Nebraska Law Review

Volume 96 | Issue 2 Article 3

2017

Beyond the Network: A Holistic Perspective on State Cybersecurity Governance

Michael Garcia
National Governors Association, mgarcia@nga.org

David Forscey
National Governors Association, dforscey@nga.org

Timothy Blute
National Governors Association, tblute@nga.org

Recommended Citation
Michael Garcia, David Forscey, and Timothy Blute, *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*, 96 Neb. L. Rev. 252 (2017)
Available at: https://digitalcommons.unl.edu/nlr/vol96/iss2/3

Michael Garcia, David Forscey & Timothy Blute*

Beyond the Network: A Holistic Perspective on State Cybersecurity Governance

TABLE OF CONTENTS

I. INTRODUCTION

Cybersecurity is no longer the sole province of computer scientists, information technology (IT) departments, and hackers. A working understanding of digital technology and its attendant risks is now a prerequisite for the effective management of any complex organization in the twenty-first century. Executives in government and business must strengthen their own internal cybersecurity programs and prepare for the fallout when preventive measures inevitably fail. They must also plan to respond to attacks on external, unrelated entities that can have cascading effects throughout the economy and society. Although

* Michael Garcia is a Policy Analyst at the National Governors Association (NGA); he earned his M.P.A from James Madison University in 2015. David Forscey is a Policy Analyst at NGA; he earned his J.D. from Georgetown University Law Center in 2015. Timothy Blute is a Program Director at NGA; he earned his J.D. from the American University Washington College of Law in 2014.

the United States has yet to suffer from a widespread, persistent cyber attack on critical systems, discrete incidents illustrate that criminals and foreign adversaries have the capability to cause massive economic and physical damage. A single "cyber apocalypse" is unlikely, but even the most mundane instances of cyber crime, in aggregate, inflict a tremendous toll on the national economy.[1]

Traditionally, the federal government has taken the lead in defending the nation against man-made national security threats. Constitutional law and practice generally left it to states and their political subdivisions to safeguard the public welfare from more mundane dangers such as crime and weather-related hazards. The September 11 attacks and the subsequent struggle against decentralized terrorist networks solidified a newly assertive role for state and local government in national-security matters.

Similarly, the distributed structure of networked communications, combined with the sheer size of the United States and the decentralized federalist system on which it is founded, means that the federal government cannot secure the nation's computer-based infrastructure alone. Whatever the origin of a given cyber attack—whether it is a disruptive attack against infrastructure or a more common email scam—its effects are inherently local, as is the response. Huge swaths of the nation's critical infrastructure are controlled or regulated by state and local entities. Citizens' and businesses' interactions with state and local officials far outstrips their engagement with federal entities. As a result, assessing the impact of cybersecurity policy requires a bottom-up flow of information from citizens and businesses to the federal government. Standards and recommendations to improve one's risk exposure often flow from national or federal organizations back down to the local level. States lie at the nexus of these information flows.

States might have difficulty contributing to cybersecurity policy if they cannot secure their own information assets. The information-security community long ago identified the best practices that can meaningfully reduce risk to the confidentiality, integrity, and availability of state-owned and -controlled data and related systems. Modern software and hardware offerings reduce the burden of integrating those best practices with IT management and adapting them to new threats. As a result, the core challenge for state cybersecurity professionals today is not technical; the cutting edge of cybersecurity is governance. From basic firewalls to the most sophisticated malware analysis, all technology solutions must be configured and imple-

[1] Steve Morgan, *Cybercrime Damages Expected to Cost the World $6 Trillion by 2021*, CSO ONLINE (Aug. 22, 2016), http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html [https://perma.unl.edu/X4SC-DBQD].

mented by humans. In academic literature and corporate guidelines, cybersecurity governance is commonly described as the process through which humans understand organizational risk, prioritize resources, and establish procedures to erect technical defenses against computer-based attacks.

We argue that state cybersecurity governance deserves a broader definition that reflects the expansive role for states in the broader cybersecurity ecosystem, one that obligates state officials to do more than defend state networks. States have a fundamental responsibility to protect constituents, including interstate businesses, from day-to-day cyber attacks and to prepare public and private institutions for a widespread cyber disruption. States also have an abiding interest in growing the cybersecurity workforce through innovative education and training initiatives. A deeper talent pool is a precondition for optimum risk management in the public and private sectors, as well as a driver of employment and economic growth more broadly. Across the nation, state chief information officers (CIOs), chief information-security officers (CISOs), homeland security advisors, and other officials or advisors are attempting to implement wide-ranging cybersecurity initiatives to achieve these purposes. However, such officials are generally equipped with small budgets and limited authority.

Success demands a whole-of-state approach that assembles stakeholders, assigns responsibilities, sets timelines, allocates resources, and establishes accountability mechanisms. Officials must involve municipalities, educational institutions, and small businesses in addition to state IT agencies and critical infrastructure operators. Good governance functions to overcome resource constraints and bureaucratic resistance, thereby empowering officials to manage technical controls and user behavior across the state enterprise, boost information sharing among public and private partners, share best practices, plan for cyber incidents and cyber disruptions, align educational standards with business needs, and prepare for future threats that have yet to materialize. This is state cybersecurity governance. It extends beyond the network's edge.

II. GOVERNANCE: THE NEW FRONTIER OF INFORMATION ASSURANCE

A resilient information-security posture requires three core competencies: (1) the deployment of technical and administrative controls to harden vulnerable information assets; (2) user awareness programs and training to maximize compliance with established controls; and (3) the collection and dissemination of information needed to adapt the current security posture to emerging threats. In implementing these key elements of cybersecurity, today's businesses and government agencies are most commonly frustrated not by technical questions but rather by organizational ones.

Widely available technical solutions can reduce cybersecurity risk to tolerable levels. Modern developments in cryptography, software applications, and hardware have simplified the process of implementing time-tested techniques to mitigate most, if not all, known security vulnerabilities. A wide array of native and third-party solutions smooth the process of conducting risk assessments, segmenting networks, whitelisting applications, disabling active content in emails, and detecting intruders, among other measures.[2] Basic defenses such as these would block many of the most common forms of cyber attack, as well as some of the most devastating ones.[3] Even when sophisticated attacks circumvent these safeguards, raising the cost of intrusions via technical best practices filters out standard criminals, freeing up defenders to focus on the most advanced threats. Although states have access to the proper technology to implement effective technical countermeasures, dispersing that technology throughout a state's bureaucracy is fundamentally an organizational problem.

Security technology cannot be effective if misconfigured, misapplied, or ignored by its users. Human error is a common cause of security breaches in the private and public sectors.[4] Many of the most

[2] *See, e.g.*, INFO. ASSURANCE DIRECTORATE, NAT'L SEC. AGENCY, IAD'S TOP 10 INFORMATION ASSURANCE MITIGATION STRATEGIES (2013), https://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf [https://perma.unl.edu/YD55-QJVS].

[3] *See, e.g.*, TERI RADICHEL, CASE STUDY: CRITICAL CONTROLS THAT COULD HAVE PREVENTED TARGET BREACH (2014), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412 [https://perma.unl.edu/Z2TH-87AW]; WATERISAC, 10 BASIC CYBERSECURITY MEASURES ii (2015) ("In reviewing its incident reports for 2014, ICS-CERT noted that implementation of the first three recommendations likely would have detected the issues, prevented the vulnerabilities, and averted the resulting impacts related to those incidents."); *see also* Anthony Kimery, *Feds Wasting Available Cybersecurity Resources, Survey Finds*, HOMELAND SECURITY TODAY (Dec. 7, 2016), http://www.hstoday.us/briefings/daily-news-analysis/single-article/feds-wasting-available-cybersecurity-resources-survey-finds/9bbea943f86012babb3b32cba89a520a.html [https://perma.unl.edu/2LDZ-EA6X] ("The federal government is under-utilizing available resources and manpower they already possess . . . ."); Steve Ragan, *Phishing Remains Top Attack Vector for Criminals, Both Novice and Professional*, CSO ONLINE (Feb. 24, 2016), http://www.csoonline.com/article/3036837/security/phishing-remains-top-attack-vector-for-criminals-both-novice-and-professional.html [https://perma.unl.edu/MXB2-DRH4] (identifying humans within an organization as a "soft target").

[4] *See, e.g.*, Brian M. Bowen, Ramaswamy Devarajan & Salvatore Stolfo, *Measuring the Human Factor of Cyber Security*, HOMELAND SECURITY AFF. (May 2012), https://www.hsdl.org/?view&did=710052 [https://perma.unl.edu/9E8N-PWRV] ("Computer security is not just about technology and systems. It is also about the people that use those systems and how their vulnerable behaviors can lead to exploitation."); James A. (Sandy) Winnefeld Jr., Christopher Kirchhoff & David

sophisticated malware variants—including those used by nation-states—depend on a lapse in human judgment to compromise target systems.[5] In the information-security community, a truism has taken hold: information assurance depends on maximizing user compliance with security policies.[6] State CISOs want to prioritize training and awareness programs for state employees,[7] but inculcating a culture of risk requires organizational change beyond mandatory training videos.[8]

Properly designed information-security programs cannot stop all attacks, particularly those that exploit unknown security vulnerabilities. Evolving threats have generated a broad desire for more information sharing among entities who might otherwise resist working together. In recent years, Information Sharing and Analysis Centers/Organizations (ISACs/ISAOs) have emerged across the private sector from finance and energy to healthcare and transportation. Federal officials have devoted significant time, funding, and political capital to establish nationwide information-sharing organizations, including the National Cybersecurity Communications Integration Center (NCCIC) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). States, too, have begun creating their own information-sharing bodies, building on the law enforcement fusion centers that emerged

M. Upton, *Cybersecurity's Human Factor: Lessons from the Pentagon*, Harv. Bus. Rev. (Sept. 2015), https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon [https://perma.unl.edu/8VCU-ZU2H] ("Mistakes by network administrators and users—failures to patch vulnerabilities in legacy systems, misconfigured settings, violations of standard procedures—open the door to the overwhelming majority of successful attacks.").

[5] *See, e.g.*, Kevin Albano & Limon Kessem, *The Full Shamoon: How the Devastating Malware Was Inserted into Networks*, SecurityIntelligence (Feb. 15, 2017), https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks [https://perma.unl.edu/4DE4-W6FB].

[6] *See, e.g.*, Aisha Chowdhry, *Officials Talk Candidly About Workforce Cyber Hygiene*, FCW (Apr. 25, 2016), https://fcw.com/articles/2016/04/25/chowdhry-cyber-hygiene.aspx [https://perma.unl.edu/3FBV-BX84]; Dan Lohrmann, *Ten Recommendations for Security Awareness Programs*, Gov't Tech. (Mar. 9, 2014), http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Ten-Recommendations-for-Security-Awareness-Programs.html [https://perma.unl.edu/JM7L-7E8S].

[7] Deloitte & Nat'l Ass'n of State Chief Info. Officers, 2016 Deloitte–NASCIO Cybersecurity Study 6 (2016) [hereinafter Deloitte–NASCIO Study], http://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf [https://perma.unl.edu/6CY8-2ZBB].

[8] *See* Stefanie Jahner & Helmut Krcmar, *Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management*, *in* AMCIS 2005 Proceedings 3327, 3330 (2005), http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1974&context=amcis2005 ("While traditional IT risk management focuses on securing processes and IT infrastructure IT risk culture additionally takes the senior management, the organizational structure, artifacts and organizational members into consideration and thus underpins the multi-level character of an integrated IT risk management.").

in response to counterterrorism needs during the 2000s.[9] Adapting longstanding information-sharing practices to the realm of cybersecurity is yet another organizational challenge as a wider range of relevant stakeholders—extending beyond the law enforcement and national-security offices common in existing fusion centers—may be reluctant to participate.[10]

In short, the frontier of cybersecurity today is ensuring that time-tested, risk-based techniques for hardening systems, training users, and sharing information are implemented, sustained, and coordinated.[11] Organizations accomplish these objectives through governance,[12] the "formal and informal institutions that [influence how] a group of people determine what to decide, how to decide, and who shall decide."[13] A large body of research has explored the importance of governance in managing information technology across large organizations.[14] States have created entire agencies, guided by comprehensive IT strategies, to align technology demands with "business

[9] *See, e.g.*, Press Release, N.J. Cybersecurity & Commc'ns Integration Cell, NJCCIC and NH-ISAC Partner to Enhance Cybersecurity Information Sharing at the State Level (Jan. 26, 2016), https://www.cyber.nj.gov/press-releases/njccic-and-nh-isac-partner-to-enhance-cybersecurity-information-sharing-at-the-state-level [https://perma.unl.edu/6JBZ-3X4D]; *California Cybersecurity Integration Center*, Cal. Governor's Off. Emergency Servs., http://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center [https://perma.unl.edu/S2LN-2UTN].

[10] According to Michael Echols, CEO of the International Association of Certified ISAOs (IACI), "[B]ecause many of the issues are not technical, we want to create opportunities to overcome challenges to cybersecurity. For instance, in many cases there are issues related to taxonomy. Too many times some term means different things to different people, creating communication barriers." George V. Hulme, *Tackling Cybersecurity Threat Information Sharing Challenges*, CSO (Jan. 18, 2017), http://www.cso.com.au/article/612824/tackling-cybersecurity-threat-information-sharing-challenges.

[11] Merrill Warkentin & Allen C. Johnston, *IT Security Governance and Centralized Security Controls*, *in* Enterprise Information Systems Assurance and Systems Security 16 (2006), https://www.researchgate.net/profile/Merrill_Warkentin/publication/292549265_IT_Security_Governance_and_Centralized_Security_Controls/links/56bcd43a08aed6959945bda0/IT-Security-Governance-and-Centralized-Security-Controls.pdf (explaining that information security goals "can only be achieved if the policies and procedures are complete, accurate, available, and ultimately executed or put into action").

[12] *Id.* at 16–18 ("It is within their structures and governance procedures that organizations are able to address the issues of responsibility, accountability, and coordination toward the achievement of their purpose and goals.").

[13] Vasudha Chhotray & Gerry Stoker, Governance Theory and Practice: A Cross-Disciplinary Approach 3–4 (2009) (explaining why the need for governance typically arises when "a plurality of actors or organizations" interact without a "formal control system").

[14] *See* Dieter De Smet & Nicolas Mayer, Integration of IT Governance and Security Risk Management: A Systematic Literature Review 3–4 (2016), http://nmayer.eu/publis/DeSmet-Mayer_I-Society_1.0.pdf [https://perma.unl.edu/BS3V-AGJM] (describing how governance defines the "location, distribution and

needs"—a term of art that refers to agency objectives or functions determined by law, policy, or discretion.[15]

One can further define cybersecurity governance as the decision processes that determine how an organization designs an information-security program, oversees its implementation, and continuously adapts it to changing business needs and threats.[16] Consequentially, both the public and private sectors have embraced it as an indispensable component of a resilient cybersecurity posture.[17]

III. STATE CYBERSECURITY GOVERNANCE EXTENDS BEYOND THE NETWORK

The general discourse on cybersecurity governance is limited to its role in defending an organization's internal or proprietary information assets.[18] This narrow view is logical when examining information security in the private sector, where managers focus first and foremost on reducing risk to their bottom line. State officials also spend considerable time and energy defending state networks, but unlike private organizations, government leaders have an inherent responsibility to assist nonstate entities. This obligation expands the scope of cybersecurity governance for states.

The preeminent duty of every state is to safeguard the public welfare. Since its inception, the U.S. Constitution has embodied this prin-

pattern of managerial responsibilities and control that ultimately affect how IT resources are applied and then implemented").

[15] James S. Denford, Gregory S. Dawson & Kevin C. Desouza, *An Argument for Centralization of IT Governance in the Public Sector*, *in* Proceedings of the 48th Annual Hawaii International Conference on System Sciences 4493, 4494 (2015), https://pdfs.semanticscholar.org/645f/6df7254278f8d514e1c4bbcbd6557211a9e4.pdf [https://perma.unl.edu/3HBW-RQF2].

[16] Douglas Gray et al., Carnegie Mellon Univ., Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution 9 (2015), https://resources.sei.cmu.edu/asset_files/TechnicalReport/2015_005_001_444963.pdf [https://perma.unl.edu/EP26-GYWU]; *see also* Deb Bodeau et al., MITRE, Cyber Security Governance 11–12 (2010), https://www.mitre.org/sites/default/files/pdf/10_3710.pdf [https://perma.unl.edu/7ZEH-GT89] (discussing aspects of enterprise risk management such as "aligning cyber security risk management").

[17] Gray et al., *supra* note 16, at 9 ("Governance and risk management are inextricably linked—governance is an expression of responsible risk management and effective risk management requires efficient governance.").

[18] *See, e.g.*, PricewaterhouseCoopers LLP, PwC's Board Cybersecurity Governance Framework (2016), https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf [https://perma.unl.edu/PSE3-GRF9]; Prakash Binwal, *Creating a Cybersecurity Governance Framework: The Necessity of Time*, SecurityIntelligence (June 29, 2015), https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time [https://perma.unl.edu/G9UR-WZHR].

ciple, as have most state constitutions.[19] The art and science of public policy involves prioritizing the most dangerous threats to the public welfare, resourcing countermeasures, and implementing them. Thousands of state officials in emergency management, law enforcement, and homeland security dedicate themselves to this mission, preparing for floods, epidemics, and terrorism—all while working daily to deter ordinary crime. The principles and frameworks for guiding government action in these areas are well-known and tested on a regular basis.

Cyber attacks are a relatively new threat to the public welfare that demands equal attention from state leaders. Criminals and foreign adversaries exploit security vulnerabilities in software and hardware to impose untold financial costs on individuals and businesses and disrupt important services. Both federal and state authorities have a corresponding obligation to protect citizens' data, guarantee public services, and provide helpful resources to nongovernmental entities.

First, state and local bodies possess an enormous trove of sensitive data that is vulnerable to compromise.[20] For instance, the intellectual property housed in systems owned and controlled by public universities is a potential goldmine for U.S. adversaries seeking a competitive edge.[21] Critics who assail private retailers for failing to protect customer information can argue that inadequate security within state agencies constitutes an even greater breach of trust. This impacts the

[19] *See, e.g.*, U.S. CONST. pmbl. ("We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."); VA. CONST. art. I, § 3 ("That government is, or ought to be, instituted for the common benefit, protection, and security of the people, nation, or community; of all the various modes and forms of government, that is best which is capable of producing the greatest degree of happiness and safety . . . .").

[20] *See 850,000 People Potentially Impacted by WorkSource Oregon Security Breach*, FOX 12 OR. (Oct. 13, 2014), http://www.kptv.com/story/26776035/worksource-oregon-data-breach-affects-850000-people; *Data Breach: Where Did South Carolina Go Wrong?*, GOV'T TECH. (Nov. 26, 2012), http://www.govtech.com/e-government/Data-Breach-Where-Did-South-Carolina-Go-Wrong.html [https://perma.unl.edu/S6SW-P3HZ]; *The Data Breach Solution Center*, UTAH DEP'T HEALTH, http://www.health.utah.gov/databreach [https://perma.unl.edu/S6YP-54XG].

[21] As one leading threat analyst explains: "Universities have a very rich intellectual property base, emerging technology, new patents and cutting-edge research in an environment meant to be open to the world and collaboration . . . ." Hannah Kuchler, *Universities Top the List for Hackers*, FIN. TIMES (Feb. 27, 2014), https://www.ft.com/content/23a25e1e-9e3a-11e3-b429-00144feab7de; *see also* Shane Harris & Alexa Corse, *Chinese Hackers Target U.S. University with Government Ties*, DAILY BEAST (Aug. 21, 2015), http://www.thedailybeast.com/articles/2015/08/21/chinese-hackers-target-u-s-university-with-government-ties.html [https://perma.unl.edu/M3WY-VUZP] (describing attempts by an APT actor to access sensitive research data at the University of Virginia, Charlottesville).

success of e-government and the allure of "smart cities" or "smart states," both of which assume that citizens will provide data to public officials—an assumption that could prove incorrect if news of security breaches casts doubt on the ability of government to safeguard private information. Examining the success or failure of state-run information-security programs is therefore critical to understanding technology policy at large.

Second, in practical terms, state and local authorities form the frontlines for incident and disruption response. Traditional risks to the public welfare—violent crime, disease, and natural disasters—manifest themselves locally. Regardless of the scale of a given crime or disaster, state and local authorities are first on the scene. This is no different in the context of cyberspace. Although cyber attacks occur in the digital realm, their effects are ultimately tied to the physical world, and they require a physical response. In the case of cyber crime, state and local law enforcement agencies normally take the lead; federal agencies limit their own involvement to major cases. In the event of a high-consequence, widespread attack on critical infrastructure, when federal agencies mobilize *en masse*, state and local involvement will remain indispensable to response and recovery activities. As the commander in chief of a state's National Guard, each governor is responsible for integrating the National Guard into emergency planning for such an event.

Third, states shape information-security practices in the private sector. At least thirteen states have passed laws requiring in-state entities that own or manage personal information to implement "reasonable" cybersecurity measures.[22] Although federal agencies issue cybersecurity standards for major components of the nation's power grid, state regulators oversee how electricity is distributed at the local level. That gives state public utility commissions direct authority over cybersecurity standards for the electric grid.[23] States are also closely involved in water-utility operations, a sector that remains highly vulnerable to disruption.[24] Furthermore, state oversight of the insurance

[22] *Data Security Laws: State Government*, NAT'L CONF. ST. LEGISLATURES (Jan. 16, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx [https://perma.unl.edu/8RY4-5P6X].

[23] *See, e.g.*, ARTHUR H. HOUSE & STEPHEN M. CAPOZZI, CONN. PUB. UTILS. REGULATORY AUTH., CONNECTICUT PUBLIC UTILITIES CYBERSECURITY ACTION PLAN (2016), http://www.ct.gov/pura/lib/pura/electric/cyber_report_april_6_2016.pdf [https://perma.unl.edu/JXN9-6LSK].

[24] *See, e.g.*, VERIZON, DATA BREACH DIGEST 39–40 (2016), http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf [https://perma.unl.edu/YD9T-RHXP]; Tod Newcombe, *As Water Utilities Move Online, Hackers Take Note*, GOVERNING (Feb. 2016), http://www.governing.com/columns/tech-talk/gov-water-utilities-cybersecurity-hackers.html [https://perma.unl.edu/FH8D-TVJW]. A 2002 law requires water utilities serving more than 3300 people to conduct

industry bestows on state insurance commissioners the power to shape the growing cybersecurity-insurance marketplace.[25]

Fourth, improving how state and local governments enhance their own data security is a national security imperative. As previously described, states have an indispensable role in safeguarding the critical infrastructure that provides essential services to communities across the nation. While security breaches inside state governments are frequently portrayed as a problem for the victim state alone, threat actors can leverage seemingly minor successes to carry out larger attacks.

Finally, states are in many respects responsible for cybersecurity education and workforce-development initiatives.[26] State education-oversight bodies manage education standards,[27] and governors possess unique authority to convene companies and schools to align curriculums with business needs.[28] Likewise, governors are spearheading initiatives to steer veterans toward cybersecurity certificates and degrees.[29]

While experts regularly analyze federal efforts to secure the federal bureaucracy[30] and assist the private sector in defending itself,[31] academic and policy analysts have neglected examinations of state-

vulnerability assessments and create emergency response plans that account for cyber threats. 42 U.S.C. § 300i-2 (2012).

[25] *See Key Issue: The National System of State Regulation and Cybersecurity*, NAT'L ASSOC. INS. COMMISSIONERS, http://www.naic.org/cipr_topics/topic_cyber_risk.htm [https://perma.unl.edu/ZSN9-Z5SX].

[26] States confront four interrelated challenges to building, recruiting, and retaining a cybersecurity workforce. First, many companies are unable to find or hire employees who possess the skills necessary for writing computer code, analyzing network traffic, using security applications, or managing cybersecurity projects. Second, while graduates with these skills often find employment, supply remains limited because schools struggle to attract new students to the field or find the resources to educate those who do show interest. Third, there is a gap in finding qualified teachers to educate students in this field. Finally, cybersecurity specialists frequently choose lucrative positions in the private sector, leaving resource-strapped government agencies struggling to fill even the most basic positions. These four problems combine to create a cybersecurity workforce shortage that holds back state economic development and imperils government networks.

[27] *See State Boards of Education*, NAT'L ASS'N ST. BOARDS EDUC., http://www.nasbe.org/about-us/state-boards-of-education [https://perma.unl.edu/5A6E-GEF6].

[28] *See, e.g.*, Press Release, R.I. Gov't, Raimondo Kicks-off State's First K–12 Computer Science Initiative (Mar. 7, 2016), http://www.ri.gov/press/view/27020 [https://perma.unl.edu/EA5K-D2DQ].

[29] *See, e.g.*, Press Release, Governor Terry McAuliffe, Governor McAuliffe Announces Cybersecurity Training Initiative for Veterans in Virginia (Nov. 11, 2016), https://governor.virginia.gov/newsroom/newsarticle?articleID=18301 [https://perma.unl.edu/BR9J-DYTS].

[30] *See., e.g.*, GREGORY C. WILSHUSEN, U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES (2015), http://www.gao.gov/assets/680/671253.pdf [https://perma.unl.edu/HVW2-9PCA].

level policy. The first step to a deeper understanding for any researcher is to recognize how states implement cybersecurity policy as it applies to state agencies *and* beyond. In the previous Part, we defined cybersecurity governance as the decision processes for designing an information-security program, overseeing its implementation, and continuously adapting it to changing business needs and threats.[32] State cybersecurity governance comprises the laws, regulations, policies, procedures, organizational structures, and personal relationships that control how states: (1) secure public information assets, (2) respond to the effects of cyber attacks on public or private infrastructure, and (3) assist private citizens and businesses in securing their own information assets. Past and current state cybersecurity initiatives reflect the growing recognition among state officials that governance structures are critical to achieving these objectives.[33]

IV. CENTRALIZING SECURITY GOVERNANCE TO DEFEND STATE NETWORKS

Our broader concept of state cybersecurity governance does not exclude the traditional mission of cybersecurity: protecting the information that states own and control through IT security management.[34] Most overarching state IT structures (as distinguished from information-security programs) fall into one of three categories. A centralized-IT governance model is one where the CIO has authority for decisions related to IT strategy, project prioritization, and infrastructure management for most or all of the state's executive branch.[35] A decentralized model devolves this authority to individual state business units. In a federalized model, state CIOs and CISOs share IT managerial responsibilities with other state business units.

The characteristics and tradeoffs of these models have a direct bearing on the success of information-security programs. Experts assert that a centralized-security governance model promotes a resilient posture.[36] This is true for technical and administrative reasons. In a

[31] *See, e.g.*, Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233 (2010).

[32] GRAY ET AL., *supra* note 16, at 10; *see also* BODEAU ET AL., *supra* note 16, at 11–12 (discussing aspects of enterprise risk management such as "aligning cyber security risk management").

[33] While we believe that governance processes are essential in managing cybersecurity workforce initiatives as well, this topic is too complex to address in a single paper of this length.

[34] DE SMET & MAYER, *supra* note 14, at 4.

[35] Denford et al., *supra* note 15, at 4494.

[36] SCOTT RASMUSSEN, CENTRALIZED NETWORK SECURITY MANAGEMENT: COMBINING DEFENSE IN DEPTH WITH MANAGEABLE SECURITY 1 (2002), https://www.sans.org/reading-room/whitepapers/bestprac/centralized-network-security-management-combining-defense-in-depth-manageable-security-659 [https://perma.unl.edu/

centralized-IT environment, CISOs and their staff can use a smaller number of security-management tools, reducing workload and increasing proficiency. Consolidating security management allows multiple organizations to purchase software and hardware at scale, reducing costs.[37] A centralized security system also encourages standardized reporting of security incidents, which facilitates a coordinated response.[38] Perhaps most important, a survey of state CISOs indicates that centralization provides them with more authority to implement best practices and assign accountability for security breaches.[39]

States pursue centralization in different ways. Some focus on legal authority. As far back as 2006, Colorado moved to strengthen the CIO's power to issue cybersecurity standards with the Colorado Information Security Act. This granted the CIO, through the CISO, express authority to review and approve agency security plans and budget requests.[40] Colorado agencies must also adhere to the CISO's standards.[41] In the event of noncompliance, and after notification of the governor, the CISO can "temporarily discontinue or suspend the operation of [the agency's] communication and information resources."[42] Other states leverage the power of the governor's office to promote centralization. In Oregon, Governor Kate Brown recently issued an executive order entitled "Unifying Cyber Security in Oregon," which transferred the state agencies' IT-security functions and employees to the CIO's office,[43] thereby emphasizing centralization's impact on security. In April 2017, Alaska Governor Bill Walker also signed an order consolidating IT management and authorizing the CIO to enforce information-security policy and practices within all executive-branch agencies.[44]

WDW7-STVX] ("With a few careful considerations for data redundancy and archival, centralized network security management can take advantage of the full power and potential for defense in depth and a hardened security posture."); Warkentin & Johnston, *supra* note 11, at 16–20.

[37] *See, e.g.*, J.D. Sartain, *Why Governments Centralize IT Security*, StateTech (Sept. 25, 2014), http://www.statetechmagazine.com/article/2014/09/why-governments-centralize-it-security [https://perma.unl.edu/U4ZK-JZE8].

[38] *See* Kurt Garbars, Implementing an Effective IT Security Program 11 (2002), https://www.sans.org/reading-room/whitepapers/bestprac/implementing-effective-security-program-80 [https://perma.unl.edu/3ENE-8CJ6].

[39] CISOs who operate within a federalized model report difficulty exercising influence and authority across the state enterprise. *See* Deloitte–NASCIO Study, *supra* note 7.

[40] Colo. Rev. Stat. § 24-37.5-403 (2016).

[41] Colo. Rev. Stat. § 24-37.5-404 (2016).

[42] § 24-37.5-404(4).

[43] Or. Exec. Order No. 16-13 (Sept. 12, 2016), https://www.oregon.gov/gov/Documents/executive_orders/eo_16-13.pdf [https://perma.unl.edu/VGW3-BPEE].

[44] Press Release, Governor Bill Walker, State of Alaska, Governor Walker Announces Overhaul of State IT Services (Apr. 25, 2017), https://gov.alaska.gov/

Other states have sought to centralize through data management. Ohio has contracted with a major computing company to build a data center for all but four of the state's twenty-six cabinet-level agencies. This single cloud-based environment allows the state CIO and CISO to deploy "centrally managed end-point protection and vulnerability management tools."[45] Moreover, officials have reported cost savings, improved service delivery, and "a diminished risk profile from a security and access perspective."[46] In Oklahoma, the Information Technology Operations Command Center provides a unified "nerve center" for threat monitoring and response for fifty-eight state agencies.[47] In February 2017, a top state official testified that the Command Center had successfully blocked a ransomware attack on all unified state agencies; the only entity infected with the ransomware was one that had yet to unify.[48] Accordingly, Oklahoma Governor Mary Fallin stated, "The importance of state agencies unifying their IT with [the state's IT agency] to have the best cybersecurity available cannot be understated."[49]

Despite its positive impact on security, centralization can provoke a bureaucratic backlash among agencies that perceive security requirements as an unnecessary burden on their respective business functions.[50] A state agency in a centralized model is not necessarily free to select its preferred IT solutions if a supervisory CISO disapproves. Resolving differences and implementing policies will be difficult without knowing an agency's needs and policy positions. Without a comprehensive "network structuring phase," during which agency stakeholders' needs and concerns are addressed, a new, centralized

newsroom/2017/04/governor-walker-announces-overhaul-of-state-it-services [https://perma.unl.edu/DP56-7EXY].

[45] Ohio Dep't of Admin. Servs., IT Optimization: Status Update 2014, at 7 (2014), http://das.ohio.gov/Portals/0/DASDivisions/InformationTechnology/IS/pdf/IT%20Optimization%20Status%20Update%20-%202014.pdf [https://perma.unl.edu/7JW4-9VH3].

[46] *Id.* at 17.

[47] Office of Mgmt. & Enter. Servs., Progress on Unification (2015), https://www.ok.gov/cio/documents/HB1304QuarterlyReport06302015.pdf [https://perma.unl.edu/4MQ7-KVUT].

[48] Grant Hermes, *Gov, OMES Confirm Agency Hacked, No Ransom Paid*, News 9 (Feb. 17, 2017), http://www.news9.com/story/34515915/governor-refutes-claim-state-agency-paid-ransom-after-att.

[49] Press Release, Governor Mary Fallin, State of Okla., Gov. Fallin, OMES on Cybersecurity Incident: Unification Essential to Prevent Cybersecurity Attacks (Feb. 14, 2017), http://services.ok.gov/triton/modules/newsroom/newsroom_article.php?id=223&article_id=29400 [https://perma.unl.edu/MKJ4-SZQ4].

[50] Mansur Hasib, Cybersecurity Leadership: Powering the Modern Organization 77 (2014) ("[C]ustomer satisfaction increases as decentralization increases—up to a certain point."); Richard Pastore, *Models for Global IT Governance*, CIO (Mar. 3, 2008), http://www.cio.com/article/2437034/it-organization/models-for-global-it-governance.html [https://perma.unl.edu/HFJ6-GJ8P].

model can fail due to a lack of engagement with stakeholders.[51] States must therefore examine and account for existing relationships between state agencies and their adherence to security policies. This process identifies all relevant personnel across the state enterprise, initiates partnerships, and lays the groundwork for successful collaboration on policy implementation and incident/disruption response. This "accountability framework" enforces norms and fosters trust.[52] This also ensures that agencies report security concerns to the state CIO and CISO and not assume they will be unduly punished.

To provide a picture of IT centralization across the states, we examined enabling statutes and executive orders establishing state IT agencies. This analysis does not measure the centralization of information security but offers insight into how states can leverage their IT centralization to improve information-security outcomes. Moreover, as mentioned previously, IT-security centralization is a launching point to expand cybersecurity governance beyond networks.

To identify a state's "degree of centralization," we used a series of indicators that are proven to increase state IT effectiveness within centralized, state IT agencies: (1) ability to craft a statewide IT strategy;[53] (2) authority over statewide IT budget or authorization for IT projects across the state enterprise, or both; (3) managerial control over IT personnel across the executive branch; (4) ability to implement statewide IT policies and standards; and (5) coordination of all IT activities. In addition to these five indicators, we add a sixth: legislative approval. This derives from a study finding that legislative approval of a CIO increases efficiency and impact of IT investments.[54] Although this indicator does not directly influence centralized-IT governance, we believe it is a relevant indicator of efficiency and effectiveness.[55]

[51] Network structuring is the process of changing relationships between actors, shifting resources, and calling for a new policy direction. *See* CHHOTRAY & STOKER, *supra* note 13, at 48.

[52] Min-Seok Pang, *IT Governance and Business Value in the Public Sector Organizations—The Role of Elected Representatives in IT Governance and Its Impact on IT Value in U.S. State Governments*, 59 DECISION SUPPORT SYSS. 275 (2014).

[53] First, when embarking on any ambitious public policy project, state governments must base their goals on individual circumstances and needs. This is true for any traditional economic, public health, or public safety initiative. This principle is equally critical in cybersecurity for reasons that are both practical and legal, and effective cybersecurity governance depends on a solid strategic foundation that recognizes a state's unique attributes. Not surprisingly, states are increasingly prioritizing the creation of comprehensive cybersecurity strategies that describe an end state for state cybersecurity, scope government initiatives, identify roles for private partners, and select metrics for measuring progress. Therefore, statewide cybersecurity strategies were identified to determine if there were gaps between states that have authority to create a statewide IT strategy and those that created a statewide cybersecurity strategy.

[54] Pang, *supra* note 52, at 274.

[55] *See infra* Appendix for an explanation of methodology.

We did not conduct a formal statistical analysis for three reasons. First, there is still debate about how to define cybersecurity effectiveness, and states may differ in how they characterize effectiveness. Secondly, states differ in how they characterize "cyber attacks," "breaches," and "intrusions."[56] Lastly, not all states publish how many cyber attacks they block, how many attacks successfully intrude into state networks, and how many attacks successfully launch their payload. As a result, we cannot conclude that a state with all six traits can successfully utilize their centralization to prevent cybersecurity incidents. Rather, this data highlights how state policymakers can integrate cybersecurity protocols through their current state-IT-centralization authorities.

Figure 1 below illustrates the findings, and Table 1 details how many states exhibited each indicator. As Figure 1 shows, as of April 2017, roughly half of the states exhibited at least four indicators.[57]

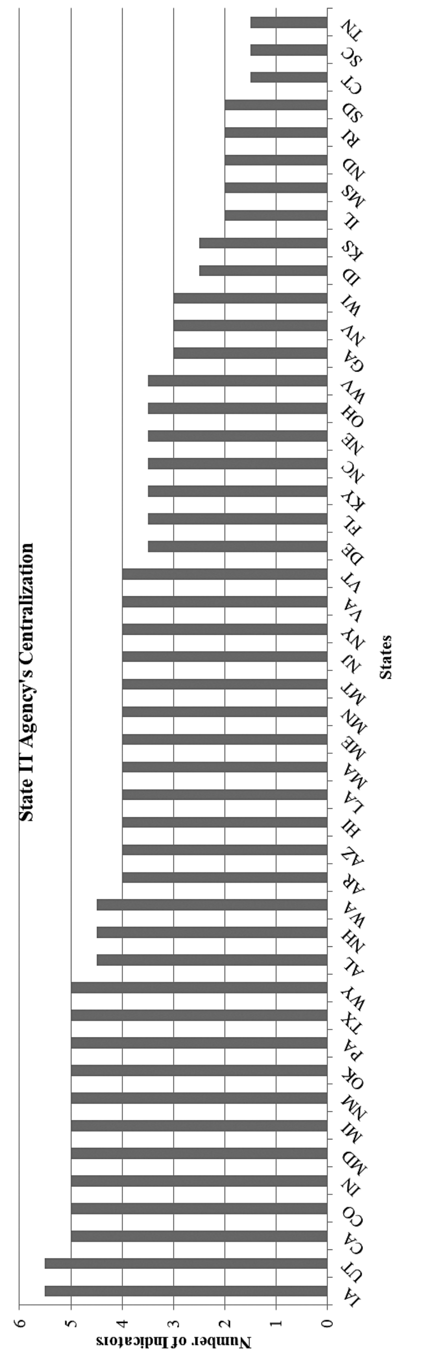
Table 1: Allocation of States by Indicator

Indicator	**States with Full Point**	**States with Half Point**
Policy	38	3
Coordination	37	1
Strategy	34	6
Budget	32	11
Legislative Engagement	13	1
Personnel	8	2

[56] PAUL CICHONSKI ET AL., NAT'L INST. OF STANDARDS & TECH., COMPUTER SECURITY INCIDENT HANDLING GUIDE 40 n.46 (2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [https://perma.unl.edu/LP8Q-G4CY].

[57] *See infra* Appendix for state-specific indicators.

Figure 1: State IT Agency's Degrees of Centralization



To the extent that states want to utilize their IT agencies' centralization to improve information security, we recommend the following. First, states wishing to further centralize their IT authorities and networks within the CIO's office should establish a governance structure that brings together all agency directors and private-sector partners. Fortunately, governors recognize this need, and several have created various cybersecurity task forces, commissions, and councils to allow these parties to collaborate on IT centralization and other issues. These bodies, usually established through executive order, are primarily tasked with identifying policies to mitigate cyber threats to the state.[58] Representing a whole-of-government approach, these bodies include representatives from IT, higher education, homeland security, emergency management, National Guard, departments of revenue, and others.[59] Through these bodies, the stakeholders not only discuss how to improve IT network security but address issues such as reinventing the workforce pipeline challenge; assisting hospitals to prepare, respond, and recover from cyber events; enhancing fusion centers' cybersecurity capabilities; and leveraging business and economic opportunities.[60] This is therefore a crucial mechanism for states to initiate centralization and to build trust to begin identifying priorities that extend beyond defending state networks.

These bodies can then be leveraged to implement our second recommendation: creating a cybersecurity strategy. State IT agencies with the authority to create a single statewide IT strategy applicable to all executive agencies should integrate cybersecurity goals and objectives. As Table 1 illustrates, in April 2017 at least thirty-four state IT agencies had the authority to implement statewide IT strategies, but only twelve of those states had cybersecurity goals and objectives in their strategies.[61] Some states have multiple agencies possessing cybersecurity elements in their respective strategies.[62] This could lead to duplication of efforts and divergent spending priorities, decreasing efficiency. Creating a single, unified cybersecurity strategy—whether stand-alone or within a single, overarching IT strategy—that details a statewide effort to achieve cybersecurity goals can drive the entire state enterprise toward the same priorities.

Finally, to facilitate the implementation of a cybersecurity strategy, IT agencies may consider utilizing their authority to reject

[58] NAT'L GOVERNORS ASS'N, MEMO ON STATE CYBERSECURITY GOVERNANCE BODIES (2016) [hereinafter GOVERNANCE BODIES], https://ci.nga.org/files/live/sites/ci/files/1617/docs/TaskForceMemoFinal.pdf [https://perma.unl.edu/RM3Q-HW57].

[59] *Id.*

[60] *Id.*

[61] NAT'L GOVERNORS ASS'N, MEMO ON STATE CYBERSECURITY STRATEGIES (2017), https://ci.nga.org/files/live/sites/ci/files/1617/docs/1703CybersecurityStrategies.pdf [https://perma.unl.edu/QWH7-SXQW].

[62] *Id.*

projects or budgets if they do not align with stated goals and objectives. By conducting risk-based analyses on all executive agencies during the formation of a strategy, priorities will be aligned based on the most vulnerable areas with the highest level of consequences if they were to be disrupted. IT agencies could then require agencies' budgets to reflect these priorities based on their individual risk assessments. This recommendation further underscores the importance of bringing agency principals together because there would undoubtedly be hostility if this policy were to be implemented unilaterally. In other words, building trust between stakeholders is paramount to state cybersecurity and is the foundation to state cybersecurity governance.

V. GOVERNANCE BEYOND NETWORK DEFENSE

As the three recommendations above illustrate, implementing state cybersecurity policies should involve emergency management, law enforcement, academia, the health sector, critical infrastructure, private-sector partners, and others. Convening these stakeholders to address the first fundamental challenge of cybersecurity—securing the state's networks—builds relationships and fosters trust that can be employed to undertake larger issues: preparing and responding to cyber disruption events, addressing cyber crime, launching cybersecurity centers, and enhancing the cybersecurity-workforce pipeline.

A. Disruption Response

Regardless of its size, population, economy, or assets, every state is vulnerable to a cyber event that exposes private data or limits access to public services. Unlike private companies, whose disruption response plans are generally limited to remediating and recovering their own business processes, states must be prepared to respond holistically to a high-consequence cyber disruption. Potential risks to water systems, electric grids, 9-1-1 dispatch centers, and hospitals have led states to apportion roles and responsibilities among homeland security, public safety, and emergency-management agencies.[63] As with any natural disaster, responding to a cyber disruption requires close coordination among these stakeholders and direction by their respective leadership teams.[64]

[63] NAT'L GOVERNORS ASS'N, MEMO ON STATE CYBERSECURITY RESPONSE PLANS (2016) [hereinafter RESPONSE PLANS], https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf [https://perma.unl.edu/6C92-2UCK].

[64] NAT'L ASS'N OF STATE CHIEF INFO. OFFICERS, CYBER DISRUPTION RESPONSE PLANNING GUIDE 2 (2016) [hereinafter NASCIO GUIDE], http://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf [https://perma.unl.edu/BM99-CQQ9].

Although it is a subcomponent of state cybersecurity governance, disruption response demands a governance structure all its own. The National Cyber Incident Response Plan (NCIRP) refers to governance as a "vital and an enabling factor in states' cyber asset response role."[65] The National Association of State Chief Information Officers (NASCIO) reiterated this point and emphasized the need to establish governance among a wide range of agencies, to detail roles and responsibilities during cyber disruptions, and to involve external partners.[66] NASCIO contends that a response plan should "apply to all State agencies, boards, commissions, and departments . . . as well as local governments," further emphasizing the need for a whole-of-state approach to cyber-disruption response.[67]

In previous research, we identified thirteen disruption response plans in states.[68] These plans are typically written as an annex to a statewide emergency operations plan (EOP), embodying the whole-of-state approach by directing fusion centers, state police, departments of military affairs, the National Guard, departments of public safety, and others to prepare and respond to a cyber event.[69] The plans therefore recognize a cyber event's potential to transition from a virtual matter to a physical one. As a result, they ensure all appropriate state agencies are ready to respond.

The NCIRP recommends that states synchronize their cyber-disruption response plans with their EOPs.[70] Executing a response plan as an annex to an EOP has at least two benefits. First, it facilitates integration with existing emergency support functions (ESFs)—such as communications, emergency management, and resource and logistics support—without duplicating or contradicting established procedures. State officials who are already familiar with ESF functions can more easily understand their own roles during a cyber response if plans interlock with existing processes and known lines of communication.

A second benefit is that a state emergency-operations center (SEOC) or a unified command system (UCS)—emergency decision-making bodies included in most EOPs—provides a ready-made governance framework that can be modified to reflect the priorities of a cyber response. For example, in Virginia, three agencies lead the UCS during a cyber event. The IT agency manages cyber-response activities, while the emergency-management agency and state police coordi-

[65] U.S. Dep't of Homeland Sec., National Cyber Incident Response Plan 16 (2016) [hereinafter NCIRP], https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf [https://perma.unl.edu/8UUW-F3F2].

[66] NASCIO Guide, *supra* note 64, at 20–21.

[67] *Id.* at 21.

[68] Governance Bodies, *supra* note 58.

[69] *Id.*

[70] NCIRP, *supra* note 65, at 16.

nate response and recovery efforts.[71] Organizing a response through the SEOC also reinforces the necessity of a whole-of-state effort, reducing the potential for bureaucratic friction.

Governance structures surrounding response efforts should always emphasize cooperation with nonstate entities prior to a crisis. Private industry owns and operates over eighty-five percent of the nation's critical infrastructure.[72] Partnerships with these owners pave the way for threat-information sharing, implementation of mitigation policies, and identification of the necessary resources and coordination efforts needed to respond and recover from a cyber disruption event.[73] Governance bodies provide an avenue for state information-security and emergency-management officials to identify private-sector resources and establish communication pathways before a significant cyber event. Critically, they also provide an organizational framework for developing and exercising response plans to identify mistaken assumptions and potential revisions.

B. Law Enforcement

Although frequently overlooked in cybersecurity-policy discussions, state and local law enforcement professionals are in fact the tip of the spear. Not only do they play a critical role in cyber-disruption response, but they also must fulfill their primary duty: investigating and prosecuting cyber criminals. How states plan for and fund this mission, by which a state fulfills its obligation to protect the public welfare, is an indispensable aspect of state cybersecurity governance. Financial losses from computer crime and identity theft can have a devastating impact on individuals, particularly those living on a fixed income, as well as small businesses.[74]

Unfortunately, many state and local investigators lack the laws, resources, and knowledge to investigate these crimes, identify suspects, and deter other potential criminals. The FBI and Secret Service

[71] RESPONSE PLANS, *supra* note 63, at 1.

[72] *Critical Infrastructure and Key Resources*, INFO. SHARING ENV'T, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources [https://perma.unl.edu/7D7G-6FWW].

[73] NASCIO GUIDE, *supra* note 64, at 22.

[74] One survey by the National Cyber Security Alliance estimated that sixty percent of small businesses close within six months of a cyber attack. Gary Miller, *60% of Small Companies that Suffer a Cyber Attack Are Out of Business Within Six Months*, DENVER POST (Mar. 24, 2017), http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business [https://perma.unl.edu/RW83-N6D5]. Aggregated data provides a more tangible picture. In 2015, the FBI received 127,145 separate complaints of Internet crimes totaling over one billion dollars in losses. Note that many of these instances involve nonpayment of online transactions or harassment. INTERNET CRIME COMPLAINT CTR., U.S. DEP'T OF JUSTICE, 2015 INTERNET CRIME REPORT 12 (2015), https://pdf.ic3.gov/2015_IC3Report.pdf [https://perma.unl.edu/ZP3D-GCRP].

lend their expertise only in the most serious cases; federal investigators rarely focus on ordinary computer crime, notwithstanding its massive impact.[75] Consequently, computer criminals with a low profile can operate with relative impunity. Closing this capability gap demands a governance structure.

First and foremost, policymakers must determine whether their criminal code satisfies law enforcement needs in this area. Some laws do not authorize investigators to pursue all computer crimes. Every state legislature has criminalized computer hacking and computer fraud, but the scope of prohibited activities varies widely. Broad statutes allow prosecutors to target a wide range of criminal acts and so do not necessarily merit regular updates to keep pace with technological change. Massachusetts law carries a criminal penalty for any person who "without authorization, knowingly accesses a computer system by any means, or . . . knows that such access is not authorized and fails to terminate such access."[76] This formulation provides great flexibility to investigate and prosecute creative cyber criminals. States with narrower prohibitions have amended their computer-crime statutes to reflect evolving criminal tactics. In 2017, New York created a new criminal prohibition focused on denial-of-service attacks.[77] California recently amended its laws targeting extortion by explicitly and clearly prohibiting the use of ransomware.[78] In recent years, many states have increased the penalty for hacking offenses. Formalizing a continuous dialogue between criminal investigators, policymakers, state technology officials, and lawmakers to keep pace with computer criminals is an important part of state cybersecurity governance.

Properly configured laws alone do not provide the practical capability to enforce them. Many state and local agencies either lack the expertise to conduct computer investigations, or they possess the proper skills but suffer from a severe personnel shortage. As the Police Executive Research Forum observed in 2014, "[M]ost of the 18,000 local and state law enforcement agencies have not yet developed plans and jurisdictional authority to enter this arena."[79] Several interrelated challenges frustrate efforts to create investigative units or develop existing ones. Building the skills and manpower necessary to track cyber criminals and prosecute them is resource intensive; most, if not all, state agencies operate in an austere budget environment. Com-

[75] Police Exec. Research Forum, The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime 2 (2014), http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf [https://perma.unl.edu/B9Y3-XZ5R].

[76] Mass. Gen. Laws ch. 266, § 120F (2012).

[77] S.B. 114, 239th Leg., Reg. Sess. (N.Y. 2017).

[78] Cal. Penal Code § 523 (West 2017).

[79] Police Exec. Research Forum, *supra* note 75, at 2.

pounding this problem is a frequent absence of political pressure for a robust cyber-crime capability. Cyber crime does not generate the widespread outrage that can persuade public safety officials to redirect resources. For various reasons, most instances of cyber crime are never reported to police.[80]

These challenges will be difficult to address without elevating cybersecurity into existing governance processes within law enforcement agencies, large or small. Coordinated outreach to local individuals and businesses, as well as larger corporations that operate across a region, will generate leads and improve situational awareness. In Madison, Wisconsin, police are launching "a multi-disciplinary, community-based approach," by creating an informational DVD, forming a cyber-safety curriculum for classrooms, establishing a Youth Cyber Detective Camp that delves into security in the context of cutting-edge apps, and organizing the Madison Area Council on Cyber Safety for Children.[81]

Proper engagement will generate many leads, and given the sheer volume of cyber crimes, agencies with limited investigatory resources must identify procedures for prioritizing cases. In Utah, the state Cyber Crimes Unit has declined to set a specific monetary threshold for prioritizing cyber crime cases, reasoning that it is too difficult to measure the value of stolen information, which may not be sold or exploited for many months. Additionally, a department with only two or three computer-forensics experts will need to balance time devoted to *computer hacking* investigations with time spent on *computer-enabled crimes*, which are traditional crimes committed with the aid of a computer.

Policymakers and legislatures commit more resources to investigations that tend to produce "success"—often measured in terms of recovered property, indictments, or prosecutions. Some cyber-crime investigations may be unable to pursue suspects that live overseas yet could be able to recover lost data belonging to the victim. Law enforcement professionals will need to carefully consider how to communicate the success of cyber-crime investigations through alternative metrics.

[80] Organizations may be reluctant to disclose a breach that could drive away business. Credit-card holders who fall victim to computer fraud normally can count on their respective banks to bear the subsequent costs and have little incentive to seek assistance from the police. *See* David Braue, *Most Cybersecurity Breaches Go Unreported, Uninsured Despite Executive Concern: Barclays*, CSO (Mar. 4, 2016), http://www.cso.com.au/article/595298/most-cybersecurity-breaches-go-unreported-uninsured-despite-executive-concern-barclays ("Nearly three-quarters of cyberattacks are going unreported even as a flood of data and fraudulent attacks sees executives losing control of their sensitive corporate data, according to a new UK survey . . . .").

[81] POLICE EXEC. RESEARCH FORUM, *supra* note 75, at 35–36.

Such decisions must be coordinated and implemented through a governance process.

State law enforcement agencies can partially address their resource gap by drawing from outside expertise. Private companies may have more investigatory experience than state or local police.[82] These experts can grab some of the "low-hanging fruit" by training all officers in basic criminal techniques for hiding and destroying evidence that, if thwarted, can dramatically reduce the burden on the limited number of forensic experts. In some states, law enforcement is working with computer science departments at colleges and universities that not only offer resources to police but also provide a potential pipeline for tech-savvy students to enter law enforcement.[83] Michigan's Cyber Civilian Corps (MiC3) is a unique model. The MiC3 is a group of information-security professionals from public, education, and private sectors who volunteer to aid public and private entities in the state when the governor declares a state of emergency due to a cyber event.[84] States may consider using a similar model when preventing and responding to cyber crime that affects citizens and small businesses, which would further lessen the burden on state police units. Outside partnerships such as these require consistent and high-level engagement by leadership across law enforcement agencies—in other words, governance.

C. Cybersecurity Centers

Apart from security operations centers, such as Oklahoma's Command Center, many states are planning organizations with a broader focus. The proliferation of so-called cybersecurity centers underscores a need for information sharing and broader coordination within and outside of state government. These centers fortify and advance the whole-of-government approach by including a wide range of public and private actors to overcome complex challenges.

New Jersey and California are two states that have established cyber centers specifically to enhance information sharing across entities. The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) was created by executive order in May 2015 to be "the central State civilian interface for coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the

[82] *Id.* at 41.

[83] *Id.*

[84] *Michigan Cyber Civilian Corps*, STATE OF MICH., http://www.michigan.gov/som/0,4669,7-192-78403_78404_78419—-,00.html [https://perma.unl.edu/JU6N-P49G].

public and private sectors."[85] The California Cybersecurity Integration Center (Cal-CSIC) was also created by executive order, with the main purpose to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or its public and private-sector computer networks.[86] To carry out this mission, Cal-CSIC includes a wide range of representatives such as highway patrol, the health and human services agency, state universities, and the attorney general's office.[87] In addition to responsibilities similar to the NJCCIC, the Cal-CSIC is charged with developing a cybersecurity strategy and cyber-incident response team, both of which will be leveraged to assist law enforcement agencies.[88]

Colorado's National Cybersecurity Center (NCC) resembles the previous two centers as it also coordinates responses for members and acts as a one-stop shop for organizations that need immediate assistance to resolve an active attack or breach. Yet, the NCC also includes the Cyber Research, Education, and Training Center (CRETC) and the Cyber Institute to provide other services. The CRETC, led by the University of Colorado, will foster technical research and development, education programs, and general cybersecurity workforce development, and it will serve as the state's key focal point for partnerships with federal and local agencies. For instance, CRETC will establish education, training, and academic symposia for government leaders at all levels, as well as coordinate with community colleges in the development and transferability of appropriate curriculum and technical certification programs.[89] Lastly, the Cyber Institute provides a location for officials from the federal government, the state, cities, and counties to share real-time information on cyber trends, security and cutting-edge best practices.

Most recently, Missouri's cybersecurity task force recommended that the state establish its own Cybersecurity Institute, which would have a broader mandate than that in Colorado. The Cybersecurity Institute would act as a clearinghouse for schools "seeking cybersecurity designations and accreditation" and a "one stop sho[p]" for businesses and government agencies in need of cybersecurity advice—a conduit to channel state and federal cybersecurity research funding, select grantees for scholarships, and offer career services.[90] Missouri's center remains only a proposal, but it further reflects the growing

[85] N.J. Exec. Order No. 178 (May 20, 2015), http://nj.gov/infobank/circular/eocc178.pdf [https://perma.unl.edu/A2SV-ZPBW].

[86] Cal. Exec. Order No. B-34-15 (Aug. 31, 2015), https://www.gov.ca.gov/docs/B-34-15.pdf [https://perma.unl.edu/4D8F-URAE].

[87] *Id.*

[88] *Id.*

[89] Colo. Rev. Stat. § 24-33.5-1904 (2017).

[90] Mo. Office of Cyber Sec., Mo. Office of Admin., Cybersecurity Task Force Action Plan 8 (2016), https://cybersecurity.mo.gov/files/task_force/plans/FINAL_

trend toward holistic centers designed to enhance cross-sector cybersecurity outside of government. However, concerns have been raised regarding the sustainability and effectiveness of these centers, and the utility of such centers demands close observation.

VI. CONCLUSION

As public agencies and services increasingly incorporate networked devices, business risk deriving from cyber threats is unlikely to abate. Absent a major shift in federal budgeting policy, federal authorities simply cannot offer the necessary level of assistance. Protecting citizens from this threat has been and will continue to be a state responsibility, just as it is the state's responsibility to protect citizens from robberies, assaults, and natural disasters. Cybersecurity is no longer an IT issue that relies on IT professionals implementing IT solutions. It requires a concerted effort by the state to convene CIOs, hospital administrators, university provosts, public utility commissioners, police chiefs, and private company CEOs (among others) to address the vast implications of cyber risks.

This is not a simple task. The history of public policy is riddled with examples of failures to bring a diverse group of stakeholders together to solve complex challenges. Yet, through formal governance mechanisms, as described throughout this Article, states can better position themselves and their constituents to adopt a mature risk posture. This will ensure that citizens are adequately protected from cyber threats, while enjoying the benefits of an ever-expanding, digitally-connected world.

Our observations and recommendations outlined above are neither final nor unimpeachable; we have merely marked a path for future researchers who want to assess cybersecurity policy. Cybersecurity as a discipline cuts across virtually every public policy field, and yet it lacks the research tools for measuring progress that are common to other policy arenas. More researchers must examine the effectiveness of state cybersecurity governance through a framework to assess cybersecurity strategies, funding priorities, response plans, cybercrime units, cyber centers, and workforce initiatives.

Cybersecurity_Task_Force_Action_Plan_12.29.16.pdf [https://perma.unl.edu/SJV3-LZM7].

APPENDIX: STATES AND INDICATORS

Our methodology allocates for each state a full point for every criterion it meets fully, and a half point for partial completion. Full points were only allotted if the IT agency had authority to implement a strategy, policies, and standards over all executive branch agencies. A full point was allocated to states whose IT agencies had complete control over the state's IT expenditures or approved agencies' expenditures. Half points were allocated if the IT agency could only recommend budget needs for state agencies. A full point was given if the agency had full authority over all statewide IT personnel across the executive branch, and half a point if they could recommend the hiring of personnel. "Coordination" was ambiguously defined in research, so a state was allotted a point if "coordinate" or "coordination" was in the statute or executive order. Lastly, half a point was given for legislative engagement to a state if a legislative committee was created or designed to oversee the IT agency but did not have authority to approve the CIO. These points were not weighted due to the sixth indicator deriving from a separate study. State officials were not consulted for this analysis, and therefore, a state's degree of centralization is solely based on statutes and executive orders. Alaska and Missouri were not included in this analysis due to lack of access to their legislative materials. Oregon was omitted due to the re-organization of its IT governance structure during the writing of this paper. Territories were also not examined.

State	Strategy/ Master Plan	Budget/ Finance	Personnel	Policy	Coordination	Legislative Engagement
AL	X	X		X	X	/
AR	X	X		X	X	
AZ	X	X		X	X	
CA	X		X	X	X	X
CO	X	X	X	X	X	
CT	/	X				
DE	X	/		/	/	X
FL	/	X		X	X	
GA		X		X	X	
HI	X	X		X	X	
IA	X	/	X	X	X	X
ID		/		X	X	
IL (EO)			X			X
IN	X	X	X	X	X	
KS	X	/		X		
KY	X	/		X	X	
LA	X	X		X	X	
MA	X	X		X	X	
MD	X	X		X	X	X
ME	X	X		X	X	
MI	X	X	X	X	X	

State	Strategy/ Master Plan	Budget/ Finance	Personnel	Policy	Coordination	Legislative Engagement
MN	X	X		X	X	
MS		X				X
MT	X	X		X	X	
NC		X	/	X	X	
ND	/	X		/		
NE	X	/		X		X
NH	X	X		/	X	X
NJ (Two EOs)	X	X		X	X	
NM	X	X		X	X	X
NV	X	X		X		
NY	X	X		X	X	
OH	/	X		X	X	
OK	X	X	X	X	X	
PA (EO)	X	X	X	X	X	
RI	X				X	
SC (multiple EOs)	X	/				
SD				X	X	
TN		/		X		
TX	X	X		X	X	X
UT	X	X	/	X	X	X

State	Strategy/ Master Plan	Budget/ Finance	Personnel	Policy	Coordination	Legislative Engagement
VA	X	X		X	X	
VT	X	X	X		X	
WA	/	X		X	X	X
WI (and EO)	/	/		X	X	
WV	X	/		X	X	
WY	X	/	/	X	X	X