Free markets. Real solutions.

R STREET POLICY STUDY NO. 229
May 2021

ENHANCING STATE AND LOCAL CYBERSECURITY RESPONSES

By John Bansemer, Greg Rattray and Franklin Lee

CONTENTS

EXECUTIVE SUMMARY

The R Street Institute has conducted a study of the challenges associated with improving state and municipal responses to cyber attacks. This study leverages existing reports, interviews with defenders at the state and municipal level, experts studying these challenges, as well as workshops conducted in conjunction with the New York Cyber Task Force. It describes the shape of the challenges and offers recommendations for action to improve state and municipal cyber response capabilities. Further, understanding the associated challenges and extending the work on the recommendations within this report requires significant follow-on efforts. This report seeks to engage and assist those on the front line—governors, mayors, personnel, and state and local governmental organizations. While the federal government and the private sector play key roles, they were not the specific focus of this study.

INTRODUCTION

No school for the next week. Normally students would be elated, but in 2020 with a remote learning environment and already frazzled parents the announcement just made a difficult year that much tougher. Adding even more frustration, the cause of the shutdown was a ransomware attack targeting the school district of Baltimore County.[1] Beyond dealing with response and recovery efforts, school and county officials had to determine if personal data had been compromised. As a result, children already struggling in distance learning environments suddenly faced the prospect of ransomware-induced shutdowns.

Baltimore has faced these types of attacks before. In May 2019, the city fell victim to a ransomware attack that blocked access to data and services including systems to pay bills, property taxes and a parking fines database.[2] Citing advice from federal officials, Baltimore refused to pay the ransom of approximately $80,000 and ultimately spent over $18 million in recovery expenses. While far more costly than paying the original ransom, Baltimore had no guarantee the attackers would restore services. Additionally, the costs would not have ended at a ransom payout as the city would still have to rebuild or replace vulnerable systems.

Note: This is a corrected version of the paper originally published. One edit has been made to the Introduction section to correct a factual error.

1. Lillian Reed et al., "As Baltimore County recovers from ransomware attack, state audits have routinely found security problems in other school districts," *The Baltimore Sun*, Dec. 4, 2020. https://www.baltimoresun.com/education/bs-pr-md-baltimore-county-ransomware-20201203-20201204-5g3he4yi2je6npug3vcf7zih3i-story.html.

2. Niraj Choksi, "Hackers are Holding Baltimore Hostage: How They Struck and What's Next," *The New York Times*, May 22, 2019. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

Baltimore is by no means alone in the fight against cyber criminals. In August 2019, more than 20 organizations in Texas were hit with a widespread ransomware attack.[3] The majority of the victims were small, local governments that relied on the same managed security service provider (MSSP) to secure their systems. By subverting this single provider, attackers were able seek ransom from multiple localities. Later that year in November, hackers nearly compromised the fingerprint database for the New York Police Department (NYPD) after a contractor inadvertently installed a system infected with malware on the network.[4] While the fingerprint database had to be taken off-line as the attack was mitigated, the effects could have been much worse if not for the quick discovery and response.

In recent years, ransomware has become a dominant feature of the cyber threat landscape. According to one report, ransomware attacks increased by 485 percent from 2019 to 2020.[5] In 2020, ransomware attacks extended to the education sector such as the Baltimore case and healthcare providers as they struggled to manage the COVID-19 pandemic.[6] While final 2020 ransomware numbers are still being tallied, it appears that over 70 state and local government organizations were impacted in the last year.[7] In fact, Chris Krebs, the former director of the Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) called ransomware the "biggest threat" facing organizations.[8]

Once a ransomware attack occurs, states and localities face an unpalatable choice, either pay the ransom thus rewarding criminal behavior and financing the attacker's continued assaults or refuse to pay the ransom and work to restore services. From a monetary perspective, the costs of recovery are high. For example, following the Baltimore attack, the budget office estimated a cost of $18.2 million due to a combination of lost or delayed revenue and direct costs to restore systems after the May 2019 ransomware attack.[9] In August of 2019, the city was forced to transfer $6 million, initially a fund for parks and public facilities, for cyber-attack remediation and other information technology (IT) expenses. This is part of a broader, disturbing trend: ransomware costs are going up with potentially devasting effects on organizational budgets. Likewise, the average requested ransom has increased from about $5,000 in 2018 to nearly $200,000 in 2020.[10] The tactics have changed as well with more focus on organizations that can pay larger ransoms rather than individuals.[11] However, the costs do not end with payouts and remediation as cybersecurity insurance firms will likely raise their on-going rates to cover these and other losses. As a result, debates over the limits of cyber insurance continue in cases where nation-states may be involved.[12]

Ransomware is just one of many potential cyber attacks. In these situations, state and local governments are enticing targets. Beyond purely financial motivations, under the right circumstances more sophisticated attackers could disrupt the life and commerce of major municipalities. Blame is often placed on victim organizations, suggesting they should have been better prepared. However, many state and municipal IT departments lack the necessary funding and requisite cyber expertise to prepare, defend and respond to various cyber threats. Ironically, organizations that shortchange cybersecurity may face far greater future expenses related to remediation and recovery. Some vendors have even started to "grade" the overall security posture of states and suggest that many are either failing or just getting by in defending their respective states.[13] Such report cards could potentially provide a valuable service if the methodologies and the data used to score states were accessible to the relevant organizations and third parties for verification and validation, but this is not always the case.[14] For example, one report—generated prior to the 2020 election—drew significant criticism from state election officials who questioned the company's methodology.[15]

The U.S. Chamber of Commerce has issued a set of principles for security ratings which represents an important step in the

3. "Update on Texas Local Government Ransomware Attack," Texas Department of Information Resources, Sept. 5, 2019. https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213.

4. Tara Seals, "NYPD Fingerprint Database Taken Offline to Thwart Ransomware," Threat Post, Nov. 25, 2019. https://threatpost.com/nypd-fingerprint-database-ransomware/150592.

5. "2020 Consumer Threat Landscape Report," Bitdefender, 2020, p.8. https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf.

6. Ana Bera, "22 Shocking Ransomware Statistics for Cybersecurity in 2021," SafeAtLast, 2021. https://safeatlast.co/blog/ransomware-statistics.

7. "Ransomware Attacks Map," StateScoop, last accessed Feb. 25, 2021. https://statescoop.com/ransomware-map.

8. Kiran Stacy and Hannah Murphy, "Former U.S. Cyber Chief Call for Military to Attack Hackers," *Financial Times*, Feb. 5, 2021. https://www.ft.com/content/27c09769-ceb5-46dd-824f-40b684d681ae.

9. Ian Duncan, "Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts," *Baltimore Sun*, May 29, 2019. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

10. Lily Hay Newman, "Ransomware is Headed Down a Dire Path," *Wired*, Dec. 29, 2020. https://www.wired.com/story/ransomware-2020-headed-down-dire-path.

11. Ibid.

12. Jon Bateman, "Does Your Cyber Insurance Cover A State-Sponsored Attack?", *Harvard Business Review*, Oct. 30, 2020. https://hbr.org/2020/10/does-your-cyber-insurance-cover-a-state-sponsored-attack.

13. Alexander Heid, "Security Scorecard's 'State of the States' Report Explained," SecurityScorecard, Oct. 15, 2020. https://securityscorecard.com/blog/securityscore-cards-state-of-the-states-report.

14. Phil Venables, "Security Ratings: Love, Loathe or Live With Them?", Risk & Cybersecurity, Dec. 13, 2020. https://www.philvenables.com/post/security-ratings-love-loathe-or-live-with-them.

15. Jessica Huseman, "Security Election Report Gains Attentions, and a Sharp Rebuke," ProPublica, Sept. 13 2019. https://www.propublica.org/article/report-on-election-security-gains-attention-and-a-sharp-rebuke.

right direction to make these assessments more beneficial.[16] However, effective cybersecurity remains a difficult challenge even for well-financed businesses and the federal government, as the recent Solar Winds-related hacking activity demonstrates.[17] While the desire to find fault might be understandable, blaming the victim will not improve defenses particularly when the root causes are often multi-layered.

As noted, ransomware is just one of the many cyber threats faced by state and local governments as they provide essential services for citizens while seeking to protect their personal data. While ransomware attacks have recently proved the most frequent type of attack, in 2020, concerns about potential vulnerabilities in state voting machinery leading up to the election were front and center. In this instance, the cybersecurity news was decidedly good. The former CISA director, Chris Krebs, called the 2020 election the most secure in U.S. history and most experts have lauded this effort.[18] While not all voting infrastructure was exposed to the internet, the overall lack of hacking and cyber-related disruptive incidents was encouraging.[19] In some respects, this relatively good news may be a function of where attackers and nation-states focus their attention.

Our society increasingly relies on digital services for almost all aspects of life. For those in state and municipal government that must manage the technologies, networks and the data that underpin these digital services, such reliance also presents risks. To date, the number of state and municipal governments impacted has been relatively small. Moreover, the experimentation within the states and the best practices that many municipalities have developed point to a path of lower-risk profiles and more effective response and recovery. Moving forward, a greater understanding of both the challenges facing state and local government and the progress they have made can help plot a way forward.

METHODOLOGY

With these growing threats as a backdrop, R Street initiated a study to illuminate key challenges and to provide insight on measures to reduce the risks to state and municipal governments and the services they provide resulting from cyber attacks. Regarding municipalities, the study focused on large cities who might be the target of coercive attacks, and who may need to marshal resources from the federal government, state and private sector. The investigation began with an examination of the growing set of reports and analyses regarding incidents, responses and organizational models engaged in state and municipal cyber responses, including the role of the federal government. Over the course of this project, various practitioners and experts were interviewed to discern how state and key municipal governments have dealt with cyber attacks and how they are preparing for future events. The goal was not to criticize past actions or grade current efforts but to understand valuable lessons learned from these experiences and highlight best practices, some of which are nearly universal in their applicability and others that may be more tailored to individual organizations.

The project concluded by identifying and injecting specific challenges and questions into a series of table-top exercises built in support of the New York Cyber Task Force (NYCTF). These questions were designed to force participants to wrestle with a sophisticated attack scenario and consider what actions, if taken before a major cyber event, could reduce their impact. A key dimension of the NYCTF work was to look out to the year 2025, examining severe but plausible cyber attacks rising to the level of national security concerns including challenges for response at the state and municipal levels. The NYCTF conducted two workshops in fall of 2020 that intersected with the work in this study. The first scenario focused on nation-state attacks that used disruption of life in major municipal centers as the focus of coercive disruptive attacks. The second focused on the potential of domestic extremism using cyber attacks including those against law enforcement and other municipal services. As leaders and participants in the NYCTF efforts, the insights and learning from these workshops are incorporated within the analysis presented.[20]

Over the course of several months, a number of insights emerged. First, many organizations are doing better than what many commenters and security vendors might suggest. With a large number and diversity of state and local targets for would-be attackers, the fact that more organizations have not been impacted is good news. Yet it is not clear whether this situation exists because other organizations are more secure or have just yet to be targeted by a significant attack. Likewise, absence of evidence of an attack is not evi-

16. "Principles for Fair and Accurate Security Ratings," U.S. Chamber of Commerce, June 20, 2017. https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

17. Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," Dept. of Homeland Security, Dec. 17, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

18. Cybersecurity and Infrastructure Security Agency, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," Press Release, Nov. 12, 2020. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

19. Paul Rosenzweig, "The Capitol Insurrection and Pineapples on Pizza," R Street Institute, Jan. 26, 2021. https://www.rstreet.org/2021/01/26/the-capitol-insurrection-and-pineapples-on-pizza.

20. For further reading on the NYCTF, see "Building a Defensible Cyberspace," Columbia School of International and Public Affairs, 2017. https://www.sipa.columbia.edu/ideas-lab/techpolicy/building-defensible-cyberspace.

dence that an organization is not vulnerable. Second, there is no single best way for a state or municipality to organize, respond or recover from a major cyber attack. The diversity of approaches observed suggests there are many ways of tackling the hard problem of defending cyber assets, systems and public services with limited resources. Third, state and local organizations should apply key contingency planning and organizational response principles that have the potential of improving their capability to protect against a severe attack and, if such an attack should occur, recover gracefully and quickly.

Understanding the Challenges of Effective State and Local Cyber Responses

After investigating how organizations have been affected by cyber attacks and talking with those on the front line managing these responses, the fundamental complexity of issues facing efforts to improve state and local cyber response became increasingly clear. In some ways daunting, the complexity of the observed approaches can also be viewed as a strength as it provides organizations with many potential options for collaboration across all levels of government as well as with the private sector. When a cyber attack occurs, these external organizations may play an important role in response and recovery beyond the specific state or locality under attack. Designing flexible approaches allows organizations to orchestrate many types of assistance; however, challenges remain.

At the federal level, the various departments and agencies—especially the Federal Bureau of Investigation (FBI), the DHS and the Department of Defense (DoD)—have important, well-defined roles. Depending on the nature of the incident, the FBI may lead the investigation to uncover who is responsible for the attacks. Local FBI offices have already established strong relationships with the state and larger municipalities and participation in the InfraGard program to protect critical infrastructure that usefully brings together state, municipal and private sector cyber responders.[21] In addition to the provisioning of threat-related information, the DHS can provide advice, threat information and limited technical support. However, if attacks are widespread, the ability to provide on-site support becomes even less likely. For its part, when authorized, the DoD, through U.S. Cyber Command, can provide technical support to other federal departments and agencies and may be tasked to provide support to state or municipal civil authorities when properly requested and approved. Here again, technical support could be limited if attacks hit multiple jurisdictions simultaneously or the attack falls below thresholds that warrant a federal response.

Given these limitations, states and municipal operators of digital services and their security teams have also turned to alternative sources of support. The following table summarizes several of the options available to states.

TABLE I: STATE OF CYBER DEFENSE ORGANIZATIONAL OPTIONS

Options	Features
State National Guard forces	Activated under a variety of authorities to support state emergencies. Well-understood resource available to states.
State defense forces *(also known as state militia or state guard forces)*	Funded by the states, operate exclusively under the authority of the governor and have no federal missions. Can aid with missions and incident response when the National Guard might not be available.
State cyber reserve forces	All volunteer civilian forces. Allows rapid response assistance during a cybersecurity incident.
State IT departments	Somewhat similar to state cyber reserve forces, can provide on-call personnel from the state's IT departments during a cyber emergency.

As cybersecurity issues have increased in prominence and reach, many state National Guard units have begun to support cyber defense missions. This development is a natural evolution of National Guard missions in support of state emergencies and, over time, as they build out their teams may provide critical manpower and expertise in a crisis. Given its long history of supporting the states with natural disasters and other emergencies, the National Guard is a well understood resource available to states who know how to activate these units in an appropriate situation.[22]

However, complicating factors exist related to activation authorities and funding related to use of the National Guard in cyber response. For example, under state active duty (SAD), the guard unit falls under the command of the state's governor, who generally exercises control via the state's adjutant general (the TAG). When activated under SAD authorities, the state is responsible for all funding.[23] In some circumstances, the president or the Secretary of Defense can authorize or direct the use of National Guard forces under different provisions of Title 32 such as in the Hurricane Katrina response, or, more recently, in 2017 when over 50,000 National Guard personnel from 43 states were activated to assist in hurricane relief efforts.[24] In devasting scenarios like these, governors can deploy National Guard members to support state activities with federal funding once granted the federal authority to do so. However, when

21. "What is InfraGard?", The Center for Information Security Awareness, last accessed Feb. 25, 2021. https://www.cfisa.com/what-is-infragard.

22. "Enter the Newest Domain in Warfare," Army National Guard, 2021. https://www.nationalguard.com/careers/cyber.

23. "Understanding the Guard's Duty Status," National Guard Association of the United States. http://giveanhour.org/wp-content/uploads/Guard-Status-9.27.18.pdf.

24. Monica Ruiz, "The Hybrid Benefits of the National Guard," *Lawfare*, July 23, 2019. https://www.lawfareblog.com/hybrid-benefits-national-guard.

operating in Title 32 status, whether providing support as an incident to training or providing operational support under Title 32, Section 502(f), the National Guard forces remain under the command and control of the state governor. Lastly, under "federalized" Title 10 activations, guard units directly support federal missions, are federally funded, and operate under the command and control of the president through the Secretary of Defense and the Commander, U.S. Northern Command.

Ultimately, the authorized duties for National Guard units are prescribed by their specific activation status. Conversations with state and local personnel indicated these limitations can also lead to confusion as to what support can and cannot be provided in specific cyber response situations. For example, for incidents that affect a single municipality, both how National Guard personnel will be funded and their associated authorities can delay support. There can also be experience and training mismatches. For instance, if cyber support to an impacted municipality primarily involves system and network rebuild, support by a National Guard unit focused on red teaming may be misaligned or fall outside the scope of what can be authorized.

Perhaps the most challenging aspect relates to the specific activities that National Guard units are allowed to conduct. Command lines, funding and authorized activities vary depending on the status and authorities under which the National Guard units operate.[25] Suffice it to say that questions remain on the duties and missions these units can perform under various scenarios. A range of interpretations continue to exist regarding the appropriate authorities to be used in cyber response and recovery situations. Additionally, the current Defense Support of Civil Authorities (DSCA)/Defense Support to Cyber Incident Response (DSCIR) process is geared toward significant or catastrophic scenarios, leaving many commentators to believe that incidents such as the ransomware attacks described above may fall below the threshold of the DoD's priorities.[26]

Greater clarity would certainly help states plan for and prepare for the provisioning of support from the National Guard. The most recent National Defense Authorization Act contains a provision to establish a pilot program to assess the feasibility of provisioning remote cybersecurity technical assistance to states from National Guard units of other states.[27] Such assistance could also include response to cyber incidents. While the pilot program is only slated to last 24 months, this should be ample time to capture valuable lessons about the provisioning of high demand but limited National Guard talent across state lines. Ideally, part of this effort would include simplifying the process for requesting support and clarifying authorities for employing the National Guard short of a major cyber incident.

Due to these complexities and the need for additional flexibility, some states have created alternative cyber response forces. State defense forces (SDF) organized under the control of the governor or the TAG can aid with missions and incident response when use of the National Guard forces might not be available. Additionally, there are a number of creative, voluntary frameworks that have emerged since the creation of the National Emergency Technology Guard (NET Guard) through the Homeland Security Act of 2002.[28] While the NET Guard was never fully established and realized, the concept of voluntary cyber response forces has evolved in a number of ways.[29] Today, such voluntary frameworks now include the Michigan Cyber Civilian Corp (2013), an organization comprised of civilian volunteers with cyber expertise who can volunteer at the invitation of an affected organization to provide, "rapid response assistance to a municipal, educational, nonprofit, or business organization in need of expert assistance during a cybersecurity incident."[30] One noteworthy aspect is how the state legislation, Michigan's Cyber Civilian Corps Act, effectively reduced barriers for volunteers to aid the state's cybersecurity efforts by implementing basic requirements, such as criminal background checks, while allowing local departments to recruit the necessary talent to respond quickly during a cyber incident.[31] Similar programs include Wisconsin's Cyber Disruption Teams and Ohio's Cyber Reserve.[32]

Taken in total, many states now have a means to coordinate direct support in a cyber crisis from a variety of state and National Guard organizations all under the purview of the TAG. The organic growth of coordinated state level cyber response focused organizations is a positive development. However, to be fully successful, municipalities need to understand the type of support available and how to request

25. Ibid.

26. Ibid.

27. H.R. 6396, National Defense Authorization Act for Fiscal Year 2021, 116th Congress. https://www.govtrack.us/congress/bills/116/hr6395/text.

28. Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?", War on the Rocks, Jan. 9, 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states.

29. Gerry Smith, "The Nerd Reserves: Sandy Recovery Renews Call For Tech National Guard," *The Huffington Post*, Nov. 21, 2012. https://www.huffpost.com/entry/tech-national-guard_n_2168374.

30. "Michigan Cyber Civilian Corps," Michigan.gov, 2020. https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html.

31. Act 132, Cyber Civilian Corps Act, Michigan Legislature, Jan. 24, 2018. http://www.legislature.mi.gov/(S(aexktz02js5cm0xw0b33ginn))/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.

32. Homeland Security Council, "Wisconsin Cyber Disruption Response Strategy," State of Wisconsin, October 2015. https://det.wi.gov/Documents/Cyber%20Disruption%20Response%20Strategy%20Plan%20Revised%2010_16.pdf; The Ohio Senate "Governor DeWine Signs Gavarone Bill to Better Protect Ohioans from Cyber Attacks," Press Release, Oct. 25, 2019. https://www.ohiosenate.gov/senators/gavarone/news/governor-dewine-signs-gavarone-bill-to-better-protect-ohioans-from-cyber-attacks.

that support in a crisis. To assist in this effort, simplifying organizational constructs and having single points of entry when requesting support can be hugely beneficial in a crisis when time is of the essence.

Mobilization of Human Capital and Leveraging the Private Sector

Like nearly all organizations, state and municipal cyber response forces and those who might support them are challenged by lack of experienced, skilled cyber personnel. To be effective, any unit—whether National Guard or a state defense force—needs to have trained cyber professionals available on demand. Under ideal circumstances, a state defense force can recruit, train and mobilize local technical talent to provide a pool of technically competent cyber professionals ready in a crisis. Key considerations include appropriate vetting of personnel in advance of a crisis and, when possible, previous exposure to the organizations and IT infrastructure they might be called to support in a crisis. These pre-crisis touchpoints allow IT professionals on both sides to understand how crisis response activities would be structured (who's in charge), the role of individuals augmenting the response (task management) and to the extent possible the networks and data that they will need to defend and recover.

States and localities are also leveraging the private sector in three distinct areas: the provisioning of cyber-threat information, managed security service providers (MSSPs) to manage organizational networks and monitor them for attacks and private cyber response teams on retainer to assist in response and recovery actions. The growing use of MSSPs makes sense particularly for smaller jurisdictions that cannot afford a comprehensive IT department. In many cases, MSSPs are also responsible for managing response and recovery activity as well as monitoring cyber threat information for the organization, in effect providing a one-stop service for stretched IT departments.

However, MSSPs are not a panacea. These security providers may lack critical context related to the key information assets and network terrain and the necessary resources to create customized defenses for each client. Heavy reliance on MSSPs can also result in risk as they a make an enticing target when they support multiple cities or jurisdictions.[33] Recently, FireEye—a major cybersecurity provider of both monitoring and response services—was breached and had Red Team assessment tools stolen although customer data appears to have been unaffected.[34] FireEye's public disclosure is laudable and is in line with one of the recommendations on responsible disclosure discussed later in this report. It is not surprising that attackers focus on MSSPs and security vendors since success can mean access to multiple customers. Similarly, in the event of a major cyber event or series of events impacting a wide range of governmental and/or private organizations, private cyber response firms might be stretched too thin to provide the needed capabilities to many clients simultaneously.

Another approach to mitigate the tech and cybersecurity skills gap at the state and local level is to leverage cloud services. When implemented securely, these services can provide strong cybersecurity and data management functionality, and they can increase resiliency against many types of cyber risks. Like MSSPs such centralization is not without risk. In the case of cloud providers, they may open new avenues of attack if a major provider is broadly breached or disrupted, but the benefits often outweigh the costs particularly for smaller organizations that have less expertise in data management.

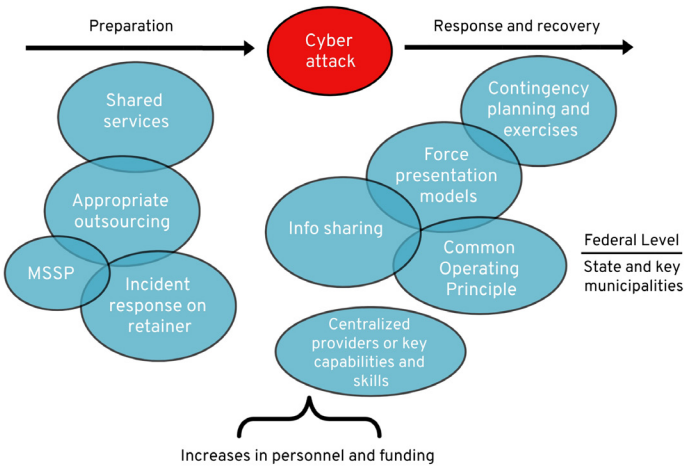
FINDINGS AND RECOMMENDATIONS

It is not possible for states and municipalities to eliminate all risk from cyber attacks. However, there are a number of steps organizations can take prior to an event to better prepare and recover more quickly. Once a state or municipality is attacked, the focus naturally turns to incident response and recovery. State governments and municipalities all have firsthand experience with emergencies—either natural disasters or human-induced ones—and cyber incident response often leverages existing emergency response procedures and coordinates activities through state emergency operations centers. In some instances, the response may include the activations of state or National Guard resources to assist in recovery efforts. Applying similar emergency management procedures in a cyber emergency makes sense. However, respondents having robust, generalized incident response procedures is not enough. To be truly effective, a great deal of effort is required before an attack, which is termed left of the cyber boom. After an attack, or right of the cyber boom, improving cyber-specific response capabilities informed by lessons learned prepares organizations for future incidents. The findings and recommendations detailed below represent some of the ways states and municipalities can strengthen their collective cyber defenses in light of the increasing cyber threats they face. While it may not be realistic for states and municipalities to eliminate all risk from cyber attacks, the diagram below reveals a number of steps organizations can take prior to an event to better prepare and recover more quickly.

33. Bobby Allyn, "22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault," NPR, Aug. 20, 2019. https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault.

34. Kevin Mandia, "FireEye Stories: FireEye Shares Details of Recent Cyber Attacks, Actions to Protect Community," FireEye, Dec. 8, 2020. https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

FIGURE I: CAPABILITIES TO PREPARE AND RESPOND



TARGETED INCREASES IN PERSONNEL AND FUNDING

"Two percent of two percent" is the rough rule of thumb that some state chief information security officers (CISOs) use to describe the amount of state IT budgets dedicated to cybersecurity. It is a truth nearly universally acknowledged that states and municipalities need more cyber defense and response resources in the form of people and dollars. A recent study largely confirms the 2 percent rule finding that states on average allocate between 1 and 3 percent of their total IT budget on cybersecurity.[35] A biennial survey of state CISOs has listed inadequate funding as the number one cybersecurity challenge in the last six surveys and inadequate staffing was number two in 2020. Faced with these challenges, these same organizations have been remarkably innovative and far more resilient than some commentators would suggest, but with rising threats from cyber attacks this level of investment is clearly insufficient. However, open-ended pleas for "more resources" without a clear explanation as to how the investments will improve security will find a cold reception in today's fiscally constrained environment. Instead, organizations must focus any new resources on investments with the greatest likelihood of return.

The question of where to spend the next cyber dollar is not unique to governments as corporate leaders wrestle with the exact same question. Recognizing inherent constraints, organizations should consider the following:

Outsource Appropriate Cyber Defense and Response Services

Expecting a resource-constrained municipality to have the same level of cyber protection as large, well-funded federal governments or global corporate organizations is unrealistic. Instead, leaders need to accept that in the absence of additional resources, state and local government organizations may need to outsource some critical services such as cloud with enhanced cybersecurity practices including identity and access management and data backup. Similarly, managed security service providers (MSSPs) can apply scare cyber expertise in conducting monitoring and incident identification across a broader set of organizations and attack surfaces. The proviso, of course, is that cloud providers and MSSPs themselves must be highly secure as they have already become natural targets of attack. Assisting states and municipalities in the complex decision-making required for such outsourcing choices will enhance the effectiveness of such an approach.

Establish Shared Cybersecurity Services at the State or Regional Level

Some states have started to provide shared services related to security or key IT services such as cloud computing. Centralizing services makes both fiscal and security sense. By pooling resources, states and localities should be able to negotiate reduced rate and fee structures compared to each organization contracting separately. Providing these services through a state or regional contract may also provide localities with security services they couldn't afford independently. This approach could also work in large municipalities where large organizations involved in public safety, education and mass transit all have to secure digital services. By pooling requirements, shared resources can provide either access to a service or expertise that a municipality could not afford otherwise. Leveraging scale can result in lower costs for the services than individual organizations could negotiate. The degree to which states and municipalities balance outsourcing versus shared services will be context dependent.

IMPROVE AVAILABILITY AND CAPACITY TO UTILIZE CYBER RESPONSE RESOURCES

Enable Varied Approaches for Cyber Response

State governments continue to experiment and develop novel organizational constructs. Many are building a bench of cyber expertise to assist the state or municipal agencies during a cyber emergency. These approaches range from leveraging the state's cyber National Guard units, state cyber militia capabilities or other volunteer forces. It has been said many times in similar ways that: "If you've seen one state's

35. Srini Subramanian and Meredith Ward, "2020 Deloitte-NASCIO Cybersecurity Study," Deloitte and The National Association of State Chief Information Officers (NASCIO), 2020, p. 17. https://www.nascio.org/wp-content/uploads/2020/10/2020-Deloitte-NASCIO-Cybersecurity-Study-1.pdf.

approach, you've seen one approach."[36] Each of these capabilities has various strengths and challenges; however, the number and diversity of approaches provides a long-term strength. Rather than try and suggest that there is a single approach applicable across all 50 states and the even more varied thousands of municipalities, the following recommendations may enable states and municipalities to build necessary cyber response capabilities as more of a menu of options for implementation.

Augment Personnel and Skills Gaps

Personnel and the requisite expertise for effective cyber response are limited. While there are diverse approaches to organizing these resources within states and municipalities, nearly all of the associated state-level and federal cyber response forces are small, often under 50 people.[37] This size may be sufficient for small-scale attacks directed against a limited number of municipalities within a state or across the United States. However, for large-scale attacks hitting multiple states or jurisdictions, more on-call support will be needed. Moreover, with limited numbers an open question is whether the needed expertise will be available to cover the diversity of potential attack scenarios. Many states have approached the shortage of personnel by creating more generic positions that can support a variety of response and recovery roles. This "jack of all trades" approach can result in even smaller numbers of qualified personnel for specific roles that may be required. For example, cyber threat intelligence specialists may not have the skills to monitor networks. Similarly, cyber forensic analysts may not have the training to restore networks or rebuild systems. To aid in recovery, a strong mapping of specific skills needed to available resources for key response contingencies is necessary.

In a crisis, federal assistance may be limited depending upon the scale of the attack. While the interviewed state officials were universally appreciative of the support they do receive, they also noted crucial limitations. First, much of the support comes in the way of providing cyber threat information. While undoubtedly important, during the onset of an attack on-the-ground support in the areas of forensics and system/network restoration will be in greater demand. While states may welcome threat information through federal sources, they also leverage commercial and homegrown sources for cyber threat information. Moreover, the likelihood of receiving specific warnings of impeding attacks is low.

Understanding that advanced warning of an attack is unlikely places more importance on preparation and response actions. State and municipal responders will be more interested in understanding cyber attack impacts that may affect their ability to provide essential services. Second, while fly-away response teams are available at the federal level, such low-density, high-demand capabilities may have even more limited availability than the states.

Gaining access to such teams requires reaching a threshold for activation. A routine ransomware attack, while impactful for the locality, probably will not justify a fly-away federal response. Furthermore, if an attack is hitting multiple locations the likelihood of receiving outside assistance is reduced further. Finally, federal agencies that do respond may have specific responsibilities related to a criminal or national security investigation, particularly in multi-jurisdictional or multi-state events. For these reasons, it is not surprising that states are developing their own response forces that they can better control and direct. However, municipal responders need to understand the types of forces available during a significant cyber event.

Establish Force Presentation Models

In a crisis, it is often too late for an organization to incorporate ad hoc, outside personnel support. Instead, these organizations need to understand pre-crisis what specific types of expertise will be available. That expertise could include assistance with remediation to get networks and systems back up and running, forensic capabilities to understand the severity of the attack, or the more mundane tasks of just reimaging and restoring servers and systems.

Supported organizations often struggle with how to best manage and integrate outside support when it arrives. While knowing that a response augmentation team is available, a smooth integration of the responding team's expertise is not a given. For example, if an augmentation team arrives without pre-coordination, the local cybersecurity response team may already be overwhelmed conducting response and remediation activities. On more than one occasion, research respondents discussed how localities—when responding to a cyber event—had neither the time nor the available personnel to effectively receive and integrate newly arrived response teams. If response forces from the states or National Guard can signal before the onset of a crisis the specific types of expertise and numbers of personnel available, supported organizations can better prepare to integrate the arriving influx of talent. Higher levels of effectiveness could be achieved when response forces have pre-designated roles that have been planned with the receiving organization and people. Ultimately, the responsibility for providing this information rests with the states since they are the ones who are organizing the various response forces. Ideally, they can communicate the types of expertise available through CISO channels. Better yet, particularly for larger municipalities, is

36. Michael Daniel, "Interview by John Bansemer and Greg Rattray: R Street State and Local Findings and Recommendations," R Street Institute, Sept. 1, 2020.

37. Monica Ruiz, "The Hybrid Benefits of the National Guard," *Lawfare*, July 23, 2019. https://www.lawfareblog.com/hybrid-benefits-national-guard

to have augmentation teams exercise with or at least perform site visits to large cities in the state. Such activity provides the city an opportunity to preview the type of support available and gives augmenting forces the chance to see the types of networks and city services that they may have to support or protect in a crisis.

ESTABLISH A FULLY INTEGRATED CYBER RESPONSE CAPABILITY

The current ad-hoc state and local cyber response approach could be significantly enhanced by establishing a national-to-state-to-local cyber response framework that forms the basis for ensuring command and control, crisis situational awareness and exercise programs. The approaches detailed below are recommended to help state and local municipalities develop such a framework.

Continue to Focus on Improving Information Sharing

Information sharing is vital as a means to improve readiness, preparation, response and remediation. Understanding the evolving nature of threats, which adversaries are active, what attacks are on-going and what defensive measures are required are all essential elements of effective cyber defense. As this subject remains a focal point of many efforts, this study did not focus on the topic, leaving the ground to others. However, the successful, continuing effort of the DHS, the FBI (particularly the aforementioned InfraGard program), the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Cyber-Forensics and Training Alliance (NCFTA) are worthy of note in regard to empowering efforts that assist state and municipal cyber defenders.[38]

Identify and Contract a Ready Response Team

One point made repeatedly was that jurisdictions, regardless of size, should consider having cyber response capabilities on retainer to assist the city or state's cybersecurity team during a crisis. By doing so, organizations know in advance the types of services they can expect to receive and work to fill in any perceived gaps. During a crisis, municipalities and states are likely to find it difficult and expensive to negotiate reasonable rates and get assistance on the ground in a timely manner. As touched on before, centralizing the contracting and acquisition of ready response teams at the state level is more likely to allow smaller jurisdictions immediate and cheaper access during a crisis.

Establish a Clear Command and Control Structure

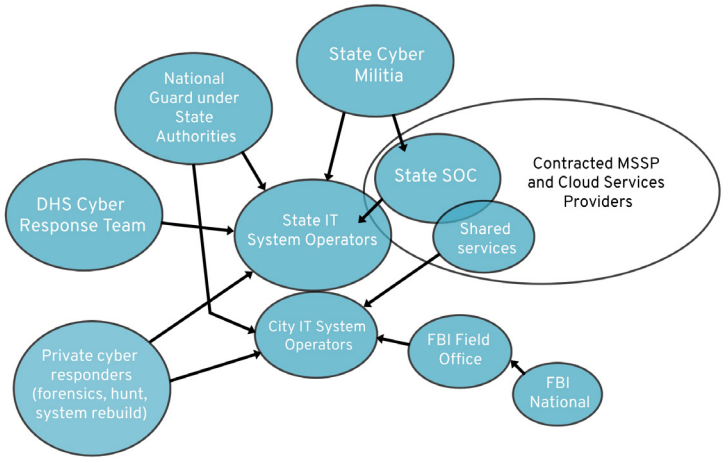
The military concept of support relationships used in planning and conducting operations applies to cyber response activities as well. Establishing these relationships can assist organizations in delineating distinct responsibilities and authorities. In essence, supporting units provide assistance to the organization that has the lead for the overall operation or effort. The lead or supported organization designates how and when supporting organizations are used, designating their tasks and responsibilities.

An old adage states that when everyone's in charge no one is. A number of considerations including whether multiple jurisdictions are under attack, the nexus of the attacks to nation-state or cyber criminals, and the abilities of the organization to respond will all affect the command relationships in a crisis. Identifying who is in charge of an operation and the specific missions under that operation are essential. Assigning roles and responsibilities during a crisis can lead to confusion among individuals and the organizations involved. Besides having pre-defined rules for selecting the on-scene commander, identifying liaisons with state and federal responders can help in the integration and collaboration with these resources should they be activated. Another consideration is whether there are thresholds in terms of the severity of the crisis or the number of organizations affected that would change who would lead the response and recovery.

The good news is that these types of relationships can be ironed out well in advance of a crisis. Who will be the "on-scene" commander, what direction can the supported organization provide cyber response forces and how will the forces be integrated into the supported organizations recovery efforts are all questions that organizations should consider before a major cyber event. State and municipal cyber response teams should seek to clearly identify and exercise scenario-specific command relationships and how they might evolve as part of contingency plans and procedures. Diagrams—like Figure 2 below—that clearly identify scenario-specific command relationships can aid more effective cyber responses.

38. "One Team, One Goal," The National Cyber-Forensics and Training Alliance, last accessed Feb. 25, 2021. https://www.ncfta.net; "InfraGard: Partnership for Protection," InfraGard, last accessed Feb. 25, 2021. https://www.infragard.org.

FIGURE 2: NOTIONAL TYPES OF CYBER RESPONSES



Establish a Common Operational Picture

In the event of a severe cyber incident, understanding the adversary and their tactics, the attack's impact and the likely effects of potential future attacks is essential. Mayors will want to know when outages that have disabled their citizen's ability to access critical services might be resolved. Cyber responders will need to know if adversaries are seeking to corrupt information or if systems that have been brought down by ransomware have adequate backups for restoration. Governors will want to know if ransomware plaguing hospitals will spread as emergency rooms are shut down. National leaders will want to know if the stock market will have to close due to firms lacking the proper information to trade. Stakeholders and decision-makers want relevant, accurate and timely information to enable a coordinated response, preferably in advance of an attack. Put another way, they want relevant and actionable situational awareness.

Today, cyber threat information is often abundant but neither applicable to every organization nor focused on the adversary's next move during an attack. Moreover, sifting through threat information for relevance and making forward-looking estimates requires analytic tools, approaches and skills that are likely beyond the ability of smaller, more resource-challenged organizations. One possible solution is to maintain a national common operational picture (COP) at the federal level that states and key municipalities can access for shared situational awareness. The DHS would be the natural home for such a system. States and municipalities would be able to establish capabilities to plug into and leverage such a COP during a cyber crisis with trained personnel. Additionally, a COP could provide worldwide threat information, status of response resources, attack impact and projected courses of action in the event of a contingency. Ideally, a national COP would also be fed information from states and key municipalities since they are often best positioned to know what is happening on their networks at any moment in time. Whether states would be willing to share this information in support of a national COP is unknown and would require further investigation. Furthermore, authorities would have to address privacy and civil liberty concerns. Fostering transparency on the nature and type of data collected and shared will be essential.

Conduct Stand-alone and Integrated Cyber Exercises

Interview and workshop participants noted the utility of and the need to scale up exercises and table-top events. Many such events are already occurring, such as CyberShield which provides a virtual environment for National Guard cyber units from multiple states to participate in highly realistic training exercises.[39] However, after examining the exercise experiences of state and local cyber professionals, there is a need for both integrated state-led public safety exercises and cyber-specific standalone events.

Integrated public safety exercises are beneficial because they often have all of the requisite emergency and disaster response players at the table. By leavening these exercises with cyber injects, decision makers can gain broader exposure to potential cyber threats and their resultant impacts. However, a criticism of these approaches is that the cyber scenarios inserted into such exercises are often an afterthought, bolted on to a larger disaster scenario. The end result is that cyber discussions can be cursory without enough discussion of the challenges states and municipalities would face or considerations of effective responses. Even further, documenting lessons learned and assigning responsibilities for follow-up actions is inconsistent or fails to occur. At its most basic level, discussions surrounding a potential response to a cyber event could stop at a hypothetical activation of one or more state response capabilities. Such a notional activation risks assuming resolution of the situation without a full exploration of what that would entail, the limitations of available forces and other potential complications. Ideally, these events need to move beyond the somewhat superficial stage of activation to a more detailed discussion of command and control of forces; authorities and responsibilities; known weaknesses; and the relevant expertise available to respond to a specific cyber attack.

Acquiring deeper insight on gaps and needed capabilities may require dedicated cyber-related exercises or tabletop events at both state and municipal levels. These events would allow the daily practitioners and the cyber response teams to have the more in-depth discussions necessary to explore the

39. Staff Sgt. George Davis, "Cyber Shield 2020 features fully virtual training exercise during COVID-19, pandemic," Ohio National Guard, Sept. 23, 2020. https://www.ong.ohio.gov/stories/2020/sep/20200923-cybershield.html.

implications of major cyber-related events. For these standalone events to have value, they do not necessarily need to involve senior decision-makers. Exercise organizers should draft after action summaries of these events with necessary recommendations around authorities, expertise and resource requirements to ensure senior leaders are aware of their findings. Ideally, these findings would also serve as the injects to larger all-hazard exercises. This approach helps address the challenges of perfunctory exposure in a statewide disaster response exercise. Having already examined a specific scenario in-depth, the lead cyber representatives in an integrated exercise can summarize their findings and expose the full cadre of state exercise participants to the findings. Ultimately, for these exercises to be beneficial, it is critical that leadership provide the necessary time and resources during their execution.

Continue to Leverage Red and Blue Teaming

Moving beyond exercises based on notional scenarios, the use of network assessors (red and blue teaming) offers those responsible for ensuring security and resiliency deeper understanding of their current security posture and can be an important part of shoring up defenses. These capabilities have limitations in that they offer a snapshot at a given point in time; therefore, organizations need to establish on-going programs to provide lasting value. Further benefits can occur when potential cyber response forces conduct the red teaming. A red team, constituted in this way, can provide municipal IT teams with experience responding to realistic attack scenarios while the red team members gain an understanding of the services and networks they may be called upon to defend in a crisis. Just as it can be difficult for an organization to integrate outside assistance in an emergency, responders can struggle to learn the networks, systems and applications during a crisis if they have not been previously exposed to the systems. As state response teams conduct pre-crisis exercises or red teaming events, they gain a better understanding of the networks and systems of municipalities they may be asked to defend. These activities allow a crossflow of ideas, rehearsals of possible crisis situations and pre-coordination of responsibilities during a crisis. For its part, the supported municipality better understands the skills and expertise available from outside response organizations. Finally, the assessments can help future response forces understand the current security posture of organizations, and they can provide recommendations to better secure the assessed organization.

Rigorously Document Response Actions

Comprehensive investigation and follow through of after-action reports generated following a major cyber event often prove extremely challenging. Organizations may fear detailing the findings because of criticism if the reports become part of the public record. Depending upon the findings, such reports could be exploited for political advantage by suggesting poor security practices or mismanaged responses. We believe a different perspective should prevail. Most significant cyber events are eventually disclosed and reported in some fashion—either by the governmental authorities or the media soon after they occur. Moreover, most attacks are less the result of negligence and far more often the result of mistakes, lack of properly resourced defenses or skilled attackers, often a combination of all three. As recent cyber attacks affecting the federal government have shown, it is essential to recognize that a perfect cyber defense is not possible, victims should not be blamed and retrospective analysis is crucial for all to learn valuable lessons to improve operations going forward.

For the entity that suffered the attack, introspection allows for discernment and can answer a number of questions: Where should the next security dollar be placed? What data or security services should be outsourced? What expertise was missing before, during and after the crisis? How easy or hard was it to receive outside cyber expertise and was their integration easy or did this create new challenges? Moreover, bad news normally does not get better with age and shared after action reports (AARs) can assist other state and municipal peers who are also striving to defend networks. As part of a responsible disclosure process, these reports can describe how the attacks occurred, who provided responses (and their effectiveness), and broad lessons learned or observations.

If the sharing of AARs becomes more commonplace, there is a greater chance that other municipalities and states will follow suit. Adding additional reports from multiple entities enables broader sharing of information and helps remove concerns around specific findings in a single report. Moreover, the collective sharing of information helps all organizations under threat to better understand the tactics and techniques threat actors are applying against similar organizations.

ESTABLISH A PLANNING FRAMEWORK FOR RESPONSE

State and local cyber response capabilities will likely be overwhelmed by the severe, but plausible, cyber attacks that may confront them going forward, especially if attackers hit multiple jurisdictions with near-simultaneous outbreaks and broad impacts. The ransomware wave that came in 2019 and continues to this day has stressed response capabilities for localities, but they may face even more challenging threats in the future as supply chain and other attacks multiply. The scenarios examined and workshops conducted by the NYCTF made the challenges even clearer. If attackers use sophisticated techniques or tactics causing mass effects, state and local capabilities will be overwhelmed. As a sys-

tem, our national efforts to empower state and local response are characterized by severely insufficient and centralized resources, lack a clear understanding of which capabilities and skills are needed for which contingencies, and difficulty in assimilating outside assistance such as state or National Guard response forces.

To assist in meeting these challenges, a cyber response planning framework for a state or municipality would identify major contingencies of concern, the key tasks and processes necessary for effective response, and would map the necessary levels of capabilities such as personnel, skills, tools and technology. The key players orchestrating cyber response to major incidents are likely the CISO and TAGs at the state level. At the municipal level, a designated cyber response lead should also be designated in advance of any event. These leaders should identify the minimum desired levels of cyber response capabilities that are necessary across various levels of severity. These requirements can set objectives for a wide range of preparatory activities and, more importantly, guide investment strategies for centralized cyber response resources at the state and national levels across a range of contingencies.

Ideally, state planning frameworks would nest under a national planning framework that is developed and agreed to across federal, state, municipal players and the private sector. Planners could use the national framework to analyze the sufficiency of resources and illuminate gaps that must be addressed for national-level contingencies. The key stakeholders in this framework should be the cyber response leaders at the national, state and local level: the DHS, the FBI and the DOD; governors and TAGs; and mayors and emergency response leaders. Crucially, the providers and orchestrators of centralized capabilities including the National Guard, the MS-ISAC, the Cyber Threat Alliance and other major response companies must help develop the framework.

Establishing a capability requirements baseline involves the clear identification of potential attack profiles and associated severity levels. A starting point might be the types of scenarios and cyber risk drivers developed during the work of the NYCTF. Building a baseline of key contingency planning scenarios is crucial to enable serious, scalable progress focused on the most important risks. Potential scenarios include disruptive attacks on essential municipal services, major data breaches or targeted efforts to harm trust in public safety organizations.

One of the most essential challenges is determining the number of scenarios and their severity as this will drive planning efforts and long-term requirements. At the state and municipal level, the development of planning contingencies should be driven by the nature of key industries, the assets exposed to cyber attacks and risks to the people, economy and social functioning of the jurisdiction. At the national level, deciding on key attack scenarios and their scale will be challenging but it is a critical step in realistically planning in advance of a crisis. The mapping of realistic threat scenarios to required response forces and cyber threat intelligence requirements is critical for adequate preparation.

If the nation could establish such a contingency planning structure, it could guide the implementation of the recommendations made above to effectively centralize key cyber resources, determine the size and skill sets necessary across organizations, develop shared situational awareness capabilities and train and exercise cyber response plans and organizations. States will undoubtedly want a vote in the structure and nature of potential support and thus will be looking for augmentation rather than ceding control during major events. While challenging, establishing a national cyber response identification and planning process that explicitly guides capabilities development and investment would provide a systematic way to enable and reinforce organic growth of capabilities at the state and local level, create awareness of shortfalls and allow investment to effectively manage risk at all levels.

CONCLUSION

Throughout this study both deep challenges and opportunities were apparent. The organic growth of cyber response approaches and capabilities at the state and municipal level has been significant and leverages a complex set of organizations to maximize available resources. While no one structure is necessarily superior to another, key benefits arise from pre-crisis planning and establishing roles and responsibilities and command relationships across response organizations. Likewise, building capabilities that are best suited for individual states rather than a top-down imposition of a national structures enables approaches tailored for the unique situation of each locale.

However, most state and local cyber responders remain significantly under-equipped to handle cyber attacks, and the cyber threat shows no signs of abating. Of course, there is a need for efficiency in cyber investment coupled with the fiscal constraints that have been exacerbated by COVID-19 responses. Yet, building digital resilience will prove an essential element of our society's ability to recover and move forward. Strengthening state and municipal cyber responses is an opportunity for smart investment now to avoid estimable risk and even catastrophes in the future.

ABOUT THE AUTHORS

John Bansemer is a non-resident senior fellow with the R Street Institute. Bansemer served in the U.S. Air Force for over 30 years before retiring as a Lieutenant General.

Greg Rattray, a non-resident senior fellow with the R Street Institutes, brings extensive cyber experience from the DoD and corporate cybersecurity. He served as the cyber lead on the NSC staff and was responsible for drafting some of the foundational cyber policy directives. He has led large cyber units within the Air Force, including having operational control of four National Guard cyber units. After leaving the Air Force, he served as the Chief Information Security Officer at JP Morgan Chase and stood up the Financial Systemic Analysis and Resiliency Center among other high-profile roles in the non-profit and private sector. He currently is the Executive Director of the NY Cyber Task Force focused on outlining challenges and making recommendations to improve our nation's cyber defenses.

Franklin Lee is a research assistant with the R Street Institute where he has helped produce a variety of op-eds, journal articles and videos for R Street related to civil society and educational topics. Previously, he worked as a paralegal for a social agency in New York City—mainly providing support to immigration cases. He is a published author and his second book, *From Harvard to Homeless* is due to be published in August 2021.