Continuous Measured Improvement: A New Approach to Meeting the Municipal Cybersecurity Challenge

by

Avital Baral

B.S. in Computer Science and Engineering and in Planning,
Massachusetts Institute of Technology (2020)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
February 2022

Author . . . . . .
Department of Electrical Engineering and Computer Science
January 14, 2022

Certified by . . . . . .
Lawrence E. Susskind
Ford Professor of Urban and Environmental Planning
MIT Department of Urban Studies and Planning
Thesis Supervisor

Certified by . . . . . .
Daniel J. Weitzner
3Com Founders Principal Research Scientist
MIT Computer Science and Artificial Intelligence Laboratory
Thesis Supervisor

Accepted by . . . . . .
Katrina LaCurts
Chair, Master of Engineering Thesis Committee

Continuous Measured Improvement: A New Approach to Meeting the Municipal Cybersecurity Challenge

by

Avital Baral

Submitted to the Department of Electrical Engineering and Computer Science
on January 14, 2022, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

This thesis examines the cybersecurity challenges facing municipal governments and proposes a new policy approach. Through a review of existing public-sector cybersecurity concerns and an interview-based case study of Massachusetts municipalities in partnership with the Massachusetts Cybersecurity Center, this thesis identifies the main problem as a lack of a proper incentive structure for municipalities to prioritize cybersecurity improvements. I propose a new approach to state / local government efforts to improve cybersecurity. I establish the goal of continuous, measured improvement in cybersecurity posture for municipalities, and propose a state-sponsored, eligibility-restricted insurance mechanism for municipalities to systematically lower their cyber risk to meet that goal. In exchange for commitments to implementing regularly-updated cybersecurity best practices, municipalities would receive high-quality, affordable insurance against catastrophic cyber-related losses, and a commitment from the state to aggregate loss and resource-use data to provide best-in-class cybersecurity infrastructure help. I lay out a roadmap for the implementation of such a Massachusetts Cyber Disaster Insurance Program (MCDIP) along with proposals for data-driven refinement of state cybersecurity resource offerings through the use of the new MIT SCRAM platform. This public-sector cybersecurity goal and implementation strategy has implications far beyond Massachusetts and the potential to change the course of cybersecurity policymaking.

Thesis Supervisor: Lawrence E. Susskind
Title: Ford Professor of Urban and Environmental Planning
MIT Department of Urban Studies and Planning

Thesis Supervisor: Daniel J. Weitzner
Title: 3Com Founders Principal Research Scientist
MIT Computer Science and Artificial Intelligence Laboratory

Acknowledgments

I would like to thank Prof. Lawrence Susskind in the MIT Department of Urban Studies and Planning (DUSP) for advising this thesis work and for providing me with extremely valuable feedback and guidance throughout the course of my degree.

I would also like to thank Daniel Weitzner, Director of the Internet Policy Research Initiative (IPRI) in the Computer Science and Artificial Intelligence Lab (CSAIL) for co-advising this thesis and serving as a mentor to me as I navigate the intersection of technology and public policy.

I would like to acknowledge the valuable help of Aaron Robles (MIT Class of 2021), undergraduate researcher in the Science Impact Collaborative, who helped in the data collection process for this work. I would like to thank my colleagues Jungwoo Chun, Rebecca Spiewak, and David Hong for their help with honing my thinking throughout the research process. I would also like to acknowledge Dr. Taylor Reynolds, Technology Policy Director at IPRI, for his valuable input on drafts of this thesis.

I would like to thank the municipal IT professionals throughout Massachusetts who agreed to participate in the interview-based study described in this thesis and shared their insights with me. I would like to thank the staff at the Massachusetts Cybersecurity Center, including Stephanie Helm, Meg Speranza, and Raine Brown for their help throughout our collaboration on this project. I would also like to acknowledge the help of the Municipal Cybersecurity Sub-working Group within the Massachusetts Cybersecurity Center.

On a more personal note, I would like to thank Dr. Katrina LaCurts in the MIT EECS Undergraduate Office for her mentorship in my role as Graduate Teaching Assistant in 6.033, and for her instrumental advice throughout my five years at MIT. I would also like to thank Prof. Rob Miller, my undergraduate and graduate academic advisor in EECS, and Prof. Lawrence Vale, my undergraduate academic advisor in DUSP.

I am extremely appreciative of the communities I found at pika, East Campus, and the MIT Sport Taekwondo Club for their support throughout my time at MIT and during the unprecedented Covid-19 pandemic disruption.

I would like to thank the friends and trail maintenance volunteers I encountered on the Pacific Crest Trail while hiking through my home state of Washington this August 2021. The beauty and peace I experienced out on the trail allowed me to find the energy to complete my degree.

Thank you to my friends and family - Alex M., Andrea F., Andrea M., Avidan B., Avinoam B., Avishai B., Emily C., Hudson C., Jack R., Jessie G., Jocelyn T., Joe S., Kai K., Kevin L., Mayukha V., Micheline B., Milka P., Nisha D., Rebecca R., Rian F., Sarah P., Simon S., Yiran H., and numerous others who have been there for me in these wonderful, turbulent, exhilarating years. As cliché as it may sound, you have in countless ways made me who I am today.

Contents

Chapter 1

Introduction

In recent years, organizations of all types have been facing the evolving threat of cyber-attack. Cyberattacks and ransomware-based attacks specifically are of particular concern to local governments, because municipalities face unique resource constraints while providing essential services to constituents. This thesis chronicles a collaboration between the Massachusetts Cybersecurity Center and the author to carry out a deep dive into the problem of improving cyber resilience in municipalities, with a focus on the state of Massachusetts. This thesis first provides background on cybersecurity in the public sector and reviews existing research, then describes an interview-based survey of a set of Massachusetts municipalities regarding the municipal cybersecurity challenges they face. This thesis integrates information from the interview study and existing scholarship into a proposal for a novel approach to municipal cybersecurity policy, outlining the goal of Continuous Measured Improvement and a policy proposal for achieving that goal. This work provides specific recommendations for Massachusetts but has broad applicability to cybersecurity policy in other states.

1.1 Background: Cybersecurity in the Public Sector

Ransomware-based attacks on municipalities have multiplied within the last 10 years [33]. Freed cataloged over 245 attacks since 2013, which, given underreporting bias, is in all likelihood lower than the actual number of attacks that occurred.

Recent high-profile attacks include ransomware-based attacks on Baltimore's [26, 65] and Atlanta's [33, 68] municipal systems. The attacks cost the cities $18 million and $17 million in recovery costs respectively, and were immensely disruptive to city services operations. The WannaCry ransomware worm is estimated to have caused $4 billion in damages [12]. NotPetya, a destructive malware which technically fails to meet the definition of ransomware but emulates ransomware characteristics, is estimated to have created $10 billion in damages [38, 67]. Attacks on critical infrastructure and services abounded in 2021, including attacks on hospital systems [35, 67], the Colonial Pipeline [46], and global meat producer JBS [36, 67].

The federal response on critical infrastructure cybersecurity has picked up steam in 2020 and 2021 - partly as a response to the SolarWinds attack. The SolarWinds attacks showed a dangerous new supply-chain based attack vector which could enable malware, including ransomware, to be delivered through benign-appearing software updates, and prompted a national reprioritization of cybersecurity [67]. Key US government response milestones following SolarWinds include the CISA September 2020 Ransomware Guide [18], the US White House Executive Order on Improving the Nation's Cybersecurity (May 2021 - guidelines on cybersecurity best practices for federal agencies) (Exec. Order No. 14028, 2021) [1], and the US White House Memo (June 2021 - follow-up on guidance for US firms)[5]. Most recently, the Federal Trade Commission (FTC) issued an update to its Safeguard Rules, compelling financial institutions to develop comprehensive cybersecurity plans and practices to ensure the security of consumer data [19].

The groundswell of federal action on cybersecurity shows an increased recognition of the dangerous repercussions of cyberattacks, as well as an acknowledgement that current approaches to systematically lower the frequency and impacts of cyberattacks are insufficiently robust. There is an appetite for introducing centralized strategies and plans for lowering cyber risk, albeit for now limited to certain sectors where the federal government has direct authority (for example, federal contractors).

The following Research and Policy Survey compiles scholarship on the costs and impacts of cyberattacks on the public sector, reviews existing cybersecurity approaches at the state level and at the municipal level, and highlights emerging strategies for improving

local cybersecurity.

Chapter 2

Research and Policy Survey

The following Research and Policy Survey provides an overview of the current understanding of public sector cybersecurity attacks and costs, as well as an overview of policy approaches to this challenge. In itself, the relative sparsity of peer-reviewed literature on the topic points to a critical gap in scholarly research and the need for a more rigorous approach. Overall, reports from industry groups and existing academic research point to the mounting frequency and costs of cyberattacks on public sector entities, and to a lack of implementation of effective preventative measures. States across the U.S. are experimenting with several novel mechanisms for helping municipalities in facing cyber risk, but these experiments are so new that they have not yet been thoroughly evaluated for effectiveness. Policy proposals on the topic focus on the need to move beyond more traditional compliance based approaches to cybersecurity into risk assessment based approaches, but do not put forth any particular concrete or specific policy implementation details.

2.1 Cybersecurity and the public sector: estimated attack frequencies, vectors, and costs

Existing research suggests that organizations of all types, including the public sector, are under constant threat of cyberattack, often through technically uncomplicated tactics in-

cluding phishing and social engineering. While only a fraction of attacks are successful, the costs to recover post-attacks are high.

The 2019 IBM report *Cybersecurity for state and local governments: Protecting Public Infrastructure* [64] enumerated widespread and costly attacks on public services and infrastructure such as health services, emergency services, election administration, and user-interfacing services such as the DMV. The 2021 *Microsoft Digital Defense* report [66], while not specific to public sector organizations, supports the oft-repeated cybersecurity claim that most cyberattacks are carried out through technically unsophisticated means. Basic cybersecurity hygiene practices such as the use of multi-factor authentication protects against 98% of attacks, and sophisticated attacks such as those conducted by Advanced Persistent Threats (APTs) are much much rarer than basic attacks such as phishing and social engineering tactics more broadly. In a nationwide survey of municipalities, Norris et al. (2019) found that 27.7% of respondents reported being attacked at least hourly, and another 19.4% reported being attacked at least once a day.

The recovery costs for cities that fall victim to cyberattacks are notoriously hard to estimate because the municipalities and other public entities in question have incentive to work hard to keep the details away from the public and the press. Firm data regarding cyber risk and the efficacy of mitigation strategies are hard to come by, not systematically collected, and often unreliable [67]. Nonetheless, existing figures highlight the very high cost of ransomware attacks and provide a legitimate backing for the urgency of finding effective solutions. The Economic Impact of Cyber Attacks on Municipalities, a report by cybersecurity firm KnowBe4 [42], compiled examples of ransomware payment demands and recovery costs faced by municipalities and found evidence of demands for ransom in the magnitude tens of thousands of dollars and overall recovery costs for affected cities in the millions.

The 2018 White House Council of Economic Advisors report *The Cost of Malicious Cyber Activity to the U.S. Economy* [56] found an extremely broad range for the cost of cyberattacks directed at state and local governments, chronicling successful breaches with costs from $665,000 to $40.53 million, with a median cost varying from $60,000 to as high as $1.87 million [42, 56]. The average demand for ransom in ransomware contexts from

2013 to 2020 was $835,758.33 [33].

2.2 The State of Municipal Cybersecurity

A number of national surveys regarding cybersecurity in the public sector have been conducted, and together they paint a dire picture of state and municipalities' cybersecurity preparedness. Municipalities report themselves to be unprepared to effectively face the threat of cyberattack, chiefly citing lack of funding, lack of qualified staff, and lack of prioritization of information technology by their organizational leadership as barriers to an adequate cybersecurity posture [51], conducting a nationwide survey of municipalities, found that only a minority of responding municipal IT professionals considered their municipalities well-prepared to detect and recover from ransomware attacks and cyberattacks generally. Norris et al. (2019) [50] identified top barriers to cybersecurity readiness in municipalities as the inability to pay competitive salaries to IT professionals, lack of funding for cybersecurity, and lack of dedicated security staff. A consistent and concerning thread through the surveys is that a significant portion of respondents report that they do not know if or how often they are being attacked, and are unable to rate their own levels of preparedness, indicating in itself a lack of preparation and prioritization of cybersecurity [51, 63].

A biennial survey of state CIOs conducted jointly by Deloitte and the National Association of State CIOs (NASCIO) repeatedly affirms the findings above [24, 23]. The Deloitte-NASCIO reports highlight the need for greater cybersecurity funding at the state level and for a coherent, centralized policy strategy for local government. CISOs consulted in the 2018 and 2020 Deloitte-NASCIO surveys reported that they viewed state-level regulations backed by funding commitments as most effective in improving cybersecurity posture. Only a minority of states had a cybersecurity budget line item [24, 23].

A 2020 survey of the Coalition of City CISOs [53] in partnership with the International City/County Managers Association (ICMA) of chief security officers serving 14 large American cities echoed the findings of prior surveys, and found that attacker demands for ransoms had increased in 2020 [49]. The ICMA survey identified leadership

buy-in as another top barrier to improving cybersecurity posture in local governments.

2.3 State Level Policy Regarding Cybersecurity

The following section compiles the most noteworthy state-level actions and programs on cybersecurity, with a particular emphasis on state and local government interactions. This section also highlights noteworthy policy recommendations by qualified third parties on the challenge of municipal cybersecurity and state/local government interactions.

The 2020 *Stronger Together: State and Local Cybersecurity Collaboration* report [70], jointly published by NGA and the NASCIO, highlighted noteworthy state/local government collaboration initiatives on cybersecurity. Programs include:

- versions of skilled volunteer assistance to local governments: Illinois Cyber Navigator Program [32], Michigan Cyber Civilian Corps [45].
- state-provided cybersecurity awareness training available to municipalities.
- state-run cybersecurity tabletop exercises and scenarios. State-organized gathering and facilitated information exchange between cybersecurity stakeholders, including through participation in the Multi-State Information Sharing and Analysis Center (MS-ISAC) [30].
- states providing IT and cybersecurity services to municipalities, directly or through a contracting program.
- states providing dedicated incident response teams to municipalities, sometimes directly accessible through a phone hotline.

While these programs are for the most part still in their infancy and have limited to no data to show effectiveness, they can provide inspiration for similar programs that can be implemented elsewhere and more rigorously evaluated. Section 4.5 digs into these innovative state programs as well as existing cross-domain programs in Massachusetts to propose options for bolstering Massachusetts cybersecurity resources for municipalities. The implementation of new programs will need to be paired with the iterative evaluation

process described in Section 4.3 in order to gauge success over time and readjust according to data-driven insights.

Defining a data breach as a security breach resulting in the loss of personal data affecting individuals [62], McFarland et. al [44] reports that while some form of data breach reporting is mandatory in all 50 states, the specific requirements vary. In 14 states as well as DC, organizations are not required to notify government entities, only the affected individuals. 18 states require organizations above specific size thresholds to report breaches to the state government, while 36 states, including Massachusetts [55]) have mandatory reporting regardless of an organization's size.

The NASCIO conducts regular surveys of the priorities and goings-on of Chief Information Officers in 49 states, and found evidence of the need for improvement in the cooperation and coordination among state CIOs and local government officials. Only 31% of state CIOs indicated that their state had a "formal awareness and marketing campaign to promote state offerings to local governments", and only 42% of respondents answered affirmatively to the question "in your acquisition process for contract vehicles that would be available to local governments, do you consult with local governments about their needs prior to issuing a solicitation" [61].

Pairing the results of the NASCIO state CIO surveys with the results of a 2020 Municipal Cybersecurity Survey by the Massachusetts Municipal Association (MMA) [7], a clear difference in adherence to cybersecurity best practices between performance at the state level and the performance of MA municipalities can be identified. While 92% of respondents to the 2019 NASCIO survey indicated that they had "developed security awareness training for workers and contractors", only 47 out of 76 (62%) municipalities responded yes to the question, "Have you received information security training for job-related activities through your municipality or another organization". Only 8 out of 76 MA municipalities responded that they "had a cyber incident response plan (IRP)", while 61% of state organizations responding to the NASCIO survey indicated that they had "developed a cybersecurity disruption response plan".

2.4 Emerging Approaches to the Municipal Cybersecurity Challenge

Thinking beyond current approaches at the state and local level, a number of scholarly works have highlighted the need to move to a risk-based cyber-mitigation approach and to grounding cybersecurity efforts in a more data-driven and systematic way.

The final report of the Ransomware Task Force, a collection of experts on ransomware ranging from leaders in the technology sector and policy specialists, aggregated research and insights into the ransomware phenomenon from a variety of sectors, and outlined several recommendations that are particularly relevant to the problem of municipal cybersecurity [31].

Highlights from Goal 3 of the report - "Help Organizations prepare for ransomware attacks" include:

> Action 3.3.2: Require local governments to adopt limited baseline security measures.
> Action 3.4.1: Highlight ransomware as a priority in existing funding provisions.
> Action 3.4.3: Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance [with the Ransomware Framework.]
> Action 3.4.4: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.

In its 2016 Memo on State Cybersecurity Strategies, the National Governors Association (NGA) compiled state-level strategic plans (as of September 2016) [8]. The NGA report gathered 22 state plans from 18 states, differentiating among cybersecurity-specific plans, Information Technology plans more broadly, and homeland security plans that include cybersecurity provisions. The report found recurring themes throughout the compiled plans, including the goals of "protecting state IT infrastructure and data; developing and exercising a cyber response plan to protect critical infrastructure; training employees on cyber hygiene [and] improving the cybersecurity workforce; talent pool; creating a governance structure and metrics; and creating partnerships."[8]

Importantly, the report included a call to move from a compliance-based approach to a

risk-based approach as a best-practice, to move past a 'checking-off' mindset into a more substantial examination of particular organizational cyber risk and mitigation approaches.

In its 2020 report *Managing Cyber Threats through Effective Governance: A Call to Action for Governors and State Legislatures* [10], the National Conference of State Legislatures (NCSL) and partner organizations highlighted action items for cybersecurity policy at the state level, including the importance of "building a whole-of-state risk management program".

> "As governors and state legislatures commit to taking action to manage their risk, they must also recognize that creating and strengthening cybersecurity governance requires a continuous process of understanding cyber threats and translating that knowledge into appropriate cybersecurity actions. A cyclic "risk-based" approach ensures that a state has the agility necessary to successfully evolve its cybersecurity risk management capability. Cybersecurity governance must be tailored to keep up with current risks and agile enough to adapt to future risks"

In their 2020 paper Preis and Susskind [63] conducted a review of existing academic as well as practice-based understanding of state and local government interactions in the context of cybersecurity. The conclusions reached after reviewing and cataloging scholarship throughout this emerging field included that "state governments need to be more fully involved in strengthening local cybersecurity [...] as long as states set no "minimum standards" or a "standard of care," we have no way of judging whether the various forms of state involvement are helping [...] State governmental assistance is needed to bring cooperation and coordination for cybersecurity across local governmental entities that likely will not materialize otherwise".

The paper calls for "research within states that compares cybersecurity improvement efforts among local governmental entities— those that have and haven't taken advantage of state assistance". "At the local level, researchers must begin the difficult work of engaging closely with partner communities, over long periods of time, to provide richer accounts of cybersecurity improvement efforts."

Chapter 3

Case Study: Municipal Cybersecurity in Massachusetts

3.1 The Massachusetts Municipal Cybersecurity Landscape

This section sketches a picture of Massachusetts municipal cybersecurity and provides necessary background on the Massachusetts Cybersecurity Center and the MIT Cybersecurity Clinic, the two parties in the collaborative research effort described in this thesis.

Currently, responsibility for improving municipal cybersecurity in Massachusetts primarily falls under the Massachusetts Cybersecurity Center (MassCyberCenter) and the Executive Office of Technology Services and Security (EOTSS), with a variety of support with federal-level partners. EOTSS is primarily concerned with technology infrastructure for public services in the Commonwealth in general. The primary way in which EOTSS provides services to municipalities in particular is the Cybersecurity Awareness Training Grant [27], a grant program through which municipalities and other local government organizations can receive cybersecurity awareness training. EOTSS also offers a Cybersecurity Health Checks service for basic risk assessment for municipalities at no cost to them [29]. EOTSS also administers competitive IT grant and services programs: the Community Compact Cabinet IT Best Practice Program and the Community Compact Cabinet

IT Grant Program [28].

The Massachusetts Cybersecurity Center (MassCyberCenter) is a Massachusetts state agency launched in 2017[14]. Its mission is "to enhance conditions for economic growth through outreach to the cybersecurity ecosystem of Massachusetts, while fostering cybersecurity resiliency within the Commonwealth."[14]. One of the key projects of MassCyberCenter is fostering cyber-readiness in the public sector, and in particular in Massachusetts' 351 cities and towns. Though fostering municipal cybersecurity is not explicitly a responsibility of the MassCyberCenter, the Center sees these municipalities as particularly vulnerable to the threat of ransomware and other forms of cyberattack and action and sees municipal cybersecurity as key to fostering overall cybersecurity resiliency. The high level of vulnerability among municipalities is a function of their combination of often-limited levels of financial and technical resources, as well as the fact that municipalities provide critical services for constituents.

Within the MassCyberCenter, the Cyber Resilient Massachusetts Working Group (CRMWG) is made up of MassCyberCenter staff as well as stakeholders across the public and private sectors and was established by Governor Baker to facilitate cyber resiliency across the Commonwealth. The Municipal Cybersecurity Sub-working Group of the CRMWG is responsible for the development of MassCyberCenter's municipalities-oriented programs and resources. In particular, CRMWG was the focal point for the development of the Minimum Baseline of Cybersecurity for Municipalities (Minimum Baseline), which is a framework of four basic cybersecurity goals that Massachusetts municipalities are encouraged to meet in order to improve their cybersecurity posture [15].

The four goals of the Minimum Baseline are:

Goal 1: Trained and Cyber-secure Employees
Goal 2: Improved Threat Sharing
Goal 3: Cyber Incident Response Planning
Goal 4: Secure Technology Environment and Best Practices

An archive of the webpage presenting the Minimum Baseline can be found in Appendix A.

The Minimum Baseline is accompanied by the Municipal Cybersecurity Toolkit [16], a

compendium of resources aggregated by the MassCyberCenter with the intent of helping municipalities get started on meeting the goals of the Minimum Baseline.

While the MassCyberCenter's role is not limited to the public sector, the Center has been the primary driver of cybersecurity initiatives for municipalities, chiefly through the aggregation of resources in the form of the Municipal Cybersecurity Toolkit as discussed above. The MassCyberCenter serves as a convener of the major players in public sector cybersecurity, working in partnership with the Department of Homeland Security, and the Multi-State Information Sharing Analysis Center (MS-ISAC). A noteworthy convening initiative by the MassCyberCenter was a series of Cyber Incident Response Planning Workshops [17] held in the summer of 2020 for the commonwealth's 351 municipalities, providing a guide for meeting Goal 3 (Cyber Incident Response Planning) of the Minimum Baseline.

Another aspect of municipal cybersecurity in Massachusetts is the voluntary cyber liability protection [6] program offered by the Massachusetts Interlocal Insurance Association (MIIA), a member service of the Massachusetts Municipal Association (MMA). Massachusetts municipalities are eligible to purchase cyberinsurance at a negotiated rate through the MIIA program. However, municipalities do not currently need to meet any particular cybersecurity standard to be eligible to enroll in the insurance program.

The Massachusetts municipal cybersecurity landscape is undergoing change at the time of writing. In September 2021, MassCyberCenter released new video learning modules to go along the Municipal Cybersecurity Toolkit and dive deeper into the Minimum Baseline goals and associated resources. Also in September 2021, the state released a new Statewide Contract for Data and Cybersecurity (ITS78) [25], prequalifying some third-party cybersecurity vendors for use by cities and towns.

3.2 Background: the MIT Cybersecurity Clinic

Founded in early 2020, the MIT Cybersecurity Clinic (the Clinic) is an initiative headed by Prof. Lawrence Susskind in the Department of Urban Studies and Planning. The Clinic's goal is to engage in research and teaching on the challenges posed by cybersecurity in

the public sector, in particular around vulnerabilities that are the result of social engineering approaches such as phishing. Through a course offered in DUSP (Cybersecurity For Critical Urban Infrastructure 11.074/11.274), student participants first learn the basics of cybersecurity best practices, then take a test certifying their learning, and finally partner with client organizations (municipal agencies and hospitals in the New England area) to prepare a cybersecurity vulnerability assessment.

Beyond offering the field-based class, the Clinic serves as a nexus at MIT for research around public sector cybersecurity, including engagement with relevant external partners and stakeholders. The MassCyberCenter Minimum Baseline Project, described below, is one such partnership between the Clinic and a public sector partner, in this case the MassCyberCenter. The work described in this thesis is the result of this collaboration, providing benefits to the MassCyberCenter as an external evaluation of the possibilities of expansion of their programs targeted towards municipalities, as well as benefits for the Clinic, in terms of pioneering new policy approaches to the problem of cybersecurity readiness in local governments.

3.3 The MassCyberCenter Minimum Baseline Project

In January 2021, MassCyberCenter and the MIT Cybersecurity Clinic entered into a research agreement to interview a subset of Massachusetts municipalities regarding their understanding and use of the resources of the Minimum Baseline of Cybersecurity for Municipalities, combined with a review of applicable cybersecurity policy initiatives across the United States. The aim of the collaboration was to develop recommendations for improvements to the Minimum Baseline and associated resources, and more generally explore mechanisms by which the MassCyberCenter could help further its goal of increasing cybersecurity preparedness in Massachusetts municipalities. The full initial research proposal and agreement between the MIT Cybersecurity Clinic and the MassCyberCenter can be found in Appendix B.

3.4 Massachusetts Municipalities Minimum Baseline Interviews

In order to ground our recommendations for improvements to Massachusetts' state/local cybersecurity resources and policies in stakeholder engagement, I strove to interview a sample of Massachusetts municipalities diverse in terms of population size and geography. In particular, I requested interviews with municipal employees most likely to be responsible for cybersecurity (e.g., IT Director, Network Administrator).

3.4.1 Methodology

I refined a standardized interview questionnaire in partnership with Stephanie Helm (MassCyberCenter Director) and Meg Speranza (Resiliency Program Manager). The interview questions centered around the four goals of the Minimum Baseline of Cybersecurity for Municipalities (Minimum Baseline):

Goal 1: Trained and Cybersecure Employees
Goal 2: Improved Threat Sharing
Goal 3: Cyber Incident Response Planning
Goal 4: Secure Technology Environment and Best Practices

The questionnaire sought to solicit from interviewees their current perspective on their successes and challenges in meeting each goal and the resources they had utilized to help them meet each goal. The questionnaire also asked what resources they wished were available in order to make it easier to achieve a minimum baseline of cybersecurity readiness.

The final version of the full questionnaire can be found in Appendix C. This study received an Exempt determination from the MIT Committee on the Use of Humans as Experimental Subjects (COUHES).

Recruitment of interviewees was conducted through email and phone outreach to municipal IT employees. Interviews were conducted over Zoom, recorded with prior permis-

	State Total	State %	Sample Total	Sample %
Extra-Small	271	77.21%	7	50.00%
Small	54	15.38%	4	28.57%
Medium	12	3.42%	2	14.29%
Large	9	2.56%	0	0.00%
Extra-Large	5	1.42%	1	7.14%

Table 3.1: Municipality Distribution by Size

sion of the interviewee. A total of 14 municipalities were interviewed over the summer of 2021, out of 50 attempted municipality contacts. Recruitment of municipalities proved challenging, with email and phone outreach most often resulting in no response. The author would like to note the contribution of Aaron Robles (MIT Class of 2021) who helped conduct some of the interviews.

I classified municipalities into size categories based on their number of residents:

- Extra-small: 0 - 25,000 residents
- Small: 25,000 - 50,000
- Medium: 50,000 - 75,000 residents
- Large: 75,000 - 100,000 residents
- Extra-Large: 100,000+ residents

Table 3.1 summarizes the size distribution of municipalities in the sample.

I also classified municipalities in terms of geographical region: Western Massachusetts, Central Massachusetts, and Eastern Massachusetts (see Map 3-1. I assigned each municipality a region based on its county:

- Western: Berkshire, Franklin, Hampden, Hampshire
- Central: Worcester
- Eastern: Essex, Middlesex, Suffolk, Norfolk, Plymouth, Bristol, Barnstable, Dukes, Nantucket

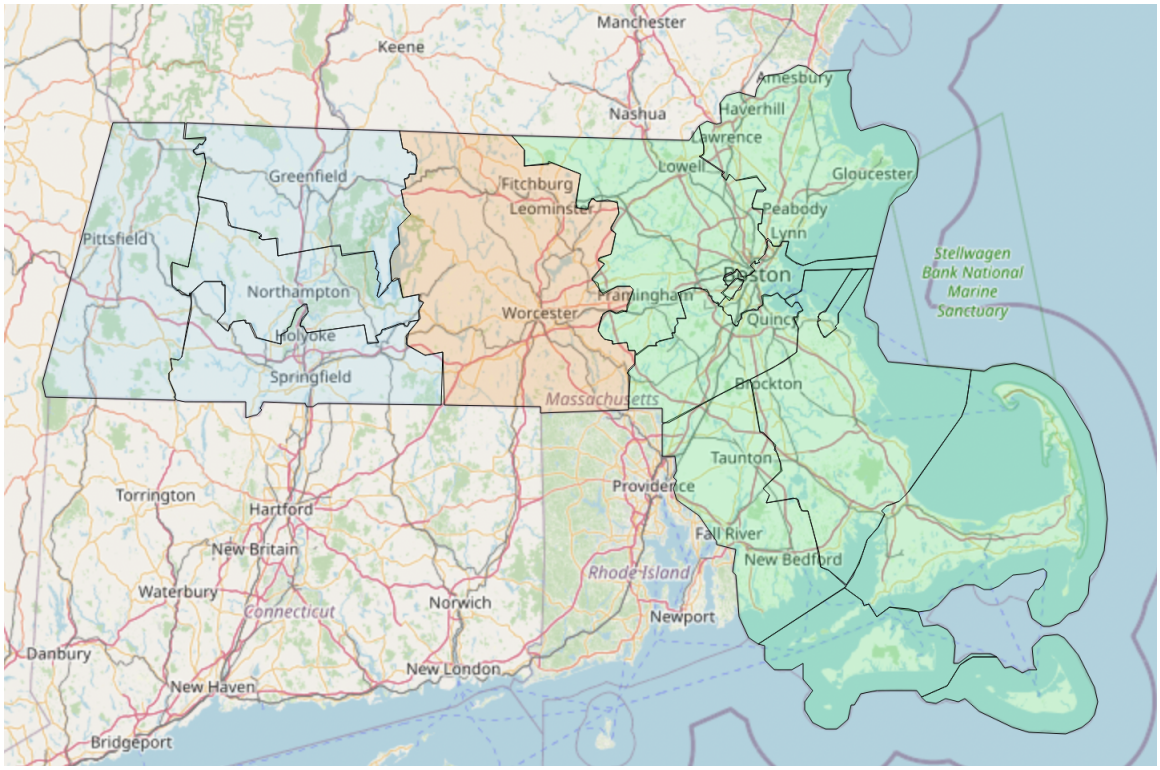

Figure 3-1: Counties in Western, Central, Eastern Massachusetts

	State Total	State %	Sample Total	Sample %
East	88	25.07%	4	28.57%
Central	162	46.15%	8	57.14%
West	101	28.77%	2	14.29%

Table 3.2: Municipality Distribution by Region

Out of a total of 351 cities and towns in Massachusetts, I classified 271 as extra-small, 54 as small, 12 as medium, 9 as large, and 5 as extra-large. I also classified 88 as being in the east, 162 centrally located, and 101 in the west. Table 3.2 summarizes the regional distribution of municipalities in the sample.

Additional conversations with relevant stakeholders were conducted ad-hoc throughout the research process, including an interview with MassCyberCenter staff Stephanie Helm and Meg Speranza in October of 2021.

3.4.2 Contextualizing Findings

Due to the difficulty of finding enough municipalities willing to participate in the study and the resulting small sample size, the following findings should not be taken as an authoritative picture of the state of cybersecurity in Massachusetts municipalities. Sampling bias is an obvious factor here, where municipalities and IT professionals who were already more involved in cybersecurity initiatives were more likely to respond to a request for an interview. Rather, I think of the findings from the interviews, combined with existing scholarship in the field highlighted in Section 2, as a starting point for thinking about policy proposals to improve local government cybersecurity in Massachusetts and bring about more systematic data collection regarding municipal cybersecurity risk posture and cybersecurity resource utilization.

3.4.3 Key Findings

Responses to each interview question were transcribed and then findings were summarized across interviews. The following are key patterns uncovered in the responses. Keeping in mind the issue of small sample size discussed above, these results should not be taken to generalize across all Massachusetts municipalities, and at most can be interpreted as weak confirmation of trends highlighted in existing scholarship highlighted in Section 2.

Municipal Cybersecurity Resources Areas of Strength:

- All municipalities interviewed reported being a part of MS-ISAC, and most reported finding the program valuable. While this cannot be generalized to mean that every municipality in Massachusetts finds value in MS-ISAC, it is encouraging to see enthusiasm for information sharing and interlocal cooperation.

- Similarly, a large majority of respondents reported that regional IT director listservs or similar mechanisms helped them carry out their job duties and stay informed of threats and other cybersecurity goings-on.

- A majority of respondents reported using the EOTSS Cybersecurity awareness training grant, and found the training helpful, while noting the challenge of compliance and of getting municipal employees to actually complete the training.

Municipal Cybersecurity Resources Areas In Need of Improvement:

- The biggest challenges faced by interviewees in promoting cybersecurity in their organization were lack of funding for cybersecurity improvements and lack of time to implement improvements.

- Interviewees repeatedly identified competition for scarce municipal resources and the importance of municipal leadership buy-in as barriers to improving cybersecurity posture. Interviewees cited cybersecurity being pitted against other essential but more visible municipal services (such as fire service, trash collection, etc). Several cited, unprompted, the need for state level requirements.

- Several interviewees mentioned in particular the difficulty of recruiting qualified IT professionals willing to work in government settings. Municipal IT professionals often need to cover a wide range of separate job functions (network administration, security, payroll systems, etc).

- When asked for what action they wished to see from the state government, a majority of participants cited additional help in terms of one-on-one technical support, additional funding, especially funding not reliant on year-to-year grant applications, and more accessible cybersecurity contacts at the state level.

The above findings, while anecdotal due to the small sample size, confirm existing scholarship on the challenges of cybersecurity at the municipal level examined in Section 2. The following Recommendations section takes a more systematic approach to proposing mechanisms to address the root cause of the problem: misaligned incentives.

Chapter 4

The Municipal Cybersecurity Challenge: Aligning Incentives

The MassCyberCenter Minimum Baseline Project interviews, paired with my examination of existing scholarship, point to a clear finding about the municipal cybersecurity challenge: the problem is not technological, but rather organizational in nature. Municipal IT professionals are unable to get access to the resources and time they need to implement substantial cybersecurity practices because local governments face an acute resource shortage. Investments in cybersecurity improvements, no matter how worthy they may turn out to be in preventing or mitigating the fallout from cyberattack, are pitted against other municipal needs. These needs are seen as less urgent and important in the near term, and therefore are put off. There is no real incentive to invest immediately in cybersecurity despite the threat of catastrophic loss. In the sections below, I will identify and define the goal of **continuous measured improvement** in municipal cybersecurity posture. I explore the current regulatory landscape - cybersecurity at the national, state, and local levels, and propose a regulatory mechanism for aligning municipalities' incentives towards the continuous improvement goal, as well as concrete improvements in the resources available to municipalities to help them enhance their cybersecurity readiness. I draw relevant policy analogies from existing academic and practice-based literature.

4.1 Status quo: voluntary participation

The status quo of municipal cybersecurity in Massachusetts is that of voluntary participation by municipalities in programs run by the MassCyberCenter and the Executive Office of Technology Services and Security (see Section 3.1), often relying on the initiative of municipal IT directors or other local champions of cybersecurity.

4.2 Goal: Continuous Measured Improvement

Moving forward, there is a need for a more comprehensive strategy at the state level to make municipal cybersecurity a priority, beyond voluntary and uncoordinated engagement. I propose that the goal for all municipalities should be that of continuous measured improvement in their cybersecurity posture. I propose this goal because it reflects that cybersecurity preparedness cannot be accomplished by checking off a discrete set of unchanging requirements, but rather requires careful implementation of a constantly-evolving assortment of best technological and managerial practices at the organizational level with regular re-evaluation to align with emerging information about cyber losses and best practices. Municipal cybersecurity is too critical an issue to rely on the ad-hoc initiative of certain local governments and municipal workers, no matter how dedicated those public servants may be. Cybersecurity readiness is a moving target; no one checklist or series of requirements will prevent all cyberattacks from occurring. However, there is a broad consensus that basic cybersecurity hygiene practices such as proactive software updates, multi-factor authentication, and other interventions will limit the risk of falling victim to cyber attack in the first place, as well as limit the recovery costs [19, 66]. There is a need for a more centralized approach to accurately measure the cyber risk that municipalities face and help the state champion effective measures to lower that risk over time.

In order to achieve this goal of continuous measured improvement, I identify the need for a concrete incentive and measurement system at the state level paired with investment in resources to help municipalities meet the requirement without undue burden.

I recognize that another possible path to improving municipal cybersecurity may be to impose a particular set of cybersecurity standards on all municipalities; I find that path unadvisable for several reasons. The issue of municipal cybersecurity is vitally important, but shifting all of the costs and implementation challenges onto municipalities is a non-starter given their resource-constrained environment. Municipal organizations in general and in Massachusetts in particular have sounded the alarm on "unfunded mandates" by state legislatures or the federal government [11]. In addition, directly mandating a particular set of unchanging cybersecurity standards for municipalities without setting up structures to measure progress, reassessing those standards, and distinguishing effective assistance measures from relatively less effective ones, is a recipe for ineffective spending of both state and municipal funds. In addition, such mandates would violate the understood independence of municipal governments and set up an adversarial rather than cooperative relationship between the state and local government. I instead chose the path of suggesting a course that will align the proper incentives for all stakeholders (municipalities, the state, and insurance firms) to lower overall cyber risk (and cost), encouraging municipal participation while remaining non-mandatory. As such, I propose an insurance-based incentivization mechanism that would enable cybersecurity to be prioritized by every municipality, regardless of prior involvement with state initiatives or current cybersecurity posture.

4.3 Proposal for a Massachusetts Cyber Disaster Insurance Program

I propose a new **Massachusetts Cyber Disaster Insurance Program** as a means for incentivizing local-level improvements in cybersecurity posture.

The Massachusetts Cyber Disaster Insurance Program (MCDIP) would provide high-quality, negotiated-rate cyberinsurance for Massachusetts municipalities to help them face the potentially catastrophic costs of restoring access to municipal services after a cyber attack. In order to be eligible for the Cyber Disaster Insurance Program, a mu-

nicipality would need to show year after year improvement in its cybersecurity posture. The MCDIP would utilize a secure cyber risk aggregating tool developed at MIT known as SCRAM (Secure Cyber Risk Aggregation and Measurement) (see Section 4.3.2) to measure cybersecurity improvement over time. SCRAM allows the collection and aggregation of data related to cybersecurity control implementations, utilizing the cryptographic concept of Secure Multiparty Computation to keep responses from individual respondents private. Data collected from SCRAM would also be utilized to develop/improve existing cybersecurity resource programs targeted at municipalities. This mechanism would serve to lower overall cyber risk in municipalities, leading to a redirection of funds from recovery costs to effective preventative spending. Section 4.3.1 gives a general overview of MCDIP. Section 4.3.2 and Section 4.3.3 provide relevant background on the SCRAM platform and on insurance economics, respectively. Section 4.3.4 lays out a parallel use of an eligibility-restricted insurance program to achieve a risk reduction policy goal in the case of the National Flood Insurance Program. Finally, Section 4.5 makes recommendations for cybersecurity capacity-building programs for municipalities, drawing on actual examples from other states.

4.3.1 Overview of the Massachusetts Cyber Disaster Insurance Program

Figure 4-1 provides an overview of the proposed MCDIP program. A summary of the commitments and responsibilities of each stakeholder in the proposed MCDIP can be found in Table 4.3.6.

Year 0

The focus of Year 0 is to finalize the specifics of the Mass Cyber Disaster Insurance Program, using MassCyberCenter's convening infrastructure to get input from critical stakeholders and make decisions that will best enable the program to meet its goals. For more details, see Section 4.3.7.

Year 1

In Year 1, the focus is on achieving strong enrollment from municipalities and es-

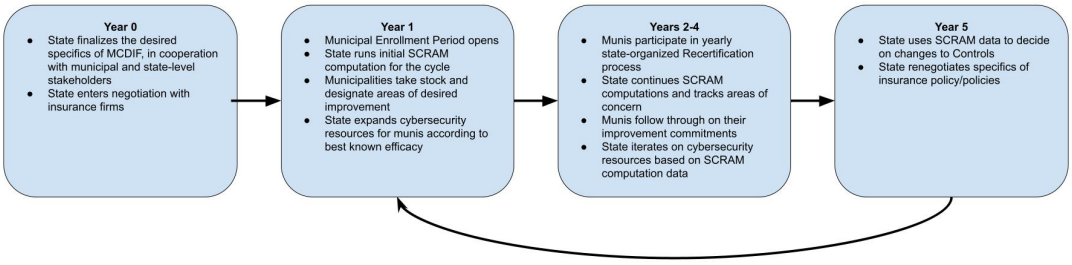

Figure 4-1: Overview of the Massachusetts Cyber Disaster Insurance Program

tablishing regular SCRAM computations and improvement tracking. MassCyberCenter should enlist the help of partners such as the Massachusetts Municipal Association, EOTSS, and the Massachusetts Homeland Security Regional Advisory Councils, as well as directly reach out to potential municipal participants.

In conjunction with the start of the cybersecurity posture improvement measurement process further described in Section 4.3.2, MassCyberCenter should start a process of enhancing cybersecurity resources available to municipalities. I suggest that at first, ideas for improvement be drawn from Section 4.5 of this report, which summarizes existing state-local government collaboration best practices regarding cybersecurity in other states and in different domains across Massachusetts. However, after the first MCDIP cycle, improvements made to resources should be based on data collected through the SCRAM computation process regarding aggregated areas of strength and of weakness.

Years 2-4

In Years 2 through 4, the program operates in earnest. MassCyberCenter continues to orchestrate SCRAM computations and improve municipal cybersecurity resources using SCRAM data and municipalities continue to make improvements to their cybersecurity posture. Yearly, municipalities engage in a Recertification process coordinated by MassCyberCenter, where they provide data showing that they are meeting the continuous improvement benchmarks (see Section 4.3.2).

Year 5

At the end of each 5 year cycle, the MassCyberCenter will update the controls used

in the municipal SCRAM assessment, based on data on emerging areas of concern. I.e, because the SCRAM assessment will ask for reported cyberattack losses and attack vectors used against municipalities, MassCyberCenter can iterate on the controls in future SCRAM assessments to specifically target known challenge areas and steer an even further decrease of municipal cyber risk. The changes made to the controls should be done in partnership with municipal stakeholders to ensure a smooth transition and manageable aspirations for participants. Municipalities will be asked to re-enroll in the insurance program and acknowledge the new controls and parameters (see Section 4.3.5).

4.3.2 SCRAM and the Measured Continuous Improvement Mechanism

I propose the use of the SCRAM (Secure Cyber Risk Aggregation Measurement) platform developed by leading researchers from MIT's Internet Policy Research Initiative [13] to implement the suggested Continuous Improvement Mechanism. Specifically, I recommend the use of the Ransomware Readiness Index (RRI) set of SCRAM controls [67], developed with lower-resourced organizations in mind, as a starting point for evaluating municipal cybersecurity systematically.

The SCRAM platform relies on cryptographic principles to provide a mechanism by which participants (in this case, municipalities) can enter data regarding their implementation of cybersecurity controls, and the aggregated results can be viewed without any party in a given computation - a term to refer to a run of the aggregation program on a set of participant information - seeing any other party's responses.

The Ransomware Readiness Index (RRI) is a fusion of existing cybersecurity frameworks such as the NIST framework [48], distilled to a small set of security controls that serve as a proxy for evaluating the readiness of organizations such as municipalities to face the threat of ransomware. The report outlines 10 categories of controls, including: Multifactor Authentication, Endpoint Detection and Response, Encryption, Empowerment, Training, Backup, Patching, Incident response, Checking the work, and Segmenting. In many ways, the Control Categories align with the four goals of the Minimum Baseline for

Municipalities, outlining it in more specific details and relating each goal to existing and well-regarded cybersecurity frameworks.

The RRI paper labels each control as Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented. The SCRAM platform is used to produce aggregated measurements of where the parties in each computation face the most risk, while letting each member of the computation keep their own answers private.

I propose that on an annual basis, the MassCyberCenter run a computation with all of the members of the Massachusetts Municipal Association. At the end of the computation, municipalities would share back with MassCyberCenter their aggregated RRI score, which is a measure of their overall cybersecurity readiness. Municipalities would not be asked to share their specific answers to the questionnaire, only their overall score. In order to remain in good standing with the Cyber Disaster Insurance Program and ensure continued coverage, municipalities would need to either meet a RRI score of 90 percent overall, or show an improvement of 10 points, which corresponds to improvement in one of the control categories from Not Implemented to Fully Implement (though it could also correspond to more incremental improvements in several categories).

I propose a state-sponsored municipal cyberinsurance program, where the state would agree to organize a lower-rate, better-coverage cyber insurance pool for municipalities, in exchange for a guarantee of continuous improvement by participating municipalities. I propose that the MassCyberCenter would be responsible for administering this insurance program, as they are well situated to serve as a nexus for municipal cybersecurity in Massachusetts, but it is possible that with further investigation, another, better-suited central administrative location could be agreed upon.

The closest existing equivalent to this Cyber Disaster Insurance Program proposal is the Massachusetts Interlocal Insurance Association (MIIA) cyberinsurance program. The Massachusetts Municipal Association (MMA) currently administers a member service known as the Massachusetts Interlocal Insurance Association (MIIA) [6], which allows member municipalities to purchase several types of insurance, including cyberinsurance, at a discounted price. However, there are currently no underwriting requirements to participate in the MIIA cyberinsurance program, thereby providing little incentives

for municipalities to engage with state resources to become less vulnerable to cyberattack. I propose that this insurance program be eventually discontinued and migrated into the Cyber Disaster Insurance Program. The MCDIP would provide all of the benefits of group-purchase lower rates of MIIA cyberinsurance, while actually ensuring a mechanism for continuous improvement of municipal cybersecurity posture and encouraging further engagement with state cybersecurity resources.

4.3.3 Background: Insurance Economics

This section aims to provide background on insurance terms and insurance economics, to lay the theoretical groundwork behind the MCDIP proposal and show how lowering overall municipal cyber risk serves all stakeholders involved, including municipalities, the state, and insurers.

At its core, insurance is a mechanism designed to mitigate the risks of catastrophic loss for any single entity/individual by spreading out the risk over an entire pool of individuals/entities. The contract (insurance policy) between the entity and the insurer spells out the terms under which the insurer will take responsibility for losses by the entity, in exchange for regular insurance premium payments [39].

Insurance works because it enables entities to engage in important activities (for example, the provision of municipal services) that carry a low probability but potentially high cost risk. By spreading out the cost of each adverse event throughout the insurance pool (the subscribers to a set of insurance policies) in the form of premiums, insurance makes doing business/engaging in economic or other activities safer.

Insurance premiums and policies are set by insurers based on an estimate of the overall risk incurred by the insurance pool, and some amount of profit. The loss ratio is defined as the ratio of losses incurred to premiums collected - insurance firms strive to keep their loss ratio low. Loss ratios in cybersecurity insurance are considerably higher than in other insurance categories [59], indicating a combination of poor understanding of cyber risk incurred and high risk conduct/insufficiency risk mitigation undertaken by policyholders.

Using this admittedly idealized understanding of insurance mechanisms, it can be postulated that lowering over cyber risk (through the incentivization of cyber hygiene best

practices) is advantageous for all stakeholders involved. Insurance firms should be willing to offer lower premiums and better coverage to entities taking steps to lower their risk profile (as spelled out by the MCDIP eligibility requirements), because they can expect to pay out less in damages. Lowering cyber risk is obviously beneficial to municipalities, as they will incur less risk of disrupted services and high recovery costs. Lowering cyber risks is also beneficial to the state administering the program, both because the state has an interest in municipal services continuing to be provided, and because the state would likely be saddled with extra responsibility should a cyber attack cause a municipality to declare bankruptcy [37].

Another important concept when discussing insurance is that of moral hazard. Moral hazard is defined as the hazard that an insured entity that does not bear the full weight of the consequences of an adverse event will behave in a less careful manner, causing their risk to increase [41]. In the case of municipal cyber insurance, it is important to design an insurance system that will not cause municipalities to believe that they may decrease their level of care because their losses will automatically be covered by insurance.

4.3.4 Parallel to the National Flood Insurance Program

Incentive-correcting insurance mechanisms are a proven, reliable mechanism employed in relationships between federal, state, and local governments. A prime example is the National Flood Insurance Program (NFIP) and the Community Rating System (CRS) [3]. The National Flood Insurance Program, administered by the Federal Emergency Management Agency (FEMA), offers federally-backed flood insurance for homeowners and businesses located in high and moderate risk flooding areas. The NFIP was created in 1968 by the passage of the National Flood Insurance Act [3]. The enactment of the National Flood Insurance Act was itself a response to lack of market-based flood insurance for high-risk areas and mounting federal flooding disaster assistance costs [58]. As part of remaining eligible to participate in the National Flood Insurance Program, participating communities, as they are known, must fulfill minimum NFIP requirements regarding proper floodplain management practices.

The Community Rating System (CRS) is an incentives-based extension of the NFIP.

> "The Community Rating System was created to encourage communities to establish sound programs that recognize and encourage floodplain management activities that exceed the minimum NFIP requirements. By conducting mitigation and outreach activities that increase safety and resilience, including CRS credits for regulating to higher standards, communities can earn credits and discounts (up to 45 percent within the Special Flood Hazard Area) on flood insurance premiums for property owners." [4]

Participating communities that meet the higher CRS standards are eligible for reduced flood insurance premiums. The CRS Coordinator Manual [2] details a series of flood preparedness goals, and relates fulfillment of those goals with reduction of flood insurance premium prices, up to a 45% discount. Each community participating in CRS must attest yearly that it is implementing its stated flood mitigation policies, in a process known as Recertification. Communities are subject to a lengthier Verification process at the conclusion of three-year or five-year cycles, depending on community classification and risk profile.

The structure of the proposed Cyber Disaster Insurance Program has many parallels to the Community Rating System. With the MCDIP, participating communities reap benefits in terms of lower-priced protection against potentially devastating cyberattack, while the state incentivizes greater cybersecurity preparedness, lowering overall risks to communities and the residents who rely on their services. I draw a parallel between flood risk and cyber risk; while appropriate mitigation (eg., appropriate building construction practices, cyber hygiene practices) can greatly reduce the risk of costly infrastructure damage, no particular set of practices can entirely eliminate the risk of floods or cyberattacks. The goal of government is to ensure safety and well-being for citizens; in these cases of inherent but proactively manageable risk, its strategy should be to provide incentive structures for following known best practices, and step in to provide an avenue for affordable insurance against the non-eliminable risks.

4.3.5 Iteration on Cyber Disaster Insurance Program Eligibility

Recognizing that state-of-the-art understanding of what cybersecurity readiness means and entails is constantly evolving, I propose an additional mechanism to ensure that the

Cyber Disaster Insurance Program continuous measured improvement benchmark itself stays up to date.

I propose a meta-continuous improvement process loosely based on the NFIP CRS recertification and verification mechanism. Each year, enrolled municipalities would participate in a state-wide SCRAM computation. Municipalities would ensure continued eligibility in the CDRF by reporting their score to the administering agency. Critically, the aggregated results of the SCRAM computation will contain crucial anonymized information on areas of strengths in preparedness throughout municipalities, areas in need of work, and information on recent cyber incident-related losses and the mechanisms by which they occurred. The administering agency would then, on a five year cycle, iterate on the SCRAM controls themselves to incentivize participants to make improvements in their cybersecurity posture in a data-driven way (promoting improvements in particular areas that have been shown by the SCRAM computation to have led to substantial losses for municipalities). Every five years, municipalities would need to recommit to participating in the MCDIF under the updated controls, akin to the Verification process in the NFIP CRS. This mechanism ensures both that municipalities get fairly evaluated on a clearly stated set of standards, but also that those standards evolve in a data-driven way to correctly incentivize especially worthwhile cybersecurity posture investments and do not become obsolete.

4.3.6 Summary of Commitments and Benefits for Stakeholders

Table 4.3.6 summarizes the commitments and benefits of MCDIP for each of its stakeholders.

As outlined by the Table 4.3.6, the MCDIP system realigns the incentives in the municipal cybersecurity problem. Participating municipalities benefit from decreased cyber risk through an iterative improvement process, lowering the chance of service disruption and potentially catastrophic cyberattacks. The state benefits from increased data collection regarding cybersecurity resource use and municipal cybersecurity losses. Because of the adherence of eligible municipalities to the continuous improvement process, the state

Stakeholder	Commitment	Benefits
Municipalities	• Take part in regular SCRAM computations • Make necessary changes to meet improvement benchmarks • Participate in annual Recertification and quinquennial Verification and re-enrollment	• Lowered cyber risk profile • Protection against catastrophic losses due to cyberattacks • Increased connection to and support from state cybersecurity resources
State	• Run regular SCRAM computations • Provide expanded cybersecurity services and iterate based on SCRAM data • Negotiate cyberinsurance package(s) with insurer(s) • Run the Recertification and Verification processes for participating municipalities	• Decreased risk of catastrophic municipal cyberattack • More efficient deployment of limited state resources based on SCRAM data • Inform Federal Policy
Insurer(s)	• Provide high-quality cyberinsurance to eligible MA municipalities at a rate negotiated with the state	• Reduced cyberinsurance loss ratio by lowering overall risk in insurance pool • Guarantee of data-driven improvements in cybersecurity posture

Table 4.1: Summary of MCDIP Stakeholder Commmitments and Benefits

will be able to negotiate lower insurance premiums and better insurance coverage (higher maximums, lower deductibles) than municipalities would otherwise be able to get on their own. The insurance firms get the benefits of a much lower-risk insurance pool, and the guarantee of data-driven improvements in cybersecurity posture. Insurance firms in the cyberinsurance markets have low profitability and very high loss ratios compared to other subfields of insurance [59]; a mechanism such as MCDIP would both drive down risks and increase knowledge of the risk, therefore making the cyberinsurance market more hospitable for the firms themselves as well in addition to its direct benefits to municipalities and the state.

4.3.7 Degrees of Freedom in Implementing the MCDIP

I believe that the MCDIP as outlined above will help align the incentives in municipal cybersecurity to ensure an overall decrease in cyber risk and improvement in cybersecurity posture. Some implementation details are left as of now unspecified, and should be decided upon collectively by stakeholders after careful consideration of the tradeoffs required. The following section describes the remaining degrees of freedom in the MCDIP implementation, for consideration in the final design.

Framework/ Controls Set for SCRAM computation

The description of MCDIP above uses the RRI as an example of an initial framework/benchmark that could be utilized for the SCRAM computation. However, several other cybersecurity frameworks exist (e.g, the NIST Cybersecurity Framework) that could be used as the controls for the computation. While I believe that the RRI strikes a good balance of depth and breadth of questions and relevance to low-resourced organizations, while remaining relatively lightweight in terms of time required from participants, a final design for implementing MCDIP could utilize any other set of controls as desired.

Frequency of Recertification and Verification cycles

The current proposal suggests a 1-year Recertification cycle (where municipalities certify they have met the improvement benchmark) and a 5-year Verification cycle (where the state re-evaluates the set of controls used and municipalities re-enroll in the program), mirrored on the timeline followed by the National Flood Insurance Program. In

implementing the MCDIP, it may make sense to decide on different Recertification and Verification timelines, either uniformly or depending on factors such as municipality size.

Level of State Involvement in the Insurance Process and Specifics of Negotiated Cyberinsurance Policy/Policies

The MCDIP proposal outlines a role for a state agency (in our assessment, best taken on by the MassCyberCenter) as the negotiator on behalf of eligible municipalities in acquiring cyberinsurance, and as the organizer of the Recertification and Verification processes. I believe that this proposal offers value to all of the stakeholders involved, as summarized in Table 4.3.6, and avoids the moral hazard problem that could be caused by the state (e.g subsidizing some of the cyberinsurance premiums itself). However, it is possible that over the course of actual implementation of MCDIP, the role of the state could be redefined to include: taking financial responsibility for covering municipal recovery expenses above the maximum insurance coverage limit, or another deeper level of financial guarantee. I recommend that the MassCyberCenter pay special attention to designing the MCDIP with an eye towards attracting the participation of the most under-resourced municipalities. This could take the form of offering discounts on state-provided cybersecurity infrastructure services (see Section 4.5).

In addition, the specifics of the insurance policy or policies to be offered to municipalities as part of MCDIP have obviously yet to be determined. The state could choose to undertake negotiations with multiple insurance providers in order to get to an agreement most beneficial to all municipalities in terms of premiums and coverage conditions. The state could choose to provide several different insurance policies, all following the same core continuous measured improvement eligibility criteria, but perhaps providing different benefits that could be of interest to different municipalities (e.g based on size, location, current risk profile, etc).

4.4 Pairing the Cyber Disaster Insurance Program with Improvements in State-provided Cybersecurity Resources and Services

In order to be genuinely helpful, any state-level incentivization program such as the MCDIP must be accompanied by funding and other resources to assist municipalities, especially lower-resourced municipalities, in meeting the program goals. In order to maximize buy-in and positive outcomes, it is extremely important to avoid giving municipalities unfunded mandates. The following section details a collection of possible improvements to state-provided cybersecurity resources, based on information collected during the MassCyberCenter project interviews as well as on a review of innovative state-level cybersecurity programs throughout the United States. As explained in earlier sections, these recommendations should serve mostly as a starting point for thinking about improvements in resources offered to municipalities. While several states have established a variety of innovative programs regarding state and local government cooperation on cybersecurity, most of these programs are so new that they have no non-anecdotal, rigorous evidence regarding their success. It is hard to tell whether any of them, and if so which ones, are a good use of limited state funds and person-time. This lack of existing research on program efficacy is why it is critical for MassCyberCenter to help design the SCRAM questionnaires and utilize SCRAM information in order to make data-driven decisions about which resource programs to invest in.

Within the MCDIP system, data from the SCRAM questionnaires should be used to review and revise the resources provided by MassCyberCenter and help point to where new investments should occur. For example, if data from the SCRAM assessments points to large municipal losses due to poor firewall and endpoint security, MassCyberCenter would redirect resources towards giving municipalities access to time from technical experts to help address these problems. This continuous improvement process on the part of MassCyberCenter, in addition to the annual efforts on the part of municipalities, is essential to providing effective and efficient support and decreasing municipalities' cy-

bersecurity risk by making the best use of constrained resources

4.5 Recommendations on Resources

To assist Massachusetts municipalities meet cybersecurity goals, Massachusetts state agencies responsible for cybersecurity must reinforce existing programs, as well as launch new programs to better meet municipal needs. Below, I propose an array of options for meeting the goal of increasing municipal cybersecurity capacity, taking inspiration from existing Massachusetts programs in domains other than information technology, as well as from pioneering programs in other states. Changes in resources provided to municipalities should be tied into the MCDIP by systematically collecting data about program use and efficacy through the yearly SCRAM surveys, as detailed above. I recommend that MCDIP SCRAM questionnaires include a set of questions for each cybersecurity resource administered by the state. The survey should include questions about whether a respondent has utilized a given resource and ask which controls the resource helped the respondent properly implement. The questionnaire should also include an option to indicate that the respondent did not utilize the given resource, but believes the resource would have prevented a cybersecurity-related loss their organization suffered. This data would be used year to year to more effectively allocate limited state resources towards programs that actually best serve municipalities.

4.5.1 Improving Existing Programs and Resources

1. Improving vendor guidance

   Several interviewees noted the difficulty in identifying which technology vendors best meet the needs of their organization. I recommend that the MassCyberCenter in partnership with EOTSS develop a guide to selecting appropriate technology vendors for municipalities, especially as they pertain to cybersecurity. I understand that it would be inappropriate for state agencies to recommend that municipalities contract with specific vendors to purchase specific services. Therefore, I recommend compiling a more general guide for how to select a technology vendor in broad

strokes. The guide would include information explaining how to evaluate the technology needs of a particular municipality, where to search for vendors and how to request quotes and demonstrations, and how to formulate a plan for regularly re-evaluating services provided by a vendor. The September 2021 ITS78 contract mentioned in Section 3.1 is a good start, but more explicit guidance would be helpful to municipalities.

2. Improving ease of access to existing resources

   While the MassCyberCenter's Municipal Cybersecurity Toolkit is a good start at aggregating resources available to municipalities when it comes to cybersecurity, I propose that more could be done in terms of guiding municipalities through the process of actually taking stock of and ultimately improving their cybersecurity posture. A fruitful next step may be to provide a direct way for municipalities to access help and guidance regarding existing resources. A relevant parallel is Louisiana's cyber incident response 1-800 Hotline [44]. In Massachusetts, the Municipal Law Review section of the Attorney General's office serves as a direct person-to-person point of contact for municipalities to get feedback on legal matters [69]. I propose that offering a clearer way for municipalities to get engaged with state cybersecurity resources, especially with the possibility of person-to-person live interaction through the phone or in person, may be beneficial in helping a greater number of municipalities access already-existing services. In Section 4.5.3, I describe a proposal for a Regional CISO program, which could fill this connecting role as well.

4.5.2 Creating New Resources Targeted at Municipalities

1. Hands-on cybersecurity assistance

   Several of the municipalities interviewed raised the concern that while they often are aware of cybersecurity practices and have a desire to implement them, they have limited time and resources to do so. IT Directors and similarly-positioned professionals often wear many hats in small organizations such as municipalities and are stretched thin. The following recommendations attempt to address one of

the biggest obstacles to cybersecurity readiness in municipalities: the scarcity of skilled labor.

(a) Proposal for a Massachusetts Cyber Corps

The Michigan Cyber Civilian Corps (MiC3) "is a group of trained, civilian technical experts who individually volunteer to provide rapid response assistance to the State of Michigan in the event of a critical cyber incident." [45] The Corps is composed of IT professionals who already hold certain IT and security certifications, and participate in additional training regarding the nuances of working in the public sector in particular. MiC3 operates with an annual budget of $300,000 and as of 2020 included 50 volunteer participants, with the goal of scaling up to 200 participants [9].

Massachusetts is one of the most well-educated states in the country, with over 416,300 people working in the technology industry [20]. A Massachusetts Cyber Corps could serve to bolster the cybersecurity readiness of the state's municipalities and increase engagement of residents with their own local communities. Members of such a Corps could help municipalities implement effective specific cybersecurity interventions, such as the development of explicit cyber incident response plans, and the implementation of IT best practices such as multi-factor authentication. A Massachusetts Cyber Corps could be a part of a well-rounded and comprehensive municipal cybersecurity capacity building effort. Within the MCDIP framework, I recommend that priority access to such a Massachusetts Cyber Corps be given to municipalities who pledge to enroll in the MDCIP, with further priority given to smaller and lower-resourced municipalities.

(b) Parallel to the MAPC Technical Assistance Program

Another example of a model for state-level agencies providing technical assistance to municipalities beyond simply redirection to resources is the Metropolitan Area Planning Council Technical Assistance Program (MAPC TAP). TAP

provides assistance to municipalities and regional entities within the greater Boston Area with regional and environmental planning problems [21]. The District Local Technical Assistance program (DLTA) within TAP works to expand municipal capacity by providing funding and technical expert consulting on planning issues for local governments. The Massachusetts Cyber Corps could serve as a DLTA-like program spearheaded by the MassCyberCenter to be the nexus for the careful implementation of proven measures for improving municipal cybersecurity posture throughout the state's communities.

(c) Creating an educational pipeline for municipal cybersecurity leadership
Massachusetts is home to fifteen Community Colleges; these institutions are critical in providing job training and upward mobility for thousands of Commonwealth residents. Community college graduates contribute significantly to the vitality of Massachusetts' economy [54]. Several IT professionals interviewed over the course of this project expressed concern over difficulties hiring qualified technology professionals into municipal government, given that salaries for government positions are generally lower than similar positions in industry. A partnership between the MassCyberCenter and the Massachusetts Association of Community Colleges to offer mechanisms to earn well-regarded cybersecurity certifications especially in underserved areas could serve as a mean to increase the pipeline of graduates ready to engage in work with municipalities, either in permanent town government positions or in volunteer positions such as in the aforementioned proposed Massachusetts Cyber Civilian Corps.

4.5.3 Infrastructure Coordination

Another space where state agencies such as the MassCyberCenter are uniquely well-positioned to assist municipalities in meeting their cybersecurity goals is in the development of coordinated infrastructure projects involving multiple municipalities.

As mentioned earlier, an existing example of such coordination is the Municipal Interlocal Insurance Association (MIIA), a member service of the Massachusetts Municipal Association (MMA). MIIA provides several different types of insurance, including cyber insurance, at a discounted rate to Massachusetts municipalities.

I propose a broadening of cybersecurity services offered by the MassCyberCenter to Massachusetts municipalities, both in terms of expert labor through a Regional CISO program, as well as in terms of technical services, in the form of a Massachusetts Shared Technical Services program.

1. Regional CISO Program

   Many Massachusetts municipalities employ very few IT professionals. The 2020 MMA Municipal Cybersecurity Survey found that out of 76 respondents, 15 municipalities employed 0 IT professionals and 41 employed 1 to 2 IT professionals. The cost of a Chief Information Security Officer (CISO) is likely prohibitive for all but the most well-resourced municipalities. A system of regional-level cybersecurity professionals who could provide assistance to municipalities in a specific region and be their point of connection to resources in the Commonwealth would greatly assist in the development of a coherent cybersecurity strategy for public entities and would further connect municipalities with the MCDIP.

   I recommend that the idea of regional CISOs be explored for Massachusetts, in particular as it pertains to assisting municipalities with meeting cybersecurity goals. The key responsibilities of regional CISOs should include:

   (a) Serving as a central point of contact to state and federal cybersecurity and IT resources, including organizing MCDIP recruitment, enrollment, recertification, and verification processes

   (b) Coordinating information and threat sharing between municipalities (e.g administering municipal MS-ISAC nodes)

   (c) Providing one-on-one assistance to municipalities in evaluating their cybersecurity postures, proposing concrete actions for improvements, and regularly checking on progress

Given the fact that the Department of Homeland Security State Homeland Security Program grants (SHSP) are administered in Massachusetts through four already-existing Regional Advisory Councils, I propose that the regional CISOs would also be based within those Councils.

The idea of a Regional CISO program seems to be gaining traction within Massachusetts; as of late October 2021, the MAPC put out a Request for Proposal for a Regional CISO Feasibility Study [22]; I am therefore optimistic that this model may be implemented within the next few years and provide direct assistance to Massachusetts municipalities in meeting cybersecurity goals.

Parallels in other states to the regional CISO program idea include the Cyber Navigator Program in Illinois and the Michigan CISO as a Service pilot program. The Cyber Navigator Program in Illinois, which focuses on deploying cybersecurity professionals to local Election Authorities to conduct election security oriented goals, reached all 108 election authorities in Illinois in 2020 employing the services of eight Cyber Navigators [32]. The Michigan CISO as a Service Program aims to help municipalities and counties that cannot afford the expense of a full-time CISO by splitting CISO time between multiple different organizations. The pilot CISO-as-a-Service program underway in Michigan has shown early positive results in engaging harder-to-reach municipalities [40].

2. Shared Technical Services

   A way of enabling municipalities, especially lower-resource municipalities, to reach cybersecurity milestones, could be for the state to provide more ready-to-use technical solutions.

   An example of shared technical services provided to municipalities by a state agency comes from the Texas Department of Information Resources (DIR). Texas DIR administers a program known as Shared Technology Services (STS), essentially managing a contracting program for local governments to access technical services. Two subprograms of interest within STS are the Data Center Services (DCS) program and the Managed Security Services (MSS) program [57]. Several distinct cybersecurity

services are provided through the STS, including services that address some of the core controls prioritized by the RRI and NIST frameworks - incident response planning, endpoint detection and firewall services.

Eligible entities for the Shared Technology Services program include not only local governments, but also state agencies, public institutions of higher education, and public school districts. In addition, the Texas DIR administers a free cybersecurity assessment program for state agencies and public institutions of higher learning only (local governments are not eligible)[57].

I recommend that the MassCyberCenter utilize SCRAM data about cyber-related losses to identify specific cybersecurity services that would be most beneficial to facilitate for municipalities, with discounts or preferential provision for municipalities committed to engaging in the MCDIP.

4.6 Existing and Emerging Sources of Funding

The proposed investments in municipal cybersecurity capacity building will require sustained funding streams. In this section, I review existing sources of funding that may be applicable, as well as emerging funding sources.

4.6.1 Department of Homeland Security State Homeland Security Program (SHSP)

The State Homeland Security Program (SHSP) is a grant program administered by the Department of Homeland Security (DHS) designed to increase security preparedness at the state and local level. As of Fiscal Year 2021, DHS designated cybersecurity as a National Priority Area, and as such directed that 7.5% of all SHSP grants must be spent on cybersecurity. Massachusetts received $6,731,000 in SHSP grants in FY20 [43], leaving approximately $500,000 specifically set aside for cybersecurity spending. SHSP grants within Massachusetts are administered by the four Regional Advisory Councils covering the state, including the Northeast, Southeast, Central, and Western regions [60].

4.6.2 Infrastructure Investment and Jobs Act Funding

The Infrastructure Investment and Jobs Act (Infrastructure Investment and Jobs Act, 2021), signed into law by President Biden on November 15th, 2021 [47], will deliver at least $15.7 million for cybersecurity and infrastructure resilience in Massachusetts (Beckwith, 2021). Some of this investment could be directed towards the programs introduced above.

A variety of other federal programs at the federal level also provide funding dedicated to fighting cybercrime [34], though it is unlikely that that funding could be redirected from its current uses.

4.6.3 Prioritizing Funding for Data-Driven Cybersecurity Initiatives

In order for cybersecurity to truly become a Commonwealth priority, the state legislature and governor's office must make a renewed commitment to appropriately fund evidence-based resources and systems for municipalities. The new, data-driven and self-improving cybersecurity policy approach described in this report is an opportunity for Massachusetts to lead the way in quelling the rash of municipal cyberattacks and setting municipalities on a better course.

Chapter 5

Conclusion

This thesis explores the challenge of lowering cyber risk for municipalities and other entities in the public sector. Using a case study of Massachusetts, this thesis proposes a novel mechanism for correcting mis-aligned incentives with regards to municipal cybersecurity and providing data-driven, effective resources to help municipalities meet their cybersecurity goals.

This work calls for action at the state level and coordination among stakeholders to implement policy with a large potential for positive results. Massachusetts has an opportunity to become a trailblazer in rethinking cybersecurity policy for the public sector and constructive cooperation between state governments and local governments to achieve a shared goal.

Beyond this case study of Massachusetts, I see broad applicability of the continuous measured improvement idea to cybersecurity policy for other states and local governments. There are 50 states and 35,879 local government entities in the United States alone [52], and our review of the status quo and existing scholarship shows no coherent and effective cybersecurity policy in this space to date.

Appendix A

Minimum Baseline of Cybersecurity for Municipalities

This link contains an archive of the MassCyberCenter Minimum Baseline of Cybersecurity for Municipalities.

Appendix B

MIT Cybersecurity Clinic / MassCyberCenter Research Proposal

This link archives a copy of the original research proposal between the MIT Cybersecurity Clinic and the MassCyberCenter on the Minimum Baseline of Cybersecurity for Municipalities, agreed upon by both parties in January 2021.

Appendix C

Massachusetts Municipalities Minimum Baseline Interview Questionaire

This link archives a copy of the questionaire for the Massachusestts Municipalities Minimum Baseline Interviews.

Bibliography

[1] Exec. Order No. 14028, 2021.

[2] Federal Emergency Management Agency. Community Rating System Coordinators Manual, 2017. URL: https://www.fema.gov/sites/default/files/documents/fema_community-rating-system_coordinators-manual_2017.pdf.

[3] Federal Emergency Management Agency. Laws and Regulations, 2021. URL: https://www.fema.gov/flood-insurance/rules-legislation/laws.

[4] Federal Emergency Management Agency. Local Government Officials - Floodplain Management Resources, 2021. URL: https://www.fema.gov/floodplain-management/manage-risk/local.

[5] American Hospital Association. H-ISAC TLP White Threat Bulletin: White House Memo to Protect Against The Threat of Ransomware , June 2021. URL: https://www.aha.org/h-isac-reports/2021-06-03-h-isac-tlp-white-threat-bulletin-white-house-memo-protect-against-threat.

[6] Massachusetts Interlocal Insurance Association. About MIIA. URL: https://www.emiia.org/about.

[7] Massachusetts Municipal Association. Municipal Cybersecurity Survey. 2020.

[8] National Governors Association. Memo on State Cybersecurity Strategies. Technical report, 2016. URL: https://www.nga.org/center/publications/memo-on-state-cybersecurity-strategies/.

[9] National Governors Association. Building A Civilian Cyber Corps, 2020. URL: https://www.nga.org/wp-content/uploads/2020/05/MiC3-Memo.pdf.

[10] National Governors Association, National Conference of State Legislatures, and Center for Information Security. Managing Cyber Threats through Effective Governance: A Call to Action for Governors and State Legislatures. Technical report, October 2020.

[11] Geoff Beckwith. Cybersecurity and IT investments emerge as key priorities, 2021. URL: https://www.mma.org/advocacy/cybersecurity-and-it-investments-emerge-as-key-priorities/.

[12] Jonathan Berr. "WannaCry" ransomware attack losses could reach $4 billion. *CBSNews*, May 2017. URL: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[13] Leo de Castro, Andrew W. Lo, Taylor Reynolds, Fransisca Susan, Vinod Vaikuntanathan, Daniel J. Weitzner, and Nicolas Zhang. SCRAM: A Platform for Securely Measuring Cyber Risk. *Harvard Data Science Review*, July 2020. doi: 10.1162/99608f92.b4bb506a.

[14] Massachusetts Cybersecurity Center. About MassCyberCenter, 2021. URL: https://masscybercenter.org/about-masscybercenter.

[15] Massachusetts Cybersecurity Center. Minimum Baseline of Cybersecurity for Municipalities, 2021. URL: https://masscybercenter.org/municipalities/minimum-baseline-cybersecurity-municipalities.

[16] Massachusetts Cybersecurity Center. Municipal Cybersecurity Toolkit, 2021. URL: https://masscybercenter.org/municipalities.

[17] Massachusetts Cybersecurity Center. Response Plans Materials, 2021. URL: https://masscybercenter.org/Response-Plan-Materials.

[18] CISA. Ransomware Guide, September 2020. URL: https://www.cisa.gov/stopransomware/ransomware-guide.

[19] Federal Trade Commission. ftc strengthens security safeguards for consumer financial information following widespread data breaches, October.

[20] CompTIA. Tech Employment in Massachusetts Grows by 11,500 Net New Jobs, 2020. URL: https://www.comptia.org/newsroom/2020/04/21/tech-employment-in-massachusetts-grows-by-11-500-net-new-jobs.

[21] Metropolitan Area Planning Council. Funding Opportunities, 2021. URL: https://www.mapc.org/about-mapc/funding-opportunities/.

[22] Metropolitan Area Planning Council. Legal Notice of Request for Proposals for Regional CISO Feasibility Study, 2021. URL: https://www.mapc.org/wp-content/uploads/2021/09/SWFT20-Regional-CISO-Feasibility-Study-Legal-Notice.pdf.

[23] Deloitte and National Association of State Chief Information Officers. 2018 Deloitte-NASCIO Cybersecurity Study - States at Risk: Bold Plays for Change. Technical report, 2018. URL: https://www.nascio.org/resource-center/

resources/2018-deloitte-nascio-cybersecurity-study-states-at-risk-bold-plays-for-change/.

[24] Deloitte and National Association of State Chief Information Officers. 2020 Deloitte-NASCIO Cybersecurity Study - States at Risk: The Cybersecurity Imperative in Uncertain Times. Technical report, 2020. URL: https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf.

[25] Operational Services Division. Contract User Guide for ITS78 ITS78: Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services, 2021. URL: https://www.mass.gov/doc/its78/download.

[26] Ian Duncan. Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts. 05 2019. URL: https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-.

[27] EOTSS. apply for the municipal cybersecurity awareness grant program.

[28] EOTSS. All Office of Municipal and School Technology (OMST) Programs, 2021. URL: https://www.mass.gov/info-details/all-office-of-municipal-and-school-technology-omst-programs.

[29] EOTSS. Executive Office of Technology Services and Security | Mass.gov, 2021. URL: https://www.mass.gov/orgs/executive-office-of-technology-services-and-security.

[30] Center for Internet Security. Multi-State Information Sharing and Analysis Center, 2018. URL: https://www.cisecurity.org/ms-isac/.

[31] Institute for Security and Technology. Ransomware Task Force Report: Combatting Ransomware. Technical report, 2021. URL: https://securityandtechnology.org/ransomwaretaskforce/report/.

[32] Adam Ford. Launching the Cyber Navigator Program in Illinois, April 2021. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-spring-2021-government-spotlight.

[33] Benjamin Freed. Ransomware Attacks Map chronicles a growing threat. 10 2019. URL: https://statescoop.com/ransomware-attacks-map-state-local-government/.

[34] Michael Garcia. Follow the Money: Few Federal Grants are Used to Fight Cybercrime, February 2021. URL: https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime.

[35] Dan Goodin. Advisories: "Brazen" Russian ransomware hackers target hundreds of US hospitals. October 2020. URL: https://arstechnica.com/information-technology/2020/10/us-government-warns-of-imminent-ransomware-attacks-against-hospitals/.

[36] Dan Goodin. Shortages loom as ransomware hamstrings the world's biggest meat producer. June 2021. URL: https://arstechnica.com/gadgets/2021/06/ransomware-striking-.

[37] John Gramlich. Municipal Bankruptcy Explained: What it Means to File for Chapter 9, url = https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2011/11/22/municipal-bankruptcy-explained-what-it-means-to-file-for-chapter-9, November 2011.

[38] Andy Greenburg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. August 2018. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[39] Jonathan Gruber. *Public Finance And Public Policy*. Worth Pub, 2021.

[40] Calvin Hennick. Michigan's CISO as a Service Boosts Local Cybersecurity, 2020. URL: https://statetechmagazine.com/article/2020/04/michigans-ciso-service-boosts-local-cybersecurity.

[41] International Risk Management Institute. Moral Hazard | Insurance Glossary Definition, 2020. URL: https://www.irmi.com/term/insurance-definitions/moral-hazard.

[42] KnowBe4. The Economic Impact of Cyber Attacks on Municipalities, 2020. URL: https://info.knowbe4.com/economic-impact-of-cyber-attacks-municipalities.

[43] Grants Office LLC. State Homeland Security Program (SHSP) (Massachusetts), 2020. URL: https://www.homelandsecuritygrants.info/GrantDetails.aspx?gid=17084.

[44] C. McFarland, B. Rivett, K. Funk, R. Kim, and S. Wagner. State and Local Partnerships for Cybersecurity: A State-by-State Analysis. Technical report, 2020. URL: https://www.nlc.org/wp-content/uploads/2020/04/SML_2020Report_web-1.pdf.

[45] Michigan Department of Technology, Management, and Budget. Michigan Cyber Civilian Corps (MiC3), 2021. URL: https://www.michigan.gov/dtmb/0,5552,7-358-82548_78404_78419-389506--,00.html.

[46] Sara Morrison. What the Colonial pipeline ransomware attack means for gas prices. May 2021. URL: https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

[47] Brian Naylor and Deirdre Walsh. Biden signs the $1 trillion bipartisan infrastructure bill into law. *NPR*, November 2021. URL: https://www.npr.org/2021/11/15/1055841358/biden-signs-1t-bipartisan-infrastructure-bill-into-law.

[48] NIST. Cybersecurity Framework, July 2019. URL: https://www.nist.gov/cyberframework.

[49] Donald Norris. A Look at Local Government Cybersecurity in 2020, 2021. URL: https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020.

[50] Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin. Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, 79:895–904, February 2019. doi:10.1111/puar.13028.

[51] Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin. Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, pages 1–23, April 2020. doi:10.1080/07352166.2020.1727295.

[52] National League of Cities. Cities 101 — Number of Local Governments, December 2016. URL: https://www.nlc.org/resource/cities-101-number-of-local-governments/.

[53] Coalition of City Chief Information Security Officers. Global Community of City CISOs, 2021. URL: https://cityciso.org/about-us.

[54] Massachusetts Association of Community Colleges. Fast Facts, August 2020. URL: https://masscc.org/fast-facts/.

[55] Office of Consumer Affairs and Business Regulation. 201 CMR 17: Standards for the protection of personal information of residents of the Commonwealth, 2009. URL: https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the.

[56] The Council of Economic Advisors. The Cost of Malicious Cyber Activity to the U.S. Economy, 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[57] Texas Department of Information Resources. Shared Technology Services, 2021. URL: https://dir.texas.gov/shared-technology-services.

[58] National Association of Insurance Commissioners. Flood Insurance/National Flood Insurance Program (NFIP), 2021.

URL: https://content.naic.org/cipr_topics/topic_flood_insurancenational_flood_insurance_program_nfip.htm.

[59] National Association of Insurance Commissioners. Report on the Cybersecurity Insurance Market. Technical report, 2021. URL: https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf.

[60] Commonwealth of Massachusetts. Homeland Security Grants, 2021. URL: https://www.mass.gov/service-details/homeland-security-grants.

[61] National Association of State Chief Information Officers. The Responsive State CIO: Connecting to the Customer. Technical report, 2019. URL: https://www.nascio.org/resource-center/resources/the-2019-state-cio-survey/.

[62] National Conference of State Legislatures. Security Breach Notification Laws, 2018. URL: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[63] Benjamin Preis and Lawrence Susskind. Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review*, page 107808742097376, November 2020. doi:10.1177/1078087420973760.

[64] IBM X-Force Incident Response and Intelligent Services. Cybersecurity for State and Local Governments: Protecting Public Infrastructure. Technical report, 2019.

[65] Lucas Ropek. Over a Month On, Baltimore Still Grappling with Hack Fallout. June 2019. URL: https://www.govtech.com/security/Over-a-Month-On-Baltimore-Still-Grappling-with-Hack-Fallout.html.

[66] Microsoft Security. Microsoft Digital Defense Report. Technical report, 2021. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report.

[67] Rebecca L. Spiewak, Taylor W. Reynolds, and Daniel J. Weitzner. Ransomware Readiness Index: A Proposal to Measure Current Preparedness and Progress Over Time. Technical report, September 2021. URL: https://dspace.mit.edu/handle/1721.1/132615.

[68] Reuters Staff. Atlanta officials reveal worsening effects of cyber attack. *Reuters*, June 2018. URL: https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M.

[69] Attorney's General Municipal Law Unit. Municipal Law Review, 2021. URL: https://www.mass.gov/municipal-law-review.

[70] Meredith Ward and Maggie Brunner. Stronger Together: State and Local Cybersecurity Collaboration. Technical report. URL: https://www.nga.org/wp-con-tent/uploads/2020/01/NASCIO_NGAStatesLocalCollaboration.pdf.