award Winners. Retrieved from SANS: https://www.sans.org/press/announcement/2017/12/05/1

4 New State Ice Co. v. Liebmann, 463 (US Supreme Court 3 21, 1932). Retrieved from https://supreme.justia.com/cases/federal/us/285/262/case.html

5 Garcia, M., Forscey, D., & Blute, T. (2017). Beyond the Network: A Holistic Perspective on State Cybersecurity Governance. Nebraska Law Review, 96 (2)

6 PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other Department of Homeland Security offices. They also advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators. Protective Security Advisors. (2018, 4 12). Retrieved from Official website of the Department of Homeland Security: https://www.dhs.gov/protective-security-advisors

7 Wilke, B. (2018, 3 2). Chief, CSA Field Operations, Department of Homeland Security. (N. Cohen, Interviewer)

8 About ISACs. (n.d.). Retrieved from National Council of ISACs: https://www.nationalisacs.org/about-isacs

9 Information Sharing and Analysis Organization Standards Organization (ISAO SO). (2016, 10 14). Introduction to Information Sharing and Analysis Organizations (ISAOs) v1.01. Retrieved from ISAO Standards Organization: https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pdf

10 Kimbriel, T. (2018, 4 26). CIO, Cybersecurity Coordinator. (N. Cohen, Interviewer); OCISO, D. (2017, 7). The DIR Cybersecurity Insight. Retrieved from Texas Department of Information Resources: http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20Cybersecurity%20Insight%20Newsletter%20FY2017%20July.pdf; Matz, S. (2017, 8 4). Texas Governor Signs into Law Texas Cybersecurity Act. Retrieved from CompTIA: https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2017/08/04/texas-governor-signs-into-law-texas-cybersecurity-act; The Texas Cybersecurity Act. (2017, 9 1). Retrieved from https://capitol.texas.gov/tlodocs/85R/billtext/html/HB00008F.htm

11 The U.S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year (FY) 2017 Port Security Grant Program (PSGP). (2017). Retrieved from FEMA: https://www.fema.gov/media-library-data/1496328927518-cfc5486f1846263e697754eb2e7fed50/FY_2017_PSGP_NOFO_508.pdf

12 Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government. (2016, 9 22). Retrieved from Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/

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

13 RAND has a study forthcoming regarding FEMA's role in cybersecurity

14 North Carolina's state government has a Memorandum of Understanding with the North Carolina National Guard that enables them to act as force augmentation in the case of an emergency. Soldiers are issued credentials to state systems and exercise such assistance regularly, which reduces friction and increases efficiency during an actual event. Thompson, M. (2018, 5 8). Chief Information Risk Officer, North Carolina. (K. Jackson, Interviewer)

15 Wynne, M. W., & Bement Jr., A. L. (2007, 5 1). Memorandum Of Agreement Between The Department Of Defense And The National Science Foundation For The National Science Foundation's Polar Programs. Retrieved from Joint Chiefs of Staff: http://www.jcs.mil/Portals/36/Documents/Doctrine/Interorganizational_Documents/doe_mou_nat_sci_found2007.pdf

16 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer)

17 Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8

18 InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for public-private collaboration with government to expedite the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.

19 Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8

20 Governor Ducey Announces Appointments to Arizona Cybersecurity Team. (2018, 3 7). Retrieved from Office of the Governor Doug Ducey: https://azgovernor.gov/governor/news/2018/03/governor-ducey-announces-appointments-arizona-cybersecurity-team

21 Figueroa, C. (2018, 1 19). Protective Security Advisor for Arizona, Department of Homeland Security. (N. Cohen, Interviewer)

22 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

23 Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8

24 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer); ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

25 Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Office. (N. Cohen, Interviewer)

26 Subject Matter Expert

27 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

28 Grimmelmannn, F., Halla, D., & Nix, M. (2016). A Development Guide for Regionally Based Information Sharing and Analysis Organizations. Laurel, MD: Johns Hopkins Applied Physics Laboratory.

29 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

30 Halla, D. (2017, 12 7). Senior Advisor, Johns Hopkins Applied Physics Laboratory. (N. Cohen, Interviewer)

31 DoD SkillBridge: https://dodskillbridge.com/

32 U.S. Army Installation Management Command. (2017, 7 12). Army Career Skills Program. Retrieved from Stand-To!: https://www.army.mil/standto/2017-07-13

33 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer); Mellor, J. (2018, 1 18). Vice President of Economic Development, Phoenix Chamber of Commerce. (N. Cohen, Interviewer)

34 Arizona State Emergency Response and Recovery Plan. (2016, 9 1). Retrieved from Arizona Department of Emergency Management: https://dema.az.gov/sites/default/files/publications/EM-PLN_State_Emergency_Response_and_Recovery_Plan-Basic_Plan_SERRP_2016FINAL_Oct7.pdf

35 Nakashima, E. (2016, 8 29). Russian hackers said to have targeted Arizona election system. Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.743ef514efce

36 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

37 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

38 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

39 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

40 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer); Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Office. (N. Cohen, Interviewer)

41 Shakarian, P. (2017, 12 13). Fulton Entrepeneurial Professor, Arizona State University. (N. Cohen, Interviewer)

42 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer); ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

43 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

44 ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

45 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer)

46 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

47 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer)

48 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.; Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Office. (N. Cohen, Interviewer)

49 Eastman, J. (2018, 3 15). CEO, WICTRA. (N. Cohen, Interviewer)

50 Eastman, J. (2018, 3 15). CEO, WICTRA. (N. Cohen, Interviewer)

51 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

52 Figueroa, C. (2018, 1 19). Protective Security Advisor for Arizona, Department of Homeland Security. (N. Cohen, Interviewer)

53 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.; ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)

54 ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

55 CIS Center for Internet Security: https://www.cisecurity.org/

56 Duffy, T. (2018, 3 13). Vice President of Operations, MS-ISAC. (N. Cohen, Interviewer)

57 Suver, R. (2018, 3 13). MS-ISAC Representative to the NCCIC. (N. Cohen, Interviewer)

58 Duffy, T. (2018, 3 13). Vice President of Operations, MS-ISAC. (N. Cohen, Interviewer)

59 Weinstein, D. (2018, 2 9). Former Cybersecurity Advisor, State of New Jersey. (N. Cohen, Interviewer)

60 Geraghty, M. (2018, 3 1). Chief Information Security Officer, State of New Jersey & Director, NJCCIC. (N. Cohen, Interviewer)

61 Liss, J. (2018, 2 14). Former Analyst, NJCCIC. (N. Cohen, Interviewer)

62 Geraghty, M. (2018, 3 1). Chief Information Security Officer, State of New Jersey & Director, NJCCIC. (N. Cohen, Interviewer)

63 Leo, J. (2018, 3 12). Director, PwC. (N. Cohen, Interviewer)

64 Liss, J. (2018, 2 14). Former Analyst, NJCCIC. (N. Cohen, Interviewer)

65 Geraghty, M. (2018, 3 1). Chief Information Security Officer, State of New Jersey & Director, NJCCIC. (N. Cohen, Interviewer)

66 Weinstein, D. (2018, 2 9). Former Cybersecurity Advisor, State of New Jersey. (N. Cohen, Interviewer)

67 Weinstein, D. (2018, 2 9). Former Cybersecurity Advisor, State of New Jersey. (N. Cohen, Interviewer)

68 Geraghty, M. (2018, 3 1). Chief Information Security Officer, State of New Jersey & Director, NJCCIC. (N. Cohen, Interviewer)

69 Geraghty, M. (2018, 3 1). Chief Information Security Officer, State of New Jersey & Director, NJCCIC. (N. Cohen, Interviewer)

70 RTI. (2017). Understanding Demand for Cyber Policy Resources. Hewlett Foundation's Cyber Initiative

71 Spidalieri, F. (2015). State of the States on Cybersecurity. Newport, RI: Pell Center.

72 Spidalieri, F. (2018, 3 7). Senior Fellow, Pell Center. (N. Cohen, Interviewer)

73 Earls, A. R. (2017, 10). Agnes Kirk on the role of CISO, Washington's state of mind. Retrieved from

TechTarget: http://searchsecurity.techtarget.com/feature/Agnes-Kirk-on-the-role-of-CISO-Washingtons-state-of-mind; Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers)

74 RTI. (2017). Understanding Demand for Cyber Policy Resources. Hewlett Foundation's Cyber Initiative. P58

75 RTI. (2017). Understanding Demand for Cyber Policy Resources. Hewlett Foundation's Cyber Initiative. P58

76 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

77 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

78 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

79 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

80 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers); Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers); Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers)

81 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

82 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

83 Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers); Top 17 State & Local Cybersecurity Leaders to Watch. (2017, 10 18). Retrieved from StateScoop: https://statescoop.com/monthly/top-state-local-cybersecurity-leaders-to-watch-2

84 Spidalieri, F. (2015). State of the States on Cybersecurity. Newport, RI: Pell Center. P37

85 Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers)

86 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

87 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

88 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

89 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

90 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

91 Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers); Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers); Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers); 15th Congress H. R. 3712. (2017, 9 8). Retrieved from Congress.Gov: https://www.congress.gov/115/bills/hr3712/BILLS-115hr3712ih.pdf

92 See Appendix I

93 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

94 Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers)

95 Inslee, J. (2015, 8 19). Letter to the Honorable Alejandro Mayorkas, Deputy Secretary, Department of Homeland Security. Retrieved from Washington Military Department: https://mil.wa.gov/uploads/pdf/emergency-management/governorletteroncybersecurity.pdf

96 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers); Kirk, A. (2018, 3 30). Chief Information Security Officer, State of Washington. (N. Cohen, & B. Nussbaum, Interviewers)

97 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

98 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

99 Daugherty, B. (2018, 3 9). The Adjutant General, Washington State National Guard. (N. Cohen, & B. Nussbaum, Interviewers)

100 Lang, R. (2018, 3). Cybersecurity Manager, Washington Military Department. (N. Cohen, & B. Nussbaum, Interviewers)

101 Revised Code of Washington (RCW) Chapter 38.52. (2017, 10 23). Retrieved from Washington State Legislature: http://app.leg.wa.gov/rcw/default.aspx?cite=38.52

NEW AMERICA