Local Government Cybersecurity:
How Michigan Counties Cope with Cyber Threats

by

Marilu F. Duque

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
(Information)
in the University of Michigan
2021

Thesis Committee:

Assistant Professor Florian Schaub, Chair
Clinical Assistant Professor Sol Bermann
Executive Fellow Edward Happ

marilud@umich.edu

Dedication

This thesis is dedicated to Mami and Papi, my lifelong cheerleaders, whose consistent love and support encouraged me to pursue my dreams, wherever they may take me. I promise to keep making you proud.

Thank you to my thesis advisor Dr. Florian Schaub for being super cool and guiding my evolving thesis topic over the past year.

In hopes that this work will one day contribute to the advancement of U.S. local government cybersecurity research, this thesis is dedicated to this country's public sector cybersecurity workforce, whose passion and commitment to service inspire me to constantly keep learning.

I dedicate this thesis to myself because, boy, was this a lot of work.

Acknowledgments

Throughout the research and writing of this thesis, I received tremendous support from local Michigan governments, professors, friends, and family.

I would first like to thank the Michigan counties interviewed and Michigan Cyber Partners, without whom I would not have been able to conduct this critical research. Their interest in this study, openness in sharing their network, and kindness throughout this process meant the absolute world to me.

I would also like to thank my MTOP faculty advisor, Dr. Florian Schaub, whose security & privacy research expertise provided invaluable advice in formulating my research questions and choosing the appropriate methodology. Your insightful feedback challenged my perceptions of the cybersecurity landscape and empowered my abilities to pursue academic research.

I would also like to acknowledge my committee members, Edward Happ, for introducing me to technology and crisis management research and Sol Bermann for his time and energy throughout the thesis defense process.

I would also like to thank my fellow UMichigan Security Privacy Interaction Lab (SPILab) members for their unwavering support, spicy memes (a welcome distraction), and fascinating Zoom meetings.

Finally, I could not have completed this thesis without the support of my parents. Thank you, Mami y Papi, for always being there for me and understanding the hectic research schedule of a graduate student. Los Amo!

Table of Contents

List of Tables & Appendices

Abstract

In the age of global interconnectedness, we can all be equally affected by cyberattacks. Given the evolving nature of threat landscapes, comprehensive and preemptive practices are needed now more than ever to keep local government and citizen data secure. According to Recorded Future, in 2019, local U.S. government infrastructure was targeted by ransomware attacks 100 times. Cyber threats to local government systems have been increasing exponentially over the last several years, and the frequency of attacks will only continue to grow.

Although cyberattacks on local government entities are rising every year, the challenges county IT departments face in combating the thousands of yearly attacks remains largely unexamined. This research study aims to understand how Michigan counties are currently protecting their IT systems, define the challenges they face in improving their cybersecurity posture, and address the potential improvements regarding current cybersecurity practices. This thesis addresses these goals through semi-structured interviews and a post-interview questionnaire with local government IT leaders across the State of Michigan. The results of this research study found challenges local Michigan governments face in enhancing their county's culture of cybersecurity, operating with limited funding and support, and inability to properly utilize state resources due to limited staffing needed to operationalize. A surprising finding was learning how essential communication and relationship building are to cybersecurity and how these relationships impact the culture of cybersecurity in an organization. By identifying these challenges, policymakers can introduce evidence-based policies that will address the essential needs of local Michigan counties and provide actionable and implementable solutions. Additionally, it will enable researchers and cybersecurity professionals to develop recommendations and mitigating solutions to improve local Michigan government cybersecurity.

Keywords: local government, cybersecurity, culture of security, Michigan, phishing, ransomware, data breach

Chapter 1
Introduction

In the age of global interconnectedness, everyone can be equally affected by cyberattacks. Given the evolving nature of threat landscapes, comprehensive and preemptive practices are needed now more than ever to keep local government and citizen data secure. According to Recorded Future, in 2019 [32], local U.S. government infrastructure was targeted by ransomware attacks 100 times. Cyber threats to local government systems have been increasing exponentially over the last several years, and the frequency of attacks will only continue to grow. The 2017 U.S. Census of Governments [2] states there are currently ~90,000 total local government units serving residents across the country. These local governments collect, process, and store a vast amount of personally identifiable information (PII) such as full names, addresses, social security numbers (SSN), birth dates, voter registration information, driver's license numbers, as well as other information, including court records, and business filings. Securing government systems is essential because nefarious actors could use them for malicious purposes, leaving millions of residents at risk for future cyber crimes and attacks. Gaining access to these systems leaves local governments vulnerable to service disruptions on industrial control systems (ICS) for public infrastructure (i.e., water, gas, electrical), gives unauthorized users the ability to falsify police records and gain access to residents PII. According to Recorded Future [16], compromised government databases can be a highly lucrative business for cybercriminals who sell/use the information to gain access to networks, perform attacks, and monitor desktops remotely.

Local governments are already coming face to face with such challenges. For example, in 2013, Maricopa County in Arizona experienced a data breach that impacted over 2 million people due to the improper repair of an earlier breach in 2011 [22]. The county was later notified that Maricopa residents' stolen data was being sold online. This breach resulted in many class-action lawsuits for violation of the Federal Education Privacy Rights Act (FERPA), as a large portion of the counties' breached data belonged to local students. Other lawsuits included those in violation of the Driver's Privacy Protection Act (DPPA) due to breach and mishandling of PII, including Social Security numbers and banking information. Overall, this breach cost taxpayers over $26 Million to settle lawsuits, notify those impacted, credit monitoring, upgrade computer systems and address the breach itself. Such cyber-attacks have also reached Michigan local governments; according to the U.S. Department of Justice (DOJ) [75], in 2017, a Ypsilanti, MI man conducted a phishing attack on Washtenaw county employees to gain access to and control their computer networks. In doing so, he gained access to over 1,600 individuals PII, including past and present Washtenaw county employees. Additionally, he accessed the county jail records in hopes of altering the release date of an inmate. Although this attack was eventually thwarted and the hacker was arrested, the attack cost taxpayers over $235,000. Local governments are already struggling to keep up with the evolving nature of cyber threats, and these challenges will only continue to grow.

The consequences of cyberattacks on local government databases extend past the overall cost to repair and into the personal lives of those affected. The Identity Theft Resource Center's 2019 End of Year Data Breach Report [4] concluded that once PII has been breached, "the likelihood of identity theft increases" with actions being taken such as social media account hacks and bank and SSN fraud. This means that the individuals involved in a breach have added risk pertaining to not only their social lives but extensive economic impact. The Maricopa and Washtenaw County breaches are a clear example of some of the significant consequences that occur when local government computer security is not adequately protected and left vulnerable to malicious actors.

Currently, academic research in local government, cybersecurity, and policy fields is limited, especially those pertaining specifically to the State of Michigan, and the few published papers belong to a handful of researchers. By pursuing this line of research, we are better able to assess the various set of challenges local U.S. governments might face in ensuring cybersecurity and cater solutions specificity to their broad needs or organizations. Additionally, the focal point has often been on urban localities rather than a broad look at suburban and rural localities. The cybersecurity capabilities of larger counties in Michigan like Wayne county, with a population of ~1.74 Million [51], may be vastly different from smaller counties like Schoolcraft County, with a population of ~8,000 [51]. By researching a broader range of counties' capabilities, we can better assess the varying needs of IT departments and understand the different approaches they might require in ensuring cyber safety. In this thesis, I explore the current cybersecurity practices of fourteen participating Michigan county IT departments to include urban, suburban, and rural counties, and understand the challenges they face in improving their overall cybersecurity posture.

In collaborating with local government cybersecurity leaders to pursue this line of research, we can more cohesively identify processes that are currently working well within the various Michigan counties' IT departments and what could be improved. This research can positively impact public sector security goals in gaining the exposure and resources needed to ensure cyber protections for all constituents.

1.1 Research Goals

This study aims to understand the existing capabilities and challenges local Michigan governments face in protecting their IT systems. This thesis discusses issues at the nexus of local government resources, cybersecurity threats, and local, state, and federal policy. Research findings will help add to the limited body of academic work about the study of cybersecurity practices in local U.S. governments. The findings of this research aim to inform policymakers and elected officials on areas of improvement to guide future recommendations for local governments on improving their cybersecurity posture.

1.2 Research Questions

RQ1: How are local Michigan governments currently protecting their governmental systems from cyber threats? (e.g., Cyber risk assessments, hiring practices, security resources, information sharing)

RQ2: What challenges are counties facing in improving their cybersecurity posture?

RQ3: What are some potential opportunities for improvements that can be made regarding current cybersecurity practices?

I explore these research questions through fourteen semi-structured interviews of county-wide IT department leaders within the state of Michigan. These research components involve learning about the current cybersecurity practices in the counties interviewed, challenges they face, and improvements they need to meet department goals.

1.3 Key Findings

Throughout this research study, three central themes emerged that showcase the current state of local Michigan government cybersecurity practices and their challenges in ensuring cybersecurity. First is the importance of an enhanced culture of cybersecurity within local governments. To improve a county's cybersecurity posture, all Michigan local government employees and leaders need to make security a personal priority and adopt an organizational security mindset. Secondly is the need for an increase in funding and staffing across local Michigan county IT departments. Providing local Michigan counties with the needed cybersecurity resources will enable them to overcome any future challenges they might encounter in the cyber domain. Lastly, counties need more guidance on operationalizing existing local government resources as they do not have the time or the staff to implement those resources. IT departments are constantly forced to postpone cybersecurity projects, which will eventually cause them to become a victim of a successful cyberattack.

1.4 Overview of Thesis Chapters

This thesis presents a research study with the goal of understanding the challenges local Michigan government IT departments face in improving their cybersecurity posture. “Chapter 1: Introduction” establishes the importance of researching local government cybersecurity through detailed accounts of recent cyberattacks on municipalities, presents the research goals, questions and findings. “Chapter 2: Related Work” gives background into the field of cybersecurity, state of cybersecurity within local U.S. government and international communities, as well as cyber threats they face. “Chapter 3: Background” provides information as to the various aspects of cybersecurity specific to the state of Michigan to familiarize the reader with the state’s cybersecurity landscape. “Chapter 4: Research Design and Methods” details the study’s protocol, participant recruitment procedure, interview protocol, post-interview questionnaire, data analysis process, and limitations of this research in hopes of understanding the challenges Michigan local governments face in securing their IT systems. “Chapter 5: Key Findings” details the study’s research results by notable themes. “Chapter 6: Discussion” addresses the key findings, includes critical recommendations for local Michigan government cybersecurity practices, and details future work in this field. “Chapter 7: Conclusion” concludes the implications of the findings and summarizes the thesis. Lastly, the Appendix and Bibliography include all the research material and references mentioned throughout the thesis.

Chapter 2
Related Work

In this chapter, I discuss related work about the increasing need for qualitative and/or mixed-methods research in the field of cybersecurity. I also present related work as to ongoing cyber threats, and the current security landscape of local U.S. government cybersecurity practices, by examining academic and industry literature. Lastly, I present related work on how international communities address similar concerns and effectively bolster their cybersecurity posture.

2.1 Field of Cybersecurity

Craigen et al. [11] defines *cybersecurity* as the "organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Essentially, cybersecurity protects the property of its system users from potential manipulation and or unauthorized access. To ensure these protections of its users, security practitioners apply the Confidentiality, Integrity, and Availability (CIA) [69] Triad. The CIA Triad is the model that governs the information and cybersecurity fields, developed to help people understand its various moving parts. Confidentiality refers to the protection of sensitive information from unauthorized access. Integrity refers to preventing the modification of information, intentional or otherwise, by users, authorized or unauthorized. Integrity is key to maintaining consistency of information across an organization and holding users accountable for any changes made on a system. Availability ensures that authorized users can have timely access to a system and its resources when needed. By understanding this fundamental model, we can assess potential threats in whichever manner they may come, technical or otherwise. Organizations that apply the CIA Triad to their operational environment are better able to provide a smooth and secure user experience.

Cybersecurity has both technical components and extends to human decision-making processes. It is important to understand that the guiding model ensures protections across the security and information landscapes. By applying the CIA Triad, we can curate user-centric security training, create incident response plans, and implement quality security policies [69]. Utilizing the CIA Triad, organizations can "avoid the consequences that may come along by not understanding it [69]." This model can be violated in various ways, from direct attacks on a system to network reconnaissance and even human error. Many tools have been developed as countermeasures for the more technical element of system failures. However, less development has focused on protecting against the human element and even more so on the convergence of these two elements. This thesis focuses its research on applying qualitative methods to the quantitative field of cybersecurity to better understand the multitude of aspects, technical and non-technical, that impact a local government's ability to ensure cybersecurity protections.

According to Fujs et al. [24], applying qualitative methods, in this case, interviews, to cybersecurity research can often provide "deeper insight than sampling that resembles random sampling in quantitative methods." By utilizing qualitative methods, we can examine how security practitioners tackle cybersecurity challenges in their organization and their thoughts on the topics covered in this thesis's interview protocol. Technologies are developed to aid people in their everyday lives, not hinder their everyday processes. Taking a qualitative approach to a quantitative subject will allow for closer examination of existing challenges in bolstering a local government's cybersecurity posture, organizational security culture and "enable usable, livable, and inclusive cybersecurity [61]."

2.2 State of Local U.S. Government Cybersecurity

Although cyberattacks on local government entities are rising every year, the challenges county IT departments face in combating the thousands of yearly attacks remains largely unexamined. This gap in scholarly literature has been noted by Norris et al., who, in 2020, conducted the first nationwide survey of local government cybersecurity, stating research in this field is "the subject of few systematic studies [19]." They examined the current state of cybersecurity in local U.S. governments and produced baseline data for future research in this field. This study found that although local government computer systems "are under constant cyberattack [19]," it is the human element of cybersecurity that is their biggest challenge. They proposed the application of theories that help explain "why one set of governments might appear to have better cyber-outcomes than another." One of the suggested theories is the political science theory of incrementalism [26], which holds that no one person will hold all the information needed to make a rational decision and thoroughly address all problems because the problems themselves are not fully defined. By hearing from a wide variety of IT department leaders across the state of Michigan, we can identify the pain points local governments face in the cybersecurity space and amalgamate potential solutions. The theory of incrementalism "has been applied successfully to understand the adoption, use, and impacts of both IT and e-government among local governments [19]." Incrementalism inspired the interview questions for this research in which I asked participants about their frequency of cybersecurity training, overall improvements they have seen in their departments, and open-ended questions about cyber incidents their department has faced. This research paper covered challenges within local government cybersecurity such as "insufficient funding and staffing; problems of governance; and insufficient or under-enforced cybersecurity policies [19]," but did not thoroughly examine the roles and relationships between the end-user, IT department, and county leaders and how that impacts the organization's culture of cybersecurity.

Organizations like the International City/County Management Association (ICMA) have produced industry research relating to the cybersecurity policies and regulations local governments have to prevent them from attacks. Their 2017 research report "Cybersecurity: Protecting Local Government Digital Resources" [19] describes findings from a nationwide cybersecurity survey of the IT managers within local governments to identify the challenges they face in bettering current practices. This survey found that local governments want more situational awareness on the cyber threat landscape, as 41% of the local U.S. governments surveyed do not know how often they experience breaches and, 27.6% do not know the frequency or type of attacks that are targeting them. These troubling percentages dictated the interview questions regarding identifying the root cause and frequency of attacks allowing for comparisons between their survey and my own. Survey results also found that additional funding, better security policies, and awareness amongst local government employees were needed to ensure their systems. Moreover, their data showed subpar levels of cybersecurity awareness and support among key local government personnel. To ensure enhanced cybersecurity protections for organizations, there must be support given and action taken from those in leadership positions. ICMA proposed measures to improve security, both technical and cultural, to include updated hardware, software, and better employee training. Ultimately, this report shed light on the problems a broad number of local government units face but was not specific to the difference in challenges that local government might face by state.

Local government leadership, particularly elected officials, are elected to serve their constituents, so they often balance between what needs to be done and what constituents want. Macmanus et al. examined the stressors put on public officials to "balance privacy protection and transparency in cybersecurity policymaking [33]." Researchers surveyed Florida county government officials, which identified the pressure officials face in protecting a variety of citizens' data such as medical records, finances, and employee information. They found that local government leaders are experiencing considerable cross-pressures "to be more transparent and, at the same time, to be more attentive to securing data that might threaten individual privacy rights [33]." These often conflicting demands are becoming even harder to balance within cybersecurity as "fear of cyberattacks, even among small localities, is a growing concern" due to an increase in "retaliation-driven cyberattacks" on public sector employees who have "resisted requests to release information because of privacy-related rules and regulations [33]. The results recommend an increase in funding, training, software, and clearer standards to promote a balance between privacy and cybersecurity. These findings gave insight into the balancing act local government officials often have to perform in dealing with "budgetary constraints" and "political pressure" [33] to meet the demands of various stakeholders and budgetary decisions.

The kind of awareness needed to advance cybersecurity protections in local government is not simply a leadership stance but requires a shift in the organization's culture towards cybersecurity. According to Norris et al. [44], this shift in culture to understand the need for excellent cybersecurity practices would require the participation of all stakeholders, including elected officials. Their participation would include consistent and adequate training, practice, and accountability when standards are not met. According to Eminağaoğlu et al., cybersecurity training and ongoing awareness campaigns are "one of the most effective and powerful mechanisms for mitigating information security risks [20]." One of Norris et al.'s participants noted that "it is about being aggressive, not passive, toward cybersecurity," which requires an aggressive cultural shift. The more awareness and support an organization has for cybersecurity, the stronger its posture. This emphasis on organizational culture illuminated some potentially non-technical challenges that local Michigan counties could be facing in bettering their cybersecurity posture and thus enhanced my research questions.

According to a 2018 report by FireEye [28], by emphasizing the importance of cybersecurity before an incident occurs and being proactive in their search for malicious threats, organizations will reduce detection time and future costs of incident response. FireEye's research shows that within the federal government, the most successful cybersecurity tools are the ones that improve the speed of response and identify a wide range of potential risks. This report shows a growing need for government entities to improve the speed of response to minimize cyber risk to their constituents' data.

In 2017, the State of Illinois released a Cybersecurity Strategy [64] report discussing the executable strategy and five listed goals focused on making Illinois one of the most cyber-secure states in the U.S. Their goals include protecting their CIA Triad and cyber-resiliency to deliver critical services to its citizens, reduce cyber risk by increasing cyber awareness, improving cyber capabilities, creation of enterprise-level cybersecurity programs, and establishing themselves as a leader in cybersecurity through partnerships with the public and private sectors. This report helped understand the various steps and defining strategies state government actors can take to protect their constituents. Some of these strategies include "an evaluation of current capabilities, cybersecurity maturity and risk assessments, input from leadership from state agencies, boards and commissions and evaluation of the current and evolving cyber threat landscape [64]." Moreover, the report addressed its threat context, including protecting citizens, critical infrastructure, the economy, innovation, and health services. By addressing their goals and potential outcomes, citizens can better understand how their state government is protecting their rights in cyberspace. Publicly providing clear information about the steps the government is taking to safeguard constituents helps build trust and a culture of cybersecurity between users and the government. Additionally, it provided details about their plans in applying cyber risk management frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was created in collaboration with the public and private sectors [43]. This framework consists of "standards, guidelines, and practices to promote the protection of critical infrastructure [43]." Due to its flexible, repeatable, and cost-effective approach, local governments would find this framework valuable in assessing cyber risk and prioritizing tasks needed to implement system improvements. Other state and local government entities are also applying the NIST Cybersecurity Framework to self-assess their cyber risk. Some of these entities include Contra Costa County (C.A.) Employment & Human Services Department, Florida Agency for State Technology, City of Houston, and the Texas Department of Information Resources [66]. Overall, this report allows for greater accessibility in holding policymakers and government officials accountable for their listed goals in protecting Illinois residents while providing information on actionable frameworks to implement in an organization. Applying similar measures in Michigan focused on appropriate risk management and holding officials accountable may lead to a more developed culture of cybersecurity.

Regardless of frameworks and policies in place, to protect residents to the caliber equal to the rise in cyberattacks, local governments need more resources. According to Norris et al. [44], "insufficient funding and staffing" are one of the barriers that local governments face "in providing high levels of cybersecurity" and accordingly lack the budget or staffing needed to secure the data. Specifically, this disparity affects smaller communities due to their inherent smaller budget from population size and the vast differences in budget allocation across U.S. states. Due to insufficient funding, local governments are often forced to find alternative means of handling I.T. and security operations, generally by outsourcing contractors. According to Norris et al. [44], one county in their focus group reported that they were running 90% on cloud computing infrastructure, which involves transferring "much of the responsibility of securing the data and services to the cloud service providers for whom it is a central part of their business." Other participants also stated they were starting "to view cybersecurity as a commodity or a service that they purchase on the market" rather than something integral to their in-house I.T. operations. This is mainly due to perceived cost-saving measures and the lessening of responsibilities on small departments.

Moreover, the culture of cybersecurity within local government organizations, and its effect on limited budgeting for cybersecurity, make low-income communities (often rural) adversely vulnerable to security risks. In the U.S., the total amount of money a local government has to allocate across their departments depends on their yearly revenue [68], which comes from licenses, businesses, and taxes. Essentially, the less revenue a local government makes, the less money they have to allocate across departments. If organizations are cyber unaware, they will not allocate as much funding towards the cybersecurity budget. Additionally, this disadvantages cybersecurity because the base costs of protecting systems are high regardless of the amount of data and constituents being protected. However, costs are even higher during and in the aftermath of a cyber incident. According to KnowBe4 [70], in ransomware attacks between 2017 and 2020, the estimated ransom paid per cyberattack on a municipality was ~$125,000. These cyber-attacks can cost local governments thousands of dollars, but that is only the beginning, as recovery efforts can range anywhere from a few hundred thousand to millions of dollars. These high costs are due to required recovery measures, including victim notification, credit monitoring, and the possibility of lawsuits, as well as regulatory penalties, insurance premium increases, data recovery, audits, system updates and/or replacements, and disruption of operations [23]. Low-resourced communities who are already strapped for funds cannot afford to be impacted in this way, especially when lower-cost preventative cybersecurity measures could be in place. This also personally leaves constituents in these low-resource communities at much greater risk for cybercrimes, such as identity theft [73], if their local government IT systems were breached. These communities, who are already facing socioeconomic inequality, will feel the additional emotional, psychological, and economic effects of their local governments' low cybersecurity posture. These lower-income communities face the same cyber challenges, namely on a smaller scale, as other communities, but with a small percentage of their budget. Cybercriminals are starting to realize how easy it is to gain access to these under-protected systems, which is why we have seen a rise in ransomware attacks in recent years. According to Barracuda Networks [60], in 2019, 45% of municipalities attacked had populations of less than 50,000, and 24% had less than 15,000, while 16% of municipalities had populations over 300,000. Due to a lack of funding, technology, and resources, smaller communities are much more vulnerable to various cyberattacks. These attacks on local government systems are an ongoing and pervasive threat that is only increasing in frequency and becoming more coordinated. By understanding the challenges counties of varying populations face in the cyber domain and the scale of these challenges, we can recommend potential solutions for a specific population and improve their cybersecurity.

2.3 Cyber Threats on Local Governments

In recent years, local governments have faced an increase in the number of cyberattacks targeted at their systems. For this research, cyber incidents and/or attacks are defined as “a security event that compromises the integrity, confidentiality or availability of an information asset [5].” According to a 2018 report by Deloitte and the National Association of State Chief Information Officers (NASCIO) [3], the top threats governments face include phishing and ransomware. Phishing is a social engineering method “used to bypass technical controls implemented to mitigate security risks in information systems [52].” According to PhishLabs, phishing attacks are the “number 1 cause of data breaches [58]” with stolen credentials being the second. As users are generally the “weakest link in the security chain [29],” this method exploits human decision-making processes to gain access to a targeted system [52]. Ransomware is “a type of malware (malicious software)...[which] attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid,” generally through a cryptocurrency, such as Bitcoin [21]. Apart from these cyberattacks causing undue stress on an organization, they also contribute significantly to the economic challenges in the aftermath of a cyberattack on an organization.

Cybercriminals do not take a day off, even during a global crisis. During the COVID-19 pandemic, they have taken advantage of every opportunity afforded to them during this crisis by disseminating a wide range of cyberattacks across organizations. These cybercriminals have targeted critical national infrastructure (CNI), such as healthcare services and ICS systems, worldwide. One of these cyber events of the past year (2020) includes a ransomware attack on University Hospital Düsseldorf [53] which comprised the hospital’s digital infrastructure and forced them to turn patients away. This limitation in hospital capacity resulted in the death of a woman suffering from an aortic aneurysm in which her ambulance was diverted to a hospital further away [53]. This incident showcases the critical relationship cybersecurity has with physical industries such as healthcare and the need to strengthen those relationships. Another cyber incident of note is the February 2021 system breach of a water treatment plant in Oldsmar, Florida, in which an unauthorized user “boosted the level of sodium hydroxide—or lye—in the water supply to 100 times higher than normal [7].” Although this breach was thwarted by an employee using the organization’s computer system, it very well could have resulted in poisoning some 15,000 residents in the Tampa Bay area. After this incident, leaders in the water supply space have stated that this incident has opened their eyes to the connections between public health and the cybersecurity of their systems [7]. Incident officials say that their goal is to constantly stay ahead of cybercriminals and that it's a constant game of cat and mouse [7]. Unfortunately, according to Pew Charitable Trusts, many "local governments that run water systems lack the money or the personnel to strengthen cybersecurity [7]." U.S. local governments do not have the resources to keep up with the growing demands needed to ensure their cybersecurity.

According to Lallie et al. [31], as a result of such attacks, the U.K's National Cyber Security Centre (NCSC) and the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory report dictating the ways cybercriminals have been exploiting the COVID-19 pandemic. Some of the mentioned exploitations include "phishing, malware and communications platforms (e.g., Zoom, Microsoft Teams) compromise." These cyber-threats have been exacerbated due to the decentralized nature (i.e., remote workforce/teleworking) of organizations during the pandemic. This abrupt switch to a remote workforce has made training and protecting users from possible cyberattacks and responding appropriately an increasingly tricky process due to suggested social distancing [63]. According to a study by Georgiadou et al. [25], not only do experienced technology users report phishing, ransomware, and spyware violations, but 53% of participants reported not receiving any cybersecurity guidelines from their employers regarding teleworking during the COVID-19 pandemic. A survey by Barracuda Networks [59] reports that 51% of respondents state an "increase in email phishing attacks since shifting to a remote working model" and do not feel adequately trained to handle the cyber risks associated with this shift. Additionally, 40% of respondents organizations "have cut their cybersecurity budgets as a cost-saving measure to help tackle the COVID-19 crisis." Both of these survey findings show an evident lack of cyber readiness in transitioning safely to a remote working environment, which gives cybercriminals more entry points to take advantage of users and their organizations. Cyberattacks are a 24/7 365 days a year phenomenon, so organizations must always be prepared for any attempts to wreak havoc on their IT systems. These findings help us understand how the future working environment will continue to shift in years to come and give insights into challenges local governments will face in ensuring their cybersecurity posture evolves with this shift.

Apart from re-centralizing an organization’s workforce, local governments can bolster their cybersecurity posture by embracing a culture of cybersecurity. According to a 2019 report by the U.S. Census Bureau [1], local governments are the largest part of the government in employing 14.2 million workers compared to the 5.5 million state government employees. This means that local government employees must reach a high caliber of cyber awareness as they are the ones on the front lines of our nation’s IT systems and cybersecurity. Some steps local governments can take include following best practices as indicated by the cybersecurity industry, using secure video conferencing, implementing two-factor authentication, backing up and encrypting data, create and follow incident response plans, ensure adequate funding and tools, and establish a culture of cybersecurity across the county [34]. By focusing part of this research study on understanding the current cybersecurity practices of Michigan counties, we can recommend additional best practices and methods to address the challenges they face in bolstering their cybersecurity posture.

Chapter 3
Background

In this chapter, I provide background information about Michigan's current state of cybersecurity operations, resources, and support. To better illustrate the state's cybersecurity landscape, I present Cybersecurity in the State of Michigan and Recent Michigan Cybersecurity Incidents.

3.1 Cybersecurity in the State of Michigan

The State of Michigan has been increasing its state-sponsored initiatives to bolster cybersecurity across the state. Some of these initiatives include creating five organizations focused on addressing various cybersecurity threats and challenges across the state. First is the Michigan Cyber Security (MCS) [14], which handles information security concerns for the State of Michigan and is managed by the Department of Technology, Management, and Budget (DTMB). Second is the Michigan Cyber Civilian Corps (MiC3) [37] is made up of civilian technical experts who volunteer their time to “provide rapid response assistance to the State of Michigan, [all levels of government], in the event of a critical cyber incident [37].” DTMB also manages MiC3. The third is the Michigan Cyber Command Center (MC3) [38] which is operated by the Michigan State Police, whose aim is to coordinate cybersecurity-related events, mainly focused on “emergency response during critical cyber incidents [38].” The fourth is Michigan’s National Guard, which combines the efforts of “Michigan’s Army Cyber Protection Team and Air National Guard’s Cyber Squadron [13]” to defend “against the cybersecurity threats targeting our state and nation [13].” Lastly, are the Michigan Cyber Partners (MCP) [40], which is a collaboration between various state entities including MCS, MC3, and other “local public entities across Michigan [aimed at] strengthen[ing], improv[ing], and promot[ing] cybersecurity resources and best practices [40].” MCP brings together county and local governments IT leadership from across Michigan and provides a means for county and local governments to share information regarding cyber threats and best practices. Currently, MCP is pursuing projects helping local public entities improve their cybersecurity posture through the adoption of “the Securing Your Organization Cybersecurity Framework “and use one of their ten “pre-approved vendors to conduct a Cybersecurity Assessment [40].” At present, MCP is partnered with the aforementioned organizations as well as others, including, but not limited to, CISA, mentioned in Chapter 2, Michigan Government Management Information Sciences (MI-GMIS) [27], and the Multi-State Information Sharing and Analysis Center (MS-ISAC) [41]. MI-GMIS is an organization aimed at “developing professional relationships among public sector peers” while also promoting “educational opportunities that enhance public sector IT leaders’ knowledge, skills and abilities [27].” The MS-ISAC, part of the Center for Internet Security (CIS) [41], works to “improve the overall cybersecurity posture of the nation’s state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery [41].” Organizations such as MI-GMIS and MS-ISAC operate as beacons for IT leaders in the state of Michigan to share current challenges, gain potential solutions, share resources, and stay abreast of cyber threats.

According to a 2020 report by the National League of Cities (NLC) [35], Michigan continues to be at the “forefront of developing an effective cybersecurity ecosystem model,” which implements “innovative solutions to educate government employees on cybersecurity protection measures [35].” Moreover, Michigan is one of the twenty-two states that offers voluntary, but not mandatory, “cybersecurity training programs for state employees [35]” which include “online cybersecurity training videos, toolkits and in-person classes through partnerships with post-secondary education institutions [35].” Currently, this training is only “offered to state-level government employees, [but] Michigan’s state government has collaborated with local partners” to expand such resources to local government employees across the state. One of these partnerships was a collaboration between five Michigan counties which resulted in the “development of CySAFE, a free IT security assessment tool [35].” CySAFE aims to “help small and mid-sized governments assess, understand and prioritize their basic IT security needs [39].” Initiatives such as those mentioned in this section inform technology users about the “urgency of complex cybersecurity issues” and helps local governments “develop effective cybersecurity measures to prepare for potential cyber threats [35].”

One of these more policy-focused initiatives includes the introduction of S. 1846 - State and Local Government Cybersecurity Act (SLGCA) of 2019, which was a “unanimously approved bipartisan legislation [56]” introduced by Senators Gary Peters (Michigan) and Rob Portman (Ohio). This act promotes “stronger cybersecurity coordination between the Department of Homeland Security (DHS) and state and local governments [57]" by sharing information and resources to help state and local governments "prevent and recover from cyber-attacks [57]." This act authorizes the DHS National Cybersecurity and Communications Integration Center (NCCIC) to continue providing "assistance to state and local governments [10]" while requiring the hiring of "additional cybersecurity advisors, deploying sensors to nonfederal networks, and sharing [of] classified information [10]." Specifically, they expect the implementation of this act to include, "on average, 15 full-time [cybersecurity] employees in each year beginning in 2020, at an average annual rate of about $150,000 per employee [10]." Overall, the Congressional Budget Office (CBO) "estimates that enacting S. 1846 would cost $31 Million over the 2019-2024 period [10]." The SLGCA Act passed the Senate in November 2019 but has not moved since then [49].

In support of expanding cybersecurity initiatives across Michigan, Governor Whitmers state executive budget for Fiscal Years (FY) 2021-2022 included the adaptation of a One-Time $20 Million Investment for Advanced Persistent Cyber Threats "to mitigate cyber threats from entities that are hostile to the State of Michigan [72]." This budget specific to cybersecurity will "be used to support a number of measures, including emergency response, threat intelligence, and vulnerability assessments that will enhance protections for Michigan's critical information technology infrastructure [72]." This added investment is a stark increase from FY 2020-2021, which did not include any added provisions for enhanced cybersecurity measures [71].

3.2 Recent Michigan Cybersecurity Incidents

Cyberattacks are a constant and ever-growing threat, especially those targeting government systems. Chris Derusha, Chief Security Officer for the State of Michigan, has stated that "Michigan firewalls repel over 90 million potentially malicious probes and actions every day [17]." This section details a few recent cyberattacks in the State of Michigan since the beginning of 2021.

On January 22nd [47], Flagstar Bancorp, a bank headquartered in Michigan, fell victim to a breach caused by a zero-day vulnerability found in a File Transfer Appliance (FTA) software owned by Accellion, Inc. Flagstar Bancorp states they "acted immediately to contain the threat and have engaged a team of third-party forensic experts to investigate [6]," and reassured that networks such as core banking and mortgage systems were not affected. To mitigate this incident, they informed customers of the cyber incident in March and have offered them free credit monitoring services.

On January 23rd, Mott Community College identified a data security breach where an unauthorized user had “obtained access to its systems between November 27th and January 9th [30].” Some of the acquired files contain information regarding “name, date of birth and dental plan enrollment, along with claims information related to individuals who were enrolled in Mott Community College’s self-insured dental plan between 2014-2015 and in 2019 [30].” Mott Community College has since then addressed the breach and notified individuals whose information was accessed.

Total Health Care experienced a data breach between December 16th, 2020, and February 5th, 2021, involving “unauthorized access to several employee email accounts [47].” Some of the email accounts contained PII relating to company employees and partners, such as “may have included your Social Security number and/or member ID, claims information or your name, date of birth, and address [47].” In recovering from this breach, Total Health Care notified those affected, hired security personnel to assess best practices, and is “offering free credit monitoring for up to two years [47].

In February, Saginaw Township Community Schools fell victim to a ransomware attack that “infected the district’s computer network [8].” Investigators do not “believe any data was stolen by the hackers [8].” The schools’ computer systems were back to normal within the week.

In March, the Troy School District’s website was overtaken by a hacking group who posted this message on the schools’ website: “Good evening Troy School District! All the sites connected to your district have been hacked [74].” Additionally, they posted “racial, religious and gay” slurs, which forced “the district to take down its site temporarily [74].” This hack came from outside the U.S. “using a known malicious IP address [74].” Luckily, no student information or PII was compromised by this hack. To mitigate this attack, the school district has reset its passwords.

These recent cyber events serve to inform about the diverse nature of cyberattacks that can occur within a single location (U.S. State) and in a short amount of time (January - March 2021). Noting these events can help future researchers track trends in analyzing the type of cyberattack, frequency, target, location, and mitigation strategies to conduct cyber threat analysis and better understand how cyber threats are evolving in a given region. For example, the cyberattacks detailed above mainly target the financial, academic, and healthcare sectors, and a majority had some data breach. This information could suggest that within the State of Michigan, the aforementioned sectors are more prone to data breaches than other forms of cyberattacks. Understanding the demographics of a cyberattack is crucial to conducting an effective cyber threat analysis that guides IT leaders' management of resources to prevent future attacks.

Chapter 4
Research Design and Methods

In this chapter, I present the methods and practices utilized to conduct this research study. I describe the overall study protocol, participant recruitment procedure, interview and questionnaire process, data analysis approach, and limitations.

4.1 Study Protocol

In this research study, I apply qualitative methods and exploratory analysis to understand the existing capabilities and challenges local governments face in ensuring cyber safety. The methods applied include semi-structured interviews combined with a post-interview questionnaire with IT department leaders across counties in the State of Michigan to understand how those on the frontlines handle cybersecurity incidents. Using semi-structured interviews, I identified central themes amongst county IT departments related to cyber threats, practices, and resources needed to bolster their cybersecurity posture.

To best analyze the challenges local Michigan governments face in ensuring their systems, interview questions were designed to understand the various moving parts of an IT department. These moving parts included questions regarding their user base training, department employee composition (job roles, training, background), technical cyber threats, department strategies, and state legislation awareness. Similar questions were reiterated during the post-interview questionnaire to gain deeper knowledge on specific areas.

Fourteen interviews were conducted virtually using the video communication platform, Zoom. Interviews were recorded and transcribed for later analysis. All interviews ranged between thirty to sixty minutes in length. The study was determined to be exempt from oversight by the University of Michigan's Institutional Review Board (IRB).

4.2 Participant Recruitment

I recruited employees who held leadership roles within Michigan county IT departments. For this study, I define a leader in this space by their job title, ranking, and/or decision-making abilities within their organization. Understanding their thought process as well as success and challenges would add context to the study. By interviewing these professionals, we get a better understanding of what it means to combat cyber threats in a local government setting.

Recruitment was conducted by aggregating all 83 Michigan county web page URLs from the state of Michigan's director of counties [36]. I searched through each web page and looked for the IT department's contact information (email or phone number) and added it to a document. If no IT department page or contact information existed, I gathered either the county clerk's contact information or saved the link for the general county contact form. Once the appropriate contact information was acquired, I contacted the various IT departments and/or county clerks to gauge interest in participating in this research study. The main form of contacting the departments was done through email. The email recruitment message is available in Appendix 1.

I used Google Calendar to set up a sixty-minute time block for the virtual interview for those wanting to participate. Twenty-four hours before the interview, I emailed the participants a consent form to read and verbally consent to participate at the beginning of the interview. The consent form is available in Appendix 2.

4.3 Interview Protocol

An interview protocol with six themed sections was created to guide the semi-structured interview with participants.

The first section of questions focused on assessing the overall cybersecurity literacy of general county employees, actions taken to enhance literacy, and understanding changes that can be made to improve cyber safety. These questions were asked to gain perspective on the macro-level cybersecurity practices in the county and assess the limitations and resources needed to enhance practices for both technical and non-technical staff.

The second section of questions was focused on gaining a micro-level understanding of the IT department's overall team composition and existing roles and responsibilities. I asked participants about discerning between cybersecurity-focused staff or IT generalists, job hiring requirements, and cybersecurity responsibilities. This question was asked to get an idea as to the makeup of a county IT department and ascertain how much of a county's human capital is dedicated to cybersecurity.

The third section of questions dives deeper into the technical cyber incident threats their department is facing. Topics covered the classification of cybersecurity incidents, examples of past incidents handled, strategies, overall rating of cybersecurity posture, and current department priorities. One of the questions asked participants to describe a successful/unsuccessful cyber incident they have faced, which helped us understand what resources, steps, and practices were crucial to the outcome. The overall section is used to assess the technical needs of the departments that could yield more conducive results in future cyber incidents. The NIST Cybersecurity framework inspired these questions to identify an organization's level of cybersecurity preparedness.

The fourth section of questions focused on local, state, and federal policy and compliance awareness and opinions on existing and/or proposed Michigan-specific cybersecurity policy. These questions were asked to gain participants' awareness of the current landscape of cybersecurity policy and gain their professional opinions on the usefulness and ability to implement the proposed policy.

The fifth section of questions asked about staffing, security goals, and resources need to improve cybersecurity posture. These questions were asked to solidify the main pain points cybersecurity leaders in these counties are facing. This section helped in summarizing and having a clear understanding of the challenges previously stated throughout the interview.

The sixth section of questions was asked if time allowed and consisted of an open question focused on gaining perspective on lessons these cybersecurity professionals have learned throughout the years. This question was asked to gain a personal perspective, understanding challenges they have faced in the field and how they overcame them. This question can often lead to more personal stories regarding their role in the departments and professional history, which could enrich our knowledge of how IT department leadership operates.

Throughout the six interview sections, the question of resources and challenges is asked multiple times to gauge the varying resources needed as per the section's theme. The full interview protocol is available in Appendix 3.

4.4 Post-Interview Questionnaire

After participants have been interviewed, they completed an exit questionnaire, hosted by Qualtrics, with additional questions regarding their thoughts on their organization's readiness to handle cyber threats. This helped assess what systems these IT departments are responsible for, their cyber incident handling process, technical tools they use, and changes made to their process due to COVID-19. By asking these questions through a survey after the interview, we can spend the interview ascertaining opinions on greater cybersecurity topics while still gathering more detailed and comparable information about their organization afterward. Additionally, these post-interview questions can help jog the memory of some details that might have been missed during the interview and provide rich complementary data. The post-interview questionnaire content is available in Appendix 4.

4.5 Data Analysis

The recording of each interview was saved to the cloud and transcribed by Zoom's transcription tool. Once the interviews have been transcribed, they were downloaded from the cloud, verified, and corrected for clarity by the researcher. Any corrections made were done in conjunction with examining the researchers' notes and rewatching the interview recordings. Each separate transcript was imported to Google Docs and color-coded to differentiate between interview questions and the participants' responses. Within Google Docs, quotes were flagged by their corresponding interview questions. Tangential discussions relating to the participant's experience in the cybersecurity field and opinions on various matters were also noted.

The analysis of the post-interview questionnaire took a similar approach to that of the interview. A codebook was developed with the transcripts and post-interview questionnaire data, which were combined in a Google Sheets file to track emerging themes and aid in its overall analysis. Within the Google Sheet, the post-interview questionnaire and each interview section (six sections) had their tabs with corresponding coded data. The open coding took an inductive approach to understand the main themes present throughout the data. In this process, I developed the codes based on the studies set research questions and themes that emerged throughout the various interviews. This data analysis approach is used to pinpoint specific cybersecurity-centric pain points common across Michigan local governments.

Towards the beginning of the coding process, themes generally revolve around the main interview questions, but as coding progressed, it was clear that sub-themes had emerged. Although interview questions were mainly separated by technical vs. non-technical aspects of cybersecurity, the coding process revealed a convergence of these themes. The responses to the non-technical questions foreshadowed the responses for the technical questions, and thus these themes are dependent on one another. The assumed themes at the beginning of this research had evolved as the coding process continued.

4.6 Limitations

The limitations of this research can be evaluated in three ways, access to potential participants, the use of self-reported data, and limited academic research in this field.

Unless you are well connected within the tight-knit community of local government employees, it can be challenging to identify the right people to contact regarding research participation. I resorted to cold contacting potential participants through emails found on each of the Michigan counties' websites. This limitation resulted in a small pool of participants with 13/83 Michigan counties represented and a total of 14 interviews conducted. In emailing all potential participants, a total of 18 counties responded. Those that declined to participate noted not being interested or not considering themselves applicable for the research study due to lack of cybersecurity knowledge and/or outsourcing their IT operations. Participation rates could also have been affected due to the current COVID-19 pandemic. In a sense, the migration to Work From Home (WFH) has been beneficial as I could interview participants in the further regions of Michigan. On the limiting side, because everything has been virtual for the past year, potential participants could be experiencing "Zoom Fatigue [54]," and thus are overwhelmed with the number of virtual meetings they have to attend and do not have the mental bandwidth to meet for this study. This limitation would contribute to having a limited pool of data for which to analyze.

Due to the nature of this study, the data accumulated is largely self-reported by the participant. I did not examine their departmental budgets or observe their day-to-day organizational operations, so I relied on the participants to share this information. Factors such as interpretation of questions, rating scales, self-assessability, and response bias, can add limitations to the data.

As mentioned in Chapter 2, academic research on the nature of local government cybersecurity and its various aspects is limited and thus a contributing limitation in this research study. Future research in this field is needed to better assess the factors that go into a local government's cybersecurity posture.

Chapter 5
Findings

This chapter presents the research findings from our analysis of the interviews and questionnaire. I include a Sample Characterization and the various themes that emerged in coding and analyzing the interview data from the six interview sections and the post-interview questionnaire. The main themes include Michigan's Cyber Threat Landscape, Jack of All Trades, Vendor Relationships, It's Not a Bug, It's a Feature: Culture of Cybersecurity, Operationalizing Resources for Local Governments, Impact of COVID-19, Challenges Faced in Smaller Michigan Counties, and Recruiting Talent.

5.1 Sample Characterization

This research study included 14 interviews with cybersecurity leaders in local governments, 13 currently working for different county IT departments around the State of Michigan and one state cyber-focused organization representative with previous work experience in local government. Excluding the state representative, this study includes counties with populations ranging from a min of 9 thousand and a max of 1 million. The mean population amongst the counties is ~317,000, and the median being ~750,000. 7/10 regions in Michigan are represented in this sample, including the Upper Peninsula, Northwest, West Michigan, East Michigan, Southwest, Southeast, and Detroit Metro Prosperity Region [65].

The median number of years participants have spent in their current role is 9.5 years with a min of 1.5 years, a max of 20 years, and a mean of 10. Job titles ranged from team lead to the director, clerk, manager, and Chief Information Security Officer (CISO). Their previous related experiences range from working at other local governments, federal cybersecurity positions, private sector consulting, business leaders, computer programming, network administration, and teaching.

Regarding department demographics, the median county IT department size is six people on staff, with a min of 0, max of 250, and mean of 30. Additionally, participants were asked if they had anyone focused on cybersecurity or if their staff were generalists focused on broader IT needs. Excluding the state representative, two counties stated they had at least one person explicitly focused on cybersecurity, and 11 indicated their staff are more generalists and thus shared cybersecurity responsibilities. Notably, the only two counties with staff explicitly focused on cybersecurity have the largest populations in this research sample.

For the purposes of this thesis, each participant will be labeled with an identifier, P1-P14. A summary of the sample characterization is detailed in Table 1 below.

Total Interviews	14
County Population Range	~9,000 - 1 Million
County Population Mean	~317,000
County Population Median	~750,000
% of Michigan Regions Represented	70%
Range of years participants have spent in their current role	1.5 - 20 Years
Mean # of years participants have spent in their current role	10 Years
Median # of years participants have spent in their current role	9.5 Years
IT Department Staff Size Range	0 - 250 People
IT Department Staff Size Mean	30
IT Department Staff Size Median	6

Table 1: Sample Characterization Summary

5.2 Michigan's Cyber Threat Landscape

The key points mentioned in this section about the county's cyber threat landscape pertain to the daily threats aimed at their IT systems, their cybersecurity posture rating, technical tools used to combat these cyber threats, and current department priorities.

Counties are subjected to spyware/malware, drive-by downloads attacks, and unpatched software vulnerabilities, but the most common daily threat targeting their organization are phishing attacks. When participants were asked about a time when assessing a potential cyber incident was beyond their current capacity, one participant detailed an event where they were "really worried that something had gotten in" when "somebody clicked on a link that should not have gotten through our spam filter." (p5) They continued, stating that the threat "had to do with a zero-day flaw," which had symptoms of being malware which "was a concern right away" due to potential "lateral [movement] between machines." (p5) The threat turned out to be "more of a tracking" or spyware threat and was mitigated with the expertise of organizations like MSP and MS-ISAC who are "always really good about coming up with [steps to] try this, check this, run this." (p5)

I asked participants to rate their county's overall cybersecurity posture on a scale from 1-10, one being the lowest and 10 being the highest. The average amongst the 14 interviews was a 5.8/10 rating, with some participants noting that they "don't think anybody's at a 10" or ever will be; "it's just a matter of when [they will be attacked], how serious and how we respond." (p6) This finding is consistent with other statements regarding county IT systems being subject to daily cyber threats. One participant noted that "it's a daily process and it's a daily struggle" (p9) to keep up with the never-ending threat landscape. Based on the types of threats, frequency of cyber incidents, and the 5.8/10 rating above, there is a need for county IT departments to stay abreast of any potential threats and continuously improve their cybersecurity posture.

While interviewing participants about the technical tools they use in day-to-day threat monitoring operations, most respondents noted utilizing commercial Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) tools, with few incorporating open source technologies such as Snort. One participant also stated having "reporting tools in place… to protect the endpoints tools [and]...the servers tools." (p2) A majority of respondents also stated they become aware of cyber incidents by receiving notifications from threat monitoring tools such as Varonis, various "log aggregation" (p13) software, and other undisclosed tools. Some counties are also currently trying to incorporate some built in-house tools for their "reporting and [threat monitoring] dashboards." (p13) They also utilize services from vendors that alert them to "a workstation that's really infected or if there's unwarranted traffic" (p13) in their network as well as handle any "incident management [and] forensics" (p12) necessities after a breach. Inspection of data stored before and after a breach has been viewed favorably as participants have stated: "lacking better automatic controls" (p7) to aid in post-breach root cause analysis. Additionally, they noted not having the resources to conduct full root cause analysis due to running on "very old" (p2) and outdated systems or legacy technology, such as Windows Server 2003 and the now-defunct Windows XP operating system. At present, 43% of participants do not have the capability to conduct a root cause analysis post-cyber incident. They continued stating they are "working very hard this year to get rid of it" due to it being such a "huge security threat and until we get rid of it there's nothing we can do." (p2) Understanding the varied current technical tools departments across the state have incorporated into their daily operations, it is clear that tool usage is decentralized. There is a common need for updated technologies and direct guidance on reporting and monitoring tools that would not only improve their cybersecurity posture but be cost-effective to their budgets.

Moreover, participants expressed interest in incorporating new technologies, mainly those focused on using Artificial Intelligence (AI) and automating necessary cybersecurity processes. One participant states that applying the use of AI technologies in their cybersecurity operations applying threat monitoring and mitigation to act as "force multipliers" making them "stronger than we would be by ourselves." (p6) Essentially, by using AI to automate cybersecurity defense processes, they can free IT department staff from various tedious tasks. Hence, they have more time to focus on tackling more pressing challenges. Additionally, multiple participants mentioned wanting to automate inter-county security training and phishing exercises to enhance security awareness. One participant stated that "it would be nice to have more resources in place...better software" to automate security training "but it takes time to set that up." (p9) Another stated wanting to use automation to run random and consistent phishing "campaigns behind the scenes [which] gives the users...hopefully some good practical knowledge." (p3) One county is already applying similar automation techniques in which they automatically enroll employees in remedial security training when they "get caught in a phishing email, and they actually click on a link." (p6)

At the time of the research interviews, the top county cybersecurity priorities include various initiatives to bolster their cybersecurity posture, such as county-wide multi-factor authentication (MFA) implementation, attaining new tool resources, and updating/ implementing existing projects. The following priorities exclude those relating to the COVID-19 pandemic as those are covered in Section 5.7, Impact of COVID-19, below. Many counties noted wanting to “get everybody on MFA” (p6) and having that applied “on many more applications that it exists on currently.” (p12) One county is implementing MFA “based on risk levels” in which “higher risk groups have had MFA enabled initially, and then they work their way down the group.” (p6) Additionally, a majority of participants commented on wanting “more tools to help us monitor what’s going on better control better granular monitoring.” (p7) Currently, they are using “a lot of cobbled together low cost and free [applications] rather than built to purpose tools.” Due to the current state of their threat monitoring applications, they “can’t [appropriately] measure” and quantify the needed data and thus rely on “feeling” and intuition to ascertain threats. “Investment in additional infrastructure” as they do not have “as deep [and] as many layers as we would like [for] redundancy.” They need more people and “better tools, which cost money.” (p7) One participant also stated a “need [for] some kind of visibility tool, [like] a SIEM” as they “don’t have a core aggregation center for reviewing a lot it’s all manual it’s all human done, and since we don’t have a lot of human capital resources we’re trying to find a solution [to] that” (p8) as well. Additionally, counties are wanting to “roll out [the] NIST Cybersecurity Framework,” (p6) set up “remote access” (p11) through VPN’s, “refreshing our technical stack,” (p12), and move to a “zero-trust environment.” (p1)

In relation to the IT departments’ user base, their priorities lie within enhancing and “affecting the culture” (p1) of cybersecurity in their organization and expanded security awareness. Participants are hoping to implement “mandated security training for all of our users” (p7) as well as “continuing the momentum that we have with our security training...and making those results visible to our senior leaders” (p9) to aid in an increase for budgeting. Additionally, one participant stated they “have done a reasonable amount of [due] diligence for a local government to make sure that we protect all the data we’re supposed to” and jokingly noted their priority was to not “be the one who’s watched [on the news or in an] article on the open press... [stating] county residents identity [were] stolen right.” (p12) Interestingly, another county also noted that their “biggest goal is to stay out of the paper.” (p9)

At the state level, they are wanting to set a standard rating system for measuring a county's cybersecurity posture. Currently, counties measure their cybersecurity posture in several ways. Four follow methodologies and plans they created in-house, six utilize existing frameworks, including those suggested by state/federal organizations such as MCP's "Securing Your Organization [55]" framework, and four take a more laissez-faire approach in conducting self-assessments based on resource inventory, existing staff and cyber threats. To help mitigate potential confusion between rating scales, methodologies, and frameworks, the state is currently developing a "Cyber Incident Response" training, in partnership with the National Guard, in part to match up with the "National Cyber Incident Response Plan (NCIRP) [42]." (p14) The NCIRP incorporates the NIST Cybersecurity Framework discussed in Chapter 2 of this thesis. They hope that by standardizing their frameworks, they will be able to speak "the same language" (p14) and quickly assess the threat level a county is facing when calling in-state resources for a cyber incident.

Overall, the participants shared a wide range of priorities from technical requirements such as new tools and MFA implementation to user-centric priorities including cultural shifts and enhanced training. They also shared the vast complexities and challenges, including legacy tech, funding, and staffing, in reaching their goals of ensuring cyber protections for their constituents. The findings presented in this section provide evidence that IT department leaders are making steps towards operationalizing priorities not only for their technical operations but those which specifically inform and encourage their user base.

5.3 Jack Of All Trades

When participants were asked about their job roles in the department, responses revealed that most county IT department staff are generalists focused on broader IT needs rather than having someone solely focused on cybersecurity. One participant noted that they are "too small and serve too many customers to be able to specialize [in cybersecurity]." (P1) They noted that although some employees are interested in cybersecurity and try to foster that curiosity through additional training, they do not envision hiring solely security-focused staff unless there are massive changes in funding. Moreover, when asked if they were adequately staffed to meet security goals, 10 participants replied "No," two "Yes," one stated they completely contracted out their IT services but would like somebody in-house as well. One participant stated they would prefer to invest in more training for their existing staff.

Of note, the two participants who replied “Yes,” operate in higher populated counties of Michigan and have more staff than the other counties. Those that replied “No,” often noted not having the resources to hire, so they often opt to contract aspects of their jobs to a private vendor. Additionally, the participants who replied “No” noted that they are short-staffed by, on average, three people. This is one of the biggest challenges they face as they “do not have the budget for [a] cybersecurity expert.” (p2) This difference in budgeting is not equal across the various Michigan counties. One participant noted that larger counties “are doing [cybersecurity] better” because they have “bigger staffs [and] more money than we do.” (p2) This participant commented that when a county’s entire yearly budget is ~$5,000,000, there is minimal to no budget for cybersecurity or additional IT operations. About half of the participants noted that their budgets and/or access to new equipment have increased over the past 12 months. Still, this increase is not sufficient to tackle the wide range of projects and tasks they are charged with operating, such as “auditing” and compliance analysis to comply with “state [and] federal requirements.” (p3) These comments seem to provide evidence that not only are county IT departments underfunded and understaffed, but there is a significant problem with inequality amongst county IT budgets. This inequality in budgeting puts smaller populated counties at an extreme disadvantage in terms of cybersecurity protections as compared to larger populated counties.

Until changes can be made in regards to funding and staffing, employees must act as “jacks of all trades and master of none.” (p1) This means some of their job requirements can include anything from “desktop support” to “systems administrators,” “network administrators,” “cybersecurity analyst,” (p3) web developers, auditing support, and department leaders. As new technologies and regulations emerge, their job requirements must follow suit to learn and incorporate these changes. Employees have to keep “piling on the hats” (p3), which can be difficult because “you can only specialize in so many things[,] you can only stay [on] top [of] so many things,” as one participant noted (p3). Since departments are short-staffed, much of the staff’s time often has to go towards handling day-to-day operations like setting up computers and printers for their user base, making it “really hard to think about bigger cybersecurity.” (p4) Employees are being pulled in so many different directions, causing them not to focus on cybersecurity. One participant specifically stated that because of their numerous roles and responsibilities, which include monitoring of potential cyber threats, even when they go home for the day, it “always sits in the back of my mind, what could be going on right now” as there is “no one to compensate [for their absence] on-premise.” (p3) This participant’s IT department recently partnered with a Security Operations Center as a Service (SOCaaS) provider, which has since given them some level of comfort and peace of mind. SOCaaS providers are generally responsible 24/7 for “detecting, preventing, investigating, and responding to cyber threats [62]” across an organization’s network. Constant monitoring of threats is indispensable as participants have noted that they are in charge of not only their own departments’ systems but also (including but not limited to): Data Management, Public Work Projects, Waste Management, Record Keeping, Election Systems, Gun Registry, Board Meetings Notes, Circuit Court Records, Property Records, All County Departments, Local Business Registration Records, Budgeting, Accounts Payable, Payroll, Tax Base Information, County Website, Freedom of Information Data, 911 Dispatch, Law Enforcement Records, Jail Systems, Child Support Information, Land Management/Deeds, Public Health Data, Animal Control, Drain Systems, Youth Centers, and Emergency Management. To ensure cyber protections across the county, cybersecurity enhancement projects need to be well resourced and staffed. Based on the points raised by participants, it is clear that the various roles employees are responsible for are critical to the proper operation of a local government’s systems but are not currently being supported in a way that matches their criticality.

5.4 Vendor Relationships

12 out of the 14 departments interviewed currently employ third-party vendor(s) to handle anything from their complete IT department operations to various other tasks, including security training, phishing campaigns, incident response plan writing, threat monitoring, and general support. When one participant was asked about a time when assessing a potential cyber incident was beyond their current capacity, they detailed a vulnerability within one of their software applications (p1). By the time they were notified of the vulnerability and had updated patches, they found evidence that one computer had been compromised. In assessing the situation, they immediately called a support vendor to aid in triage and mitigation of any other potential cyber threats. This example of a cyber incident where a vendor could aid in threat

mitigation shows the critical role they play in supporting local government IT departments in areas where they are limited in either training, resources, or staffing.

While many participants noted that private vendors are one of the first sources they reach out to when faced with a cyber incident, they still face some challenges, mainly in finding the right vendor that is near their county and that they can trust. As per proximity to a county, participants noted their vendors' customer service and response rates varied across counties. Some vendors replied within half an hour; others took over four hours. One participant stated that by contracting out to vendors, even for simple tasks like copy machine upkeep, "you start to lose control, you start to lose the ability to respond effectively." (p5) The participant noted that county employees "hated it" because they had to wait hours for the appliance to be fixed when it could easily be done in 15 minutes. Additionally, they noted the wait times were inconsistent, ranging from two to four hours. These inconsistencies make them wary of the vendor market for added cybersecurity services because "the response time it's going to go down and that's going to be detrimental" (p5) to the department's security and risk management. When assessing a cyber incident, time can often work against them in trying to mitigate any potential harm to a system. Thus response time is a critical factor in a participant's choice of vendor. As per trust in vendors, this relates more to vendors who provide software applications; the most common example mentioned in these interviews are the SolarWinds [18] and Microsoft Exchange [48] hacks. Organizations, in both the public and private sectors, trust these large tech corporations to be at the forefront of security, but sometimes "stuff just happens." (p6) Incidents like this make organizations feel "powerless" as there is nothing they could do "as far as securing a supply chain for a major software vendors" which leads to "a lack of trust" (p3) with their software platforms. Local governments take on a mitigative and reactionary role rather than limiting a system's overall exposure to threats. An increase in these incidents makes organizations not only wary of vendors because they "come to find out that [they] may be no more secure than the next company" (p6) but also forces them to expand their threat monitoring landscape to include vulnerabilities from their vendors. Fortunately, MCP has already begun working on solutions for concerns local government's IT departments have in finding the right fit vendor.

5.5 It’s Not a Bug, It’s a Feature: Culture of Cybersecurity

This section presents findings relating to how a county’s culture of cybersecurity is shaped by the symbiotic relationships between IT departments, users, and organizational leadership. Currently, some IT departments feel that their county sees “security [as] an IT problem, not as a systemic issue that affects all” (p1) and requires everyone’s participation. The role of the IT department is to help support the county’s day-to-day operations. Still, one participant notes staff being “irritated with us” when trying to do their jobs and protect county systems from threats like malicious user activity. To help bridge the relationships between technical and non-technical employees, one participant notes “work[ing] hard to just build up a rapport to ensure that people know” they can “reach out to us” if they have any questions, often reminding them “there’s no such thing as a stupid question.” (p3) They continue to reassure fellow employees by doing “whatever we can to make the time,” (p3) to hear any worries they might have in operating their technologies. This community outreach has yielded positive results noting “a steady uptick in people reaching out” (p3) since their time in the department. This proactive communication between county employees leads to positive experiences in mitigating cyber threats from the users’ perspective. For example, one participant noted, “the good thing about our organization is the fact that if a user receives a weird email,” they immediately “send a helpdesk ticket asking us if it’s legit.” (p9) As depicted in the previous participants’ statements, a culture of cybersecurity helps elevate the level of communication between employees and aids IT departments in having a clearer picture of “what’s going on in the organization.” (p9) Through these comments, it is evident that county IT departments are going beyond their responsibilities in handling the county’s technologies and acting in a community outreach capacity to ensure counties employees feel comfortable asking any questions.

The relationship between users/employees and IT departments is significant as employees are essentially the first line of defense against cyber threats and vulnerabilities. When tasked with using technology to accomplish a task, users often “found a [novel] way to do something that they just couldn’t get an answer to before.” (p13) This new use case alerts IT departments to assess new applications and methods which are often “not secure” (p13) and/or previously vetted that other users could also be introducing to county IT systems. Due to the essential role users play in ensuring cyber safety, they must be as cyber aware as possible, which is why one county assigns security training to “anybody who interacts with us electronically.” (p12)

Currently, participants have noted that users in their counties often do not understand the importance of security training or the implications of breaches. One participant noted that “you can harp on things like backup[s] for example till you’re blue, and people will not get it until the first time” they are hacked, noting that it’s hard getting “people to realize how real some of these issues are because they do not see them and take them personally.” (p7) These experiences make it seem as though users do not often think about cybersecurity until a cyber incident impacts them personally. Additionally, IT departments have seen pushback in implementing cybersecurity training with county employees where it “wasn’t received well just because of the culture of the county” (p8) is used to more direct methods of training rather than a virtual platform. This participant noticed the pushback and pivoted to a method users were more accustomed to being taught, which is “old school standing up in a room somebody in front of them with slides,” but are now “looking to do online training program[s],” (p8) due to the constantly evolving nature of cyber threats, entry points, and their associated training. For example, two counties specifically mentioned one entry point being a clear target for cybercriminals: the payroll and/or HR departments. One participant stated that someone emailed payroll “saying that they were [an employee] and wanted their account number changed,” the department employee followed suit and made the changes. This employee fell victim to a social engineering attack which may have been mitigated if they had “training [which] would help with people identifying” (p10) trustworthy requests by other employees. One county stated that although employees were “apprehensive about taking the training at first,” eventually, the “spam training” became the biggest help and is “where we’ve seen the best improvement” (p5) in threat mitigation. Cybersecurity training has “raised their radar, as it were, to where they’re paying more attention even on their personal things…[where the county] has a program set up” to use at home” (p5) so now they can apply their new security skills to their family. Training users to have a security mindset is crucial because “you can put all the [technical] mechanisms in place..., but at the end of the day, it’s you and me the people behind the screens and on the keyboards and that education is the number one” (p11) priority organizations can implement to protect their systems.

Although cybersecurity training and software applications are good strategies to mitigate cyber incidents, a cultural shift is needed to improve a counties cybersecurity posture in the long term. This shift can only be implemented with actionable support from leadership within the local government, including department leaders and elected officials. One participant states they face challenges within the “cultural lens” (p1) of cybersecurity in their county. Often, they face pushback from “elected officials that pretty much answer to nobody, but the constituents” because if they “don’t like your security awareness [measures], then we sure as heck [are] not going to tell [their] people to do it.” (p1) This “decentralized leadership” (p1) structure brings added challenges in getting any cybersecurity measures implemented as well as added budgeting concerns. One county notes that “it can be a challenge to get the proper funding and resources to actually do basic things that the county needs and requires” (p8) to keep day-to-day operations running smoothly. They continue stating that their counties finance person is an elected official, “so while they have to go by certain guidelines...they can also do other things that we can’t necessarily control.” (p8) In the end, county employees end up demanding far more than “security can ever deliver, but they do not want to put their money where their mouth is” (p8) and provide the needed funding, staff, and overall support. These comments seem to provide evidence that IT department staff are facing pushback from not only users but leadership as well, and thus can lead to a negative perception and culture of cybersecurity. It could also be inferred that participants are struggling to make a convincing business case for increased cybersecurity support.

IT departments have tried a variety of ways to improve their counties’ culture of cybersecurity, such as a “publicity campaign [trying] to talk to elected officials and department heads...about the importance of security awareness” (p1) to include training and adoption of security practices such as Multi-Factor Authentication (MFA). When participating in these campaigns, the participant mentioned feeling like they are “talking to a brick wall,” and noticed their “eyes glazing over, they start looking at their phones, and they’re just not interested,” which is something they have “struggled with for years.” (p1) Some users even protested the use of MFA by demanding a “stipend or some sort of compensation for using their personally owned device...even though there was really no cost for the app.” (p1) Participants state that the “biggest barrier to [improving their] cybersecurity [posture] is [a needed] culture shift and the [existing] lack of ownership of the overall organizational security, at everybody’s level.” (p1) This could also suggest that participants are struggling to communicate the information in a way that resonates with employees and showcases how security could support their workflows.

Moreover, one participant stated that “cybersecurity awareness training and cybersecurity [in general] really only get a foothold if you have executive buy-in and support,” which is something they “have not really had up to this point.” (p13) Another participant noted that to improve the culture of cybersecurity, “it’s better to try to get buy-in from everyone involved, rather than try to force it on them by “deny[ing] them some access to something.” (p4) The participants’ previous experiences with leadership suggest that IT departments see buy-in from leadership as crucial to the overall improvement of an organization’s culture of cybersecurity.

Participants shared actionable steps that could improve a county’s culture of cybersecurity and showcase leadership’s support. They want “punitive measures to deal with people who are non-compliant” as IT departments feel like they currently have a lot of “responsibility, but not a lot of authority” to “enforce” (p7) training. One participant noted although “cybersecurity awareness training [is] mandatory,” there is no “participation enforcement [or] disciplinary action” (p13) for non-compliance like there is for the other mandated training. They stated that similar non-compliance measures are already being implemented with “sexual harassment [and] discrimination” trainings which “are mandated by the personnel department” (p13) which, although not in the same realm as cybersecurity, they would have liked to see such enforcement. By mandating and enforcing these training, users might start to take cybersecurity awareness more seriously and evolve their security behaviors. At present, this participant noted having only 50% participation in cyber awareness training throughout the county. In noticing their current methods of not “reward[ing] [employees] for taking [the training],” they are now “looking at changing our models” (p13) to gain more active engagement across the county. Furthermore, one county was facing issues with enforcing MFA implementation as users did not “want the program loaded on their personal phone” (p5), to which they responded by not giving that users access to county systems. This might suggest that sometimes, participants might not always be particularly receptive to employee concerns in accommodating security practices to their individual preferences (i.e., RSA Token, MFA App of their choice, etc.). Moreover, one participant mentioned wanting to “add security and technology questions to the interview process for the organization, so that we can try to start to assess folks” (p1) cybersecurity mindset from the beginning. The low interest and participation rates in cyber awareness training suggest that participants’ current approach to getting employees involved in cybersecurity is not working, and new methods are needed. Additionally, the lack of enforcement in counties that mandate security training and the lack of action taken on non-compliant users also seems to provide evidence that leadership is not as proactive about supporting the county's culture of cybersecurity.

Overall, users do not see cybersecurity impacting their lives, and because they cannot see its impacts, they tend not to get involved. This can be said about users in leadership positions as well. Inversely, participants are seemingly struggling to communicate why users and county leadership should care about cybersecurity awareness. As shown in the type of support leadership has given above, they are comfortable finding funding for security projects, but involvement does not seem to continue after that. Much like average users in the county, government leaders do not appear to be involved in the security process beyond budgeting. Every employee is an entry point into the county's IT systems, so it is up to all users, including leadership, to make cybersecurity a personal and organizational priority. Findings suggest that cybersecurity is not solely a technical challenge but a communications one as well.

5.6 Resources for Local Governments

Throughout the interviews, it became clear that county IT departments are well aware of the resources afforded to them, most likely because they have to be aware of outside resources due to low funding and staffing. Limitations of resources are so embedded into their security mindsets that one participant noted often having to "write [incident response] plans, knowing the limitations of our resources," and supplementing with "outside help and vendors." (p2) When discussing access to resources, most participants were quick to mention some state-sponsored resources such as those mentioned in Chapter 3, (MCS, MiC3, DTMB, MC3, MCP, National Guard), noting that they have been helpful with support in areas such as incident post mortems (p1), auditing, (p8), and threat management (p9). Notably, the only two counties to not mention and/or know about these resources are the two smallest counties in this research sample. Additionally, participants spoke to the usefulness of resources specific to information sharing such as the cross county and state communication organizations such as MS-ISAC and MI-GMIS (mentioned in Chapter 3), as well as information shared by MSP, and the professional connections formed through conferences and events hosted by the aforementioned organizations. Interestingly, half of these participants mentioned utilizing these resources specifically when asked about a time assessing a potential cyber incident was beyond their current capacity. One participant stated that they had a cyber incident recently and “was really worried that something had gotten in so we started calling on some of our contacts especially at the [MSP], and the MS-ISAC [to] have them look at the issues.” (p5) They stated these resources are a big help as they are “always really good about coming up with [ideas to] try this, check this, run [that],”(p5) noting their combined expertise is far beyond that of their small IT department. Other participants expressed similar sentiments in stating that these organizations are a great resource for information sharing. Specifically, they find the annual and/or quarterly round table gatherings to be extremely useful because they hear how other counties are coping with the challenges they face. Within a few hours, they can have “three or four potential solutions to a problem” affecting a specific county and “can help prevent it from happening at some other local government.” (p5) Overall, the participants' positive response in regards to knowledge of resources and active information sharing seems to provide evidence that counties and state organizations have a high level of communication with one another, especially in times of need.

To enhance the number of cybersecurity resources for local Michigan governments, the SLGCA Act, as described in Chapter 3, was introduced to promote stronger coordination between federal, state, and local entities, as well as information sharing and increased budgets. When asked, eight participants had a neutral to an unfavorable view of the bill, with some noting that it seems “redundant” (p13) because they have already “been doing this” (p2) through the various MCP initiatives. Those that were more neutral on the subject noted seeing its potential benefits, stating they “need something actionable” (p5), but were not sure what it would do for them at the local level “other than give us another law on the books to fill up volumes of paper.” (p5) Multiple counties also stated they see this as more of a “political” move with “a lot of hand waving” which “doesn't really do us any good until it translates into resources.”(p8) On that same note, comically, they see this bill as an item on a checklist where, for example, “I vacuumed my living room, but I didn't have [it on] my list of things to do so, I put it on my list of things to [do] just so I can [cross] it off.” (p2) Another participant noted that it just “check[s] off a list of things people are concerned about rather than actually helping them implement” (p7) any proposed changes. Of the six counties that viewed this bill favorably, one noted anything that “simply increas[es] resources to battle cyber threats...let's face it sounds good.” (p3) The participants' comments show inclinations to either strongly unfavorable towards the SLGCA Act or were favorably neutral.

Even with the proposed bills and existing resources county IT departments might have access to, the one constant theme portrayed across these interviews is the challenge of operationalizing resources. One participant noted that having access to the free resources, such as MCP, is a great benefit because they "get a lot of knowledge from it, but then when we come back to implement we just don't have the people"(p2) to operationalize those resources because they are "already so busy doing so many things that are going on in the background." (p2) Another participant stated that their "biggest challenge [in improving their overall cybersecurity posture] is really just having to implement." (p4) Counties know what they want and have to do, but they need "additional staff" (p4) not only for day-to-day operations but to train and operationalize the suggested tools and resources. Due to having multiple stakeholders, including administration and elected officials, they are required to complete tasks for them which "means that it takes longer for us to implement our bigger projects." (p4). These comments provide evidence that to best utilize the vast resources the state of Michigan offers, they need funding and staff to operationalize the suggestion of these state-sponsored initiatives.

Overall, it is clear that participants favor more actionable and interactive initiatives like those with organizations such as MCP, MC3, and DTMB, that communicate directly to counties' IT departments. They prefer these interactions over the "political atmosphere" (p5) that comes with legislation such as the SLGCA Act. The overall piqued responses to this bill can be expected, considering federal and state legislation does not directly affect their everyday operations. Regardless of any proposed bills or increases in operational resources, counties need an increase in staff and budget to accurately operationalize any suggested tools, training, incident response plans, or act on given cyber threat information.

5.7 Impact of COVID-19

At the start of the COVID-19 Pandemic, Michigan county IT departments faced major shifts in cybersecurity priorities from those detailed in the previous section (5.5.1), namely tackling user training and resource allocation challenges. As county employees migrated to Work From Home (WFH), IT departments had to quickly adopt secure remote access measures such as enabling a Virtual Private Network (VPN) and Multi-Factor Authentication (MFA), including

“RSA tokens” (p14) on all work devices. One participant stated that the “pandemic put a lot of [projects on] hold” because their “priorities changed in an instant.” (p5) Participants were suddenly tasked with assessing county employees’ varied technical ability to make sure they knew how to apply remote access measures and “mak[e] sure they understood their responsibilities.” (p5) The procedural aspect in moving to a WFH environment is critical to the cyber awareness of users. IT staff have had to inform county employees of operational security measures such that their “kids can’t play [games]” (p5) on the county’s devices, which had already happened. This rapid evolution to a decentralized working environment not only demanded a shift in the technical operations and connectivity of a counties systems, but a shift in training procedures for users to ensure “a safe environment for them and for us” (p11) as cyber threats do not stop, even for a pandemic. One of these pandemic-specific cyber threats includes seeing an increase in phishing activity targeted at county employees, luring them in with topics stating “click here for the new COVID-19 policy” (p1).

One participant stated that before the COVID-19 pandemic, “5 people were working remotely” whereas now, “it’s in the neighborhood of [a few hundred] so [remote working] has definitely exploded.” (p1) Another participant noted the counties “mindset and technology was geared towards 95% [in-person] work” and suddenly operations became “90% remote, 10% [in-person].” (p12) Due to this sudden shift, some “counties and cities were just completely unprepared for their workforce to have to go remote and unfortunately they had to do a lot of things that you really shouldn’t do security-wise.” (p8) This rapid transition in day-to-day operations can often leave participants wondering, “what does it mean to work securely from home….how do I interact with county IT infrastructure when not on campus and do so securely.” (p12) Previously, their endpoint devices were “on premise and behind our firewall” and protected with “security features [that come with] sitting [inside] the county networks,” but now these endpoints are “sitting in people’s homes” away from their vast security features. (p12) IT department leaders were now having to coordinate hundreds of employees to a new working environment having to take into consideration the various avenues of entry where cybercriminals might gain access to the county’s IT systems which “of course, brought a whole new genre of security issues.” (p5)

Not only does this transitioning to WFH affect cybersecurity practices, but it also affects resource allocation for general county staff. One participant detailed that much of their county staff have desktops that they cannot necessarily take home, which means staff started requesting laptops. Unfortunately, they do not have the resources or allocated budget to cover all requests stating "they can't just go out and buy a bunch of laptops" as they have "already exhausted our budget for new equipment." (p8) Some counties did have additional funds for WFH resources such as laptops. In discussing resource allocation during the pandemic another participant jokingly stated, they are "not going to have somebody walk home with a desktop on their shoulder" and instead had to ramp "up procurement and bought people laptops who didn't have laptops." (p12) Overall, these comments suggest that although the requirements in shifting to a WFH environment were the same (i.e., needing to provide staff with laptops), the outcome is different in which some counties are scarce in extra resources to accommodate this emergent situation. This difference in resources can vastly impact the number of security entry points a cybercriminal can access and disproportionately impact a county's IT systems.

5.8 Challenges Faced in Smaller Michigan Counties

The challenges mentioned in this thesis so far generally relate to limited staffing and funding for county IT departments. One participant states that apart from low funding and being understaffed, "they don't have the staffing with the expertise to be able to implement [the need changes] if they had the money." (p6) Due to a lack of expertise and time to properly assess cyber threats due to low staffing, "many of the small counties have contracted out their work." (p7) Although MCP offers "tabletop exercises" and "incident response" (p6) aid, at present, there is no clear path to operationalize their learned knowledge into actionable steps that ensure cyber protections for their constituents.

There are clear disparities between small and large county resources as one participant mentions listening to a presentation on "how [a specific large county] operates their GIS mapping projects" and simply thinking they "probably spent more money on this one system than my entire county has [for the year]." (p7) Participants continued stating how they would like to see a "rural counties coalition" (p7) to specifically aid smaller counties in navigating the cybersecurity landscape. On that same note, one participant suggested "adopt[ing] a shared model" (p6), which would help in "scal[ing] their activities more effectively" and "save small counties they [might] never have the money [or] expertise" (p6) to tackle their local governments evolving cybersecurity needs. This is an interesting suggestion considering it leverages "shared resources across their peers" (p6), similar to what MCP has done state-wide. However, this model is more focused on just rural communities. This participant also suggested "trying to get other smaller counties...to [also] opt-in for virtual CISO to assist them with some stuff because they don't have the expertise to [implement]." (p6)

The challenges noted and suggestions to improve the existing situation for small counties' cybersecurity environment show an apparent necessity for actionable and easily implementable solutions. At the end of the day, these smaller counties face "the same threats, but have different challenges in addressing them, that's a fairly big difference." (p7) Small counties are actively trying to apply their resources, but are limited in not only funding and staff but expertise and ability to operationalize suggestions.

5.9 Recruiting Talent

When asked about their preference in hiring an employee focused on cybersecurity, half of the participants stated they value experience in the field over college degrees and certifications. In contrast, the other half of participants said they would require at least some college degree. Of note, two participants who require college degrees, when hiring, only do so because it is stipulated by human resources (HR) and does not reflect their personal values on the importance of experience. One participant stated there "is a huge disconnect in our field between HR and technical folk" in which degree requirements are there "to make sure [applicants are] qualified, but...none of that stuff ultimately really matters, [it's just] part of the game." (p8) Another participant noted that because of these degree requirements, "we're going to miss out on some very valuable candidates." (p12) On the opposite spectrum, a few participants adamantly advocated for degrees due to the "critical thinking skills" (p11) gained at a university. Additionally, they noted that "security is becoming a much, much broader topic than it has been in the past…[and] you can't simply learn all that in one or two classes" (p6), so they need individuals with a broader background, which a college education offers.

Regardless of degree requirements, every single participant noted the overall importance of previous experience in the field. Apart from general technical knowledge in topics like "social engineering" (p11) and knowing "security methodologies" (p13), participants are looking for cybersecurity professionals who have the drive and "ability [and]...willingness to learn" (p13) and who is a "good person to work with…for eight hours a day." (p3) The characteristics mentioned of a sought-out cybersecurity professional show evidence of the importance of not only having technical knowledge but being able to effectively communicate with your team and have the drive to be continuously learning.

These conversations also brought up issues attracting talent as they are “really concerned about being able to recruit somebody who wants to work [in local government] anymore.” (p2) Participants noted wanting to invite students to professional conferences, set up internship programs, and establish K-12 cyber initiatives. One participant mentioned wanting to “sponsor students to come to our [annual industry] conference to see what local government is all about” in hopes of “really building connections” (p2) with other peers and industry professionals. Counties are already looking to form internship programs, for example, one participant mentioned working with Davenport University [67] to recruit students from their cybersecurity program (p6), another mentioned collaborating with Michigan State University’s capstone program [9] (p2). At the state level, one organization is looking to partner with colleges like the University of Michigan’s Ford School of Public Policy [50] to aid with tech governance, “help people get organized,” and assess potential “technical and social improvements [needed in] cybersecurity.” (p14) Moreover, state cybersecurity organizations are partnering with the Department of Education and various labor and economics departments to establish K-12 initiatives where they will be “building future cyber leaders.” (p14) The partnerships being formed between universities and government entities around Michigan suggest that county IT departments are interested and actively working on getting more students involved in the local government sector.

Chapter 6
Discussion

This chapter discusses the study's overall research findings relating to the central themes present across interviews. These themes include the Culture of Cybersecurity, IT Department Funding, and Operationalizing Local Government Resources. First, I discuss the key findings and how they relate to my three research questions. Then I present recommendations that aim to address the challenges identified in this study and enhance the cybersecurity posture of local Michigan governments.

6.1 Key Findings Discussion

I began the study by posing the following research questions:

RQ1: How are local Michigan governments currently protecting their governmental systems from cyber threats? (e.g., Cyber risk assessments, hiring practices, security resources, information sharing)

RQ2: What challenges are counties facing in improving their cybersecurity posture?

RQ3: What are some potential opportunities for improvements that can be made regarding current cybersecurity practices?

In pursuing this line of research, three main themes emerged through the interviews: the importance of an enhanced culture of cybersecurity within local governments, increased funding and staffing, and guidance in operationalizing existing local government resources. These central themes showcase the current state of local Michigan government cybersecurity, challenges they face in ensuring cybersecurity, and recommended improvements to current practices.

To improve a county's cybersecurity posture, all employees and departments across Michigan local governments need to adopt a security mindset. Cybersecurity is a decentralized field that affects even those who are not cognizant of the impacts it has on those around them. By providing local Michigan government IT departments with the needed resources, they will be better equipped to overcome any future challenges they might encounter in the cyber domain.

6.1.1 Culture of Cybersecurity

My research findings are consistent with similar results presented by Norris et al., who found that “the technological side of the cybersecurity equation is not most problematic for local government...instead, it is the human element [19].” Inevitably, a user will inadvertently click on something that introduces malicious software to a county system. Because of this, some IT department leaders have noted actively trying to foster a welcoming security culture for users. The relationships between the user and IT department are essential because users are the first line of defense against cyber threats. The more connected and knowledgeable they are about existing threats, the more successful they will be in mitigating them. These findings make it clear that the human being is both the “weakest link in the security chain [29]” and the most important asset in improving an organization’s overall cybersecurity posture.

Throughout the interviews, participants often mentioned the perception of cybersecurity being an IT department problem rather than something that affects all employees and requires their participation. They also noted the lack of cybersecurity culture in their county being inadvertently supported by leadership. Lack of support can be assessed by a county’s insufficient funding for cybersecurity, absence of mandated cybersecurity training, and overall lack of support. If a county leader does not buy into the culture of cybersecurity, whether through additional funding or other actionable support, then their employees will not buy in either.

This finding is supported by Norris et al., who insinuates that qualities of a local government leader who “fully embrace[s] and support[s] cybersecurity” plays a vital role in “practicing it appropriately, insisting that others in government do so as well, and holding all accountable when they do not [45].” Leadership from the top sets the tone for an organization’s perception of cybersecurity.

Throughout my research study, it became clear that cybersecurity and its application to organizations is largely a multistakeholder communications issue. Counties face challenges in getting users and leadership to understand the importance of adopting cybersecurity measures to their day-to-day operations. This could be one of two reasons; either users do not care about cybersecurity, or no one has effectively communicated the potential harm cyberattacks could cost them and their organization. Perhaps the research participants’ attitude towards users adopting cybersecurity is outdated and needs to be updated with current best practices to increase user buy-in. Additionally, this could also be a policy issue in which users do not pursue cybersecurity awareness training if not required since they have to take yearly and/or quarterly training for other programs.

To ensure cybersecurity, local governments need a county-wide enhancement on their organizational culture of cybersecurity. Participants have stated that users do not understand or care about the importance of cybersecurity until it affects them directly. To address this concern, some improvements can include a revitalized model for training that effectively communicates the importance of cybersecurity while rewarding employees for their involvement. Although content would be similar, the avenue's in which to approach these trainings might have to vary between counties depending on the staff's demographics. One participant previously noted seeing pushback in implementing training because county employees are used to more "old school" (p8) and direct training methods. A few participants advocated for the enforcement of punitive measures for those who did not comply with mandatory cybersecurity training to promote cybersecurity adherence. Additionally, to aid the users in adopting cybersecurity practices, employees can be more conducive to user requests in substituting cybersecurity requirements (i.e., using an RSA token over MFA). Guidance for the on-boarding process for incorporating tools such as MFA and VPNs in day-to-day operations could also be better communicated.

Although Norris et al. identified that local governments need to "create and maintain a culture of cybersecurity" to "improve their practice of cybersecurity [45]," my research identified more precisely the relationships between users and a local government's IT departments and how that relationship can mold a county's culture of cybersecurity. This closer look at the working relationships as it pertains to the culture of cybersecurity adds to the limited academic literature in local government cybersecurity research.

6.1.2 IT Department Funding

Throughout the research interviews, some key findings emerged about the current practices local Michigan governments utilize to protect their systems from cyber threats or RQ1. The first finding was that the most prevalent cyberattack local governments are subjected to is phishing attacks, which have increased in frequency towards county employees since the start of the COVID-19 pandemic. This was an unsurprising finding as phishing schemes are one of the easiest attacks to deploy and most influential social engineering tactics. What is a data breach if not phishing persevering? This frequent threat vector and uptick in attacks over the past year have resulted in participants wanting to automate employee cybersecurity training and phishing exercises to enhance security awareness. One county has already implemented such automation to include the automatic enrollment of employees in remedial cybersecurity training if/when they fall victim to a phishing exercise. County IT leaders have stated three main cybersecurity priorities that include: implementation of MFA across counties, finding new tools and avenues for additional resources, updating software, and implementing existing projects. These findings were not surprising as participants often stated they are always looking for new and cost-effective measures to protect their county's IT systems.

Gaining sufficient funding for basic operations is already limited, let alone having to account for budgeting regarding cybersecurity updates and the operationalizing of backlogged projects. County IT departments have to juggle multiple stakeholders, competing projects, and day-to-day operations with limited funding and staff. Limited funding prohibits a county's ability to update systems, hire new staff, source new tools, implement cyber awareness training, and operationalize additional projects. Similar to Norris et al., this ultimately leaves local governments without the adequate funding to "provide the needed level of cybersecurity protection [44]," and thus leaves them vulnerable to cyberattacks. Although Norris et al.'s research is focused on the State of Maryland, and this thesis's research is focused on the State of Michigan, both studies have come to similar conclusions around funding and staffing. Continued research on the optimal average cybersecurity funding and staffing in local government IT departments would yield interesting findings when compared across various U.S. local government cybersecurity postures.

Moreover, significant improvements can be made regarding increased funding for additional staff and resources for county IT departments and established guidance on operationalizing these resources effectively. These improvements would greatly benefit counties of all sizes across Michigan by providing them resources to solve immediate problems and guidance on operationalizing new tools to help mitigate potential threats. One of these tools includes automating daily cybersecurity processes, which help free IT department staff of tedious tasks, so they can allocate their time towards tackling more pressing challenges. Furthermore, IT departments, especially those from smaller counties, "operate in a world of budgetary constraints

[19]” and are forced to assess security risk through that lens. Whether the local government is IT department employees are Jack of All Trades or cybersecurity experts, their role in protecting the cybersecurity of their constituents is crucial to the national security of this country and must be supported as such. Insufficient funding and staffing limit their abilities to ensure a system is fully protected. Counties seek improvements that include actionable and easily implementable solutions to maximize their cybersecurity posture at any budget.

6.1.3 Operationalizing Local Government Resources

Through my own interview experience, although the technical cyber incident questions section was the longest, the most surprising findings were identified through the non-technically focused questions. One of these most surprising findings was not understanding the technical challenges counties face but the sheer importance of proper communication and relationships built with outside organizations. Throughout the interviews, it quickly became apparent that participants were well aware of the resources, organizations, and support afforded to them by the State of Michigan. When faced with a cyber incident, 84% of participants in this study detail their first few steps include reaching out to organizations such as MC3, MCP, MS-ISAC, MI-GMIS, and vendors for additional resources and potential solutions. These first steps taken by participants make it clear that developing the support network for IT departments matters. This shows evidence that one of the most effective ways local governments are currently protecting their systems is by connecting with outside organizations to gain information and solutions as to the prevention, mitigation, and recovery from cyber events.

Even with these vast networks and resources, county IT departments face challenges in operationalizing any suggested changes. Participants shared that although the resources are great, they do not have the time nor the staff to operationalize them because of the various stakeholders they answer to everyday and general day-to-day operations. Operationalizing some of the resources, including incident response plans and various technical tools, requires time, staff, training, testing, and implementation. IT departments are constantly forced to postpone cybersecurity projects which leaves them vulnerable to potential cyber-attacks. This inability to operationalize the resources offered by the State of Michigan will eventually cause them to become a victim of a successful cyberattack.

6.2 Recommendations

This research study yielded multiple challenges, technical and non-technical, that local Michigan governments face in ensuring cybersecurity protections for their constituents. To help in the improvement of these challenges and enhance current practices, four recommendations are presented.

6.2.1 Involving County Leadership in Cybersecurity

As previously stated, employees do not understand the importance of cybersecurity unless they are directly involved in it and/or it affects them directly. Moreover, employees' perceptions of cybersecurity are set, in part, by leadership's value of cybersecurity. To help improve an organization's culture of cybersecurity, one recommendation is to involve department leaders and elected officials in cybersecurity events and legislative advocacy. Apart from having them complete cyber awareness training, county leaders should also be involved in yearly and/or quarterly tabletop exercises that most participants mentioned attending as part of events with state-sponsored entities such as MCP. Tabletop exercises with county leaders will get them actively involved in the cybersecurity process and help them envision the various risk scenarios and potential cyber threats their local government could be facing. In this controlled environment, county leaders will walk through the multiple stages of a cyber incident to identify the various stakeholders, operationalize existing resources, team management, learn about cyber threats, and gauge overall cybersecurity readiness. Additionally, this hands-on approach can similarly be approached from a gamification point of view in which county leadership is involved in a simulated hack, similar to a penetration test, which most IT departments already run. By involving leadership in real-life scenarios, they will see how their role and choices actively impact their organization's cybersecurity. These hands-on training exercises will help leaders understand why making cybersecurity a personal and organizational priority is so important and share that knowledge with their employees. Expressly, these hands-on training for non-technical county leadership can be incorporated into the various conferences they already attend every year. The local government IT conferences can also offer specific tracks for county leadership where they offer not only these tabletop exercises but provide actionable steps and resources to improve their counties cybersecurity posture. The recommendation of getting leadership involved in these educational exercises is not to overburden or frighten them but to educate and reassure their perceptions of cybersecurity and its importance in organizational culture.

Moreover, by getting leadership involved in the cybersecurity process, they will become better advocates for their staff and constituents. To increase cybersecurity resources within the State of Michigan, Senator Gary Peters introduced the SLGCA act (mentioned in Chapter 3), which promotes information sharing between federal, state, and local entities and increases resources and funding. Some key points of this legislation are the hiring of, on average, 15 full-time cybersecurity professionals, continuing cyber threat notifications initiatives between federal and state entities, and increased cybersecurity training, but not specifically stating the method or user base of this training. Although this is a formidable attempt at bolstering cybersecurity budgeting, the act does not solely target sending resources to local government entities and instead covers state organizations. There is currently no specificity in how many of those resources will be allocated towards local Michigan governments versus state organizations. My recommendation is that county leaders and state allies advocate for a bill to be proposed explicitly for the funding of local government entities to bolster their technical cybersecurity posture, IT workforce, and user training. Effective cybersecurity legislation must be clear where funds will be allocated and not simply focus on acquiring new tools to solve security problems. Policymakers and leaders must improve the basic framework in which local government cybersecurity is built upon, focusing on their IT hygiene which includes patch management and limiting users' controls, and developing an efficient and cost-effective cybersecurity strategy. These recommendations are not simply nice to have but required to combat cyberattacks and ensure constituents' cybersecurity.

6.2.2 Operationalizing Best Practices

The second recommendation includes added collaboration amongst state organizations, as mentioned in Chapter 2, to operationalize best cybersecurity practices. The Michigan Cyber Partners (MCP) group was explicitly mentioned multiple times by most research participants and thus is a trusted resource amongst local government IT departments. The trust counties have with MCP should be leveraged and expanded to cover broader areas of cybersecurity protections. As counties face challenges in operationalizing the cybersecurity practices the state organizations often recommend, one solution could include collaborating with state organizations to physically spend time in those counties and assess their challenges. For example, MCP could expand their staff to include a cybersecurity professional who travels from county to county, spending a week at each county, helping them operationalize best practices. During research interviews, participants often mentioned not having time to focus on cybersecurity because of their day-to-day operations. This solution would help counties have extra staff on hand, even if for a short time, to help with backlogged cybersecurity projects, implementation of new security measures, meeting with county leadership to advocate for an increase in funding, and so on. Additionally, this solution could be implemented as a rotational program between the state organizations described in Chapter 2. A program like this would be exceptionally useful for small and/or rural counties whose IT departments only have one or two people managing an entire county's IT systems.

This research highlights that Michigan counties of all sizes communicate but do not necessarily share resources and are thus remaining technologically siloed. To aid the local Michigan government's cybersecurity posture as a whole, collaboration, especially among smaller counties, is needed. The disparity of growing cyberattacks and lack of funding and staffing within smaller local governments calls for a need to form regional coalitions to aid in sharing resources amongst IT departments. These smaller counties are often at a more significant disadvantage in the current cybersecurity landscape; a potential solution could include applying an open resource sharing model amongst small and/or rural communities in the State of Michigan. Considering how expensive cyber incidents can become and the nature of funding for local governments is so decentralized, smaller communities might never have the funding needed to reach a high level of cybersecurity. As "no single model will be the best choice for a given [12]" organization, by leveraging shared resources across these communities, they can develop strategies specifically tailored for their communities.

6.2.3 Recruiting Talent

As funding and staffing are a current limiting factor for county IT departments, the third recommendation includes collaborating with local academic institutions and organizations focused on getting students involved in Science, Technology, Engineering, and Mathematics

(STEM) and related fields. Throughout interviews, multiple participants were worried about attracting talent to the local government tech space once they retired. By collaborating with these organizations, counties will be able to attract new talent to the local government sector and introduce students to the inner workings of government operations. Doing so will help build a student to local government official pipeline that does not currently exist for Michigan county IT departments. Hiring interns is a win-win scenario for all stakeholders. Students get to learn essential technical skills, earn a paycheck (and possibly school credit), and gain real-world job experiences. Counties can pursue a cost-effective measure to hiring more technical talent since student interns are not allocated as much of a budget as full-time staff. IT departments will now have added staff that can help with backlogged projects, find innovative solutions to existing challenges, and help with day-to-day operations.

A few of these organizations local and state governments can consider partnering with include:

Organization Name
Journi
Best Buy Teen Tech Center
Girls Who Code
Detroit Area Pre-College Engineering Program
National Center for Women & Information Technology (NCWIT)
Center for Cyber Safety and Education
NSA Student Programs
CyberCorps®: Scholarship for Service
SkillsUSA

Table 2: List of Organizations Coordinating Students interested in STEM

6.2.4 Technical Recommendations

Technical recommendations could also include using AI to automate various cybersecurity processes such as phishing exercises and log analysis. AI integrated technologies are dynamic and able to analyze millions of data points from inside or outside an organization to identify potentially malicious threats and user behaviors. This would alleviate some of the many hats and tasks IT department staff is assigned to complete every day.

As for cyber awareness training, automating training might be beneficial in keeping staff abreast of best cybersecurity practices and allow for data collection to analyze if the training is impactful and which topics might be more confusing for the user. Any changes to training will be much more streamlined in this automated and virtual manner than would be if it were in-person. Moreover, it gives the user more freedom to pursue awareness training at their speed, which helps support their daily workflow. Additional research can be conducted to assess how automated security training impacts users' perception of cybersecurity.

These recommendations will help county IT departments overcome some of the more organizational challenges they face in improving their cybersecurity posture.

6.3 Future Work

There are a variety of avenues further exploration in this field could take. One would include continuing interviews with the other 70 counties in the State of Michigan to better assess differences in the cybersecurity preparedness of a broader range of counties. To further analyze the data collected in this study, we could apply a Natural Language Processing (NLP) algorithm performing a sentiment analysis to ascertain the culture of cybersecurity through the interview transcripts. Additionally, the survey methodology could also be expanded to include a recurring quarterly or yearly quantitative analysis of the cyber challenges counties experience. This would establish a set of needed resources across counties and help understand how their challenges and needed resources evolve. To balance out this research in interviewing IT department leaders, it would also be interesting to dive into how cybersecurity is perceived by repeating this study with non-technical employees and elected officials in the same counties interviewed in this thesis. As I noted the importance of the user and IT department relationship, viewing this research from the opposite perspective could yield interesting results. Moreover, due to the lack of academic literature, I would be interested in conducting specific research assessing the cybersecurity posture of low-income and/or rural communities and its potential impacts on the cyber wellbeing of constituents. Research in assessing the cybersecurity of rural communities could help inform cybersecurity policymaking, resource allocation, and budgeting for state-sponsored grants.

Chapter 7
Conclusion

Cyberattacks on local government entities continue to rise every year, but the challenges local governments face in protecting their systems remain largely unexamined. To combat these threats effectively, we must examine the challenges local governments face and the resources they require in ensuring cybersecurity for their constituents. The research findings and recommendations discussed in this thesis help guide future cybersecurity initiatives to focus on the specific challenges counties face rather than perceived challenges. By defining the problems, we are one step closer to solving them.

The results of this research study found challenges local Michigan governments face in enhancing their counties' culture of cybersecurity, operating with limited funding and support, and inability to properly utilize state resources due to limited staffing needed to operationalize. A surprising finding from this study was learning about how important communication and relationship building are to cybersecurity and how these relationships impact the culture of cybersecurity.

By identifying these challenges, policymakers can introduce evidence-based policies that will address the essential needs of local Michigan counties and provide actionable and implementable solutions. Additionally, it will enable researchers and cybersecurity professionals to develop recommendations and mitigating solutions to improve local Michigan government cybersecurity.

Research findings add to the existing gap in the scholarly literature by providing insights into the current state of local government cybersecurity affairs within the State of Michigan. By adding to the body of work within the local governance and cybersecurity spaces, future researchers will be better able to track how technical tools, cyber threats, policy, and local government cybersecurity priorities evolve. Additionally, researchers can compare their findings to other local governments and continue adding to the limited body of work in these fields. Considering the study was focused on local governments in a single U.S. state, the findings cannot be universally applied to all other U.S. states. Based on this research and the literature review findings, other U.S. local governments may be experiencing similar challenges in improving their cybersecurity posture.

The four recommendations proposed in this thesis include involving county leadership in cybersecurity through hands-on training, best practices for operationalizing cybersecurity in local government, including regional coalitions and open resource sharing model for small and/or rural Michigan communities, and recruiting talent from local academic institutions and organizations. Additionally, technical recommendations include the use of AI to automate various cybersecurity processes and user training. These recommendations aim to provide local governments with actionable steps to enhance their cybersecurity posture considering the resources they can currently access. Further research into the various aspects of local government cybersecurity should be conducted and include multi-disciplinary research methods not often applied in cybersecurity. For example, applying NLP algorithms to perform sentiment analysis on interview transcripts or creating datasets from research findings to aid future scholars in this field.

This research aims to add knowledge to the field of local government cybersecurity research and provide valuable insights and recommendations that local Michigan governments can utilize to bolster their cybersecurity posture.

Appendix 1

Recruitment Message

Hello [Name Here],

My name is Marilu Duque, a graduate student at the University of Michigan School of Information. I am currently working on my Master's thesis, advised by Prof. Florian Schaub, focused on understanding how local Michigan governments deal with cybersecurity threats. Cyber threats to local government systems have been increasing exponentially over the last several years, and with this study, I seek to better understand the existing capabilities and challenges local Michigan governments face in protecting their systems. The findings of this research aim to inform policymakers on areas of improvement and guide future recommendations to aid local governments in improving their cybersecurity posture.

I would be grateful if you would be willing to spare 30-60 minutes for a Zoom interview and short survey to share your experiences in combating cyber threats in local government. Interview recordings, survey responses, and transcripts will be anonymized before analysis to protect participant confidentiality.

In brief, I am hoping to hear an expert viewpoint on how cybersecurity threats are handled by those on the frontlines and to what challenges you are facing in ensuring cyber safety.

Please respond if you're interested, and we can then schedule the interview in the next few weeks. Additionally, if you are not the right person to talk to about this topic, I'd appreciate it if you could connect me with the correct people in your organization.

Thank you for your time, and I hope to hear from you soon!

Appendix 2

Consent Form

TITLE OF THE STUDY

Local Government Cybersecurity: How Michigan Counties Cope with Cyber Threats

INVESTIGATORS

Marilu Duque (M.S. Student, University of Michigan)

Florian Schaub, Ph.D. (Assistant Professor, Advisor, University of Michigan)

STUDY PURPOSE

The purpose of this research is to understand the current cybersecurity practices of local Michigan governments and the challenges they face in improving their cybersecurity posture. From an industry leader such as yourself, we hope to learn about the cyber challenges your organization faces, needs, and or concerns in overcoming these challenges and ways in which we may support you.

This study is part of the University of Michigan's School of Information, Master's Thesis Option Program (MTOP).

PROCEDURES FOR THE STUDY

If you agree to be in the study, you will participate in one audio-recorded interview, lasting anywhere from 30 to 60 minutes. The interview will occur at a mutually agreed upon date and time. Interviews will take place over a web-conferencing system called Zoom. It is up to you to choose a time to participate in the study. At the end of the interview, we will ask you to complete a brief questionnaire.

RISKS AND BENEFITS

There are minimal risks to you, most of which concern identifying you as a participant. See the “confidentiality” section below for how the team will address these risks.

You are not expected to personally benefit from participating in this research. However, others may benefit from the knowledge gained from this study. As the frequency of cyberattacks on local government continues to grow, we hope this research will help assess the type of support local Michigan governments need in bolstering their cybersecurity posture and provide recommendations for policymakers towards providing needed resources.

FINANCIAL INFORMATION

There is no compensation for participating in this study.

CONFIDENTIALITY

The researchers will have access to research artifacts that may identify you, including digital audio recordings, transcripts, documents, and communications created as part of the data collection process. These artifacts will be accessible to the researchers via computing devices and shared computing applications (e.g., U-M Google Drive). Efforts will be made to keep your personal information confidential, including storing all data using encryption technology and passwords, as well as removing potentially identifying information from recordings and transcripts before analysis. Your contact information will be stored separately from your study responses and will not be linked to them. Your identity will be held in confidence when the research is disseminated in reports, articles, presentations, and in other artifacts, although direct quotes from the interviews that do not contain identifying information may be used in these materials.

The interviews will be recorded and transcribed for analysis purposes. The transcription processes may be aided by the use of an automated external service (e.g., Zoom). Audio files will be manually edited to remove identifiable details, prior to being uploaded to any such service. Following the generation of transcriptions, audio files will be immediately deleted from their server. Researchers can manually transcribe your interview if you wish to keep your audio file restricted.

The research team will retain recordings until the project's completion, at which time the recordings will be securely deleted. The research team cannot guarantee absolute confidentiality. Your personal information may be disclosed if required by law. Organizations that may inspect and/or copy your research records for quality assurance and data analysis include groups such as the study investigator and research associates, the University of Michigan Institutional Review Board or its designees, and (as allowed by law) state or federal agencies, specifically the Office for Human Research Protections (OHRP), who may need to access your research records. Minus these exceptions, the research team will not allow access to identifiable data.

CONTACT INFORMATION

For questions about the study, contact the principal investigator, Marilu Duque *(Email: marilud@umich.edu)*.

The University of Michigan Health Sciences and Behavioral Sciences Institutional Review Board has determined that this research is exempt from IRB oversight.

VOLUNTARY NATURE OF STUDY

Taking part in this study is voluntary. You may at any time opt-out of answering questions and/or stop your participation completely. You may also request to have your data destroyed if you elect to leave the study. Leaving the study will not result in any penalty. Your decision whether or not to participate in this study will not affect your current or future relations with the University of Michigan.

Your Consent to Participate in the Research Study

By reading this document and verbally consenting to the research at the beginning of the interview, you agree to be in this study. Make sure you understand what the study is about before you consent. We will give you a copy of this document for your records, and we will keep a copy with the study records. If you have any questions about the study after you verbally consent to this document, you can contact the study team using the information in the section above.

I understand what the study is about, and my questions so far have been answered. I agree to take part in this study.

Print Legal Name: ____

Signature: ____

Date of Signature (mm/dd/yy):

____

[NOTE: This consent form is provided in electronic form for reading, but consent will be indicated verbally with a Yes/No to participate at the beginning of the interview.]

Appendix 3

Interview Protocol

Hello _________, my name is Marilu Duque, a 2nd-year master's student at the University of Michigan School of Information. Thank you for taking the time to participate in this study, whose overall goal is to understand the current cybersecurity practices of local Michigan governments and the challenges they face in improving their cybersecurity posture. From an industry leader such as yourself, we hope to learn about the cyber challenges your organization faces, needs, and or concerns in overcoming these challenges and ways in which we may support you.

This interview can take anywhere from 30-60 minutes. To ensure your confidentiality, any identifying information will be removed from the interview transcripts, and any recordings will be stored separately from the contact information. Access to data will be limited to the primary researcher and advisor. Additionally, any identifying information will be redacted from potential publications or presentations of this research (including my MTOP defense).

In reading the consent form sent via email and hearing more about the research, do you consent to take part in this study?

Do you have any questions before we get started?

Let's get started.

1. **Assessing Cybersecurity Literacy of General Employees**
    a. How frequently does your local government take action to improve cybersecurity, and what actions are taken?
        i. i.e., Security Trainings, MFA Authentication, Internal Policies, Frequency of Actions, Etc.
    b. What areas in your department do you see improvement in overall cyber safety, including resources for non-technical staff?

        i. What resources would be beneficial to see improvements?

2. **Understanding Overall Department Employee Backgrounds/Composition of Team & Roles:**
    a. Do you have dedicated staff focused on cybersecurity or generalists focused on broader IT needs?
    b. What are general job requirements/descriptions for security/IT-focused employees?
        i. Do you have specific requirements such as degrees, certifications, or years of experience required?
    c. Where/who in your local government holds the primary cybersecurity responsibilities?

3. **Cyber Incident Information**
    a. What is your department's criteria/classification of a cybersecurity incident?
    b. Can you describe a time when assessing a potential cyber incident was beyond your current capacity?
        i. What prevented you from achieving your desired goal?
    c. Can you describe a time when you were successful in assessing a potential cyber incident?
        i. What enabled you to achieve your desired goal?
    d. Is your local government able to determine the root cause of cyberattacks, to reduce the chance of it happening again?
        i. If yes, what is their process in identifying the root cause?
        ii. If not, what resources would they need to do this?
    e. How well prepared do you think your local government is to deal with cyber events (e.g., incident response)?
        i. For Example:
            1. Prepared: Dedicated incident responder with active security monitoring

            2. Kind of Prepared: Dedicated incident responder but no active security monitoring
            3. Not Prepared: None of the above

    f. Has your local government developed any cybersecurity strategies and/or plans?
        i. If yes, do you feel they equip you with the right resources? How would you rate 1-10 your overall cybersecurity posturing?
        ii. If not, what resources might you need to improve your cybersecurity posture?
    g. What are the current cybersecurity priorities for your department, if any?
        i. Have these priorities changed since the start of the COVID-19 pandemic?

4. **Michigan/Policy Specific Questions**
    a. Do you or others in your local government track state and/or federal security and privacy policy?
    b. Well, Michigan Senator Gary Peters introduced the State and Local Government Cybersecurity Act (SLGCA), which promotes "stronger cybersecurity coordination between the Department of Homeland Security (DHS) and state and local governments. It encourages national cybersecurity watchdogs to share information regarding cybersecurity threats, vulnerabilities, and breaches as well as resources to prevent and recover from cyber-attacks with states and localities that are increasingly targeted by bad actors."
        i. With this in mind, do you see this policy as being beneficial to improving your overall cybersecurity posture?

5. **Support & Potential Improvements**
    a. Are you adequately staffed to meet security goals?
    b. What challenges do you face or resources do you need in improving your cybersecurity posture?

6. **Personal Ending Question (Time Allowing)**

a. Throughout your time being a leader in cybersecurity, what are some lessons you’ve learned that you’ll never forget?

Appendix 4

Post-Interview Questionnaire

Q1.) Which Michigan County are you located in?

Q2.) What is your job role/title?

Q3.) How many years have you been in this role and/or similar roles at your current organization?

Q4.) What is the total number of IT-focused employees in your local government, including contractors? (Estimate is Ok)

Q5.) What percentage of IT-focused employees would you say are in-house vs. contracting positions?

Q6.) What governmental systems is your department responsible for?

▢ Mayoral Office (1)

▢ Data Management (2)

▢ Public Works Projects (3)

▢ Street Lights (4)

▢ Waste Management (5)

▢ Water Management (6)

▢ Electrical Grid (7)

▢ Other (8)

▢ Can't Disclose (9)

Q6.2.) What other governmental systems is your department responsible for? --- Display This Question: If "What governmental systems is your department responsible for?" = Other

Q7.) Do you catalog and count attacks, incidents, and breaches?

o Yes (1)

o No (2)

o Unsure (3)

o Can't Disclose (4)

Q7.2.) Do you catalog these formally (management tool) or informally? --- Display This Question: If “Do you catalog and count attacks, incidents, and breaches?” = Yes

Q7.3.) What is preventing you from cataloging these incidents? --- Display This Question: If “Do you catalog and count attacks, incidents, and breaches?” = No

Q8.) How frequently is your department subject to cyber incidents?

Q9.) In the past 12 months, how many cyber incidents (phishing, ransomware, data breaches, etc.) has your local government experienced?

Q10.) Since the start of the COVID-19 pandemic (March 2020), have you seen an increase in cyber incidents?

o Yes (1)

o No (2)

o Unsure (3)

o Can't Disclose (4)

Q10.2.) How often do you experience these incidents? --- Display This Question: If “Since the start of the COVID-19 pandemic (March 2020), have you seen an increase in cyber incidents?” = Yes

Q10.3.) What types of incidents have you been experiencing during this time? --- Display This Question: If “Since the start of the COVID-19 pandemic (March 2020), have you seen an increase in cyber incidents?” = Yes

▢ Advanced Persistent Threats (1)

▢ Phishing (2)

▢ Trojans (3)

▢ Botnets (4)

▢ Ransomware (5)

▢ Distributed Denial of Service (DDoS) (6)

▢ Wiper Attacks (7)

▢ Intellectual Property Theft (8)

▢ Theft of Money (9)

▢ Data Manipulation (10)

▢ Data Destruction (11)

▢ Spyware/Malware (12)

▢ Man in the Middle (MITM) (13)

▢ Drive-By Downloads (14)

▢ Malvertising (15)

▢ Rogue Software (16)

▢ Unpatched Software (17)

▢ None (18)

▢ Unknown (19)

▢ Can’t Disclose (20)

▢ Other (21)

Q10.1.) What others is your organization experiencing? --- Display This Question: If “What types of incidents have you been experiencing during this time?” = Other

Q11.) Does your organization use Intrusion detection system (IDS) tools?

o Yes (1)

o No (2)

o Unsure (3)

o Can't Disclose (4)

Q11.2.) Are your IDS tools open-source, privately owned/operated, or developed in-house? --- Display This Question: If “Does your organization use Intrusion detection system (IDS) tools?” = Yes

o Open Source (1)

o Private Owned/Operated (2)

o Developed In-House (3)

Q11.3.) What barriers do you face in using them? --- Display This Question: If “Does your organization use Intrusion detection system (IDS) tools?” = No

Q12.) Do you utilize any of the following IDS Tools? Zeek/Bro, Snort, Suricata, SecurityOnion, Sagan.

▢ Zeek/Bro (1)

▢ Snort (2)

▢ Suricata (3)

▢ SecurityOnion (4)

▢ Sagan (5)

▢ Other (6)

▢ Can't Disclose (7)

Q12.2.) Which others do you use? --- Display This Question: If “Do you utilize any of the following IDS Tools? Zeek/Bro, Snort, Suricata, SecurityOnion, Sagan.” = Other

Q13.) Does your organization have cybersecurity insurance?

o Yes (1)

o No (2)

o Unsure (3)

o Can't Disclose (4)

Q13.2.) What type of incidents are covered? --- Display This Question: If “Does your organization have cybersecurity insurance?” = Yes

Q13.2.1) What extent do they protect the local government’s data as well as overall constituent data? --- Display This Question: If “Does your organization have cybersecurity insurance?” = Yes

Q13.3) What barriers do you face in utilizing such insurances? --- Display This Question: If “Does your organization have cybersecurity insurance?” = No

Q14.) How has the support given to cybersecurity changed over the past 12 months? (i.e., Increased/Decreased budget, More/less employees, new/updated equipment, etc.)

Q15.) Additional Comments

References

[1] Dippold, Elizabeth, et al. “Annual Survey of Public Employment & Payroll Summary Report: 2019.” *Census*, U.S. Census Bureau, 30 June 2020, www.census.gov/content/dam/Census/library/publications/2020/econ/2019_summary.pdf

[2] 2017 Census of Governments – Organization" Table 2. Local Governments by Type and State: 2017, United States Census Bureau, 2017, https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html.

[3] “2018 Deloitte-NASCIO Cybersecurity Study – States at Risk: Bold Plays for Change.” *NASCIO*, Deloitte-National Association of State Chief Information Officers (NASCIO), 23 Oct. 2018, www.nascio.org/resource-center/resources/2018-deloitte-nascio-cybersecurity-study-states-at-risk-bold-plays-for-change/.

[4] “2019 End-Of-Year Data Breach Report.” Idtheftcenter, Identity Theft Resource Center, 2019, www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

[5] “2020 Data Breach Investigations Report.” *Verizon*, Verizon, 2020.

[6] “Accellion, Inc File Transfer Appliance (FTA) Security Assessment.” *Accellion*, Mandiant, 1 Mar. 2021, www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf .

[7] Bergal, Jenni. “Florida Hack Exposes Danger to Water Systems.” *PewTrusts*, The Pew Charitable Trusts, 10 Mar. 2021, www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems.

[8] Camp, Terry. “FBI, Michigan State Police Investigating Cyber Attack on Saginaw Township Schools.” *ABC12.Com*, A Gray Media Group, Inc, 25 Feb. 2021, www.abc12.com/2021/02/25/fbi-state-police-probing-cyber-hack-on-saginaw-township-schools/.

[9] “The Capstone Experience.” *CSE.MSU.Edu*, Michigan State University, www.cse.msu.edu/~cse498/2021-01/home/.

[10] “Cost Estimate - S. 1846, State and Local Government Cybersecurity Act of 2019.” *CBO.gov*, Congressional Budget Office, 19 July 2019, www.cbo.gov/system/files/2019-07/s1846.pdf.

[11] Craigen, Dan, et al. “Defining Cybersecurity.” *TIMReview*, Technology Innovation Management Review, Oct. 2014, timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

[12] “Cyber Information-Sharing Models - Mitre Corporation.” *MITRE.org*, The MITRE Corporation, Oct. 2012, www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

[13] “Cyber Warriors.” *MIArmyGuard*, Michigan Army National Guard, www.miarmyguard.com/service/careers/cyber-warriors.

[14] “Cybersecurity.” *Michigan.Gov*, State of Michigan, www.michigan.gov/dtmb/0,5552,7-358-82548_78404---,00.html.

[15] “Cybersecurity: Protecting Local Government Digital Resources.” ICMA.Org, ICMA, May 2017.

[16] “Database Breaches Remain the Top Cyber Threat for Organizations.” Recorded Future, Insikt Group, May 2020, go.recordedfuture.com/hubfs/reports/cta-2020-0521.pdf.

[17] Derusha, Chris. “What States, Locals, and the Business Community Should Know and Do: A Roadmap For Effective Cybersecurity.” *Michigan.Gov*, U.S Senate, 11 Feb. 2020, www.michigan.gov/documents/dtmb/C-DeRusha-Testimony-to-HSGAC-SLTT-Cyber-02-07_680963_7.pdf.

[18] Diaz, Jaclyn. “U.S. Cyber Agency: SolarWinds Attack Hitting Local Governments.” *NPR*, NPR, 24 Dec. 2020, www.npr.org/2020/12/24/949904890/u-s-cyber-agency-solarwinds-attack-hitting-local-governments.

[19] Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin (2020) Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity, Journal of Urban Affairs, DOI: 10.1080/07352166.2020.1727295

[20] Eminağaoğlu, Mete, et al. “The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study.” *Information Security Technical Report*, Elsevier Advanced Technology, 9 June 2010, www.sciencedirect.com/science/article/pii/S1363412710000099.

[21] “Fact Sheet: Ransomware and HIPAA.” *HHS.Gov*, U.S. Department of Health & Human Services (HHS), www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[22] Faller, Mary Beth. “Maricopa County Colleges Computer Hack Cost Tops $26M.” Azcentral, 17 Dec. 2014, www.azcentral.com/story/news/local/phoenix/2014/12/17/costs-repair-massive-mcccd-computer-hack-top-million/20539491/.

[23] Fancher, Don, et al. “Seven Hidden Costs of a Cyberattack.” *Deloitte*, Deloitte, 2 Aug. 2018, www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-seven-hidden-costs-cyberattack.html.

[24] Fujs, Damjan, et al. “The Power of Interpretation: Qualitative Methods in Cybersecurity Research.” *ACM Digital Library*, Availability, Reliability and Security (ARES) Conference, 1 Aug. 2019, dl.acm.org/doi/10.1145/3339252.3341479.

[25] Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur J (2021). https://doi.org/10.1057/s41284-021-00286-2

[26] Hayes, Michael T. “Incrementalism.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 3 June 2013, www.britannica.com/topic/incrementalism.

[27] *Home*. MI-GMIS, mi-gmis.org/.

[28] “How Government Agencies Are Facing Cyber Security Challenges.” FireEye.Com, Mandiant - A FireEye Company, 2018.

[29] J. Tioh, M. Mina and D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," 2017 IEEE Frontiers in Education Conference (FIE), 2017, pp. 1-5, doi: 10.1109/FIE.2017.8190712.

[30] Keefer, Winter. “Mott Community College Addresses Data Security Breach.” *MLive*, Advance Local Media, LLC, 24 Mar. 2021, www.mlive.com/news/flint/2021/03/mott-community-college-addresses-data-security-breach.html.

[31] Lallie, Harjinder Singh, et al. “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.” *Science Direct*, Elsevier Advanced Technology, 3 Mar. 2021, www.sciencedirect.com/science/article/pii/S0167404821000729.

[32] Liska, Allan. “State and Local Government Ransomware Attacks Surpass 100 for 2019.” Recorded Future, 20 Dec. 2019, www.recordedfuture.com/state-local-government-ransomware-attacks-2019/

[33] Macmanus, Susan A., et al. “Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights.” Journal of Urban Affairs, vol. 35, no. 4, Oct. 2013, pp. 451–470. EBSCOhost, doi:10.1111/j.1467-9906.2012.00640.x.

[34] Mateczun, Lauren. “Local Government Cybersecurity and COVID-19.” *Scholars.Org*, Scholars Strategy Network, May 2020, scholars.org/sites/scholars/files/2020-05/Local%20Government%20Cybersecurity%20and%20COVID-19.pdf .

[35] McFarland, Christiana K, et al. “State and Local Partnerships for Cybersecurity: A State-By-State Analysis.” *NLC*, National League of Cities (NLC), Apr. 2020, www.nlc.org/wp-content/uploads/2020/04/SML_2020Report_web-1.pdf .

[36] “Michigan Counties List.” *Michigan.Gov*, State of Michigan, www.michigan.gov/som/0,4669,7-192-29701_31713_31714-97053--,00.html.

[37] “Michigan Cyber Civilian Corps (MiC3).” *Michigan.Gov*, State of Michigan, www.michigan.gov/dtmb/0,5552,7-358-82548_78404_78419-389506--,00.html.

[38] “Michigan Cyber Command Center (MC3).” *Michigan.Gov*, State of Michigan, www.michigan.gov/msp/0,4643,7-123-72297_72370_72379_99838---,00.html.

[39] "Michigan Cyber Initiative 2015." *Michigan.Gov*, State of Michigan, 2015, www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf .

[40] "Michigan Cyber Partners." *Michigan.Gov*, State of Michigan, www.michigan.gov/dtmb/0,5552,7-358-82548_78404_103953---,00.html.

[41] "Multi-State Information Sharing and Analysis Center." *Cisecurity*, Center for Internet Security, www.cisecurity.org/ms-isac/.

[42] "The National Cyber Incident Response Plan (NCIRP)." *United States Computer Emergency Readiness Team (CERT)*, Cybersecurity and Infrastructure Security Agency (CISA), us-cert.cisa.gov/ncirp.

[43] "NIST Cybersecurity Framework." *NIST*, National Institute of Standards and Technology (NIST), 12 Feb. 2014, www.nist.gov/cyberframework.

[44] Norris, Donald, et al. "Cybersecurity Challenges to American State and Local Governments." *UMBC Ebiquity*, 15th European Conference on EGovernment, 18 June 2015, ebiquity.umbc.edu/paper/html/id/774/Cybersecurity-Challenges-to-American-State-and-Local-Governments.

[45] Norris, Donald, et al., "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity." Public Admin Rev, 79: 895-904., 2019, https://doi.org/10.1111/puar.13028

[46] Norris, Donald, et al. "Cybersecurity Challenges to American Local Governments" *UMBC Ebiquity*, Proceedings of 17th European Conference on Digital Government, 12 June 2017, ebiquity.umbc.edu/paper/html/id/811/Cybersecurity-Challenges-to-American-Local-Governments.

[47] Osborne, Charlie. "Flagstar Bank Customer Data Breached through Accellion Hack." *ZDNet*, A Red Ventures Company, 8 Mar. 2021, www.zdnet.com/article/flagstar-bank-customer-data-breached-through-accellion-hack/.

[48] Osborne, Charlie. "Microsoft Exchange Zero-Day Vulnerabilities Exploited in Attacks against US Local Governments." *ZDNet*, A Red Ventures Company, 5 Mar. 2021,

www.zdnet.com/article/microsoft-exchange-zero-day-vulnerabilities-exploited-in-attacks-against-us-local-govts-university/.

[49] Peters, Gary C. “S.1846 - 116th Congress (2019-2020): State and Local Government Cybersecurity Act of 2019.” *Congress.gov*, U.S. Congress, 26 Nov. 2019, www.congress.gov/bill/116th-congress/senate-bill/1846.

[50] “Programs & Courses.” *FordSchool.UMich.Edu*, University of Michigan - Gerald R. Ford School of Public Policy, fordschool.umich.edu/programs-courses.

[51] “QuickFacts.” *Census.Gov*, U.S. Census Bureau, 27 Aug. 2019, www.census.gov/programs-surveys/sis/resources/data-tools/quickfacts.html.

[52] Rader, Marc, and Shawon Rahman. “Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks.” *ArXiv.org*, International Journal of Network Security & Its Applications (IJNSA), 30 Nov. 2015, arxiv.org/abs/1512.00082.

[53] Ralston, William. “The Untold Story of a Cyberattack, a Hospital and a Dying Woman.” *WIRED UK*, Condé Nast Britain, 11 Nov. 2020, www.wired.co.uk/article/ransomware-hospital-death-germany.

[54] Ramachandran, Vignesh. “Stanford Researchers Identify Four Causes for ‘Zoom Fatigue’ and Their Simple Fixes.” *Stanford News* , Stanford University, 23 Feb. 2021, news.stanford.edu/2021/02/23/four-causes-zoom-fatigue-solutions/.

[55] “Securing Your Organization Cybersecurity Framework.” *Michigan.Gov*, State of Michigan, www.michigan.gov/dtmb/0,5552,7-358-82548_78404_103953_105007_105019-549360--,00.html.

[56] “Senate Passes Peters Bill to Strengthen Cybersecurity Coordination with State and Local Governments: U.S. Senator Gary Peters of Michigan.” *Peters.Senate.Gov*, U.S. Senator Gary Peters of Michigan, 22 Nov. 2019, www.peters.senate.gov/newsroom/press-releases/senate-passes-peters-bill-to-strengthen-cybersecurity-coordination-with-state-and-local-governments.

[57] “Senate Passes Peters, Portman Bill to Strengthen Cybersecurity Coordination with State and Local Governments.” *HSGAC.Senate.Gov*, Homeland Security & Governmental Affairs Committee, 22 Nov. 2019,

www.hsgac.senate.gov/media/minority-media/senate-passes-peters-portman-bill-to-strengthen-cybersecurity-coordination-with-state-and-local-governments.

[58] Shelley, Stacy. "Phishing Number One Cause of Data Breaches: Lessons from Verizon DBIR." *PhishLabs*, PhishLabs, 27 June 2019, info.phishlabs.com/blog/phishing-number-1-data-breaches-lessons-verizon.

[59] Shi, Fleming. "Surge in Security Concerns Due to Remote Working." *Barracuda*, Journey Notes, 6 May 2020, blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/.

[60] Shi, Fleming. "Threat Spotlight: Government Ransomware Attacks." *Barracuda*, Journey Notes, 15 Sept. 2020, blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/.

[61] Shilton, Katie, et al. "Qualitative Approaches to Cybersecurity Research." *IDEALS @ Illinois*, ISchools, 15 Mar. 2016, hdl.handle.net/2142/89447.

[62] "SOC as-a-Service." *Check Point*, Check Point Software Technologies Ltd, 18 Feb. 2021, www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/soc-as-a-service/.

[63] "Social Distancing." *CDC*, Centers for Disease Control (CDC) and Prevention, 17 Nov. 2020, www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/social-distancing.html.

[64] "State of Illinois Cybersecurity Strategy." Illinois.gov, State of Illinois, 2017.

[65] "State of Michigan Prosperity Regions." *Michigan.Gov*, State of Michigan, www.michigan.gov/documents/mdhhs/Prosperity_Map1_430346_7_626675_7.pdf.

[66] "State, Local, Tribal, and Territorial Perspectives." *NIST*, National Institute of Standards and Technology (NIST), 12 Feb. 2012, www.nist.gov/cyberframework/state-local-tribal-and-territorial-perspectives.

[67] "Technology." *Davenport.Edu*, Davenport University - Grand Rapids, Michigan, www.davenport.edu/academics/areas/technology.

[68] "What Are the Sources of Revenue for Local Governments?" *Tax Policy Center*, Urban Institute, Brookings Institution, May 2020, www.taxpolicycenter.org/briefing-book/what-are-sources-revenue-local-governments.

[69] "What Is the CIA Triad?" *Forcepoint*, 25 Mar. 2020, www.forcepoint.com/cyber-edu/cia-triad.

[70] “White Paper: The Economic Impact of Cyber Attacks on Municipalities.” *KnowBe4*, KnowBe4, Inc, 2020, www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf.

[71] Whitmer, Gretchen, and Chris Kolb. “FY2020 Executive Budget - Michigan.” *Michigan.Gov*, State of Michigan, 2020, www.michigan.gov/documents/budget/FY20_Exec_Budget_648023_7_648294_7.pdf.

[72] Whitmer, Gretchen, and Chris Kolb. “FY2021 Executive Budget - Michigan.” *Michigan.Gov*, State of Michigan, 2021, www.michigan.gov/documents/budget/FY2021_Executive_Budget_680297_7.pdf.

[73] “Why Do Hackers Want Your Personal Information?” *F-Secure*, F-Secure, 3 July 2020, www.f-secure.com/us-en/home/articles/why-do-hackers-want-your-personal-information.

[74] Wisely, John. “Hackers Post Racist Slurs on Troy Schools Website.” *FREP.Com*, Detroit Free Press, 15 Mar. 2021, www.freep.com/story/news/education/2021/03/15/hackers-slurs-troy-schools/4706894001/.

[75] “Ypsilanti Man Sentenced in Computer Intrusion Case.” *The United States Department of Justice*, 27 Apr. 2018, www.justice.gov/usao-edmi/pr/ypsilanti-man-sentenced-computer-intrusion-case.