The Cybersecurity Preparedness of Local Election Offices: Influences, Challenges, and the Intergovernmental Perspective

by

Lindsey M. Forson

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
August 8, 2020

Keywords: Election Administration, Cybersecurity, Local Government Capacity, Intergovernmental Relations, Emergency Preparedness, Digital Divide

Approved by

Dr. Mitchell Brown, Chair, Professor of Political Science
Dr. Kathleen Hale, Co-chair, Professor of Political Science
Dr. Andrew Cortell, Professor of Political Science
Dr. Ryan Williamson, Assistant Professor of Political Science
Dr. David Umphress, Professor of Computer Science and Software Engineering

Abstract

Recent events have heightened concerns over the cybersecurity of US elections. In the decentralized US election system, counties and municipalities have primary responsibility for election administration. Therefore, protecting elections from cyber threats is largely the responsibility of local governments. Variation across local election offices in their cybersecurity capacity and preparedness is likely given the diversity of local government entities that exist in the United States. This study explores which factors influence the cybersecurity preparedness of local election administration offices.

Literature on US election institutions, local government capacity, intergovernmental relations, emergency management, and the digital divide was reviewed to identify potential factors and build a framework for analysis. Using quantitative and qualitative primary data, this study explores how the resources and other internal characteristics of local election offices, characteristics of local jurisdictions and their populations, and intergovernmental partnerships may influence the cybersecurity preparedness of local election offices.

The findings suggest that a local election administration office's resource availability, technology use, and intergovernmental coordination are related to their cybersecurity preparedness. The influence of the human resources within local election offices on their cybersecurity preparedness is apparent through both quantitative and qualitative data analysis. A relationship between the use of electronic pollbooks by local election jurisdictions and the cybersecurity preparedness of local election offices stands out across quantitative models. The importance of relationships with intergovernmental partners was emphasized throughout expert interviews.

Acknowledgments

Completing a Ph.D. is not an independent endeavor. Rather, the process depends on guidance, collaboration, support, and a lot of love. First and foremost, I want to express my deep gratitude to my husband, Philip. Thank you for your love, friendship, and support during every step of this journey. Thanks for taking care of things when I needed to focus on my work and for being my favorite distraction when I needed to step away.

Thank you to my family for inspiring me to pursue my passions. Mom, Dad, Stacey, Kyle, Marianne, Courtney, Matt, Keaton, and Sadie – thank you for your love and care in every aspect of my life. Mom and Dad, I am grateful that you always modeled ambition, hard work, and tenacity. Thank you to my mother and father-in-law – I feel so fortunate to now have two sets of loving and proud parents. I am so thankful to my family members and friends for being one call away and for providing joy in my life outside of school. Kim, Murphy, Amanda, and Matthew – I cannot imagine getting through the past few years without our Sunday get-togethers.

Thank you to my peers. I enjoyed getting to know you, studying with you, researching and writing with you, commiserating with you, encouraging you, and receiving your encouragement. Thank you particularly to Jan and my sister, Stacey, for reviewing my work.

Finally, I am grateful to those who guided me through this process. Thank you to the professors who taught me how to research and offered advice based on your own graduate school experiences. To my committee members – I truly appreciate your thoughtful input and your help making this product what it is. Mitchell and Kathleen, thank you for inspiring me to develop a passion for election administration and for helping me grow an idea into a dissertation. Mitchell, I am so grateful for your straightforward feedback every step of the way. Thank you for pushing me to the finish line much earlier than I thought I would be able to get there.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CEO	Chief Election Official
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DRE	Direct Recording Electronic
EAC	Election Assistance Commission
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
EIS GCC	Election Infrastructure Subsector Government Coordinating Council
EISCC	Election Infrastructure Subsector Coordinating Council
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HAVA	Help America Vote Act
iGO	International Association of Government Officials
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASED	National Association of State Election Directors
NASS	National Association of Secretaries of State
NIST	National Institute of Standards and Technology
NVRA	National Voter Registration Act
ODNI	Office of the Director of National Intelligence

OLS	Ordinary Least Squares
SLTT	State, Local, Tribal, and Territorial
VVSG	Voluntary Voting System Guidelines

Chapter 1: The New Normal for US Election Administrators

Introduction

In recent years, US election security has become a topic of increased public concern. There is particular concern over the extent to which US elections are protected from foreign cyber threats. This concern stems primarily from events that occurred during and following the 2016 primary election season and general election. This study explores the cybersecurity preparedness of election administration offices within local governments in the United States. I investigate local characteristics that may influence cybersecurity preparedness, challenges local election administrators face related to cybersecurity, and the roles of local election offices and their partners within the intergovernmental network that supports US election cybersecurity.

This research contributes a preliminary understanding of what influences cybersecurity preparedness for local election offices and has implications for policymakers and administrative leaders related to how the management of cyber risks to US elections can be improved. My findings contribute to the broader literature on the digital divide and the local government capacity literature by providing insight into which factors may create both a digital divide and a cybersecurity divide for local government entities. The findings also contribute to the broader literatures on intergovernmental relations and election administration by offering a descriptive analysis of the intergovernmental network surrounding election cybersecurity and how local election officials rely on partners for cybersecurity support. This study provides a foundation for future studies of election cybersecurity and cybersecurity for local government entities.

The study uses a mixed methods research design. Primary quantitative and qualitative data were collected through an original survey of fifty local election administrators from fifty different local jurisdictions and interviews of fifteen election cybersecurity experts representing

two federal government entities, five state government entities, and five non-profit organizations. While the survey research allowed for the collection of information directly from local election offices, the expert interviews add a broader perspective.

A measure of the cybersecurity preparedness of local election administration offices was constructed through a systematic review of election cybersecurity guidance from two federal government entities and three non-profit organizations. Based on insights from the literature, my quantitative analysis explored relationships of internal characteristics of local election offices, characteristics of local jurisdictions, and intergovernmental partnerships with the cybersecurity preparedness of local election administration offices. Qualitative analysis was used to identify themes across expert responses about influential factors on the cybersecurity preparedness of local election administration offices and to describe the intergovernmental network within which local election administrators operate related to their cybersecurity efforts. While the collection and analysis of quantitative data allowed me to explore relationships between cybersecurity preparedness and potential factors of influence across many cases, the collection and analysis of qualitative data allowed for a more detailed description of the challenges local election offices face related to cybersecurity and how those challenges are being, or should be, addressed.

The findings of my quantitative analysis suggest that the human resources of local election administration offices influence their cybersecurity preparedness. I also find that local election offices which deploy electronic pollbooks tend to report higher levels of cybersecurity preparedness. The use of this specific digital election technology and the presence of in-house information technology (IT) specialists are both related to cybersecurity preparedness among the local election offices in my sample, even when accounting for other relevant factors.

My qualitative findings suggest that accepting support from state and federal government partners is key to cybersecurity preparedness for local election offices. Qualitative analysis also reveals that local election officials face deficits in the capacity needed to address cybersecurity. These deficits stem from insufficient human and financial resources. According to expert respondents, local election administration offices particularly lack in-house IT and cybersecurity expertise; therefore, they must rely heavily on outside partners for assistance.

As further described in the section below, election cybersecurity in the United States is a topic that gained broad attention immediately following the 2016 elections. In the years since 2016, US election officials and experts have become more aware of the cybersecurity threats to US election infrastructure, and cybersecurity risk management has become a persistent focus for the US election administration community. This dissertation covers the following information: First, it provides background information on the issue of US election cybersecurity and the role of local election administration offices. Second, it reviews relevant literature to identify potential influences on the cybersecurity preparedness of local election administration offices. Third, it describes a framework for analysis and a mixed methods research design based on the concepts of interest identified in the literature. Fourth, it presents a quantitative analysis of the relationships between the identified factors and the reported cybersecurity preparedness of a sample of local election offices. Fifth, it describes the findings of a systematic qualitative review of expert insight on the cybersecurity preparedness of local election offices. Finally, it presents key findings, conclusions, and directions for future research related to election cybersecurity and local government cybersecurity.

Background

In October 2016, the US Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) released a joint statement attributing influence operations targeting the 2016 US elections to the Russian government. In this statement, DHS and ODNI (2016) also said they suspected the Russian government was the source of scanning and probing activity targeting state-level election-related systems. This conclusion was later confirmed and built upon by DHS and a consensus of US intelligence agencies (Senate Intelligence Committee 2019–2020).

We now have confirmation that the Russian government targeted election-related IT systems owned and operated by US states and localities with scanning and probing activity (Mueller 2019, Senate Intelligence Committee 2019–2020). Russia most likely targeted election-related systems in all fifty US states (Senate Committee on Intelligence 2019–2020). We know the Russian Government compromised the computer network of the Illinois State Board of Elections and gained access to a database of registered voters (Mueller 2019, Senate Intelligence Committee 2019–2020). Additionally, according to the report of Special Counsel Mueller (2019), the Russian government installed malware on the network of an election technology vendor and used spear-phishing attacks to target and, in at least one case, breach the networks of county election officials in Florida. We know the Russian government conducted influence operations that attempted to impact the outcome of the 2016 US presidential election and sow distrust in American democratic institutions, and that Russian influence operations did not cease after the 2016 election (Senate Intelligence Committee 2019-2020). Sources confirming this activity and its attribution to the Russian government include bipartisan reports from the US Senate Intelligence Committee, a report from Special Counsel Robert S. Mueller, and multiple

public statements by state chief election officials, DHS, the Federal Bureau Investigation (FBI), and ODNI.

The Report of the Senate Intelligence Committee on Russian Active Measures Campaigns and Interference in the 2016 Election (2019–2020) offers an especially detailed account of the Russian government's inference in the 2016 presidential election. This report is further significant because its findings have bipartisan agreement. The report (2019–2020, Volume 2, 4) confirms that Russian actors "sought to influence the 2016 US presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin." The report (2019–2020) describes multiple ways Russia sought to interfere in the election including through a cyber intrusion of the Clinton campaign along with the subsequent release of documents, attempted and successful cyber breaches into state and local election administration infrastructure, and a coordinated social media campaign with the goal of influencing the opinions of American voters. The Committee further concluded (2019–2020, Volume 2, 8) that the goals of the Russian influence campaign, particularly those of the information warfare element, extend beyond the 2016 election.

On January 6, 2017, the former Secretary of Homeland Security ("DHS Secretary") Jeh Johnson, who served under President Obama, designated election systems as part of the critical infrastructure of the United States (DHS 2017). DHS considers US infrastructure critical when its "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS 2020). The elections as critical infrastructure designation was affirmed by former DHS Secretary

John Kelly after the Trump Administration took office. The designation has persisted throughout the Trump administration.

Currently, through the critical infrastructure designation, DHS prioritizes voluntary cybersecurity assistance for state and local election administration entities (EAC 2018, DHS 2020). As a result of the critical infrastructure designation, two coordinating councils were formed: the Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the Election Infrastructure Subsector Coordinating Council (EISCC). According to the DHS website (2020), the EIS GCC "enables local, state, and federal governments to share information and collaborate on best practices to mitigate and counter threats to election infrastructure," and the EISCC exists to "advance the physical security, cybersecurity, and emergency preparedness of the nation's election infrastructure, in accordance with existing US law." The EIS GCC is a council of federal, state, and local government entities involved in protecting elections from cyber threats, and the EISCC is comprised of private and non-profit sector entities which support elections (DHS 2020). The councils exist to coordinate efforts internally, with each other, and with outside entities. Participation from state and local governments in the EIS GCC is voluntary and is limited by the Council's charter to select representatives (EIS GCC 2017). Participation in the EISCC is open to "any owner or operator with significant business or operating interests in US election infrastructure systems or services" (EISCC 2018).

As the focus on election security has increased, risks to and vulnerabilities in election systems have been identified, and efforts to mitigate the risks and vulnerabilities have increased. DHS has reported on multiple occasions that every US state and many local jurisdictions have engaged with them, to varying degrees, to receive security-related services (e.g., Gallagher 2019). Through the EIS GCC, an election-specific information sharing and analysis center

(ISAC), called the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) was formed. The EI-ISAC, which is housed within the non-profit Center for Internet Security (CIS) and funded by DHS, provides cybersecurity and incident response services to its members and facilitates information sharing across the election ecosystem (CIS 2020). Membership in the EI-ISAC is voluntary and open to state, local, tribal, and territorial (SLTT) election offices and contractors supporting SLTT election infrastructure (CIS 2020). According to the National Association of Secretaries of State (NASS) (2020), as of February of 2020, all fifty states and about two thousand, five hundred local election jurisdictions are members of the EI-ISAC.

Sources of resilience in election systems have also been identified and built upon. For example, NASS (2017) has pointed to the decentralized nature of US election administration as a source of resilience. US elections are administered by state and local governments which, in some ways, could make widespread, national impacts on election integrity more difficult for malicious cyber actors to achieve. The EIS GCC (2020) has pointed to improved coordination across government and private sector partners, as well as efforts to prevent and detect cyber intrusions, as reasons for improved resilience. Similarly, Christopher Krebs, the current director of the DHS Cybersecurity and Infrastructure Security Agency (CISA), credited increased cybersecurity and coordination efforts from 2016 to 2018 as the reason the 2018 midterm election was the "most secure election in modern history" during Congressional testimony (DHS 2019).

Decentralization, though a source of resilience, also creates complexity in election cybersecurity efforts. Because American elections are decentralized, most of the responsibility for the administration of elections in the United States falls on counties and other local jurisdictions (Hale et al. 2015). Therefore, protecting elections from cyber threats is largely the

responsibility of the local government offices who operate many of the IT systems that are potential targets. There is ongoing public debate over whether local governments have adequate cybersecurity capacity to defend against cyber-attacks perpetrated by sophisticated nation-state actors, to what extent it should be their responsibility, and to what extent state governments and the federal government should increase their involvement in this area. Many state governments have increased their involvement over the past four years. Many state election offices now provide direct cybersecurity services and training to local election officials in their states (NASS 2020). The federal government has also increased their involvement through the critical infrastructure designation. Additionally, there have been multiple legislative efforts[1] in the years since 2016 to further shift election security responsibility and oversight to the federal government. However, US election administration, including the management and operation of much of the IT infrastructure on which elections rely, remains largely decentralized and under the purview of local government.

The capacity of local governments to serve as the party with primary responsibility for election cybersecurity probably varies based on the local government entity. Due to drastic variation in characteristics of local election offices and jurisdictions, such as differences in size, resource availability, demographics, and institutional configuration, I expect there is variation in the election cybersecurity preparedness of these local entities. This study explores the variation of cybersecurity capacity and practices of local election administration offices and, specifically, which factors influence the completion of cybersecurity practices by local election offices.

The importance of this research is clear. As elections are critical to a functioning representative democracy, protecting elections from any threat to their integrity is critical. The

[1] Examples include H.R. 1 and H.R. 2722 of the 116th Congress.

existence of a threat to election infrastructure from Russia has been established. Further, there are additional cyber threats to all state and local governments (CISA et al. 2019) which could impact election systems. Election security has been equated with national security by national leaders (e.g., DHS 2018) and bipartisan election officials (e.g., NASS 2019). Because the threat of cyber-attacks to elections is relatively new public problem, it has been studied only on a very limited basis and hardly at all within the US context by scholars of public administration (see Chapter 2). The advancement of this research agenda is warranted due to the importance and timeliness of the issue.

Further, it is important to a functioning representative democracy not only that elections are secure but also that voters are confident they are secure. This has similarly not been studied to a large degree within the US context, but international studies (e.g. Bratton et al. 2005) have shown that voters are less likely to participate in elections when their confidence in the integrity of the election is compromised. Studies of voter trust in the United States (e.g., Claassen et al. 2013; Kohut 2017) suggest that American voters have more concerns about the accuracy of the vote count when electronic machines, as opposed to paper ballots, are used for vote casting. Therefore, cybersecurity concerns, or at least technology-related concerns, may affect voter confidence in the United States. Though the impacts of cybersecurity-related issues on voter confidence is beyond the scope of this research, my findings provide some groundwork for future research in this area.

The Intergovernmental Nature of US Election Administration

The story of election authority in the United States is the classic story of the jurisdictional power struggle in the American federalist system of government. The US governmental system

of federalism is a system of overlapping authorities rather than one in which power is separated by clearly drawn lines (Wright 1974). This rings true for the US election administration system. Though power and responsibility related to elections is unevenly distributed among the three main levels of government, all layers and branches of government, as well as many non-governmental actors, have a role (Hale et al. 2015).

The elections clause of the US Constitution authorizes state legislatures to determine the "times, places, and manner" of congressional elections. This is subject, however, to the authority of the US Congress to "make or alter" state regulations (Morley and Tolson 2018). While states provide most of the legal framework for election administration in the United States today, some laws and policies which impact election administration have been established at the national level (Hale et al. 2015). Federal laws related to elections largely pertain to ensuring participation and inclusion. Further, the US Constitution sets some rules and parameters for elections, including age, residency, and citizen requirements (Morley and Tolson 2018). The federal government has also been involved in shaping the legal framework of US elections through decisions of the US Supreme Court and other federal courts (Hale et al. 2015).

Local governments hold most of the responsibility for administering elections (Hale et al. 2015). However, state governments have become increasingly involved in election administration since the early 1990s. Since the 1993 National Voter Registration Act (NVRA), all states have been required to have a state Chief Election Official (CEO) who oversees election administration across the state (Hale et al. 2015). The role of the CEO varies from state to state, but they are all involved in the implementation of the NVRA (Hale et al. 2015, 32–33).

The federal role in election administration is limited. However, federal involvement has increased since the 2000 presidential election and shows continued signs of increase. The US Election Assistance Commission (EAC) was established in 2002 by the Help America Vote Act (HAVA) (Hale et al. 2015, 83). The EAC is a non-regulatory federal commission tasked with providing assistance to state and local election administrators, particularly relating to the implementation of HAVA (EAC 2018). Part of this role is maintaining voluntary national guidelines for voting systems called the Voluntary Voting System Guidelines or the VVSG (EAC 2018). More recently, the federal government has become involved in election administration in a support and advisory role, specifically in the area of cybersecurity.

Federal assistance, now provided by DHS through the elections as critical infrastructure designation, is a welcomed development by some state and local election administrators, while others have seen it is as federal overreach and are concerned about how it could influence the way American elections are administered (EAC 2018). NASS (2017), for example, issued a formal position in opposition to the designation. Some concerns may stem from the fact that voluntary voting system guidelines set by the federal government have not remained fully voluntary in application. Though state and local election officials have discretion over their compliance with the VVSG, the voluntary guidelines affect election technology procurement processes throughout the United States. According to Hale and Brown (2013, 429), election officials commonly report that "their ability to acquire new equipment is stymied by a time-consuming, expensive, and ineffective federal certification process that, although voluntary, has become the *de facto* standard for voting equipment manufacturers." Although the involvement of the federal government in securing election infrastructure is currently voluntary for state and local election officials, the voluntary role of the federal government could eventually influence

the private market of election technology and could lead to statutory requirements at the state or federal level. Already, federal legislation[2] has sought to formalize voluntary intergovernmental relationships and voluntary election cybersecurity guidelines provided by the federal government.

The result of this decentralization, where states hold much of the legislative authority over elections and local jurisdictions lead implementation, is a diverse range of election administration rules, structures, and practices across the United State and even within some states. For example, the secretary of state is the state CEO in most US states, but in thirteen states, a different state government position serves as the state CEO (Hale et al. 2015, 34–35). Further, some state CEOs are elected, while others are appointed. Other examples relate to election practices. While most states primarily hold in-person elections, some states conduct their elections almost entirely by mail (Hale et al. 2015, 127–128). Election administration varies further at the local level, and there are approximately eight thousand local election jurisdictions in the United States (Hale and Brown 2020, 29). In most states, local election officials within county governments administer most elections. In other states, municipalities hold most of the responsibility for administering elections. Some election administration practices, such as the use of vote centers, vary within states at the local level (Hale et al. 2015). The earliest scholarly studies of election administration in the United States (e.g., Harris 1934) show that localized election rules and structures evolved from path dependent processes linked to culture during the colonial period and the early years of US expansion (Brown et al. 2020). Recent state election administration innovations have been influenced by state political culture, region, partisanship,

[2] An example is H.R. 1 of the 116th Congress

and/or pluralism (Hale et al. 2015). Any research of US election administration must strive to account for the variability across and within states.

Private vendors are also an important part of the intergovernmental structure of US election administration (Hale et al. 2015, 45), especially related to election technology and cybersecurity. Much of the election infrastructure now deemed critical to the United States is manufactured and serviced by private businesses who have been contracted by local government offices (Hale et al. 2015, 45). Therefore, when studying the capacity of local governments to protect election systems from cyber threats, their coordination with and reliance on private-sector vendors must be considered. The role of third-party vendors in securing US elections may influence voter perception. Milward and Provan (2000) argue that government contracting with third-party providers may influence its perceived legitimacy. As election administrators often contract with private business to provide infrastructure and even to provide cybersecurity services to protect election systems, the election officials must consider and account for potential unknown vulnerabilities that could be introduced by non-governmental actors playing a role in election cybersecurity. They must also consider vulnerabilities that may not actually exist but are perceived by the voting public.

Non-profit associations also play a substantial role in election cybersecurity in the United States by providing training and resources. Like most public administrators, election administrators operate in intergovernmental networks that include and sometimes rely on supporting nonprofit organizations. Hale (2011) argues that information relationships between nonprofit organizations and public administrators can enhance the ability of the public sector to deliver its responsibilities. This may be applicable to the responsibility of election administrators to protect elections from cyber threats. Professional associations of election officials, such as the

National Association of State Election Directors (NASED), NASS, and the National Association of Election Officials (the Election Center), have helped with coordination between government layers and agencies (Brown et al. 2020, 189). Professional associations play a key role in distributing information from the federal government to state and local governments. Other non-profit associations, including research institutes and advocacy groups, have engaged in research aimed at finding election cybersecurity solutions and also in providing training, outreach, and resources for state and local election administrators (Brown et al. 2020, 190).

Overview of Study

The focus of my research is on local election administration offices. The variation in cybersecurity capacity across these local jurisdictions is likely vast. Local election jurisdictions in the United States range from metropolitan counties that serve more voters than most US states, to extremely small and rural counties, townships, and villages. For example, one on end of the spectrum is the Los Angeles County Registrar's Office that, according to its website, has hundreds of staff who serve about four million, eight hundred thousand registered voters and oversee about five thousand voting precincts. Only ten US states have a larger number of registered voters than Los Angeles County, according to US Census Bureau statistics. On the other end of the spectrum, there are thousands of small election jurisdictions with one or two part-time election administrators who have additional local government responsibilities or unrelated full-time jobs. Jurisdiction sizes are as small as about three hundred fifty registered voters (Hale et al. 2015, 39). Vast differences in the population of local jurisdictions and in characteristics, such as staff size and budget allocation, of local election offices are likely to impact their capacity to prepare for cybersecurity threats. This is why this study takes the approach of trying to identify which factors lead to variation in preparedness efforts.

The purpose of this research is to provide evidence that could help localities identify areas for improvement and inform the role of state governments and the federal government in this arena. My findings highlight the need for resources and intergovernmental support for local election administration offices. These findings are consistent with conventional assumptions in the field of practice. While further research is needed to confirm causal relationships between my variables of interest, my findings propose a basis for future theory-building and provide a foundation for the advancement of a public administration research agenda focused on cybersecurity in election administration and broader inquiries into local government cybersecurity preparedness.

This dissertation is organized into six chapters: Chapter 2 provides a review of relevant literature on intergovernmental relations, local government capacity, public sector emergency management, and the digital divide. Themes across these streams of literature led me to expect that factors creating a digital divide for individuals and organizations likely influence the IT and cybersecurity capacity of local government entities and that coordination with network partners will impact the cybersecurity efforts of local election offices. Chapter 2 presents an analytic framework to explore these potential influences on the cybersecurity preparedness of local election administration offices. This framework includes several hypotheses and a research expectation based on findings from the literature.

Chapter 3 describes the mixed methods research design and the methodology used to test the hypotheses and explore the research expectation outlined in Chapter 2. Chapter 3 includes a description of how key concepts were operationalized into measurable variables. It describes the systematic review of cybersecurity guidance, which was conducted to identify key cybersecurity concepts to construct the dependent variable. This chapter also describes the sources from which

data were collected. They include an original survey of local election administrators, a series of semi-structured interviews of election cybersecurity experts, and secondary data from public data sources including the US Census Bureau and state and local government websites. I also describe how the survey and interview instruments were created and my sampling approach. Finally, Chapter 3 addresses my process for producing grounded theory and the specific data analysis techniques used to produce the findings presented in the subsequent chapters. Data were analyzed using bivariate quantitative analysis techniques, including correlation coefficients and difference of means tests as well as bivariate Ordinary Least Squares (OLS) regression analysis, multivariate OLS regression analysis, and qualitative pattern matching.

Chapter 4 presents the findings of my quantitative analysis. First, I descriptively analyzed the local election administration offices and corresponding jurisdictions in my sample. Though the local election offices in the study appear to represent higher than average levels of cybersecurity preparedness, the sample included adequate variation in the dependent variable and most of the independent variables to analyze relationships between variables. Next, I explore the bivariate relationships between the reported cybersecurity preparedness of the offices in the sample and reported characteristics of the offices, characteristics of the local jurisdictions, reported relationships with partners, and other factors I identified as potentially relevant. A number of variables positively covary with the reported cybersecurity preparedness of the offices in the sample including: (1) the office's budget; (2) the office's total number of election administration employees; (3) the number of IT specialists within the office; (4) whether the local election official has an election administration certification; (5) the office's reported partnerships within local government; (6) the use of electronic pollbooks within the local jurisdiction; (7) the size of the local jurisdiction; and (8) the racial, ethnic, and language diversity

of the local election jurisdiction. Contrary to my expectation, the reported cybersecurity compliance of local election offices in the sample is negatively correlated with the percentage of high school graduates in the jurisdiction. Finally, I present a series of multivariate OLS regression models based on my analytic framework. According to the multivariate analysis, the use of electronic pollbooks and the number of in-house IT specialists appear to be significantly related to the cybersecurity preparedness of local election administration offices when controlling for other relevant factors.

Chapter 5 presents the findings of my qualitative analysis. Throughout Chapter 5, I describe themes and patterns identified through a systematic qualitative analysis of interview responses. I present overall themes as well as themes broken down by specific subtopics and categories of respondents. Almost all of the respondents made several points related to the cybersecurity preparedness of local election offices: (1) it is essential for local election officials to accept assistance from their state's election office; (2) a lack of technical cybersecurity expertise within most local election administration offices creates challenges related to cybersecurity awareness and implementation; (3) other partnerships are also important for local election offices, including partnerships with DHS and non-profit organizations; (4) sharing information with other election offices through established forums is important to the cybersecurity preparedness of local election offices; (5) local election administrators should focus on basic cybersecurity measures because taking specific basic steps goes a long way toward protecting election infrastructure; and (6) most local election administrators need additional financial resources and training to improve their cybersecurity preparedness. Additional themes from the interview responses are discussed Chapter 5. Chapter 5 also presents

the findings of a qualitative analysis of the responses to open-ended survey questions by some of the local election administrators who participated.

Chapter 6 includes my conclusions and contributions. This chapter also addresses the limitations of my study and directions for future research. Overall, I conclude that the most important influences on the cybersecurity preparedness of local election administration offices include the human resources within the office and cybersecurity support from partners outside the office. More specifically, having election administration staff with IT expertise and receiving assistance from the state election office and from DHS tends to help local election officials improve the cybersecurity preparedness of their office. Further, most local election offices lack adequate resources to handle cybersecurity risk management on their own. Outside partners help local election officials close gaps in capacity. I also conclude that a likely reason the use of electronic pollbooks is strongly related to cybersecurity preparedness for local election offices is that offices with higher levels of technological sophistication are more likely to deploy electronic pollbooks in their jurisdiction. Finally, I conclude that since this study is exploratory and limited in scope, additional evidence is needed to confirm my findings. I present several opportunities for future research based on the foundation provided by this study.

Chapter 2: Identifying Potential Influences on Local Election Office Cybersecurity

Introduction

Public administration and public policy literature on cybersecurity issues in election administration is nearly non-existent because the issue is relatively new. Even literature broadly exploring security issues in elections tends to focus internationally with very little attention to the US context. Therefore, I reviewed literature from several broadly relevant areas of research to identify potential influences on local election office cybersecurity preparedness and construct an analytic framework for this study. Public administration literature on US election institutions, local government capacity, intergovernmental relations, emergency preparedness and management, and the digital divide together provide some common themes and individually provide unique insights on what may impact cybersecurity capacity and preparedness for local election offices. I also reviewed election cybersecurity documents from government entities and the non-profit sector as well as technology studies focused on the security of voting systems for additional insight from the information technology perspective.

The first several sections of this chapter present a review of the literature organized by topic: (1) intergovernmental relations, (2) local government capacity, (3) public sector emergency management, (4) election cybersecurity, and (5) the digital divide. Throughout these sections, themes across the multiple streams of literature are identified. The final section of the chapter describes the themes that appear to be the most prevalent across the literature and the most relevant to my topic of exploration. In the final section, I outline two series of hypotheses. The first set of hypotheses, based primarily on potential factors identified from the local government capacity literature and the digital divide literature, expects that characteristics

internal to local election offices, including human and financial resources, impact their cybersecurity preparedness. The second set of hypotheses, based on the digital divide literature, explores whether characteristics related to the population a local election office serves impact the cybersecurity preparedness of the office. Based on the relevant literature, I expect that the factors included in the first set of hypotheses are more likely to influence the cybersecurity preparedness of local election offices. Nonetheless, those in the second set of hypotheses should also be explored. Finally, this section describes my expectation for qualitative analysis. I expect the qualitative analysis will show that whether and how local election offices coordinate within intergovernmental networks will impact their cybersecurity preparedness. This research expectation is based on themes prevalent across the literature on intergovernmental relations, emergency management, and local government capacity.

Intergovernmental Relations

Election cybersecurity is a problem that largely falls on the shoulders of local government election administrators but, like most modern public problems, is being addressed within a vast intergovernmental network (Hale et al. 2015). Therefore, it is important to review the public administration literature on intergovernmental relations for insight on how networks affect the ability of local government to deal with complex public problems. Most intergovernmental relations literature acknowledges that networks can both complicate and enhance public service. For example, Kettl (2000; 2006), argues that having to manage interorganizational networks that include non-governmental actors can reduce a government agency's capacity simply due to the complexity of coordination. When public service delivery relies on a complex interorganizational network, responsibilities can become confused and accountability is difficult to track. Kettl (2006) suggests that although intergovernmental

networks lead to increased complexity and blurred boundaries, delivering services through networks has become the reality of public administration and collaborating within networks is the best option for addressing the complex public problems of the modern era. He (2006) argues that as complexity continues to increase, improving coordination will be more important than drawing additional boundaries between government jurisdictions and non-governmental organizations. Hale and Slaton (2008) offer perspective on how intergovernmental networks specifically impact local election administrators. They (2008) lend support for the argument that interorganizational collaboration may be the most useful approach for addressing challenges in public administration and specifically election administration. They (2008) found that local election administrators can increase their capacity by forming networks, professionalizing, and collaborating. Hale and Slaton (2008) further found that locally led capacity-building, rather than federal mandates, was the most important mechanism for confronting serious election administration challenges brought to the forefront by the 2000 presidential election. If Hale and Slaton's (2008) findings are also applicable to the serious election administration challenges brought to the forefront by the 2016 presidential election, then collaborating with intergovernmental partners while maintaining control of implementation may be the best approach for local election offices to build capacity and address challenges related to cybersecurity.

This study explores how working within an increasingly complex intergovernmental network impacts the capacity of local election offices to address cybersecurity. The recent introduction of the federal government as a major player into already complex intergovernmental election administration networks, which include at least the state government, multiple local government offices, private vendors, and non-profit associations could complicate coordination

even further. Alternatively, or additionally, the federal government could help address capacity deficiencies (Honadle 2001) related to cybersecurity protection that may exist within local election administration offices. The literature leads me to expect both scenarios are likely.

The concepts of control and accountability are prevalent throughout intergovernmental relations scholarship. Intergovernmental relations scholars agree that public administrators can improve their ability to address challenges by working with partners inside and outside of government but that they need to maintain control of their responsibilities. There are a range of scholarly perspectives on how well publicly accountable public administrators maintain control within intergovernmental networks. For example, Milward and Provan (2000) argue that governments often lack mechanisms of control over non-governmental actors within networks. They (2000) acknowledge that this can lead to increased flexibility in operations but caution that this introduces principal-agent problems and instability as networks will change over time. Alternatively, Agranoff and McGuire (2003) argue that government units operate at the center of intergovernmental networks, largely controlling the extent and type of collaborative public management in which a governmental unit engages. They (2003) argue that there will be variation in how local governments engage in collaborative public management and demonstrate that variation in approaches to collaborative management are associated with variation in the policy approaches of local jurisdictions. Based on these arguments, differing approaches to how to collaboratively manage within the complex intergovernmental network surrounding election cybersecurity may be related to different approaches to addressing cybersecurity for election administrators. An important factor to consider may be the extent to which local election officials are able to maintain control of their engagement in a network.

In addition to coordination and collaboration between layers of government and non-governmental actors, an important element of intergovernmental relations is the interaction and interdependencies between branches of government. Election administrators, like other public administrators, are subject to the will of policymakers. Legislative or regulatory changes could force significant changes in how the intergovernmental network surrounding election cybersecurity operates and coordinates as well as in how individual election officials administer and protect elections. Derthick (1990) argues that considering the influence of policymaking institutions is important to the study of agency performance. Further, she (1990) contends that policymakers often impede good administration by making policy without understanding administration. This could be an issue in election cybersecurity where Congress, state legislatures, state and federal executive administrations, and even county commissions or city councils can make policy dictating election cybersecurity efforts with limited understanding of election administration or cybersecurity. This study considers the role of policymakers to a limited degree through expert interviews. However, further study of the impact of policymakers and policy decisions on election cybersecurity is necessary to further our understanding.

Overall, the intergovernmental relations literature stresses the importance of collaborating with intergovernmental partners to address complex problems. There seems to be consensus that network actors can help public administrators, particularly those within local government, address complex problems and improve the delivery of public services. However, it is important for the responsible government entity to maintain control of the intergovernmental network's efforts and to create awareness for partners who are trying to provide support. Further, while operating within intergovernmental networks can improve service delivery, it also increases complexity. This suggests it is important to coordinate efforts with partners by communicating

clearly about roles and responsibilities. My study explores the influence of an intergovernmental network on the responsible government entity's ability to address a developing public problem.

Local Government Capacity

Another scholarly perspective that can shed light on what influences cybersecurity preparedness for local election administration offices is the literature related to local government capacity. Gargan (1981) argues that a difficulty in assessing local government capacity is that the concept of capacity is difficult to define. This difficulty is one reason I focus on reported levels of resources and reported execution of cybersecurity practices. My findings, however, lend insight into which concepts should be included in a measure of cybersecurity capacity for local government entities.

The topic of capacity is complex because the roles of local governments evolve as they take on emerging public problems. Honadle (2001) suggests that local government capacity is not about the capacity to address any potential challenge that comes along as that would be impossible. Rather, she (2001) argues one of the most important capacity issues for local governments is being prepared and able to add capacity as new administrative challenges inevitably arise. This idea is similar to the earlier conclusion of Gargan (1981) that the emergence of new problems is likely to be one of the most significant challenges to local government capacity. These conclusions are particularly relevant to election administrators who seemingly face new challenges with every major election cycle including widespread technology problems, major weather events, terrorist attacks, cyber-attacks and, most recently, a global pandemic. Cybersecurity in elections is an evolving problem that requires local governments to

continually add capacity. Cybersecurity risks are not static, and new ways of mitigating them are regularly introduced.

Gargan (1981) further suggests that increasing interdependencies in the public sector, changes in expectations about the adequacy of public services, and the redefinition of roles are additional challenges creating capacity deficiencies for local governments. Each of these challenges is applicable to cybersecurity in elections: (1) interdependencies are increasing as the federal government takes on an increasing role, voluntary or otherwise, related to the critical infrastructure designation; (2) what used to be acceptable election security practices are no longer adequate – for example, new checklists of election cybersecurity best practices which define new expectations for election administrators are regularly released by government and non-governmental organizations; and (3) many local election officials are now often expected to perform as IT managers and cybersecurity managers (EAC 2018), in addition to their prior roles. These challenges must be considered when assessing cybersecurity preparedness at the local level. Agranoff and McGuire (2003) also suggest that increasing interdependencies affect local government capacity. They (2003) argue that the capacities required to operate in collaborative environments are different than a local government's capacity to manage itself hierarchically. As local election officials are operating in an increasingly collaborative environment, this is an important consideration.

There is agreement across the public administration literature that information and other types of assistance from outside entities can help public administrators address challenges and deliver on their responsibilities (e.g., Hale 2011, Honadle 2001, Kettl 2006, Kim and Bretschneider 2004). Kettl's (2006) perspective broadly addresses intergovernmental coordination as he argues that public administrators must focus on coordinating with others in

their networks in order to be able to confront complex challenges. Hale (2011), more specifically, finds that information from non-governmental organizations helps public administrators improve their service design and delivery. Honadle (2001) argues that support from higher levels of government is an important aspect of capacity building for local governments when addressing new problems. Similarly, Kim and Bretschneider (2004), when specifically exploring the IT capacity of local governments, suggest that support from other levels of government as well as from other local government entities influences capacity. Overall, the literature suggests that accepting assistance from and coordinating with partners inside and outside government may help local election administrators address the challenge of cybersecurity threats.

Cybersecurity is a demanding challenge for local governments. Norris et al. (2018) suggest local governments face thousands of cyber-attacks per day and find that several factors including insufficient funding and staffing and problems of governance and enforcement impede cybersecurity for local governments. Kim and Bretschneider (2004) similarly argue that a local government's IT capacity is impacted by its financial resources and the leadership of an IT manager or lack thereof. The literature specific to cybersecurity capacity for local government is limited. This study attempts to add to our understanding of what affects the cybersecurity capacity of local governments.

In summary, a glimpse at literature on local government capacity and capacity building efforts suggests that factors influencing the capacity of local election administration offices to address cybersecurity problems include the following: their ability to adapt to new problems, new roles, and new expectations; their access to financial resources; the presence of a qualified IT or information security manager who understands cybersecurity and can lead the office; and

the availability and acceptance of support from non-governmental organizations, other layers of government, and other offices, departments, or entities within the local government.

Emergency Management

Because extant research on cybersecurity preparedness in public administration is extremely limited, I look to the broader public emergency management literature for insight into which factors influence the emergency preparedness of government entities. Due to post-9/11 federal government restructuring including the creation of DHS, disaster management and homeland security issues have become bureaucratically intertwined at the national level (Birkland and Waterman 2008; Birkland 2009; Comfort et al. 2012), and many states have followed suit. The issue of election cybersecurity falls at the intersection of the two issues, as it is a national security issue that could involve emergencies which impact the administration of elections.

According to some emergency management scholarship, the creation of DHS and the placing of the Federal Emergency Management Agency (FEMA) under DHS may have led to neglect of natural disaster preparedness, which played a role in deficient responses to major disasters such as Hurricane Katrina (Birkland and Waterman 2008; Birkland 2009; Comfort et al. 2012). Scholars of emergency management (e.g., Birkland and Waterman 2008; Birkland 2009; Schneider 2008) have also cited coordination problems, particularly misunderstandings about responsibility stemming from federalism and related interdependencies, as a contributing factor to preparedness and response failures in recent major disasters.

The emergency management literature highlights several important considerations for election cybersecurity preparedness. First, at the federal level, election administration

cybersecurity issues fall under the purview of DHS along with other emergency management and homeland security issues. Birkland and Waterman (2008) suggest that intense focus on one issue by DHS can lead to neglect of others. Therefore, if other national security issues overshadow election cybersecurity concerns or a major national disaster captures the attention of the agency, the election cybersecurity issue could be neglected by the federal government. This could lead to decreased or degraded federal cybersecurity assistance for local election administrators. As local election administrators grow more dependent on DHS for cybersecurity support, this potential decline in assistance would become more problematic. Alternatively, if cybersecurity sits at the forefront, preparedness to protect from and respond to natural disasters may be neglected. Birkland and Waterman (2008) suggest a similar relationship, noting that anti-terrorism activities distracted from natural disaster preparedness and led to a defective response to Hurricane Katrina. This failure would raise a separate concern for election administrators as natural disasters, such as Hurricane Katrina and Superstorm Sandy, have caused major election disruptions and challenges for local election administrators.

Second, and more relevant to this research, is that intergovernmental coordination problems, such as the complexity of administration and blurred boundaries of authority described by Kettl (2006), can impede emergency preparedness and response (Schneider 2008). As established above, tackling the issue of cybersecurity in election administration is and will surely continue to be an intergovernmental endeavor. However, in the current system, local election administrators tend to be chiefly responsible for carrying out elections. Following conclusions from both the intergovernmental relations and emergency management literature, a key factor influencing the cybersecurity preparedness of local election administration offices is likely to be strong coordination with relevant partners. This coordination may include efforts like formally

assigning and documenting who is responsible for which tasks and establishing formal communication processes with internal and external partners, as suggested by Kettl (2003).

Schneider's (2008, 1) research suggests that "the intergovernmental response to Hurricane Katrina collapsed because those involved in the process did not have a clear understanding of their own roles and responsibilities or how the entire governmental response system should operate." Avoiding this situation with election cybersecurity is likely to be critical to preparedness and particularly to an effective response to cyber incidents. Considering that much of the ultimate responsibility for election cybersecurity currently belongs to local election administration offices, conclusions from the intergovernmental relations literature suggest that local election administrators should ultimately take responsibility for the entire process to include establishing clear directions for which roles and responsibilities belong to which party, following through on their own roles and responsibilities, and monitoring outside partners to ensure they have followed through on their roles and responsibilities. As suggested by Hale and Slaton (2008), federal efforts can aid in locally led election administration capacity-building activities, but responses to past election administration challenges have demonstrated that the leadership and actions of local election administrators may be more important than federal intervention. In summary, there is agreement between the intergovernmental relations literature and the disaster management literature that coordination including the assignment of roles and responsibilities within intergovernmental networks is key to effective administration, and particularly to preparedness and response.

Cybersecurity for Elections

Cybersecurity in elections has distinct characteristics from other emergency preparedness issues and also from other cybersecurity issues. A review of the election cybersecurity best practice guides provided by governmental organizations including the EAC and the National Institute of Standards and Technology (NIST) as well as non-governmental organizations, including Harvard University's Belfer Center, the Election Center and the Center for Internet Security (CIS), add to the argument that interorganizational coordination is a key factor. The guides recommend communicating regularly with partners and working with partners to develop plans. However, there are also many technical components to cybersecurity preparedness addressed throughout the guides. The technical cybersecurity expertise required to accomplish some of the tasks laid out in these best practices, such as "use an intrusion detection system and monitor incoming and outgoing traffic for signs of irregularities, such as above average traffic, large amounts of data being transmitted, etc." (EAC 2018) suggests that technical cybersecurity expertise is needed. Potential human resource deficiencies, particularly in meagerly staffed election administration offices, could pose a barrier to cybersecurity preparedness (Norris et al. 2018).

A review of best practices related to election cybersecurity also reveals that there is much more involved in protecting elections from cyber threats than the issue of securing vote casting and tabulation technology. Although the security of vote casting machines is the issue that seems to get the most media and legislative attention, other election systems, most prominently voter registration systems, were targeted by Russia in 2016. Local election officials work within and often manage vast IT systems which include standard office infrastructure like computers, a network, and email and also include election-specific systems like voter registration systems, election management systems, electronic pollbooks, and election night reporting systems (EAC

2018). The election cybersecurity best practices I reviewed are more focused on the security of the IT infrastructure supporting election administration than on securing vote casting and tabulation systems. There are some recommendations in election security guides that address safeguards specific to vote casting and tabulation systems, but it is very clear these systems are just one element of the technology supporting elections that election officials must be concerned with protecting.

Further, it is clear election officials must guard against attacks from a range of potential actors. We know that foreign adversaries specifically targeting election infrastructure is one concern. However, as a government entity, another threat to local election offices are ransomware attacks perpetrated by a range of cyber actors including foreign and domestic cyber criminals. Ransomware attacks against government have become increasingly prevalent in recent years leading to calls for increased cybersecurity measures for all state and local government entities throughout the United States (CISA et al. 2019).

A brief review of election security literature from the information technology perspective reveals potential technical solutions to some election cyber threats and related voter confidence issues (e.g., Essex 2017; Moher et al. 2014). A solution that stands out in the literature is end-to-end voter verifiability which is a process for allowing voters to verify that their cast votes and recorded votes are consistent. However, computer science scholars (e.g., Essex 2017; Moher et al. 2014) find that there are social challenges which may hinder the success of this technical solution. This literature suggests that technical solutions alone may be not sufficient. Particularly, Essex (2017) and Moher et al. (2014) argue that getting voters to buy into and participate in election verification efforts may be a key element of success. Further, most of the technical solutions suggested by this stream of literature often fall beyond the direct control of

local election administrators and, therefore, are not within the scope of this study. For example, changing voting processes often requires legislation or appropriations for new technology which must come from the state or federal government, or at least from local legislative branches such as a county commission. Further, local election administrators are reliant on a small pool of election technology vendors who may or may not integrate recommended technical controls into the products available on the market.

This section primarily relies on documents from government and non-profit organizations because academic attention on election cybersecurity is extremely limited. While there has been some election cybersecurity research in recent years, very few studies explore the issue from the public administration perspective. My study aims to fill this gap and provide a foundation for further academic inquiry of how local public administrators can improve the cybersecurity preparedness of local governments.

The Digital Divide

Finally, a literature which provides insight into which factors may influence cybersecurity preparedness efforts for local election administration offices is that on the digital divide. The digital divide is a term coined by scholars to describe inequality of access, capacity to use, and use of digital technology, particularly the Internet. Most often, the digital divide literature focuses on individuals as the unit of analysis. However, some studies have explored the digital divide for organizations by considering which factors influence some organizations to have more advanced technological capacity and to employ more sophisticated technological innovations than others. Though little attention has been given to whether a digital divide impacts local governments, it seems logical that factors influencing IT sophistication for other

organizations would influence IT sophistication for local government organizations. As cybersecurity and IT rely on many of the same capabilities, it further seems logical that factors which influence an organization's IT sophistication may also influence its cybersecurity sophistication.

Most research on the digital divide has developed from the starting point of the digital divide for individuals. The Pew Research Center has conducted extensive research on the digital divide, specifically related to internet use of US residents. Their studies consider not only access to the Internet but also actual use, which will be influenced by access but may be influenced by additional factors such as ability and comfortability of use (Pew 2016). The findings from a series of Pew studies on the digital divide in the United States suggest the main indicators affecting whether a person uses the Internet and digital technologies are whether individuals live in rural locations, age, education level, income level, and the presence of disability (Pew 2016).

Pew has found that throughout most of the modern era, the digital divide has strongly affected lower-income Americans (Anderson 2017). Although low-income Americans have begun adopting technology at increasing rates, they remain less likely than the average American to have at-home internet, smartphones, computers, tablets, or any combination of these technologies (Anderson 2017). Race and ethnicity are not among the strongest indicators of the digital divide, according to Pew studies. However, Pew studies found that Black Americans and Hispanic Americans are less likely, on average, than white Americans to have internet and computers in their homes (Perrin 2017). Pew surveys suggest Black and Hispanic Americans use smartphones to bridge the digital divide, but these minority groups still own smartphones and tablets at slightly lower rates than white Americans (Perrin 2017).

According to Pew, the digital divide most strongly persists for rural Americans (Perrin 2017) and Americans with disabilities (Perrin and Anderson 2017). Adults living in rural areas are less likely than the average American adult to have internet connections, computers, smartphones, or tablets in their homes (Perrin 2017). The rural versus non-rural digital divide does not show signs of closing, according to these Pew studies (Perrin 2017). Even more striking than the differences in technology ownership are the much lower than average rates of reported internet use among rural adults (Perrin 2017). While eighty percent of urban-dwelling Americans and seventy-sic percent of those in suburban areas reported daily internet use in Pew surveys, only fifty-eight percent of rurally located Americans say they use the Internet daily (Perrin 2017). Pew's research also suggests interactive effects of some demographic characteristics related to the digital divide. For example, the digital divide affects high-income Americans who live in rural areas to a lesser extent than low-income Americans in rural areas (Perrin 2017). This finding suggests the digital divide is not simply an artifact of broadband access. Americans with disabilities are less likely than non-disabled Americans to use the internet or to own smart devices (Perrin and Anderson 2017). A prominent reason for this seems to be that Americans with disabilities are much less likely to report high levels of confidence using the Internet than the average American (Perrin and Anderson 2017).

Similar to Pew's studies, Mossberger et al. (2013) found that income, education, age, race, and geographic factors influence the digital divide. Further, they (2013) found that a person's employment experience and English language skills affect his or her internet and technology access and use. Mossberger et al. (2013) looked at the digital divide from the perspective of individuals as well as cities, and they compared cities and neighborhoods to each other and to other geographic locations. They (2013) found that although there is a substantial

rural versus non-rural digital divide, some of America's largest cities are lagging in providing internet access to residents. For some indicators of the digital divide, they found that Americans living in cities are falling behind those in suburban areas.

These findings provide evidence of what creates a digital divide for individuals. Some of these factors, such as geographic location, may also impact local government. Where a government entity is located may impact its access to IT and cybersecurity support services. Further, the factors which influence technology capacity and use for individuals may extend into the workplace. When an organization's leaders and staff are impacted by the digital divide, this is likely to influence the IT sophistication of the organization. For example, the education level and professional experience of a local government's staff may impact the ability of the staff to manage the organization's IT which would influence the IT sophistication of the local government entity. Further, since cybersecurity is related to protecting IT, the capabilities of the staff to implement IT is likely to be related to their capacity to protect the IT from cyber threats.

Some scholars have explored how the digital divide impacts not only individuals but also organizations (e.g., Riggins and Sanjeev 2005). Another example is McNutt (2008) who explored how the digital divide may affect advocacy organizations. He (2008) theorizes that prevalent digital divide indicators for advocacy organizations likely include a lack of technological expertise within the organization and inadequate financial resources. Iacovou et al. (1995) and Rogers (1995) found that the tendency of organizations to implement technological innovations and information technology solutions is related to the size of organizations. Iacovou et al. (1995) claim that small firms tend to lack IT expertise and resources. Riggins and Sanjeev (2005) found themes among organizational digital divide studies including that organization size,

the role of management, and geographic location are influencers of organizations' adoption of innovations and solutions for information and communication technology.

Research which directly questions how the digital divide affects local governments specifically is, at best, scarce. However, it seems reasonable that the factors which influence technology access, capacity, and use for individuals and especially the factors which seem to influence IT innovation and solutions for organizations may extend to local government offices. Themes across the digital divide literature suggest that some of those factors may be the education, professional experience, technical expertise, number of election administration staff and whether an office is located in a rural area. As discussed in the previous section, addressing election cybersecurity requires technical expertise which includes knowledge of the Internet, networks, software, hardware, and additional technologies. If digital divide factors affect local governments, they likely influence cybersecurity preparedness practices for local election administration offices. Given that according to DHS (2020), the United States has a growing shortage of cybersecurity workers and the public sector faces unique cybersecurity staffing and workforce development challenges, the human resource factor is further likely to be influential on local election administration offices' efforts to address election cybersecurity challenges.

Analytic Framework: Hypotheses, & Research Expectations

As this is a new research agenda, there is not a well-developed theoretical foundation related to cybersecurity efforts within US election administration upon which to build. While I do not rely on existing theory, I use empirical findings from relevant literature to inform my research design and expectations. Themes identified from the above literature review were used to generate several hypotheses and one research expectation which are laid out in this section as

an analytic framework for my research. As this research investigates a relatively new issue in public administration, exploratory research is appropriate. Rather than contributing to an existing theory, I draw conclusions from my exploratory inquiry to produce a grounded theory which is presented in Chapter 6.

The hypotheses and research expectation are based on two major themes identified throughout much of the literature: (1) factors related to the digital divide and local government capacity, most prominently a local government office's financial and human resources are likely to influence its cybersecurity capacity and therefore preparedness, and (2) as protecting elections from cyber threats is a public problem being addressed within an intergovernmental network, a local government office's coordination and collaboration within that network are likely to affect its cybersecurity preparedness. The literature suggests local election offices should accept assistance from network partners but maintain control of implementation. Throughout the study, I consider collaboration between organizations to be the sharing of resources and ideas while I consider coordination to include activities related to establishing and communicating roles and protocols within an intergovernmental network. I produce hypotheses to explore quantitative relationships related to some of the potential influences on cybersecurity preparedness because the literature provided concepts which can feasibly be captured by a quantitative measure. The research expectation is presented as such because it lends itself to exploration through qualitative thick description.

These expectations provide a framework for my analysis. A simplified illustration of my analytic framework is presented in Figure 1. I expect the digital divide factors described in the first set of hypotheses to influence the internal cybersecurity capacity of local election administration offices. However, what I aim to measure is their cybersecurity preparedness. My

dependent variable, the cybersecurity preparedness of local election administration offices, is measured as a percentage of widely recommended cybersecurity practices with which the offices responding to my survey report compliance. I expect the internal cybersecurity capacity of the offices will be an important element of their cybersecurity preparedness. However, I explore other factors which may be influential to the office's overall cybersecurity preparedness. Some factors are presented below as a secondary set of hypotheses which explores whether digital divide-related factors among the population in a local election jurisdiction influences the cybersecurity preparedness of the local election office. I also expect intergovernmental coordination and collaboration will influence the overall cybersecurity preparedness of local election offices, as suggested by my research expectation and as I try to observe through qualitative research. All of these factors are portrayed in Figure 1. As further described in Chapter 3, I try to control for additional potential factors including the technology use of the local election jurisdiction and the institutional structure of the local election authority.

[Figure 1 about here]

The first set of hypotheses is based on one of the themes identified in the literature. This series of hypotheses, in summary, are based my expectation that local election administration offices will be affected by "digital divide-related factors" including human resources, financial resources, and geography. I expect that offices with internal characteristics that have been found to lead to a digital deficit for individuals and organizations will be less likely to complete cybersecurity practices, while those with higher levels of resources and expertise will report higher levels of cybersecurity preparedness. The individual relationship of each of the identified digital divide-related factors with cybersecurity preparedness is explored in Chapter 4, and I also estimate the potential combined influence of these factors. My analytic framework provides a

simplified way to explore relationships which are likely much more complex in the real world. Most likely, these identified influential factors are related to each other and interact with each other in ways not accounted for within this framework. Due to this limitation, my quantitative findings provide nothing more than a starting point in our understanding of the influences on the cybersecurity preparedness of local election offices which, along with further evidence from qualitative analysis, were used to produce a grounded theory to inform further exploration.

- Hypotheses related to internal cybersecurity capacity:

Office-level Financial Resource Hypothesis: I expect that the cybersecurity preparedness of a local election administration office is influenced by its financial resources because the literature suggests that money has an influence on the IT and cybersecurity sophistication of organizations. I expect that as the budget of a local election administration office is larger, its cybersecurity preparedness will be stronger.

Office-level Geography Hypothesis: I expect that local election offices in rural locations will, on average, report lower levels of cybersecurity preparedness than those in non-rural locations because the literature provides evidence that individuals and organizations in rural locations tend to face technological deficits.

Office-level Education Hypothesis: I expect that the education level of the local election official will influence the local election office's cybersecurity preparedness because the literature suggests that the education levels of individuals tends to influence their ability to use digital technology. I expect that the cybersecurity preparedness of a local election administration office will tend to be higher as the level of education completed by a local election official is higher.

Office-level Professional Experience Hypothesis: I expect that local election administration offices with a certified election administrator will, on average, report higher levels of cybersecurity preparedness than those without a certified election administrator because the literature suggests that professional experience tends to influence the capacity of individuals to use digital technology.

Office-level Expertise Hypothesis: I expect that access to in-house IT expertise will lead to higher levels of cybersecurity preparedness for a local election administration office as IT professionals are likely to understand how to implement cybersecurity practices.

Office-level Size Hypothesis: I expect that the staff size of a local election office will influence its cybersecurity preparedness as the literature suggests that the staff size of an organization tends to influence its technological sophistication.

I also explore the influence of digital divide factors at the jurisdiction-level or population-level on the cybersecurity preparedness of local election administration offices. I expect the office characteristics above to be more influential, as it is the office staff who is responsible for executing cybersecurity protocols. However, digital divide factors among the population of a jurisdiction may be present in the staff of the local election administration office. Further, offices in jurisdictions with a digital deficit among the population may have diminished access to technical support from within local government and local non-governmental organizations. Based on this, I have formulated several expectations to inform my exploration of whether jurisdiction or population-level characteristics influence the cybersecurity preparedness of local election administration offices. These hypotheses can be summarized as – the presence of "digital divide factors" related to geography, income, education, age, race, ethnicity, and

language among a jurisdiction's population will be related to decreased cybersecurity preparedness by the local election office. I explore the bivariate relationships of each of the identified jurisdiction-level characteristics with the cybersecurity preparedness of the local election office. Then, as further described in Chapter 4, I account for potential jurisdiction-level influences in my multivariate models based on the results of the bivariate tests.[3]

- Hypotheses to explore the influence of jurisdiction-level characteristics:

Jurisdiction-level Geography Hypothesis: I expect that the local election administration offices in rural jurisdictions will report lower levels of cybersecurity preparedness than those in non-rural jurisdictions because the literature suggests that individuals in rural jurisdictions tend to have technological deficits. This may impact the staff of local election offices or the technological sophistication of the broader local government and other local partners.

Jurisdiction-level Resource Hypothesis: I expect that the cybersecurity preparedness of a local election administration office will tend to be lower as the median income of a local jurisdiction is lower because the literature suggests that technology-related capacity tends to be influenced by income.

Jurisdiction-level Education Hypothesis: I expect that a local election administration office will tend to have higher levels of cybersecurity preparedness as the percentage of the population who

[3] Bivariate tests related to most of these variables suggested either no influence on local election office cybersecurity preparedness or a different relationship than the one predicted. Because this research is exploratory, I opted to account for the jurisdiction-level variables in the multivariate models according to what the bivariate models suggested rather than according to these expectations.

completed high school and college in a jurisdiction is higher. The literature suggests that individual technology use tends to be influenced by education level.

Jurisdiction-level Population Size Hypothesis: I expect the cybersecurity preparedness of a local election offices to be greater as the jurisdiction's population size is larger because resource allocation is heavily dependent on population size.

Jurisdiction-level Language Hypothesis: Because, according to the literature, low levels of English language skills tend to be related to low levels of technology capacity and use, I expect that the cybersecurity preparedness of a local election office will tend to decrease as the percentage of a jurisdiction's population who speak a language other than English in their household increases.

Jurisdiction-level Age Hypothesis: Because the literature suggests older adult Americans tend to have difficulty using digital technology, I expect that the cybersecurity preparedness of a local election office will tend to decrease as the average age of the jurisdiction's population is older and as the percentage of the senior age population increases.

Jurisdiction-level Race Hypothesis: The literature suggests that race has a modest influence on the digital divide, therefore, I explore the influence of the racial composition of a jurisdiction's population on the cybersecurity preparedness of local election offices. Based on conclusions of the digital divide literature, I expect that the cybersecurity preparedness of a local election office will tend to be lower as the percentage of the jurisdiction's population that is not white is higher.

Jurisdiction-level Ethnicity Hypothesis: Based on conclusions of the digital divide literature, I expect that the cybersecurity preparedness of a local election office will tend to be lower as the percentage of the population that is Hispanic is higher.

- Research expectation to explore the influence of intergovernmental collaboration and coordination:

A theme across the literatures on intergovernmental relations, emergency preparedness, and local government capacity is that collaboration with intergovernmental partners and well-planned coordination across layers of government and within broader policy networks is key to good administration and to the ability of public administrators to adapt to new challenges. Through qualitative research using semi-structured interviews of experts who support local election officials in the election cybersecurity intergovernmental network, I explore the influence of intergovernmental network collaboration and coordination on the cybersecurity preparedness efforts of local election administration offices. My research expectation is that coordination within an intergovernmental network that includes established communication protocols, regular communication, and the acceptance of support from other entities, is key to improving cybersecurity preparedness for local election administration offices. Based on the literature, I expect it is important for local election administrators to accept cybersecurity information and assistance from government and non-governmental partners, but that it is also important for local election administrators to maintain ownership and control of their office's cybersecurity plans and implementation. Quantitative data and analyses will supplement my qualitative research to study this expectation.

The next chapter details the mixed methods research design for this study which follows the analytic framework outlined in this chapter. The overall purpose of this research, along with a lack of existing data, call for the collection of primary data. An original survey was created to ensure the data collected would allow for the testing of the above hypotheses. Semi-structured interviews of election cybersecurity experts were used to collect detailed information for

qualitative analysis. The next chapter describes these data collection processes. In Chapter 3, I also describe the methods used for quantitative and qualitative data analysis and address why those methods were selected.

Chapter 3: Research Design and Methodology

Introduction

This study uses a mixed methods research design with primary and secondary data to test the hypotheses and explore the research expectation outlined in Chapter 2. A quantitative data analysis was used to explore the plausibility of the above hypotheses. A qualitative analysis was used to explore intergovernmental coordination and gain more detailed insight about relationships suggested by the quantitative findings. The qualitative data collection approach used for this study also provides an opportunity for the identification of potentially relevant factors not addressed in my analytic framework.

Chapter 3 comprises of five sections including two sections on how data were collected and three sections on how data were analyzed. The first section addresses the need for primary quantitative data and explains how the variables were measured, how the original survey was constructed, and my sampling method. The second section describes the collection of qualitative data through semi-structured expert interviews and addresses how the interview questions and respondents were selected. The third section is an overview of my data analysis process and a description of why specific methods were chosen based on the fundamentals of social science research. The fourth section outlines the quantitative methodology used to test my hypotheses. The final section describes the systematic qualitative analysis I conducted which follows a process called "pattern matching" described by Brown and Hale (2014, 203–204).

Data Collection – Original Survey and Secondary Data Collection

I created and administered an original survey to collect mostly quantitative data along with some qualitative data to supplement interview data. Survey respondents include participants

from a sample of local election offices from each US state. Quantitative data to measure some of the digital divide-related independent variables were also collected from the US Census Bureau and other public data sources including the websites of state and local election administration offices. The survey data, along with secondary data, provide a test of the above hypotheses and help to control for other likely relevant factors including institutional structure and technology use.

Table 1 outlines the sources from which I collected quantitative data. Data related to the cybersecurity practices, human and financial resources, and technology use of a local election administration office were collected through responses to survey questions. Data related to the demographic characteristics of local jurisdictions were collected from the website of the US Census Bureau. The number of registered voters served by a local election administration office was collected from the website of the relevant state chief election official, or in limited cases it was collected from the website of the local election administration office because it was not found on the state-level website.

[Table 1 about here]

According to Brown and Hale (2014), survey research is appropriate when researchers want to collect information about individuals' practices and backgrounds directly from the individuals. This was precisely my goal for data collection. Without the availability of secondary data regarding the cybersecurity practices of local election administrators, I needed to ask local election administrators about their practices. Opportunities to observe these behaviors directly would have been extremely limited. Election administrators would be concerned that allowing researchers to directly observe cybersecurity practices could compromise the necessary secrecy

of some processes. Election administrators are unlikely to allow this type of direct observation or would only allow it on a limited basis. Further, direct observation would severely limit the number of local election offices about which I could collect information on cybersecurity practices and other characteristics due to time, cost, and other logistical constraints. This limitation would compromise the external validity of my research. I concluded that conducting survey research is the best way to collect the most accurate data about the cybersecurity practices of local election administration offices from the largest feasible number of local election administrators.

I sampled 717 local election administration offices to which to send the survey. Because election administration laws and practices vary greatly across states (Hale et al. 2015), I prioritized the need for variation across states and for representation of all states within the sample. Therefore, I sampled fifteen local election jurisdictions from each US state[4] rather than randomly sampling jurisdictions from a list of all local election jurisdictions nationwide. Doing the latter would have likely resulted in high proportions of my sample being from states that have the highest number of local election jurisdictions, such as those in which election administration

[4] Some states have fewer than 15 local election administration offices: Alaska, Delaware, and Hawaii. In those states, all of the local election offices were included in the sample. This is the reason the total sample size was 717 rather than 750.

is the responsibility of municipalities, townships, or villages, rather than counties.[5] The former ensured I sent the survey to local election administration offices in every US state and to the same number of offices per state in most states.[6] Within each state, I randomly sampled with replacement to ensure each local jurisdiction had the sample probability of being selected as each of the other local jurisdictions in the state. There were, however, differences in the probability of being selected into the sample for jurisdictions across the states. For example, a single jurisdiction in Alabama where there are about seventy local election jurisdictions had a much higher probability of being included in the sample than a jurisdiction in Wisconsin where there are more than one thousand eight hundred local election jurisdictions. Therefore, though the sample within each state was random with a few exceptions[7], my overall sample is not a random sample. This is a limitation I chose to accept due to my priority to optimize variation across states within the overall sample.

My sampling frame for each state was a list of local election jurisdictions in the state created and maintained by the US Vote Foundation.[8] According to expert advice gained during

[5] When I attempted to create a random sample of local election jurisdictions by randomly sampling from a list of all the jurisdictions nationwide, over half of the jurisdictions sampled were from Wisconsin and some states were not represented in the sample at all. This is because Wisconsin's election jurisdictions are cities, townships and villages, and there are more than 1,800. Counties are the election jurisdictions in most other states, and the majority of states have fewer than 100 local election jurisdictions.

[6] See Footnote 3.

[7] See Footnote 3.

[8] https://www.usvotefoundation.org/vote/eoddomestic.htm

three pilot interviews, the US Vote Foundation maintains the most comprehensive list that exists of local election jurisdictions in the United States. My sampling unit was an individual local election jurisdiction, such as a county or township, in each state. I randomly selected fifteen jurisdictions from each state's sampling frame unless there were fewer than fifteen jurisdictions in a state's sampling frame. In the states where there are fewer than fifteen local election jurisdictions, all of the jurisdictions were selected. Once complete, I had a sample of seven hundred seventeen election jurisdictions with about fifteen from each state.

Next, I identified the local government office with primary responsibility for election administration in each sampled jurisdiction to which to send the survey by email. I sent the email to the local election official or the person within the office with responsibility for administering elections. In most cases, the US Vote Foundation's local election official directory included this information. In any case that it did not, I collected the name and contact information of local election officials from the office's website or another source. To incentivize responses, I entered all respondents into a drawing to win a $100 Amazon gift card. I informed them of the drawing in their email invitations to respond to the survey. The survey invitation emails are included in Appendix 1.

Because I relied on survey research to collect all of the quantitative data used to measure my dependent variable, I must account for the limitations of survey research. A serious limitation of survey research is the potential for response bias. Survey respondents may provide inaccurate or distorted information because they do not know something, misunderstand a question, want to shed a positive light on themselves or their offices, make a mistake in completing the survey, or a range of other reasons (Brown and Hale 2014). To avoid ambiguity, I carefully crafted questions with the goal of making them as clear and straightforward as possible while lacking

confusing phrasing.[9] I also strived to write questions that are neutral and do not guide respondents to particular answers. This was difficult to accomplish. Asking respondents about which cybersecurity practices their office completes seems to suggest that these tasks should be completed. I was unable to write these questions in a way that they would be perceived as completely neutral. This limitation should be considered in applying conclusions based on my findings. Overall, I must take into account that the findings of survey research are always based off subjective responses (Brown and Hale 2014). I must consider that I am analyzing the relationship between the independent variables and the reported completion of cybersecurity practices rather than the confirmed completion of cybersecurity practices.

The survey was created to capture data to measure the dependent variable and some of the independent variables. For all of the jurisdiction-level independent variable measures, I relied on secondary US Census data which are less subjective and, in many cases, more reliable across jurisdictions. I used the survey to collect data to measure the digital divide factors that cannot be measured through US Census data, such as the number of IT staff and the education level of local election officials. The entire quantitative measure of the dependent variable comes from responses to the survey, which includes a set of questions about whether local election administration offices complete election cybersecurity tasks deemed important by multiple relevant government and non-governmental organizations.

I chose the election cybersecurity practices by cross-checking a series of cybersecurity checklists, frameworks, and best practice handbooks that are widely recognized and promoted

[9] In addition to review by my committee, I piloted the survey with three individuals familiar with the subject matter. I edited the questions for clarity and content based on their input.

within the US election administration community[10] including the National Institute of Standards and Technology's (NIST) Cybersecurity Framework,[11] the Center for Internet Security's (CIS) Controls[12] as well as the CIS Election Infrastructure Security Handbook,[13] the Election Center's Election Security Checklist,[14] the Belfer Center's State and Local Election Cybersecurity Playbook,[15] and a series of resources from the Election Assistance Commission (EAC)[16] which are each geared toward different election systems or different aspects of election security. I began by reading each resource thoroughly. Then, during a second review of each resource, I looked for themes. This resulted in the identification of broad election cybersecurity concepts that appeared repetitively in the resources listed above. During a third review, I tallied the number of organizations that addressed each cybersecurity concept. As shown in Table 2, I then narrowed the list down to the election cybersecurity concepts that were expressed as important by at least four of the five entities listed above in at least one of the resources that I reviewed

[10] I strived to include all of the relevant election-specific cybersecurity guidance which was publicly available at the time the variable was constructed. Since that time, additional organizations have released election cybersecurity guidance.

[11] https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[12] https://www.cisecurity.org/controls/

[13] https://www.cisecurity.org/elections-resources/elections-infrastructure-handbook-part-1/

[14] https://www.electioncenter.org/national-association-of-election-officials/election-security-infrastructure/Election-Center-Checklist-Elections-Security-Checklist-Released-2017-05-22.pdf

[15] https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[16] https://www.eac.gov/election-officials/election-security-preparedness

from each entity. If more than one of the government or non-profit entities did not include a concept in its resources, I did not ask about a cybersecurity practice related to the concept. I assumed that the most broadly relevant election cybersecurity practices and those which address the most common and critical cyber risks would be those that were consistently mentioned by the range of supporting entities that released guidance. To limit the scope of the measure, I did not include audits, incident response planning, or communication practices. Further, I included items related only to an office's efforts to prepare to prevent, detect, and respond to cyber incidents. I could not include actual detection or response items as they would not be applicable to offices that had not knowingly faced a cyber incident.

[Table 2 about here]

Next, I reviewed how cybersecurity practices related to each identified concept were worded in the documents above to consider how to articulate the series of survey questions about cybersecurity practices related to each concept. Table 2 presents examples of how each organization articulated questions or action items related to each of the selected cybersecurity concepts. The cybersecurity resources reviewed vary greatly in degrees of specificity ranging from a broad, overarching cybersecurity framework applicable to any organization to checklists with action items specific to election offices. In some cases, one item in one resource may cover the same cybersecurity practices, from a broader perspective, than two or more items in another resource. After reviewing the verbiage used by each organization, I created survey questions about cybersecurity practices with the goal of making them as broadly applicable across local election administration offices as possible. In some cases, more than one question is used to measure relevant practices related to a cybersecurity concept. Appendix 1 includes the survey instrument which includes the questions about cybersecurity practices.

Appendix 2 presents descriptions of each variable used for quantitative analysis. Table 1 outlines the sources of the data. In general, to measure whether an office is negatively impacted by a cybersecurity divide, I measure whether key digital divide factors, or factors that have shown to be associated with reduced digital technology access, capacity, and use, as identified by the literature, are present. As explained above, several of these measures were obtained through survey responses. To measure local election administrators' education, I asked them their highest level of education. To capture the professional experience of local election administrators, I asked whether they have an election administration-specific professional certification. To measure the budget of a local election administration office, I asked what their total budget was for administering elections during the last fiscal year.[17] For staff-related measures, there were two survey questions, one of which asked the total number of IT specialists who work on election administration-related systems and one which asked the total number of election administration employees in the office. Though a survey question was included which asked the approximate number of registered voters served by the office, I collected and used a secondary measure of this variable from public sources because I expect it to be more reliable and precise.

Other measures relied on secondary data collection from the US Census Bureau. For population size, I use the number of residents in a jurisdiction according to the US Census

[17] Election budgets are a difficult concept to measure. Because elections are decentralized and budgets are reported at the local government level, budget reporting processes vary drastically. For many local election jurisdictions, the election administration budget is not publicly reported as its own line item but rather is part of a much larger line item. Therefore, though subject to subjective reporting, I determined the most reliable way to measure election administration budget was to ask the election administrators.

Bureau. For age, I use the median age of the county or municipality reported by the US Census Bureau. I also use the percent of the location's residents that are age sixty-five or older, according the US Census Bureau. The literature suggests seniors are the age group most affected by the digital divide. To measure the education-level of the jurisdiction's population, I use two measures from the US Census Bureau: percent of residents that are age twenty-five or older with a high school diploma and percent of the population that are age twenty-five or older with a bachelor's degree. To measure the income of the population, I use the median family income of the location, according to the US Census Bureau. Because the digital divide literature suggests that non-white minority groups, and specifically Black Americans, are somewhat impacted by the digital divide, I measure the race of each location using the percent non-white and the percent Black from the US Census Bureau. For ethnicity, I use the percent Hispanic or Latino of the locality, according to the US Census Bureau. For language, I use the percent of the population that speak a language other than English in their household, according to the US Census Bureau. Finally, for rural, I created an ordinal measure based on US Census Bureau categories. Jurisdictions range from urban areas (the most urban), to urban cluster (somewhat urban), to not urban (rural).

To measure the dependent variable, the concept of cybersecurity preparedness is measured as the percentage of the identified cybersecurity concepts with which the office reports it completes all related practices. I measure cybersecurity preparedness as a percentage, rather than as a dichotomous variable, due to wide recognition by cybersecurity experts (e.g., CISA 2019) that perfect preparedness cannot be achieved, but rather cybersecurity preparedness is about managing risk. I do not consider the offices in my sample which report one hundred percent compliance with the cybersecurity practices about which they were asked to be

completely prepared to address cybersecurity threats. Rather, I measure offices as more prepared or less prepared based on their compliance with these commonly recommended practices.

Reported compliance with a recommendation is a "yes" answer to the applicable question in section two of the survey. The concepts and related practices were derived from cybersecurity resources provided by five government and non-governmental entities according to the criteria explained above. Based on consistency across resources from at least four of the five entities, the following cybersecurity concepts were identified: access control, anti-virus, cyber-hygiene training, data backups, encryption, firewall, intrusion detection, inventory, multi-factor authentication, passwords, risk and vulnerability assessments, security patching, and vendor management. These cybersecurity concepts are not mutually exclusive. In fact, there is a lot of overlap. For example, passwords are a method of access control. However, each concept is needed to capture a separate practice or set of practices recommended in the relevant guidance. In some cases, two questions were needed to assess compliance with the concept. In those cases, the set of practices about which the election official was asked are related to each other. An example is "anti-virus." Related to this concept, election officials were asked about whether they have anti-virus software and whether their anti-virus software is up-to-date.

In addition to the independent variables described above, I tried to control for other relevant factors identified in the election administration literature. Control variables and their data sources are also reported in Table 1. Hale and Brown (2013) found that, at the state-level, the use of direct recording electronic (DRE) vote casting machines is correlated with states' participation with the VVSG, which is partially related to election cybersecurity. This may be due to increased security risks related to the use of DRE machines, a possible tendency of states with increased technological sophistication to use DRE machines and participate with the

VVSG, or some other causal mechanism. Either way, the relationship between DRE machine use and the tendency to comply with voluntary security recommendations may exist at the local level as well. Therefore, I consider DRE use. If increased sophistication or increased cybersecurity risk associated with technology use affects compliance with voluntary security guidelines, the use of electronic pollbooks ("e-pollbooks") may also be a relevant factor. Therefore, I also consider the use of e-pollbooks by local election jurisdictions. Additionally, I consider the institutional configuration of the local election administration authority using the categories from Hale et al. (2015) of whether a single official has authority over elections at the local level, whether a board has authority, or whether duties are divided. Finally, I consider the number of registered voters in the election jurisdiction as captured from public sources.

Data Collection – Expert Interviews

I used semi-structured interviews of election cybersecurity experts to collect qualitative data to explore the extent to which and how coordination within intergovernmental networks influences the cybersecurity preparedness of local election administration offices. Responses to open-ended questions on the survey may provide additional data relevant to exploring my qualitative research expectation. Additionally, the qualitative data derived from interviews may add detail to my findings related to the digital divide hypotheses as it will provide the opportunity to learn more about the specific challenges faced by local election administration offices and what factors may drive those challenges. Finally, these data may lead to the identification of additional relevant factors not addressed in my analytic framework.

I chose to interview experts because this research is exploratory and not based on well-developed theory. Therefore, it is important to account for additional explanations which may

not be addressed by the expectations I derived from the literature. Experts working in the field are the most practical source of insight on the topic. Interviewing them provides the opportunity to learn about alternative explanations which may not be covered by existing scholarly findings.

I interviewed fifteen individuals who are broadly considered experts on election cybersecurity[18] and who actively work with local election administrators within the intergovernmental network related to cybersecurity for US elections. To capture a variety of perspectives, I selected five election cybersecurity experts who worked for the federal government at the time of the interview, five election cybersecurity experts who worked in state government at the time of the interview, and five election cybersecurity experts who worked for a non-profit association that directly engages with local election administrators at the time of the interview. I also attempted to ensure diverse political viewpoints were captured. In the case that I selected interviewees who serve in a partisan position or work for a partisan elected official, I made sure to get the viewpoint of both major political parties. I interviewed two officials who serve in a partisan position – one Democrat and one Republican. I interviewed four government employees who work for a partisan official – three Democrats and one Republican.

Because the respondents each have extensive knowledge on the subject but due to a desire to maintain reliability, I used semi-structured interviews. Semi-structured interviews are guided with a set of questions but allow the respondents to deviate from the questions (Hale and Brown 2014, 299). Hale and Brown (2014, 147) suggest semi-structured interviews strike "a

[18] All of these individuals serve or have served as advisers to election officials on cybersecurity; almost all of them have made public appearances as election cybersecurity experts; and many of them have testified to Congress on election cybersecurity.

balance between the limitations of structured and unstructured interviews." Structured interviews allow for reliable data collection, but a problem is that researchers may fail to ask the correct questions and may miss out on important details (Hale and Brown 2014). Structured interviews are rarely the best approach when respondents are experts on the topic as they are likely to know information about which researchers would not even think to ask. Unstructured interviews are open to whatever the respondents choose to share and are guided by extremely broad questions or prompts (Hale and Brown 2014), such as "tell me about election cybersecurity." A limitation with unstructured interviews is that the results are not very reliable.

I guided the interview with six questions. Each question had a purpose, but each question left respondents with a lot of discretion as to how to respond. Overall, I wanted to learn what local election administrators are doing and not doing about cybersecurity, to what extent this problem is the responsibility of local election administrators, who is helping them and who should be helping them, what challenges they are facing, and any additional information the respondents believe is important. Appendix 3 includes the interview instrument. The semi-structured interview approach allowed me to ensure I collected the information needed to answer the research question and to maintain some reliability in data collection methods across interviews. However, I left room for the experts to share the details they consider important and tried to avoid guiding them to specific responses. The only question I asked that specifically addresses my research expectation about intergovernmental coordination was asked near the end of the interview so that I could account for responses related to the research expectation both prior to and after the question was asked during each interview.

I created the interview instrument consistent with recommendations from Brown and Hale (2014). I focused the interview questions on collecting the opinions of experts. When

putting respondents at ease prior to the interview, I told them that I selected them because they are experts on the topic and I want their expert insight on the issues. I also reminded them they were responding anonymously. I began each interview with a grand tour question by asking each respondent to tell me about their role in US election cybersecurity. As experts actively working in this space, the selected respondents are passionate about this topic and most were eager to tell me about the role they serve. With the exception of some opinions which may be available through public statements the respondents have made, the vast majority of the data collected through the interviews could not have been collected elsewhere.

Data Analysis Overview

The ultimate goal of social science research is making causal arguments. Not every study is able to conclude with a causal argument. In fact, very few social science studies confirm causality. However, the goal of every study should be to move the field closer to an understanding of causal relationships between social phenomena.

Researchers must meet four conditions to establish a causal relationship (Brown and Hale 2014, Kellstedt and Whitten 2009). Kellstedt and Whitten refer to these conditions as "the four causal hurdles." The four causal hurdles are: (1) establish that a credible causal mechanism connects independent variables to dependent variables; (2) rule out the possibility that the dependent variable is the cause of the independent variable(s); (3) confirm that covariation exists between the independent and dependent variables; and (4) control for all confounding variables that might make the apparent relationships between the independent and dependent variables spurious.

Qualitative research is often an effort to clear hurdle one – through thick description, qualitative research often allows researchers to link one causal chain to the next to gain detailed insight about the complex causal mechanisms existing between concepts. The literature in Chapter 2 proposes a several hypothetical causal mechanisms between a number of potential factors and the cybersecurity preparedness of local election administration offices. These hypotheses are a sufficient basis for quantitative analysis as, according to Brown and Hale (2013, 201) the causal mechanism between variables "does not have to be observable – it can just be hypothetical." I use qualitative exploration to try to learn more about the causal mechanism between identified factors and cybersecurity preparedness for local election offices in order to produce a grounded theory.

Related to hurdle two, a relationship between cybersecurity preparedness and identified potential influences in the opposite direction from the expected relationship is simply not logical for many of the identified independent variables, and it is impossible for others. The temporal ordering of my expectations is also consistent with existing findings from the literature. Again, descriptive analysis through qualitative research may help me learn more about the nature of the relationships being investigated as the purpose of qualitative research is to understand how concepts are related rather than just whether they are related. I provide some evidence related to the temporal order of the predicted relationships based on qualitative findings.

For hurdle three, I use bivariate analyses to investigate whether covariation exists between my independent and dependent variables. In social science research, hurdle three tends to be the lowest or at least most straightforward hurdle to cross. In the instances my independent variables of interest covary with the dependent variable, it is the simplest hurdle to cross for this study.

Finally, I create multivariate models to try to confirm nonspuriousness. This is a challenge for this research as the sample size is small and several of the independent variables covary with each other. This is further explained below and in Chapter 4. My findings provide some evidence the relationship between some of the independent variables of interest and the dependent variable is nonspurious, but further research is needed to confirm. Hurdle four is often the most difficult hurdle to clear in social science research because our research questions are not often conducive to experimental research designs through which researchers can use random assignment and control groups to confirm nonspuriousness.

Overall, this study, like most non-experimental research, will not fully clear the four causal hurdles. As this is exploratory research, this is fully expected. Instead, I created a research design that is sufficient to provide some evidence that a causal relationship may exist between some independent variables and a dependent variable and plausible explanations for why those relationships may exist. The goal of this study is to pave the way for future research. Based on my findings and conclusions, I produce a grounded theory to facilitate more informed future studies of this topic.

Glaser and Strauss (1967) propose grounded theory as theory which can be formulated through an iterative review of data. Brown and Hale (2014, 24) suggest producing grounded theory is an appropriate approach when research is exploratory because there is not existing literature to specifically address the phenomena under investigation. They (2014, 203) suggest using qualitative techniques to produce grounded theory "developed out of understanding of the empirical world."

Glaser and Strauss (1967) propose a specific process for developing grounded theory. They (1967) suggest grounded theory should be produced from iterative comparative analysis. This iterative process involves the collection, coding, and analysis of data to plan what to study next. Though producing grounded theory is usually associated with qualitative research, Glaser and Strauss (1967) suggest that multiple types of data can be used for theory development.

My study aims to follow this iterative approach. To begin, I collected documents addressing my phenomena of interest and qualitatively analyzed those documents to identify key concepts and build my dependent variable of cybersecurity preparedness. Based on consideration of these documents and empirical observations from existing relevant studies, I produced a series of hypotheses and expectations. My next step involved identifying a theoretically relevant group from which to collect additional data to further explore the phenomena of interest. I did this by conducting an original survey of a sample of local election officials and analyzing survey data using quantitative and qualitative methods. Themes which emerged from survey data in addition to empirical observations from existing research informed my next step in data collection and analysis. I then identified another relevant group to study through interview research. I qualitatively analyzed interview data using a process of pattern matching which is suggested by Brown and Hale (2014). This process closely follows procedures proposed by Glaser and Strauss (1967) including identifying emerging categories as well as patterns between those categories. As is preferred by Glaser and Strauss (1967), I present my grounded theory in Chapter 6 as a running theoretical discussion. The following sections describe my data analysis methods in additional detail.

Data Analysis – Quantitative

I used quantitative data analysis to test whether there is a relationship, as expected, between the identified digital divide-related characteristics and the extent to which a sample of local election administration offices reportedly comply with broadly recommended cybersecurity practices. Using the percentage of cybersecurity concepts with which a local election administrator says his or her office complies with all relevant practices as the dependent variable, I use correlation coefficients, difference of means tests, bivariate Ordinary Least Squares (OLS) regression, and multivariate OLS regression to explore its relationship with identified independent variables. The decision to use OLS regression is further explained in Chapter 4.

I received a total of fifty responses to the survey, and therefore, had a sample size of fifty local election jurisdictions from which to analyze quantitative data. This is a small sample size for multivariate analysis. Therefore, I largely rely on bivariate analysis to identify potential relationships. This is a limitation of this study, and it is important to acknowledge the possibility that some of the bivariate relationships identified could be stochastic. While this study falls short of confirming causal relationships between concepts of interest, it provides preliminary evidence of factors which may influence the cybersecurity preparedness of local election administration offices.

I used my analytic framework to construct multivariate models using OLS regression for analysis. While these models provide some insight into the effects of key variables while accounting for other factors, these findings are preliminary. The models are exploratory, and while they do not test existing theory, they produce useful findings for theory building. The size of the sample likely limited my ability to observe statistically significant relationships as small sample sizes can lead to Type II errors. Further, I had to account for multicollinearity in my models as I identified strong correlations between some of the independent variables. The

correlations between multiple independent variables make sense considering the nature of the identified digital divide factors. Most of these factors represent different types of resources of local government offices. In the real world, we would expect several of these factors to be related to each other. For example, it is logical that the financial resources of an office may be related to the human resources of the office. Therefore, multicollinearity is not a problem that can be solved, but it is a limitation, and I need to consider how it may be influencing my findings. These limitations and how they were accounted for are further described in Chapter 4. Overall, however, the multivariate models provide a strong basis for future research as they provide further evidence of some of the relationships identified through bivariate analysis.

Data Analysis – Qualitative

According to Brown and Hale (2014, 203), the "central goal of qualitative data analysis is to draw out patterns, themes, and trends that reflect the original data as closely as possible, in a process called pattern matching." Closely following the pattern matching process as described by Brown and Hale (2014), I conducted a systematic, iterative review of interview responses. This process consisted of six systematic reviews of the data.

The first review was a thorough reading of each interview response while noting concepts that seemed to appear as themes or patterns across multiple interviews. This resulted in a list of eighty-five potential themes. The next round of review included a second readthrough of interview responses. During the second review, concepts which I identified as mentioned by only one or two respondents were dropped from the list of themes. The second review also consisted of combining similar concepts or revising themes to make them more broadly applicable. At the end of the second review, sixty-seven themes remained.

For the third review, I reviewed the interview responses again and tallied the total number of times each concept was mentioned as well as the number of unique respondents which mentioned each concept. I removed additional concepts which I identified as mentioned by two or fewer respondents. I also identified additional patterns between themes which allowed me to remove themes that fit within other broader concepts, combine some concepts, and further revise concepts to make them more broadly applicable. The third review resulted in a total of thirty-nine themes. At this point, I developed definitions for each identified theme based on the way the concepts were described by interview respondents. Some of the definitions included descriptions of how patterns existed between references to two or more themes. The process of producing definitions allowed me to further condense the themes to a total of thirty-seven because of substantial overlap of some of the definitions.

The fourth review was a repeat of the process of the third review. I tallied the total frequency of mentions for each theme, as well as mentions by individual respondents. After this review, I removed themes which were not mentioned by at least one-third of the total number of respondents. I also identified additional patterns between themes which led to combining additional themes into one theme. At the end of this review, twenty-two themes remained. This review also led to the reworking or combination of some of the definitions. Even for this most condensed list of themes, overlap of the themes and their definitions exists. This is mostly due to relationships between the themes in the way they were described by respondents. Through the fifth and sixth systematic reviews, I further identified patterns between the themes.

The fifth review consisted of pulling out deeper detail from interview responses. Again, the frequency of total mentions and mentions by unique respondents was tallied for each theme. During the fifth review, I also tallied the frequency of responses from each category of

respondent: federal government representative, state government representative, and non-profit organization representative. Additionally, I recorded two to three illustrative quotations or paraphrased examples of each theme from the interview responses. The illustrative examples provide greater insight into what the respondents meant when they mentioned each concept as well as patterns between themes.

The sixth and final review was focused on themes within each interview question and within each category of respondent. I summarized the most common responses across all respondents for each question, as well as the most common responses to each of the questions by each category of respondent. Since several of the identified themes related to the concept of interest – intergovernmental partnerships – and a question was asked about partnerships, I also tallied mentions of the intergovernmental partnerships before the related question was asked.[19]

Additionally, I conducted a systematic review of the open-ended responses from the survey of local election administrators. So as to not discourage participation, the open-ended questions requiring a substantive response were optional. The qualitative reviews of survey responses were of substantially fewer data and substantially less dense data than the reviews of the interview responses. Therefore, each review was much less extensive. First, I separately reviewed the responses to each of the three open-ended questions which called for a substantive response[20] and recorded concepts which were mentioned multiple times. Then, I tallied the total

[19] The question about partnerships was intentionally asked toward the end of the survey (question five out of six questions) so that potential bias could be considered.

[20] The other open-ended questions were only asked to collect identification information which was needed for the collection of secondary data related to each jurisdiction.

number of references to each concept for each of the three survey questions to identify themes. This led to combining some concepts into broader themes and the identification of two to five themes related to each question. Then, I reviewed the identified themes across all three questions to identify the most frequently mentioned themes overall. The findings of this analyses are described in Chapter 5.

The next chapter presents the findings of the quantitative analysis described in the previous section. The results of univariate, bivariate, and multivariate tests are presented in Chapter 4. These bivariate and multivariate tests explore the relationships between the variables of interest as predicted by the hypotheses described in Chapter 2.

Chapter 4: Influences on the Cybersecurity Preparedness of Local Election Offices

Introduction

This chapter describes the findings of the quantitative portion of this research. Through bivariate and multivariate analysis, I explore which factors are related to and seem to influence the cybersecurity preparedness of a sample of local election administration offices. These findings are based on the analysis of quantitative data sourced from the original survey and secondary data collection described in Chapter 3. The sample size of fifty for the quantitative analysis described throughout this chapter represents the fifty local election administration offices that responded to the survey. Secondary data were collected for the same fifty local election jurisdictions.

This chapter begins with an overview of survey responses. Next, I present a description of the sample of responding local election offices and their jurisdictions. Then, I present the results of a series of bivariate tests which explore the relationships between variables of interest and the reported cybersecurity preparedness of the local election administration offices in the sample. Next, I report the results of multivariate OLS regression models used to estimate potential influences on a local government cybersecurity divide based on the factors identified in Chapter 2. Finally, I summarize my findings from throughout my quantitative analyses.

Of the fifty responding election administration offices from local government jurisdictions, twenty-six different states are represented in the sample. The state with the highest

number of local jurisdictions included has seven local jurisdictions in the sample[21]. The state with the second highest number of jurisdictions has five local election jurisdictions included in the sample. For half of the states with respondents, only one local election jurisdiction responded. Overall, I was moderately successful at achieving the goal described in the previous chapter of achieving representation from as many different states as possible in the sample with representation from just over half the states. Within the twenty-six states with respondents, two of the states are clearly overrepresented. Otherwise, however, representation across most of the twenty-six states is fairly evenly distributed. There are thirteen states with one local jurisdiction represented, eight states with two jurisdictions represented, three states with three jurisdictions represented, one state with five, and one state with seven. Of course, there are twenty-four states which are not represented in the sample, but that is to be expected and is unavoidable with a voluntary survey. With fifty offices from twenty-six states represented, the local election offices in the sample represent a wide range of state and local approaches to election administration that exist in the United States.

Considering US region offers further insight into the generalizability of the results as several election administration practices tend to vary by region (Hale et. al 2015, 139). Based on the US Census Bureau regions[22], eighteen of the local jurisdictions in the sample are located in

[21] A representative from the state election office from this state called me to ask questions about the study. Based on the response rate from this state, it is likely the state election office encouraged the local election jurisdictions to participate. Based on very similar responses across these seven jurisdictions, it is also very likely the state election office supplied the local jurisdictions with some of their responses to the survey.

[22] https://www2.census.gov/geo/pdfs/maps-data/maps/reference/us_regdiv.pdf

states from the West, seventeen are in states in the South, eight are in states in the Midwest, and seven are in states in the Northeast. Clearly, local election jurisdictions from the West and the South are overrepresented in the sample compared to jurisdictions from the Midwest and the Northeast. However, importantly, the sample includes jurisdictions from all four US Census regions.

Approximately seven percent of the jurisdictions which were sampled and invited to respond to the survey participated. Eight election officials in the original sample of seven hundred seventeen replied by email to decline the invitation to participate in the study. The rest of the election officials in the original sample simply did not respond at all. I identified some likely reasons the response rate was not higher. First, cybersecurity is a sensitive topic for election officials. Election officials and their cybersecurity practices are under extensive scrutiny from the media, policymakers, and the public. While some of the eight who declined by email simply declined, a few of the election officials explained their reason for not responding to survey as not wanting to release sensitive or secret cybersecurity information. This relates to a second identified potential reason which is that I did not provide the option to respond anonymously. Though responses were kept confidential, my research design required that I identified which local election offices responded to the survey so I could collect additional relevant data about each local jurisdiction. Allowing for anonymous responses in future survey research on this topic may result in a higher rate of response. Finally, as identified through qualitative research and discussed in Chapter 5, many local election officials face severe time constraints. Two of the local election officials who declined by email informed me that they did not have time to complete the survey.

The completion rate of survey respondents was 100 percent. All of the local election offices who responded to the survey completed the entire survey, with some exceptions related to optional open-ended questions. As these questions were optional, only some participants chose to respond. Responses to the open-ended questions are further discussed in the following chapter. The median time to complete the survey was nine and a half minutes.

The Sample of Local Election Jurisdictions

The first stage in quantitative data analysis is to conduct univariate analysis to describe the data for each variable using measures of central tendency and measures of dispersion. Univariate analysis is important for learning what your data and sample look like, determining what methods of bivariate and multivariate analysis are appropriate, and identifying and correcting coding mistakes. Descriptive statistics of this study's quantitative data are presented in several tables.

Table 3 summarizes the responses of the local election administrators related to their office's compliance with each of the key cybersecurity concepts used to build the dependent variable of cybersecurity preparedness. The thirteen key cybersecurity concepts considered include: access control, anti-virus software, cyber-hygiene training, data backups, encryption, firewall, intrusion detection, inventory, two-factor authentication, passwords, risk and vulnerability testing, security patches, and vendor management. A local election jurisdiction's compliance with a cybersecurity concept was coded as "yes" if the respondent indicated compliance in each question related to that concept. Local election officials only answered one question related to most of the cybersecurity concepts. If respondents, answered "no" to any of these questions, their compliance with the corresponding cybersecurity concept was coded as

"no." For anti-virus, data backups, and security patches, respondents were asked two questions about two related practices. For these concepts, compliance was coded as "no" if the respondent answered "no" to either of the related questions as both practices are necessary to demonstrate compliance with the concept.

Because of the diversity of responsibilities across local election offices, respondents were provided the option of responding that a practice is "not applicable" and were given the option of leaving a comment to explain why something is not applicable. Related to each not applicable response, I considered the corresponding cybersecurity practice and, when applicable, the respondent's comment to determine whether it seems plausible a practice is not applicable. Not applicable responses were treated as missing responses if I determined it is likely the question is really not applicable to the respondent. There are some cases were a local election official may not be the responsible party for a task about which they were asked. An example is a respondent who indicated that their office does not work with vendors directly because vendor contracts and management are handled by the state and a separate local government agency. In other cases, a not applicable response was coded as "no" because it is virtually impossible that the practice would not be applicable or because the comment indicated non-compliance. An example is a respondent who said passwords and multi-factor authentication are not applicable. It is a safe assumption that all local election administrators use a computer or email related to their job at least sometimes. Therefore, passwords and multi-factor authentication are applicable. There were also some cases where a local election official responded "not applicable" but left a comment which indicated they are compliant with the practice. In those cases, compliance was coded as "yes." After all the "not applicable" responses were reviewed and coded appropriately, only about three percent of the total responses were treated as not applicable.

[Table 3 about here]

For compliance with all of the cybersecurity concepts other than vendor management, the modal response from local election official respondents was "yes." Of the fifty local election offices, thirty-nine indicated they have policies which restrict access to critical election systems. Forty-five offices said they use updated anti-virus software. Thirty-six offices responded that they require cyber hygiene training for local election officials and staff. Thirty out of fifty respondents said they maintain daily backups of critical election data. Twenty-two respondents said they encrypt all critical data at rest and in-transit; this modal category is fewer than half because there were six "not applicable" responses. Forty-nine offices indicated compliance with the firewall recommendation. Twenty-seven respondents said they have an intrusion detection system on their network. Forty-one offices indicated that they maintain an inventory of all critical election systems under the control of their office. Out of fifty offices, twenty-seven said they require use of two-factor or multi-factor authentication, while thirty-five reported that they require robust passwords. Thirty-six offices indicated that they complete risk and vulnerability tests at some regular interval. Thirty-five offices reported compliance with security patching recommendations. Finally, for vendor management the modal response was "no" with thirty-one out of fifty offices indicating they do not require election vendors to provide documentation of their cybersecurity practices.

Overall, most participating local election offices reported compliance with most of the cybersecurity practices about which they were asked. There are a number of possible reasons for this. One is that my approach to constructing the dependent variable was based on identifying the most uniformly recommended cybersecurity practices for election officials. This approach makes it likely that most of the cybersecurity concepts which were included relate to the most

fundamental practices or what cybersecurity experts often refer to as “the low hanging fruit.” Had I asked about more advanced cybersecurity measures, such as machine learning monitoring and vulnerability disclosure programs, I would have likely observed more variation in responses. However, I also would have increased my risk of confusing respondents, and the questions would have been more likely to lack relevance to some of the offices. Another logical explanation is that there was some bias in the way respondents answered questions because they wanted to shed a positive light on their office. The hope is that any error caused by such bias is non-systematic. Finally, a likely explanation is that some non-response bias was introduced related to who chose to not participate versus who chose to participate. It is likely that offices which are more compliant with cybersecurity practices are more likely to respond to a survey which asks about their cybersecurity practices. Though it seems my sample of participants trends toward offices which are more compliant with cybersecurity recommendations than the average local election office, there is still some variation in compliance across participants. Therefore, there is still an opportunity to analyze what factors influence the variation.

Tables 4 and 5 display descriptive statistics of the fully constructed dependent variable and the independent variables of interest which describe internal characteristics of local election offices which may be related to a cybersecurity divide in local government. Appendix 2 includes a description of how each variable is measured. The dependent variable for each observation was constructed by dividing the number of cybersecurity concepts with which the respondent reported compliance by the total number of applicable cybersecurity concepts. The result is a percentage of cybersecurity compliance for each local election office. The mean of the dependent variable is 69.2 percent compliant with key cybersecurity concepts. The standard deviation is 19.68 percent. Because the distribution of the dependent variable appears to be moderately

skewed left or negatively skewed, it is also important to consider the median. The median cybersecurity compliance score is 69.62. The local election office which reported the lowest cybersecurity compliance reported 23.08 percent compliance. Three offices reported one hundred percent compliance with the cybersecurity practices about which they were asked. As explained in Chapter 3, one hundred percent reported compliance with these cybersecurity practices does not mean an office is considered to be completely prepared. Rather, it means that, according to my measure, these offices are comparatively more prepared than the others in the sample.

[Table 4 about here]

[Table 5 about here]

Table 4 displays the mean and standard deviation for the continuous variables of interest related to internal characteristics of the local election administration offices. Table 5 displays the median and quantiles for these variables of interest. The mean reported budget is $1,472,996 with a standard deviation of $4,596,501. Because these data are severely skewed right, the mean is not the best measure of central tendency. The median reported budget is $183,636.50. The median is the appropriate measure of central tendency of the budget variable. The lowest reported budget in the sample is $700, and the largest reported budget is $30,000,000.

The mean number of IT staff is 1.28 with a standard deviation of 1.96. The median is one IT specialist. Many offices reported no IT staff, and the highest reported number of IT staff was ten. The mean number of total election administration staff is 8.14 with a standard deviation of 15.84. The median is four employees. The minimum, which applied to two offices in the sample was one. The maximum, which is an extreme value compared to the rest of the sample, was one

hundred. The next highest reported number of staff was fifty. Both staff measures are skewed right; therefore, the median is the better of measure of central tendency.

The variable for whether an office is in a rural location is ordinal. Therefore, the median is the appropriate measure of central tendency. The median value is “somewhat urban.” The variable for a local election administrator’s level of education is also ordinal. The median education level is a bachelor’s degree.

Tables 6 and 7 display descriptive statistics for the independent variables related to the characteristics of the jurisdictions of local election administration offices or the populations they serve. Table 6 presents the mean and standard deviation for each of these variables, while Table 7 displays the median and quantiles. The only variable used as both an office characteristic and a jurisdiction characteristic is the rural variable.

The mean median family income is $57,569.50 with a standard deviation of $15,894. The median is $56,728.50. The minimum median family income is $30,298, and the maximum is $108,828. The mean percent of the population with a high school degree is 88.67. The standard deviation is 4.72. The median is 89.2 percent with a minimum of 77.5 percent and a maximum of 97.4 percent. The mean percent of the population with a bachelor’s degree is 27.71 with a standard deviation of 11.42. The median is 23.95 percent. The data range from 12.3 percent to 61.3 percent.

[Table 6 about here]

[Table 7 about here]

The data distribution for population size is severely skewed right. The mean population is 279,997, while the median is 47,572 residents. The median is the appropriate central tendency measure. The lowest population size is 732, and the largest is 5,238,541 residents. The number of registered voters was also collected. These data are also skewed right. The number of registered voters will be used to measure jurisdiction size in bivariate and multivariate analysis because it does not include as extreme a value as population[23]. The mean number of registered voters is 142,650. The median is 31,100. The minimum value is 658, and the maximum is 1,570,127. These statistics indicate a wide variation of jurisdiction size included in the sample.

The mean percentage of the population which speaks a language other than English is 13.49 with a standard deviation of 11.07. The median is 9.05 percent. The data range from 0.2 percent to 37.7 percent. The mean median age is 40.56 with a standard deviation of 5.62 years. The median is 40.2 years old. The minimum median age, which comes from a college town, is 24.5 years old. The maximum is 55.3 years old. The mean percent of the population age 65 or older is 17.5. The standard deviation is 4.68. The median is 17.3 percent. The data range from 7.2 percent to 32.2 percent.

The mean percent of the population which is Black is 6.31 with a standard deviation of 7.82. The median is 2.55 percent Black. The median is the appropriate measure of central tendency as the data are severely skewed. There are two jurisdictions in the sample with a

[23] This is due to a local election office in my sample in a large metropolitan area which only serves part of the jurisdiction. Part of the jurisdiction is served by a different local election office. The population of the jurisdiction is more than three times larger than the number of registered voters served by the office.

population that is zero percent Black. The maximum percent of the population that is Black is 31.6. The percentage of the population which is not white was collected as another measure of race. The mean is 17.82 percent with a standard deviation of 12.03. The median is 15.7 percent. The data range from 1.9 percent to 47.3 percent. Finally, the mean percent Hispanic was 13.23 with a standard deviation of 12.64. The median, which is the appropriate measure of central tendency due to skewness, is 8.65 percent Hispanic. The data range from 0.4 percent of the population Hispanic to 55.6 percent Hispanic.

The mode is the only appropriate measure of central tendency for categorical variables. Table 8 displays the descriptive statistics for the categorical variables. One independent variable of interest is a categorical variable. The professional experience of local election administrators was measured by whether they reported having a professional certification in election administration. The modal response was "no." While eighteen local election administrators reported that they do have a professional certification in election administration, thirty-two local election administrators indicated that they do not.

[Table 8 about here]

The control variables are categorical. One of the control variables is the structure of the local election administration office. The categories include a single election administrator, a board, or divided duties. The modal category, applicable to twenty-two out of the fifty jurisdictions, is a single election administrator. The other two control variables consider the local jurisdiction's use of election technology. One is whether direct recording electronic (DRE) voting machines are in used in the jurisdiction. The modal response was "no." Fifteen local election offices reported use of DRE machines in their jurisdiction, and thirty-five offices

reported no DRE use. Also considered was the use of electronic pollbooks (e-pollbooks). The modal response was "yes" with twenty-seven out of fifty jurisdictions reporting use of e-pollbooks.

Other categorical variables were used to explore my research expectation. These variables measure the partnerships of local election offices with the EI-ISAC, DHS, the state election office, and other local government entities. Out of fifty, thirty-eight local election offices in the sample are members of the EI-ISAC. This number being so high is another indication that the respondents to my survey tend to have higher levels of cybersecurity preparedness than the average local election office. The total percentage of all local election offices in the United States which are members of the EI-ISAC was about thirty percent at the time of writing. Meanwhile, seventy-six percent of the local election offices in my sample were members of the EI-ISAC. Forty out of fifty local election offices reported a partnership with DHS. Again, this is substantially higher than the national average. Forty-six of the offices reported that they have received cybersecurity training from their state election office. Out of fifty local election offices, thirty-six reported that they receive cybersecurity support from outside entities within their local government. As there is little variation in the responses to these partnership variables, I do not expect the quantitative analyses of the partnership variables to be extremely informative. As expected, I will rely on mostly qualitative analysis to explore this research expectation.

Factors Related to Cybersecurity Preparedness

The next stage in quantitative data analysis is bivariate analysis. It is the first step in exploring relationships between the dependent variable and the independent variables. Bivariate data analysis is necessary to meet one of the criteria for making causal arguments – establishing

covariation between variables of interest (Kellstedt and Whitten 2013, Brown and Hale 2014). This is Kellstedt and Whitten's (2013) second causal hurdle.

I used a couple of appropriate methods for bivariate analysis to test each relationship. As the dependent variable is a percentage, it can be treated as a continuous variable. An appropriate bivariate test between the dependent variable and the continuous or ordinal independent variables is a correlation. Table 9 displays the correlation coefficients from these tests. I use the 95 percent confidence level as my criteria for rejecting the null hypothesis throughout the analyses in this chapter because that is the norm in political science fields.

[Table 9 about here]

Several of the independent variables have a statistically significant relationship with a local election administration office's reported percentage of compliance with key cybersecurity concepts. Three characteristics of the office have a positive, statistically significant correlation with cybersecurity compliance including the office's election administration budget, the number of IT specialists on the election administration staff, and the total number of election administration staff. These tests provide preliminary evidence that these internal characteristics of local election administration offices may influence the cybersecurity preparedness of local election administration offices as they establish the variables covary.

The level to which an office's location is classified as rural does not have a statistically significant correlation with the cybersecurity compliance, although the correlation is in the expected direction. The correlation coefficient is -0.1936. For the correlation between budget and cybersecurity compliance, I found a statistically significant correlation coefficient value of 0.2888. Reported cybersecurity compliance tends to increase as reported budget increases for the

local election offices in my sample. Testing the correlation between a local election administrator's education level and the office's cybersecurity preparedness, I found a not statistically significant correlation of 0.0280. Between the number of IT staff and cybersecurity compliance, I found a statistically significant correlation coefficient of 0.4206. The correlation coefficient between total staff and cybersecurity compliance is a statistically significant 0.3576. As the reported number of staff, and particularly IT staff, of the local election offices in my sample increases, their reported cybersecurity preparedness tends to increase.

Several of the jurisdiction-level or population-level independent variables have a statistically significant correlation with the dependent variable. However, most of these relationships are in the opposite direction of the predicted relationships. Several of the jurisdiction level variables related to the demographic diversity of the population including the percentage of the population who speaks a language other than English, the percentage of the population that is not white, the percentage of the population that is Black, and the percentage of the population that is Hispanic are positively correlated with the dependent variable. The percentage of the population with a high school diploma is negatively correlated with the dependent variable. These findings provide evidence that factors which have been found to be associated with a digital divide for individuals among the population served by a local election administration office do not impact the offices in a way which leads to a cybersecurity divide for the office.

I found a statistically significant correlation coefficient between percentage of the jurisdiction's population with a high school diploma and a local election administration office's cybersecurity compliance of -0.2861. As locations in my sample tend to have higher percentages

of high school graduates, the local election offices tended to report lower levels of cybersecurity compliance. This relationship is not as predicted.

The correlation coefficient between the number of registered voters served by a local election administration office and the office's cybersecurity compliance in my data is a statistically significant 0.3163 which suggests that the offices in the sample from larger jurisdictions tended to report higher levels of cybersecurity compliance than those from smaller jurisdictions. This is the only jurisdiction-level variable which has a statistically significant bivariate relationship with the dependent variable as predicted.

Between the percentage of the population which speaks a language other than English and the local election administration office's cybersecurity preparedness, the correlation coefficient is a statistically significant 0.3303. Testing the correlation between the racial and ethnic diversity of a jurisdiction and the local election administration office's cybersecurity compliance results in a statistically significant correlation coefficient of 0.344 between percent non-white and the dependent variable, a statistically significant correlation coefficient of 0.3393 between percent Black and the dependent variable, and a statistically significant correlation coefficient of 0.2801 between percent Hispanic and the dependent variable. A clear trend in the sample is that the local election offices from jurisdictions with higher levels of racial and ethnic diversity tend to report higher levels of cybersecurity compliance. I did not find a statistically significant correlation between the dependent variable and the age, higher education rates, or the median family income of the jurisdiction's population.

These findings raise the question of why I found statistically significant bivariate relationships with some of the jurisdiction-level independent variables in the opposite direction

from what I predicted. One alternative explanation I explored is that the variables in question are all proxies for jurisdiction size as it is common for large local jurisdictions to be demographically diverse. This may help explain some, but not all, of the relationships. Both variables for race and the variable for language diversity have a positive and statistically significant correlation with the jurisdiction size of higher than 0.4. This suggests that the larger jurisdictions in the sample are more diverse in terms of race and language and provides a plausible explanation for some of these findings. Jurisdiction size, however, does not explain the relationship between the dependent variable and percent Hispanic or between the dependent variable and percent high school educated. There may be an alternative explanation, or I may be observing the relationships based on random chance. Correlation does not necessarily suggest causation.

Next, I conducted a series of difference of means tests or t-tests to examine the bivariate relationships between the dichotomous independent variables and the dependent variable. Table 10 displays the results of the difference of means tests. First, I tested the relationship of the remaining independent variable of interest representing the professional experience of the local election administrator with the cybersecurity preparedness of local election administration offices. The reported mean percent of cybersecurity compliance in my sample for offices led by a local election official who reported having election administration certification is 78.53 percent. The mean percent of cybersecurity compliance for offices where the local election official does not have a certification is 63.45 percent. The difference of means is 15.08 percent. The test statistic is 2.7519. There is a statistically significant difference between the means of the two groups. This finding provides preliminary evidence that having a local election official with a

professional certification may have a positive influence on the cybersecurity preparedness of the election office. The two variables have a positive, statistically significant bivariate relationship.

[Table 10 about here]

I also estimated difference of means test for the variables controlling for election technology use. There was a statistically significant difference in the mean reported cybersecurity compliance score between offices which reported use of electronic pollbooks in their jurisdictions and the offices in jurisdictions where e-pollbooks are reportedly not used. The mean percent of cybersecurity compliance in my sample for the offices where e-pollbooks are used is 77.14, while it is 59.18 for the offices where e-pollbooks are not used. The difference in means is 17.95, and the t-statistic is 3.55. This finding suggests there may be something about the use of e-pollbooks in an election jurisdiction which influences the cybersecurity practices of the local election office. Likely explanations for this relationship include that offices which deploy e-pollbooks rather than paper pollbooks tend to have greater technological sophistication, that e-pollbooks as a digital technology introduce increased cybersecurity risk and therefore increased protections are implemented, or a combination of both. I did not find a statistically significant bivariate relationship between the use of DRE voting machines and the cybersecurity preparedness of local election administration offices. This may be because increasingly fewer election offices are deploying DRE machines due to cybersecurity risks surrounding the use of the technology[24] as well as political pressure to not use DRE machines[25].

[24] DHS and others have recommended the use of voting systems which create an auditable paper trail. DRE machines do not traditionally have this capability though some vendors are adding a paper receipt component.

The remainder of the difference of means tests explore the relationships between working with election cybersecurity partners and cybersecurity preparedness. As expected, these tests did not produce a lot of interesting findings. This is likely because there was so little variation in my sample related to partnerships as the vast majority of offices in the sample reported working with the identified partners. The one partnership for which I found a statistically significant relationship with the dependent variable was a partnership with outside entities within the local government structure, such as a local government IT department. This finding is consistent with the literature on local government capacity. The mean reported cybersecurity compliance score for offices in the sample which reported that they receive cybersecurity assistance from outside entities within local government is 72.37 percent. The mean for offices which reported that they have not received such assistance is 59.89 percent. The difference of means is 12.48 with a t-statistic of 2.0674. None of the other partnership variables have a statistically significant bivariate relationship with the dependent variable.

I also tested the bivariate relationship of an office's cybersecurity preparedness with the control variable for the structure of the local election authority. Because this control variable is categorical with more than two categories, the appropriate bivariate test is an analysis of variance (ANOVA) test. I did not find this control variable to have a statistically significant relationship with the dependent variable.

Then, I tested the bivariate relationships between the independent variables and the dependent variable using Ordinary Least Squares (OLS) regression analysis. OLS regression

---

[25] State and federal legislation which would ban the use of DRE machines has been introduced. Use of DRE systems is prohibited in some states.

analysis can only be used when a dependent variable is continuous or close enough to continuous to be treated as such. It is common in social science research to treat a percentage measure as a continuous variable.

According to Lewis-Beck (1980), some assumptions must be met to use OLS regression without producing biased or inefficient results. It is difficult to determine whether some of the assumptions are met, but they should be considered before choosing OLS regression as the method for analysis. First, it is important the models are correctly specified. This means that the relationship between the variables is actually linear, as assumed by OLS regression, and the correct variables are included in the model. The second part of this assumption comes into play with multivariate OLS regression. Based on my hypotheses, I expect a linear relationship between my variables of interest and the dependent variable, and I will include the "correct" variables in the multivariate models, according to my analytic framework. It is important to note this research is exploratory and is not based on well-established theory. Therefore, it is extremely unlikely the model is perfectly specified. Rather, these models are exploratory tests, and the findings should be considered preliminary.

The next assumption according to Lewis-Beck (1980) is that there is no measurement error in any of the variables. The reality is that there is always some measurement error, but as long as the measurement error is random and not systematic, it will not bias the findings. Chapter 3 explains my data collection methods through which I attempted to collect data that allow me to measure each variable with as little error as possible.

The rest of the assumptions relate to the errors in the model or the error in the population. Related to the model's errors, OLS regression assumes the errors are homoscedastic, are not

correlated with X, and have no serial or autocorrelation. At this stage, the best way to consider these assumptions is to review scatter plots of the data. I reviewed scatter plots between the dependent variable and each of the independent variables of interest and did not identify any obvious issues with the error. Some of these and other potential issues were further considered after the models were estimated.

Finally, an assumption of OLS regression which is key to hypothesis testing is that the population error should be normally distributed. Of course, the population error is unobserved, so this can be considered using the distribution of the dependent variable. As stated above, this distribution appears to be moderately skewed left or negatively skewed[26], but it is not severely skewed. One indication the skewness is not severe is that the mean and median are nearly equal. I also used the Shapiro-Wilk test for normal data and found a p-value of .1584 which means I do not reject the null hypothesis that the variable is normally distributed.

I cannot confirm my data and models perfectly meet the assumptions for OLS regression, and I acknowledge they likely do not. However, I did not identify any obvious violations of the assumptions for OLS regression. Further, my options for qualitative analysis are severely limited by the number of observations for which I was able to collect data. Based on these considerations, I determined OLS regression is the most appropriate method for this exploratory quantitative research.

Table 11 displays the results of a series of bivariate OLS regression models which estimate the effects of the independent variables of interest related to internal characteristics of a local election administration office on an office's reported compliance with key cybersecurity

[26] The skewness is -0.6.

recommendations. Of course, these tests provide similar information to the above bivariate tests as they are investigating the same relationships. I find a statistically significant bivariate relationship between the dependent variable and an office's total number of election administration staff, number of IT staff who work on election administration, budget, and the professional experience of the local election official. I did not find that a local election official's education level or whether the office is in a rural jurisdiction have a statistically significant estimated effect on cybersecurity preparedness.

[Table 11 about here]

Overall, these findings suggest that it is the financial and human resources of a local election office which affect its cybersecurity preparedness. This leaves the question of why a local election official's education level is not significant. One explanation may be a lack of variation in education level among the local election officials in the sample. Out of fifty, forty-one of the local election administrator respondents ranged between a high school degree and a bachelor's degree with thirty out of fifty having at least a two-year college degree.

According to a bivariate OLS regression model and this sample of local election offices, as the number of IT staff in a local election office increases by one IT specialist, the estimated percentage of cybersecurity compliance of an office increases by a statistically significant 4.3 percent. The estimated percentage of cybersecurity compliance for offices with no IT specialists is a statistically significant 63.4 percent. The variable for the number of IT staff explains about eighteen percent of the variance in the dependent variable in this sample.

I found that as the reported budget of a local election office increases by one dollar, the estimated cybersecurity preparedness score of the office increases by a statistically significant

0.000001 percent. One reason the estimated effect appears small is that the unit of the independent variable is very small – one dollar. The constant is a statistically significant sixty-seven percent, although this is not substantively significant as no local election administration offices have a budget of zero. The independent variable for budget explains about eight percent of the variance in the dependent variable in this sample.

A bivariate OLS model estimates that local election administration offices with a certified election administrator, on average, are about 15.1 percent more compliant with cybersecurity recommendations than those without a certified election administrator. This finding is statistically significant at the 95 percent confidence level. This model estimates that offices without a certified local election administrator are about 63.5 percent compliant with cybersecurity recommendations. The certification variable explains about fourteen percent of the variance in the dependent variable in this sample.

Finally, through a bivariate OLS regression, I found that as an office's total election administration staff increases by one employee, the estimated cybersecurity compliance of an office increases by a statistically significant 0.45 percent. The constant is a statistically significant 65.2 percent, though it does not make logical sense to estimate a staff size of zero as all local election offices have at least one person who works on election administration. The total staff variable explains about thirteen percent of the variance in the dependent variable.

The next series of bivariate OLS regression models explores whether jurisdiction-level characteristics may influence a local election office's cybersecurity preparedness. For this series of models, I chose one measure of each variable. For the variables for which I collected two measures (age and race), I chose the most relevant measure of the variable according to the

findings of prior research described in Chapter 2. The results of these models are displayed in Table 12. Similar to the results of the previous bivariate tests of these relationships, I did not find a statistically significant relationship between the dependent variable and the income or age of the jurisdiction's population or whether the jurisdiction is rural. I did find a statistically significant estimated bivariate effect of the variables which reflect a jurisdiction's size and demographic diversity. The following interpretations reflect the statistically significant findings of bivariate OLS models of my sample. The constant of each model is presented in Table 12, but only the constants which could be interpreted as substantively meaningful are interpreted below.

[Table 12 about here]

As the percent of the population with a high school education increases by one percent, the estimated cybersecurity preparedness of the jurisdiction's election office decreases by a statistically significant 1.2 percent. This variable explains about eight percent of the variance of the dependent variable in the sample. As the number of registered voters in a local election jurisdiction increases by one voter, the estimated reported cybersecurity compliance of the office increases by a statistically significant .00002 percent. This variable explains about 10 percent of the variance in the dependent variable. As the percentage of the population which speaks a language other than English increases by one percent, the estimated cybersecurity preparedness of the jurisdiction's election office increases by a statistically significant .6 percent. This model predicts that local election offices in jurisdictions with no speakers of other languages are about 60.9 percent compliant with cybersecurity recommendations. The language diversity variable explains about eleven percent of the dependent variable in the sample. As the non-white percent of the population increases by one percent, the estimated cybersecurity preparedness of a local jurisdiction's election administration office increases by a statistically significant .6 percent. The

constant is a statistically significant 58.8 percent. This variable explains about twelve percent of the variance in the dependent variable. Finally, as the percent of a local jurisdiction's population that is Hispanic increases by one percent, the estimated cybersecurity compliance of the election office increases by a statistically significant .4 percent. The constant is 63.1 percent and statistically significant. The diversity in ethnicity variable explains about eight percent of the variance in the dependent variable in this sample.

Overall, these findings suggest that local election administration offices in larger and more demographically diverse jurisdictions tend to have greater cybersecurity preparedness. I attempt to control for this in the multivariate models. A likely causal mechanism between jurisdiction size and cybersecurity compliance is that larger jurisdictions have greater financial resources. In fact, the correlation coefficient between the number of registered voters in a jurisdiction and the budget of the local election offices in the sample is .89. These two variables are so highly correlated that one could serve as a proxy for the other. This makes sense as population tends to be a major factor in local government budget allocations. The explanation for why the demographic diversity of the population is related to greater cybersecurity compliance for the local election offices in the sample is less clear, but it is likely at least partially due to the relationships between jurisdiction size and demographic diversity.

The final set of bivariate OLS regression models estimates the effects of the control variables related to technology and institutional structure and the partnership variables on the dependent variable. These results are displayed in Table 13. As was the case above, I did not find a statistically significant effect of the DRE machine variable and cybersecurity preparedness. Also like above, the local institutional structure variable does not have a statistically significant bivariate effect on cybersecurity compliance.

[Table 13 about here]

The use of e-pollbooks appears to be important. According to the model and this sample, local election offices which deploy e-pollbooks tend to, on average, be approximately eighteen percent more compliant with key cybersecurity recommendations. This finding is statistically significant. This model estimates the cybersecurity compliance of local election offices which do not deploy e-pollbooks to be a statistically significant 59.2 percent. This variable explains about twenty-one percent of the variance in the dependent variable in this sample.

Also consistent with the above bivariate tests, I did not find a statistically significant effect of most of the intergovernmental partnership variables on the dependent variable. I did find that local election offices who reported receiving cybersecurity support from outside entities within their local government are, on average, about 12.5 percent more compliant with recommended cybersecurity practices. This bivariate relationship is statistically significant, and the local government partnership variable explains about four percent of the variance of the dependent variable in the sample. This model estimates that local election offices which do not receive support from outside local government entities are about sixty percent compliant with key cybersecurity recommendations. It will be important to control for the use of e-pollbooks and include local partnerships in the multivariate models.

Influences on Cybersecurity Preparedness

The final stage in this exploratory quantitative research is a series of multivariate OLS regression models to estimate potential influences on a local government cybersecurity divide based on the factors described in Chapter 2. The results are displayed in Table 14. The first two models are based directly on my analytic framework. Subsequent models were estimated to help

account for and consider the effects of multicollinearity in the models and to improve compliance with the assumptions of OLS regression. None of the models include a variable for jurisdiction size. Because a local election administration's budget is so strongly correlated with the jurisdiction's size, the budget variable accounts for both budget and jurisdiction size.

[Table 14 about here]

The first model in this table, Model V, looks only at the independent variables of interest from the first stage of my analytic framework about the effects of the internal characteristics of a local election office on its cybersecurity preparedness. This model includes the office's budget, geographic location, IT staff, total staff and the local election official's level of education and professional experience. The model fit can be measured by the adjusted R^2. This model explains about twenty-one percent of the variance of the dependent variable in the sample. It is important to note that this full model only has a slightly better model fit than the e-pollbook variable alone. There is only one finding in this model that is statistically significant at the 95 percent confidence level and that is the effect of the number of IT staff on an office's cybersecurity preparedness. The constant is also statistically significant, but it is not substantively meaningful as local election offices with a value of zero for all of these variables do not exist. According to this model and this sample, as a local election office's number of IT staff increases by one IT specialist, the estimated percentage of reported cybersecurity preparedness of the office increases by a statistically significant 5.3 percent, holding the other variables in the model constant. Though other variables in the model have statistically significant bivariate relationships with the dependent variable, the findings related to budget, total staff, and certification are not statistically significant at the 95 percent confidence level when accounting for all of these independent variables of interest.

The next model, Model W, includes the independent variables of interest from the previous model as well as variables to account for the second stage in my analytic framework and my control variables. According to my expectations which were derived from the literature, the digital divide-related factors of an organization that were included in the previous model are likely determinants of the cybersecurity capacity for local election administration offices, but other factors may influence an office's overall cybersecurity preparedness. Model W attempts to account for these additional relevant variables. The technology use variables were added. The variable accounting for the institutional structure of the local election authority was added. The intergovernmental partnership variables were added. Finally, the percent of the population that is not white was added to account for a jurisdiction's demographic diversity.

Only one variable in Model W has a statistically significant estimated effect on the cybersecurity compliance of local election offices. That variable is the reported use of e-pollbooks. According to Model W, local election offices which deploy e-pollbooks are, on average, 17.2 percent more compliant with cybersecurity recommendations than those which do not use e-pollbooks, all other variables in the model held constant. The statistically significant constant is not substantively meaningful. The model fit improved with the additional variables. Model W explains about twenty-four percent of the variance of the dependent variable in the sample.

Because many of the independent variables of interest reflect an office's resources, I suspected there was multicollinearity in the models. Multicollinearity exists when two or more independent variables in a model are strongly related to each other. This can lead to findings that are not statistically significant even though a variable is substantively important. Therefore, I tested how related the independent variables are to each other and found some very strong

correlations between independent variables. I found that an office's budget and an office's IT staff have a correlation coefficient of 0.81. IT staff and total staff have a correlation coefficient of 0.86. Because both the literature and several of the prior tests suggest IT staff has a particularly important influence on cybersecurity preparedness and it is so strongly correlated with two other independent variables, I dropped the other two variables from the additional models as the IT staff variable can also account for the dropped variables. I also found that the variable for state training is strongly correlated with some of the other partnership variables. For example, state training and receiving support from DHS have a correlation coefficient of 0.59. Because the DHS variable has more variation than the state training variable, I chose to drop the state training variable from additional models to consider how this may affect findings related to the other partnership variables. Based on the results described below, dropping this variable did not change my findings.

Model X is the same as Model W except that the above referenced collinear variables have been dropped from the model. This is not to suggest these variables are unimportant. Rather, dropping them from the model allows me to consider how the multicollinearity may be affecting my findings. The model fit improved modestly. Model X explains about twenty-seven percent of the variance in the dependent variable of this sample. However, I still only find a statistically significant estimated effect of e-pollbook use on cybersecurity preparedness. It makes slightly more substantive sense to estimate the cybersecurity preparedness of an office with a value of zero for all of the independent variables once budget and total staff are no longer in the model. However, it is not likely that an office in an urban location would have a zero value for the other variables. The constant is a statistically significant 67.6 percent. According to Model X, local election offices in jurisdictions where e-pollbooks are used are, on average, 16.9

percent more compliant with cybersecurity recommendations than those that do not use e-pollbooks, all other variables in the model held constant. This suggests that multicollinearity may not be the only reason I did not observe additional statistically significant relationships in the previous models. However, below, I consider whether there is still multicollinearity in Model X.

The use of e-pollbooks clearly has an important relationship with cybersecurity preparedness for local election administration offices. However, it is important to consider whether other variables may also be substantively important. Two additional independent variables I found to have a relatively strong correlation with each other were the use of e-pollbooks and a local election administration office's IT staff. This makes logical sense as IT knowledge is needed to implement e-pollbook use across a jurisdiction. These two independent variables have a correlation coefficient of 0.49. Additionally, while the certification variable does not have an extremely strong correlation with any one of the other independent variables, it has a moderately strong correlation with three other variables: IT staff (0.36), e-pollbook use (0.36), and racial diversity (0.41). These correlations indicate there is still multicollinearity in the model.

In Model Y, I dropped the variable for e-pollbook use to consider the effects of the other variables. The model fit got substantially worse when e-pollbook use was dropped which is another indication that this variable is particularly important. The adjusted R^2, of Model Y is .1767. In Model Y, IT staff again becomes the only independent variable with a statistically significant estimated effect on the dependent variable. This suggests that the number of IT staff likely influences the cybersecurity preparedness of local election offices even though it is not statistically significant in models which include the e-pollbook variable. Collinearity between these two variables hinders my ability to observe the estimated effects of both variables in the

same model. According to Model Y, as a local election office's IT staff increases by one IT specialist, the estimated percentage of cybersecurity preparedness of the office increases by a statistically significant 4.1 percent, holding the other variables in the model constant. The constant is a statistically significant 65.9 percent.

The final model, Model Z, drops all the independent variables that I expected would be important but which do not influence the dependent variable according to any of the previous bivariate or multivariate models. According to Lewis-Beck (1980), one assumption of OLS regression is that the model is correctly specified. This means it includes all relevant independent variables but also that it does not include any irrelevant independent variables. Model Z is an attempt to improve the specification of the model based on the findings thus far. This model drops the rural variable, the local election administrator's education level, the local election authority structure, and all of the partnership variables except for local government partnerships as none of these variables have a statistically significant bivariate relationship with the dependent variable and therefore may be irrelevant.

Model Z has the best model fit of any of the models explaining about twenty-nine percent of the variance of the dependent variable in this sample. Again, e-pollbook use is the only variable with a statistically significant effect on the dependent variable. According to Model Z, offices in jurisdictions where e-pollbooks are used are, on average, about thirteen percent more compliant with key cybersecurity recommendations than local election offices in jurisdictions where e-pollbooks are not used, all other variables in the model held constant. The constant is statistically significant in Model Z, and it makes substantive sense to consider it. This model estimates that local election offices without a certified election administrator, with no IT staff, which do not use e-pollbooks, which serve a racially homogenous population, and which do not

receive support from outside entities within local government will report about 47.3 percent compliance with cybersecurity recommendations.

Overall, these multivariate models provide strong evidence that the use of electronic pollbooks in a local election jurisdiction has an important relationship with the cybersecurity preparedness of local election administration offices. A likely explanation for this is that the use of e-pollbooks reflects technological sophistication of the local election office. The correlation of e-pollbook use with IT staff lends support to this explanation. As e-pollbooks are a digital technology, this variable may simply be a proxy for the digital divide across the offices in the sample. In this case, it makes obvious sense that it would be strongly related to the cybersecurity divide across these offices, and it makes sense that it would wash out the estimated effects of other relevant variables when included as an independent variable in multivariate models. Another possible explanation is that the use of e-pollbooks introduces cyber risk which requires additional protections. While this may be a factor, the cybersecurity practices included in the dependent variable are recommended for all election administration offices whether or not e-pollbooks are used.

These models suggest that the size of a local election office's IT staff is another factor which influences cybersecurity preparedness. However, because the IT staff and use of e-pollbooks by local election administration offices appear to be related to each other, I was not able to see the effects of both variables in the same model. Further, it is very possible that additional variables are also important but that a small sample size and multicollinearity in the models impeded my ability to find statistically significant estimated effects of some variables in the fully specified models. Type II errors are likely when conducting multivariate analyses on a sample size of only fifty observations. Therefore, future studies should further investigate

whether the variables which have a bivariate relationship with cybersecurity preparedness in my sample actually influence cybersecurity preparedness even though I did not observe statistically significant effects in multivariate models.

Summary of Quantitative Findings

When considered in full, the quantitative findings in this chapter suggest that the human resources of a local election administration office positively influence the office's cybersecurity preparedness. Through bivariate tests, I found that the IT staff size, total staff size, and the professional experience of local election offices are related to offices' cybersecurity preparedness. Multivariate tests further provide some evidence of an influence of IT staff on cybersecurity preparedness for local election administration offices. Additionally, the use of e-pollbooks require human resources with some degree of technological expertise, and the correlation between the two independent variables supports this assumption.

The strongest evidence which can be drawn from these findings when considered in full is evidence that local election offices with greater IT expertise within the office tend to be more compliant with key cybersecurity recommendations. It is possible that other resources, specifically the financial resources of a local election office, influence cybersecurity preparedness, as indicated by the bivariate tests discussed above. However, when considering these analyses in full, it appears the that financial resources may only be important because they enable local election offices to acquire more staff, and particularly more staff with IT and cybersecurity expertise.

Other factors that may be influential according to my findings are the size and diversity of the population served by a local election office and local government partnerships. Based on

these quantitative findings alone, factors which should be considered in future studies of impacts on election cybersecurity include the human and financial resources of local election administration offices; the technological sophistication of local election offices; the expertise of election administration staff related to IT, cybersecurity, and election administration; the size and demographic diversity of the population served by the offices; and the partnerships the office has with other government entities. These factors and others are further explored through qualitative analysis in Chapter 5.

Chapter 5: The Perspective of the Election Cybersecurity Intergovernmental Network

Introduction

This chapter describes the findings of an iterative, systematic qualitative analysis of responses to semi-structured interviews of fifteen election cybersecurity experts as well as responses to open-ended survey questions by the sample of local election officials. While the previous chapter explores potential relationships between concepts of interest identified from the literature, this chapter reveals the findings of a qualitative exploration of the insight of experts on cybersecurity preparedness for local election administration offices. The findings presented in this chapter not only shed light on what factors influence cybersecurity preparedness but also provide greater detail of how and why certain factors may be influential. The qualitative data also allowed for a descriptive analysis of the intergovernmental network that supports the cybersecurity work of local election administrators. These findings are useful to theory building for future studies within this area of research.

Most of the findings presented in this chapter are based on semi-structured interviews of fifteen election cybersecurity experts. Five of the experts work on election cybersecurity in a federal government role. I interviewed federal representatives from two different US government agencies. Two of the respondents are presidential appointees. One of the respondents is an employee of a federal agency. Two of the respondents were full-time contractors for a federal agency at the time of the interview. Two of the interviewees from the federal government serve in partisan roles. One is a Democrat, and the other is a Republican. One of the federal respondents previously served in a partisan role as a Republican. The other two have not served in partisan roles to my knowledge.

Five of the interviewees worked for non-profit organizations at the time of the interviews. Each of these selected experts was from a different organization. All five of these experts have provided training or resources to US election officials. Two of the respondents from non-profits worked as both advocates and as consultants or trainers for local election officials related to election security. One has prior experience in a partisan position as a Democrat and the other has previous experience in a partisan position as a Republican. One of the respondents works for a bipartisan professional association in a role focused on cybersecurity issues for state and local governments. The remaining two interviewees work for non-partisan organizations that provide cybersecurity support to election officials and are not widely viewed as having an ideological tilt. Neither of these respondents engages in advocacy as part of their role. One focuses strictly on election cybersecurity issues in his or her current role. The other focuses on election administration and election cybersecurity issues.

Five of the interviewees work as state government employees within offices of the state chief election official (CEO). I did not interview any elected state officials. Two of the interviewees from state government focus on providing election cybersecurity support to local election officials in their states. Three of the respondents lead the IT efforts of the state CEO's offices, and part of their role includes engagement with local election officials on cybersecurity. One of these respondents currently works for a Republican elected official. Three of these interviewees currently work for a Democrat. One works for a non-partisan office. At least two of these respondents have served in an IT-related position under elected officials from both major parties.

This chapter is organized into several sections. First, I present overall themes identified across the responses from all of the experts I interviewed. Second, I explore similarities and

differences in expert perspectives based on the role of the experts. In this section, I also explore themes across responses to specific interview questions. Third, I present themes identified through a qualitative analysis of open-ended survey responses by local election administrators. Finally, I summarize my key qualitative findings.

Themes across Expert Interviews

Through the systematic qualitative data analysis of the interview responses described in Chapter 3, twenty-two key themes were identified related to the cybersecurity preparedness of local election offices. Each of these key themes was mentioned by at least one-third of interview respondents. Table 15 displays the themes in alphabetical order with corresponding definitions which were created based on how the respondents described each concept. There is significant overlap between many of the themes; many topics which fall under cybersecurity are naturally related to each other. Many of the interview responses provide insight into how the concepts are related. Findings described throughout this chapter include patterns identified between the themes based on how they were discussed by respondents. The definitions in Table 15 also provide descriptions of how some of the themes are related. For example, a note within the "need for improvement" theme describes how references to that theme from the interview respondents were often discussed in conjunction with other themes related to resources shortages. Each concept in the list was included as a separate theme because there was something about the way it was discussed by interviewees that provides insight into the topic that is unique to insight provided by the other themes.

[Table 15 about here]

Table 16 presents the themes in order of prevalence across interviews. The themes were ordered based on the number of individual respondents who referred to each theme. The first column ranks the themes in order of the number of total respondents who mentioned the topic. When two or more themes were mentioned by the same number of interviewees, they were ranked within the list in order of total cumulative mentions including multiple separate references by the same respondent. The next three columns list the themes based on the number of experts who referred to them within each category of respondent. The second column orders the themes according to the number of non-profit respondents who discussed them. The third column ranks the themes by the number of individual federal government respondents who referenced each of them. Finally, the fourth column ranks the themes according to the number of state government respondents who mentioned them.

[Table 16 about here]

The most commonly mentioned theme across the fifteen interviews was the importance of local election officials working with the office of their state's CEO on cybersecurity. Respondents made references to the state CEO's office as an important provider of cybersecurity services, training, and information for local election officials. Several of the interview respondents stressed that the office of the state CEO is the most important partner for local election officials related to cybersecurity. One state government respondent said local election officials need to take a more proactive approach to working with their state election office. This respondent suggested it is always the state office reaching out to the local officials and that the state office would like to see the local offices reach out to ask for what they need. Another respondent suggested, that though the local election administration office is primarily responsible for implementing cybersecurity measures, the state CEO's office has a responsibility to provide

the local offices with the information and resources they need for cybersecurity implementation. Several others similarly explained that the state CEO's office serves in a support role while local election officials tend to be the implementers. Some respondents, however, suggested that the state election office plays the leading role in election cybersecurity implementation or that they are at least responsible for some of the implementation.

The second most prevalent theme was the need for increased IT staff or general references to a lack of IT expertise within local election administration offices. One respondent said, "For local election officials, the biggest challenge is a lack of a technical, cybersecurity background." This respondent further explained that the election industry at-large is not currently attracting professionals with a cybersecurity skill set. Several respondents who discussed local election offices' need for increased resources stressed that the need is not just for money but for human resources. They explained that local election offices need staff with IT and cybersecurity expertise who can oversee the implementation of cybersecurity programs.

References to partnerships with the Cybersecurity and Infrastructure Security Agency (CISA) within DHS or references to DHS broadly were also made by most interviewees. Most of these references were to the usefulness free cybersecurity services that CISA makes available to local election administration offices. A few respondents describe CISA's services, such as cybersecurity assessments, as services that would not otherwise be available to local election offices due to prohibitive costs or a lack of awareness. A couple of respondents pointed out limitations to CISA's resources including that it can take too long for local election offices to receive services or that information from CISA needs to be filtered through the state CEO's office who can help local election officials understand what is relevant to them. However, the

vast majority of references to DHS/CISA were positive and indicated that DHS/CISA is an important partner and service provider for local election officials related to cybersecurity.

The next most common theme was a reference to the value of cybersecurity-related information sharing for local election officials and staff. Many of these mentions were suggestions that local election offices should be members of the EI-ISAC so they can share information with and receive information from other election offices throughout the United States. Several respondents explained that the EI-ISAC and its counterpart, the Multi-State Information Sharing and Analysis Center or MS-ISAC[27], are the best mechanisms through which local election officials can increase and maintain their awareness of the threats and risks to election systems. A couple of respondents said the information from the MS-ISAC can be daunting for local election officials both due to the quantity of the information and because the information is technical in nature. Some respondents also referenced the EIS-GCC as important to information sharing for local election officials.

The next theme is cyber hygiene. This is a very broad concept which was mentioned in reference to both what local election officials are doing about cybersecurity and what they should be doing. This theme includes mentions of the cybersecurity best practices that are broadly considered the most basic or fundamental. The most commonly mentioned specific practice within this topic was two-factor authentication which one respondent suggested is the single most important cybersecurity practice for local election officials to implement. Several

[27] The MS-ISAC is open to all SLTT government entities and, like the EI-ISAC, is funded by DHS and operated by CIS. Though the inverse is not true, SLTT entities which join the EI-ISAC automatically become members of the MS-ISAC as well.

respondents described cyber hygiene as one area where many local election officials are successfully implementing best practices; others mentioned a need for improvement in this area. One respondent suggested that if all local election officials would just implement the most basic cyber hygiene best practices, such as two-factor authentication and keeping software up to date, the cybersecurity posture of election systems nationwide would drastically improve. This respondent explained that while many local election offices have adopted these key practices, the majority of offices are still lacking some of the most basic protections. Another respondent agreed saying, "the basics go a long way."

The importance of having partnerships with non-governmental organizations was also frequently discussed by respondents. Several of these references were to professional associations through which election officials can receive information and share best practices including NASS, NASED, the Election Center, and the International Association of Government Officials (iGO). Respondents also suggested that non-profit organizations that provide cybersecurity resources or consulting services can help local election officials fill gaps in capacity and expertise. Several respondents also mentioned cybersecurity services that private companies have made available to local election officials at no cost; there were multiple references to free services available through Microsoft.

The next theme in ranked order is the need for additional funding. Several of the experts argued that a lack of adequate funding is by far the greatest challenge related to cybersecurity for local election administration offices. Most of the mentions of a need for funding were discussed in conjunction with the need to hire additional staff or to contract with cybersecurity vendors. Some mentioned the need to purchase technology. One respondent said, "Elections are the

cornerstone of our democracy, and they're grossly underfunded - not just in terms of securing them but also even just administering them."

Following funding in order of prevalence is training. Similar to implementing cyber hygiene best practices, some respondents referenced cybersecurity awareness training as something many local election administrators are doing, while others referred to it as an important practice that should be implemented more broadly. Multiple interviewees suggested training for election administrators should cover the basics of cybersecurity such as how to avoid falling victim to phishing attacks. Some respondents suggested training can help local election officials raise their awareness of cybersecurity risks and of the services available to them. References to training included training provided by the federal government, the state government, and non-profit partners.

The next most common theme relates to mentions of "shared responsibility." Most respondents suggested that the cybersecurity of US elections is not the sole responsibility of one party, but rather, they suggested the responsibility is shared between multiple actors. Key to this theme was the idea that multiple parties need to assist each other and that they rely on one another. One respondent said, "Ideally it's a team effort. That's the only way we can be successful on this." Most respondents included local election officials, state election officials, and the federal government in their references to shared responsibility. Some also included vendors. A few additionally mentioned non-profit organizations. A couple of interviewees even included voters.

Similar to but separate from the above theme, several respondents suggested that election cybersecurity responsibility is split across multiple actors. This theme includes any references to

the owner and/or operator of a specific system as ultimately responsible for the security of that system. Respondents explained that, in our decentralized system, election systems are owned and operated by a range of entities. For example, some election-related systems are owned and operated by the office of the state CEO in which case, the state CEO's office is primarily responsible for security, while other systems are managed by local election offices in which case, they are primarily responsible. Some experts suggested that responsibility is both shared and split. For example, local election administrators need help from their partners related to the systems for which they are ultimately responsible, but other systems are the sole responsibility of other actors.

The next theme is federal partners. This includes any references to the importance of working with the federal government broadly or any references to specific federal departments or agencies other than DHS. One respondent indicated that within the shared responsibility model, the federal government provides an important role in terms of intelligence, grantmaking, and support services. Several others mentioned an advisory or support role of the federal government. A few of the interviewees argued that the federal government's role in election cybersecurity should increase from its current status. In terms of specific agency mentions, the EAC and the FBI were each mentioned by more than one respondent.

After federal partners, the following theme in order of prevalence is mentions of the importance of working with vendors on cybersecurity. This includes references to working with vendors who provide IT or cybersecurity services to local election offices as well as mentions of coordination with election technology providers to protect the equipment or systems they provide. Several respondents explained that, in light of staffing shortages, working closely with vendors is an important way local election officials can improve their cybersecurity posture

because vendors can provide cybersecurity as a service. Some respondents argued that local election officials are too reliant on vendors when it comes to cybersecurity and that they lack the necessary awareness to hold vendors accountable.

Shortly behind vendor partnerships is the theme of partnerships with the state government. Within this theme are references to the state government broadly as well as references to specific state government agencies other than the office of the state CEO. Potential state partners for local election officials which were mentioned by more than one respondent include the office of the state Chief Information Officer (CIO) and state-specific National Guard units.

Next on the list is another partnership-related theme. Several respondents stressed the importance of local election administration offices having strong partnerships with their local government's IT department or CIO. One respondent suggested county election offices should have daily contact with their county's IT department. Several of the experts explained that local election officials are often completely reliant on their broader county government for IT provision and support because they do not have any IT specialists on staff.

Another theme was variation. Some respondents explained that it is difficult to discuss the cybersecurity efforts of local election administration offices in a broad or general way as there is great variation in the capacity of local election offices to address this challenge. Most of the experts who mentioned variation suggested that offices in large jurisdictions are more capable and prepared to address cybersecurity than those in small jurisdictions.

The next theme relates to a need for local election officials to improve their cybersecurity efforts. Most of the experts who mentioned a need for improvement were quick to point out that

it is not due to a lack of concern or a lack of effort on the part of local election administrators. Rather, they suggested that local election offices simply lack the necessary resources, awareness, or expertise. One expert said, “we have a long way to go, but they are taking it seriously and working within the scope of the resources they have to implement best practices.” A few respondents, however, suggested local election offices are not taking ownership of the issue or are not taking cybersecurity seriously enough. One respondent explained that local election officials have a hard time understanding why their tiny county would be a target for Russia.

Another commonly discussed theme was “procedural controls.” This includes any references to security-related measures that are procedure-based rather than technical in nature. Examples include audits, maintaining strict chain of custody, and logic and accuracy tests. Most of the experts who mentioned procedural controls suggested that election officials are very skilled at implementing them. One respondent said, “local election officials are really, really good at procedural controls. They've been doing these things forever.” Another respondent suggested that procedural controls are engrained in the culture of local election administration offices, and technical controls need to be embraced in a similar way.

The next most frequently mentioned theme includes suggestions that local election officials are primarily responsibility for election cybersecurity in the United States. While most respondents discussed a shared or split responsibility model, several respondents suggested that as local election officials are primarily responsible for administering elections, they are ultimately responsible for the cybersecurity of elections. Most of these references were within references to split or shared responsibility. These respondents argued that, while responsibility is shared, it is local election officials who have primary responsibility.

The following theme is “time constraints.” Some of the experts mentioned a shortage of time as a barrier to cybersecurity implementation for local election officials. One specifically said he or she believes local election officials would be better about embracing cybersecurity assessments if they had more time.

Next, is the concept of federal grant use. This includes references to grant funds which are already available and is separate from mentions of the need for additional grant funds which were included in the “need for additional funding” theme. One respondent suggested recent federal grants have helped local election offices implement additional cybersecurity measures. Alternatively, another expert said that federal grant funds rarely make it beyond the state election office down local election offices.

Another theme relates to mentions of creating and exercising incident response plans. A few of these references were made in conjunction with a discussion of the risk of ransomware. One expert argued that creating and exercising a cyber incident response plan is the most important thing local election officials can do to protect their offices and systems from cyber threats. A couple of others suggested its among the most important practices. One respondent advised that the quality of incident response plans is a concern. This respondent said that while many local election offices have plans, they are often not very robust or are too heavily reliant on vendors to execute.

The final theme on the list is US critical infrastructure. This theme includes references to the designation of elections as critical infrastructure or to the nation-state threat that requires a whole-of-government response. A pattern related to this theme was to mention it in reference to why the federal government has a role in election cybersecurity. One respondent said, “our

current posture which involves foreign adversaries, creates a role for the federal government to provide assistance and deterrence. It's unrealistic to expect state and local election officials to thwart nation-state threats on their own."

Similarities and Differences in Expert Perspectives

While the above section describes the themes identified across all fifteen expert interviews, this section explores how themes were the same or different across the three categories of interview respondents: election cybersecurity experts who work for non-profit organizations, election cybersecurity experts who work for the federal government, and election cybersecurity experts within state government. The second through fourth columns in Table 16 display how the prevalence rankings of the identified themes by the number of individuals who mentioned them looks slightly different across the three categories. This reflects slightly different perspectives of the experts based on their roles.

Across the three groups of experts, working with the office of the state CEO was a priority item. It was discussed by almost all of the respondents from each of the three categories. The only group for which it was not the most prevalently mentioned theme was the group of state government election cybersecurity experts, all of whom work within offices of a state CEO. For the state government group, it is second on the list.

The need for IT expertise within local election administration offices was the second highest ranking theme from non-profit respondents and federal government respondents. This topic fell further down the list for state-level respondents. This is probably because most of the state respondents explained that local election administrators are heavily reliant on outside

entities such as their county IT department, vendors, and the state government for their IT support.

From state respondents, information sharing was the highest-ranking theme as it was referenced by all five respondents. The state respondents stressed the importance of local election officials belonging to information sharing groups, such as the EI-ISAC, so they maintain awareness of the threats. These respondents also argued that regular communication with government partners at the local, state, and sometimes federal level is essential. Information sharing and awareness was also mentioned by almost all of the federal respondents. However, only two of the non-profit respondents discussed information sharing. This reflects a difference in perspectives from those whose roles in the intergovernmental network may not be as central. Relatively few non-profit groups belong to the EI-ISAC or EISCC, for example.

Almost all of the experts from all three groups stressed the importance of basic cyber hygiene practices. A related theme with interesting differences across the three groups is training. The importance of training was mentioned by almost all of the non-profit and state respondents but only two of the federal respondents. This may be because state and non-profit partners are more likely to deliver cybersecurity training to local election administrators than federal government entities.

Overall, the partner-related themes were discussed by most respondents. As described above, almost all of them suggested a partnership with the state CEO's office is important. Almost all respondents across the three categories also mentioned DHS or CISA as an important partner or service provider. Unsurprisingly, non-governmental organizations were referenced as an important partner by almost all of the non-profit respondents. Non-profit partners were

discussed by slightly fewer but still most of the experts from the other two categories. References to federal partners other than DHS or broad references to the federal government were made by most of the non-profit respondents and federal respondents but only one state-level respondent. The state government representatives tended to focus on DHS/CISA as the key federal partner related to cybersecurity for local election administration offices. Partnerships with vendors and local IT were mentioned more by the experts from the federal government than those from the other two categories. In general, some interviewees tended to focus on vendors as a key IT and cybersecurity provider for local election officials while others focused on local government IT departments as serving that role. This likely reflects a difference in perspective based on state and local experiences. State partners other than the state CEO's office were mentioned by two to three respondents from each group.

There appears to be a difference in perspective related to whether funding needs are a top priority or challenge for local election offices, at least among the respondents. The need for additional funding was argued by all of the federal respondents, most of the non-profit respondents, and two of the state respondents. One state respondent explained that the lack of IT expertise within local election administration offices diminishes the usefulness of cybersecurity funding. This respondent argued that funds are only useful if there is someone who knows how to effectively implement them. Further, this respondent suggested that money cannot just buy expertise because the cybersecurity recruitment issues for local government are not something that can be remedied by sporadic grant payments. More federal respondents also discussed the current use of federal grants than respondents from the other two categories.

Federal respondents were also more likely than the others to argue that local election officials are primarily responsible for the cybersecurity of US elections. Only one state-level

respondent suggested local election officials have primary responsibility. Non-profit respondents were slightly more likely than those from the other two categories to mention time constraints of local election officials. This may be because those from non-profits organizations geared toward elections see their role as helping to fill gaps for election officials that are left open by a lack of time, expertise, or money. Variation and the need for improvement were each discussed by two to three respondents from each category. Incident response plans and the critical infrastructure designation were each mentioned by one to two respondents from each group.

Tables 17 and 18 each provide additional detail on how prevalent each theme was in the responses from each group of interviewees. Table 17 focuses on the themes related to the roles and responsibilities of actors within the election cybersecurity intergovernmental network as well as partnerships between these actors. Table 18 displays the themes related to the resources and practices of local election administration offices. In the two tables, each identified theme is broken down according to the three categories of respondents as well as summary of all respondents. The darker the circle, the more prevalent a theme was for that group. Where there are black circles, themes were discussed by all or almost all of the relevant respondents. The gray circles reflect themes that were mentioned by about half of the respondents from the relevant group. The white circles indicate topics that were mentioned by the smallest number of respondents from each group but were still prevalent enough overall to be considered a theme.

[Table 17 about here]

As you can see in Table 17, the importance of partnerships with the office of the state CEO and with DHS stand out as among the most prevalent themes across all respondent groups. Partnerships with non-governmental organizations were mentioned by most respondents from

non-profits and also trended to be one of the most prevalently mentioned themes from all respondents. Non-profit respondents also stressed shared responsibility and broad federal involvement more than the other respondents. More respondents from the federal government emphasized that owner and operator of a specific system is the primarily responsible party for cybersecurity than those from the other two groups. Federal respondents were also most likely to discuss partnerships with vendors and local government IT. State partners other than the office of the state CEO were mentioned by a moderate number of experts across each category. Mentions of the critical infrastructure designation and arguments that local election officials have primary responsibility for election cybersecurity were made by fewer state-level respondents than respondents from the other two categories. Federal grant use and the critical infrastructure designation, though identified as themes, were mentioned with lower frequency overall than the other themes outlined in this table.

[Table 18 about here]

Table 18 organizes the qualitative findings in the same manner as the previous table but displays the results for the themes which relate to the resources and practices of local election administration offices. Across all categories of respondents, Table 18 shows that training was mentioned by most of the experts. Cyber hygiene, information sharing, and IT needs were themes which trended near the top overall and were mentioned by most of the respondents in two of the three categories and by a moderate number of respondents in the third category. Non-profit respondents were the least likely to mention information sharing. Federal respondents talked about cyber hygiene at lower rates than those from the other two categories. Funding needs was among the highest frequency themes overall. A moderate number of the respondents from state government and non-profits referenced funding needs for local election officials, while almost all

of the federal respondents argued local election officials need increased funding for cybersecurity.

Procedural controls, time constraints, the need to improve, and variation across local election administration offices were each discussed by a moderate number of respondents overall. Variation and the need for improvement were classified with a moderate frequency of mentions for each category of respondent. Time constraints of local election officials were mentioned by fewer respondents from state government than those from the other two groups. Procedural controls were referenced by more respondents from non-profit organizations than those from state government and more respondents from state government than those from the federal government. Incident response, while still theme, was the lowest frequency theme among those in Table 18. The importance of creating and exercising incident response plans was mentioned by fewer state government respondents than experts from the other two categories.

Table 19 provides a different viewpoint into how responses broke down across categories of respondents. Table 19 summarizes the most common responses to each interview question across respondents from each of the three categories as well as for the entire group of respondents. The categories listed across the top of the table relate to each of the interview questions which are included in Appendix 3.

[Table 19 about here]

After the grand tour question which asked respondents about their own job, the first interview question was, “who do you believe has primary responsibility for election cybersecurity in the United States?” The modal response across all categories of respondent and the overall group was that there is no one responsible party but rather responsibilities are shared

and/or split across multiple actors. Almost all of the respondents from non-profits additionally stressed that there is a role for the federal government in protecting elections from cyber threats. At least one respondent from each category said that while they are not solely responsible, local election officials are primarily responsible. Of the respondents who chose one party as primarily responsible, the most common choice was local election officials. However, there was strong consensus across the experts interviewed that several different actors play a role in protecting elections from cyber threats. Many respondents emphasized that some of the actors are implementers and others play a support or advisory role.

The next question was, "what are local election administrators doing to protect elections from cyber threats?" The most common response across all respondents can be summarized as local election officials are working with government partners and the EI-ISAC to make use of available resources and information. The most commonly mentioned practice by just the respondents from non-profit organizations is that local election officials are participating in cybersecurity training. The modal response from federal government respondents is the same as that of the overall group. Most respondents from state government said that most local election officials are relying on outside entities to provide cybersecurity for their systems and offices. State government respondents mentioned reliance on the state government, local IT departments, and vendors.

Next, I asked "what are the most important things a local election administrator can do to protect the election systems they manage from cyber threats?" The most frequent response overall can be summarized as, local election officials should develop trusted partnerships and utilize the resources made available by their partners. There is no modal response from state government respondents as each of the five provided a distinct answer. This may be reflective of

variation in election administration and available resources across the states. The most frequent response from respondents from the federal government was that local election officials should build their awareness about existing threats, common risks and vulnerabilities, and available resources. The modal response of the experts from non-profit organizations was that local election officials should develop relationships with those they can call on for help if and when it is needed.

Then respondents were asked, "who are the key partners for local election officials related to cybersecurity?" The overall modal response was that the state CEO's office is the most important partner followed by DHS/CISA. The most common response from non-profit respondents was the same. The state election experts added an additional partner. Their most frequent response can be summarized as, the state election office followed by CISA and the EI-ISAC/MS-ISAC are the key partners. Most federal respondents said the key partners for local election offices are their state CEO's office followed by their federal partners followed by their vendors.

Finally, I asked about the greatest challenges for local election administrators related to cybersecurity. Almost every interviewee responded that the most prominent challenge is a lack of resources. There were several variations of this response. Across all fifteen respondents and two of the three categories, the best summary of the modal response is that shortages of human resources, expertise, and money are the biggest challenges for local election offices related to cybersecurity. Most state respondents added a lack of awareness as an additional key challenge. The references to awareness were slightly different than references to expertise. Those who discussed awareness were talking about awareness of the cyber threats to local election

administration offices, while expertise refers to the knowledge and ability necessary to implement cybersecurity controls.

Those respondents who chose to provide additional insight beyond the interview questions stressed the importance of partnerships. One respondent suggested that cybersecurity experts need to improve their approach when reaching out to local election officials to offer their assistance but also that many local election officials should be more accepting of assistance. Another suggested that more partners, including experts on emergency management, should be brought into the election cybersecurity conversation.

Because I asked one question which was directly related to my research expectation, I also reviewed the number of references to intergovernmental partnerships and their importance that were made during interviews before the question about partnerships was asked. All of the interviewees except for one discussed the importance of intergovernmental partnerships to the cybersecurity efforts of local election administration offices before the question was asked. The one respondent who did not mention partnerships until the question was asked is from a non-profit organization.

Finally, it is worth noting that one topic identified as potentially important through a review of the literature was not identified as a theme in interview responses from election cybersecurity experts. That topic is relationships or work with policymakers. While a few respondents noted that it is important for local election officials to promote awareness about election cybersecurity issues among policymakers, not enough experts referenced the importance of working with policymakers for it to be considered a theme. One related theme which was identified was the need for additional funding which is reliant on policymakers in most cases.

One reason there were not more general references to the role of policymakers may be that much of the policymaking around election cybersecurity and administration occurs at the state-level while local governments are more focused on implementation. For that reason, it may be that state election officials are more focused on working with policymakers than are local election officials.

Perspectives of Local Election Officials

I also conducted a systematic qualitative analysis to explore themes within open-ended responses to three survey questions or prompts. Answering the open-ended questions was optional for the fifty local election administrators who completed the survey. I analyzed the responses to each of the three questions and identified themes within each question. I also identified the two most prevalent themes across the three sets of open-ended responses.

The first open-ended question was created to serve the same purpose as the grand tour question of the interview. The question was, “What do you believe is the single most important task a local election administration office can complete to protect the election systems they manage from cyber threats?” It was intended to be an easy-to-answer question which calls for a short response. It was meant to help respondents feel comfortable with the topic before moving on to more difficult questions. Of the fifty respondents, forty-five answered the question. Three themes were identified. The most prevalent theme was training. Seven responses related to cybersecurity training. Shortly behind training, is information sharing and awareness. Six of the responses related to sharing information with partners or building awareness. The last theme was access control. Five local election administrators gave responses related to passwords or generally referred to controlling access to the voter registration database.

The next prompt which called for an open-ended response was, “Please list any other organizations (governmental or non-governmental) that your office works with on election cybersecurity efforts.” Prior to this prompt, respondents were asked yes or no questions about partnerships with DHS, their state election office, the EI-ISAC, and outside entities within their local government. Twenty-six participants responded, but most of them listed more than one partner. I identified the five most frequently mentioned partners: the state election office, emergency management and homeland security departments, general mentions of federal partners, local IT departments, and the EI-ISAC/MS-ISAC. Twelve respondents mentioned the state election office. Seven respondents listed emergency managers or departments of homeland security. There were five general references to federal partners or the federal government. Four respondents referenced the IT department within their local government. Three respondents mentioned the EI-ISAC, the MS-ISAC, or both.

The final open-ended question was, “is there anything else you would like to share?” Sixteen participants chose to respond to this question. One theme was identified across eight of the responses – split or shared responsibility with the state election office. Eight respondents made some reference to how some of the election systems on which their office relies are protected by the office of the state CEO or at least that the state election office provides support services to help them protect the systems. Several respondents said the state election offices provides direct IT and cybersecurity services to their office. One of these responses focused on coordination difficulties. The respondent suggested that their coordination with the state election offices is “challenging in the best of times.” He or she suggested that trying to coordinate with their local IT department adds additional complexity and challenges.

Overall, there were two themes that stood out across the three sets of responses. Each of these themes were mentioned in responses to at least two of the three questions. The most prevalent theme was the office of the state CEO. There were several references to the importance of working with the state election office on cybersecurity efforts or receiving cybersecurity support with the state election office. The other theme was information sharing. Outside of the responses specific to working the state election office, there were several responses related to sharing information with partners and building awareness.

The qualitative findings from the survey responses are substantially less robust and extensive than the interview findings. However, these findings provide additional evidence which strengthens some of the findings in the above section. It is clearly important for local election officials to have strong partnerships, particularly with the office of their state CEO. It is also clear that they are often reliant on the state election office for cybersecurity services. Sharing information within their intergovernmental network also stands out as an important aspect of cybersecurity preparedness for local election officials.

Summary of Qualitative Findings

Several findings are clear from a systematic analysis of the opinions and insight of election cybersecurity experts and local election administrators related to the cybersecurity preparedness of local election administration offices. The first is that intergovernmental government partners are extremely important for local election administration offices because partners provide cybersecurity information and services that may not otherwise be within reach. The second is that most local election officials are facing a shortage of the resources which are

essential to cybersecurity preparedness. A third key finding is that basic cybersecurity practices are more important for local election offices than are advanced cybersecurity measures.

The findings produced by the qualitative portion of this study improve our understanding of the intergovernmental network related to cybersecurity within which local election administrators operate. Figure 2 is a simplified representation of the intergovernmental network which exists around election cybersecurity. This figure is informed by my qualitative data as well as the background research presented in Chapter 1. This figure and the next figure reflect the intergovernmental network of a local election administration office only as it relates to cybersecurity. A local election office's intergovernmental relationships related to election administration broadly or other elements of their job is likely different and is beyond the scope of my findings.

[Figure 2 about here]

My interviewees suggest that local election administration offices should and often do have partnerships with each of the other actors displayed in Figure 2. Information and services from some of those partners including DHS/CISA, other federal partners, organizations within state government, and the EI-ISAC is often filtered through the office of the state CEO. Local election offices usually have direct relationships with their vendors, the IT department within their local jurisdiction, and non-governmental organizations with which they partner. The office of the state CEO has partnerships with almost all of the other intergovernmental actors in the network including DHS/CISA, other federal partners, the EI-ISAC, partners within state government, vendors, non-governmental organizations, and each local election office. As the

lead federal agency on election cybersecurity, DHS/CISA has relationships with other federal agencies involved in this effort, state election offices, local election offices, and election vendors.

Figure 3 displays the flow of cybersecurity information and services between local election administration offices and their intergovernmental partners as described by the election cybersecurity experts I interviewed. The directions of the arrows reflect the direction of cybersecurity information, services, and other resources, according to responses. This figure displays an incomplete, preliminary understanding of the information flow within the election cybersecurity network as it is limited by the scope of my findings. Given the breadth and diversity of local election offices throughout the United States, this figure does not perfectly capture intergovernmental interactions for all local election offices. Rather, it is an attempt to describe the movement of information and services within its network for a typical local election administration office. There is variation in how local election offices interact with partners which is not fully captured by my data. Figure 2 displays only the relationships within the election cybersecurity intergovernmental network involving local election officials and only those which were identified through this research. While relationships exist between other entities in the intergovernmental network, as displayed in Figure 2, describing how information flows within those relationships is beyond the scope of this study.

[Figure 3 about here]

My findings strongly suggest that the office of the state CEO tends to be the most important partner for local election offices related to cybersecurity. According to experts, state election offices provide resources, services, information, and training directly to each local election office in their state with the intention of helping local election offices improve their

cybersecurity preparedness. State election offices also filter information coming from other partners and relay it to local election offices. DHS/CISA is the next most important partner according to my findings, but the information and services they provide often go through state election offices on the way to local election offices. The direction of the arrow is one way from DHS/CISA to a local election office and from state election offices to a local election office because the experts I interviewed described the flow of services and information between these entities moving in only one direction. This does not confirm that information and services only move in one direction in the real world as this diagram is only based on the data collected through this study. Similarly, the EI-ISAC, which is funded by DHS, is key to information sharing and maintaining awareness for local election officials. However, in the case of the EI-ISAC, the arrow points in both directions. While experts generally described the EI-ISAC as a service and information provider to local election offices, some additionally reported that local election offices feed information into the network through the ISAC. Information or assistance from other federal partners as well as from additional state government partners can also be important to local election administration offices. Again, the local election offices sometimes receive information from federal and state partners through the state election office.

According to experts, local election offices tend to maintain their own relationships with local IT departments, with the vendors they contract directly, and often, with non-profit organizations. The arrows representing all of these relationships point in both directions as some respondents described an interactive relationship between local election officials and these partners. For example, one respondent from state government explained that local election officials in his or her state are educating themselves on cybersecurity best practices so they can have more productive conversations with their IT providers and gain a better understanding of

the measures they are asking their vendors or IT department to implement. One respondent from a non-profit organization said some local elections officials are becoming increasingly proactive about reaching out to non-governmental organizations to partner on projects.

The qualitative findings described throughout this chapter do not provide as strong of explanatory evidence as descriptive evidence. Overall, while the interview respondents, and to an extent survey respondents, provided opinions which are largely consistent with my research expectation, I must consider the fact that these findings are based on subjective opinions. The opinions are those of well-recognized experts in the field, but they are subjective opinions nonetheless. This qualitative research approach did not provide me with enough evidence to make a causal argument about the effects of intergovernmental partnerships because this research design did not allow me to compare the differences between offices with strong partnerships and offices that lack strong partnerships. However, the experts I heard from stressed that government partners are critical to cybersecurity preparedness for local election officials. In addition to government partners, experts also believe non-governmental organizations and vendors often help local election officials improve their cybersecurity preparedness. However, some of the respondents who addressed the role of vendors suggested local election administrators are too reliant on vendors to provide cybersecurity and sometimes have little understanding or control over what their vendors are doing to protect critical election systems.

Digging further into the research expectation for this study, my findings are consistent with the overall expectation that coordination and collaboration within an intergovernmental network is key to election cybersecurity preparedness for local election administration offices. Additionally, I expected to find that it would be important for intergovernmental partnerships to include specific elements: communication protocols, regular communication, and the acceptance

of support from other entities. The local government capacity research suggested that accepting assistance from higher levels of government is an important way local government entities can fill gaps in capacity including IT-specific capacity. The experts I interviewed agree. Several experts suggested that local election officials who accept cybersecurity assessments, services, and resources from partners who offer them are likely to have a stronger cybersecurity posture. Although, some respondents suggested that many local election officials are not even aware of what is available. This is the reason many of the experts also stressed the importance of regular contact with partners who can provide services, broad information sharing, and being a member of the EI-ISAC. While there was consensus across most experts that the acceptance of support from partners who offer it and regular communication with partners is important to the cybersecurity preparedness of local election offices, I did not gain any insight about the role of communication protocols from my qualitative research. While the EIS GCC has established formal yet voluntary communication protocols for the election cybersecurity intergovernmental network, there was no mention of the protocols during interviews or in survey responses. Therefore, this research does not provide insight into whether they are followed by the network or enforced by election officials.

I also expected to find that while accepting assistance from government and non-governmental partners is essential, it will also be important for local election administrators to maintain ownership and control of their office's cybersecurity plans and implementation. My findings are inconsistent with this part of the expectation. None of the experts interviewed referenced the importance of local election officials maintaining control of their cybersecurity program. Most of them described a situation where local election officials are heavily reliant on state government and often the federal government, local IT departments, and vendors. In some

cases, they reported that local election officials maintain little control over the cybersecurity of their office and the systems they manage. Many of the responses, including some from both expert interviews and the survey of local election administrators, suggest that it is the state election office rather than local election offices that operates at the center or the position of control of the intergovernmental network for election cybersecurity. Looking at the qualitative findings comprehensively, it may be that local election administration offices simply lack the resources and expertise to lead their own cybersecurity efforts rather than relying on the expertise of the state government and other outside entities. Several respondents suggested this lack of resources is why local election offices are so reliant on the state and other outside entities like local IT departments and vendors. The intergovernmental relations literature suggests this could be problematic. For example, Milward and Provan (2000) suggest this lack of control could lead to principal-agent problems and instability. Some of the interviewees who suggested that local election officials fail to hold their vendors accountable provided some evidence of principal-agent problems. Future research should investigate this further.

This leads to another major finding from this qualitative analysis which is that the resources or lack thereof of local election administration offices influences their cybersecurity preparedness. The impacts of resources and resource shortages were addressed in some way by every interview respondent. Most prominently, the election cybersecurity experts argued that local election officials lack the necessary cybersecurity expertise on their staff to implement cybersecurity risk management programs in-house. After IT needs, the next most frequently mentioned resource shortage was funding. While many of the interviewees argued that funding shortages for local election administration offices are related to cybersecurity deficiencies, several of them argued that funding alone is not enough. They suggested local election offices

cannot simply buy cybersecurity improvements, rather they need experts who can oversee implementation long-term. While money is related to staffing shortages, it is not the only factor leading to human resource deficits, according to some respondents. Other factors include recruitment and workforce development challenges. Several interview respondents referenced time as another resource deficiency for local election administrators. Time constraints are likely related to a lack of human resources and a lack of funding. While several respondents explained that there is a lot of room for improvement for local election offices related to mitigating risk to the election-related systems they control, most of these responses were directly tied to a lack of resources including time, money, expert staff, and awareness.

Finally, many of the election security experts focused much of their discussion on cybersecurity fundamentals. Most of the respondents referenced basic cyber hygiene practices such as two-factor authentication and updating software as the most important steps local election officials can take to improve their cybersecurity preparedness. Several interviewees suggested that many local election officials are implementing these practices. Other respondents highlighted these practices as the most important things local election officials need to do. This suggests that focusing on the fundamentals of cybersecurity to construct my dependent variable for the quantitative analysis was an appropriate approach. Several respondents also stressed the need for ongoing cyber hygiene and cybersecurity awareness training for local election administrators. Specifically, some respondents suggested that training will help administrators maintain awareness of the most prevalent risks to their systems but also of the services and resources available to help them mitigate risk.

In summary, election cybersecurity experts talked about a lot of work being done and a lot of work left to do related to the cybersecurity preparedness of local election administration

offices throughout the United States. They suggested that intergovernmental partnerships will be key to continued improvement. They explained that most local election administrators are in a position where they must rely heavily on the office of their state's CEO for cybersecurity support and on DHS and other outside entities who provide free and affordable services. These experts pointed to resource needs as the primary reason for some of the deficits they identified. Though most experts seem to believe that accepting assistance from partners can help local election officials fill gaps left by resource shortages, many suggested that IT expertise within election administration offices is an ongoing need that cannot be completely solved by money or outside assistance.

The next and final chapter presents the conclusions and contributions of this study which are based on the findings presented this chapter and the previous chapter. Chapter 6 identifies the key findings which appeared across both analysis approaches. It also evaluates the consistency of the overall conclusions of this study with my expectations and identifies implications of these conclusions for other researchers, policy makers, and administrative leaders.

Chapter 6: Conclusions, Implications, Limitations, and Directions for Future Research

Introduction

Election administrators throughout the United States are facing a new normal. Since the issue of cybersecurity for US elections was raised to the forefront following the 2016 elections, many local election officials have had to add cybersecurity risk management to their growing list of responsibilities. Through a mixed methods research design, this study explores the cybersecurity preparedness of local elections administration offices, including which factors influence preparedness, the current state of preparedness, remaining challenges, and how local election officials are working with partners to address challenges.

This study was comprised of two stages of data collection and analysis: First, I created an original survey and asked a sample of local election administrators from throughout the United States to respond. I collected supplemental information from secondary data sources about the fifty local government jurisdictions from which the local election administration office participated. Through bivariate and multivariate analysis, I analyzed the relationships between the reported compliance of local election offices with cybersecurity recommendations and internal characteristics of the offices, characteristics of the local jurisdictions, intergovernmental partnerships, and other factors. Second, I conducted semi-structured interviews of fifteen experts in the cybersecurity of US elections. Through systematic qualitative analysis, I identified themes across the interview responses.

While most of my findings are consistent with the literature, others were somewhat surprising. For all but one of the surprising findings, an alternative explanation from that which I

expected provides a potential explanation for the observed relationship between the concepts. Additional research is needed to further explore this.

The section below is an evaluation the consistency of my findings with the expectations I derived from the literature. In this chapter, I also present implications of my conclusions for consideration by policy makers and administrative leaders. Additionally, I acknowledge limitations of this study and how future research can help address remaining gaps. Further, I present opportunities for future studies of election cybersecurity and local government cybersecurity based on the foundation provided by this study. Finally, I summarize my contributions which include laying a groundwork for future research on cybersecurity issues in US election administration as well as contributions to broader literature on election administration and public administration.

Evaluation of Hypotheses and Research Expectation

Table 20 presents determinations of the consistency between my expectations and my findings. The names of the hypotheses in the table correspond with the names of the hypotheses presented at the end of Chapter 2. Table 20 includes an assessment of the extent to which the findings of my quantitative research are consistent with each hypothesis, the extent to which the findings of my qualitative research are consistent with each hypothesis, and my overall conclusion related to each expectation.

In the second and third columns of the table, I assess that the evidence is inadequate if the analysis did not yield any evidence in support of the hypothesis, but it also did not provide evidence that the hypothesis is not correct. While the lack of evidence may indicate that the hypothesis is not correct, it is also possible other factors, such as the survey or interview

instrument or the small sample size contributed to the lack of evidence. Additional research is needed to make conclusions related to these hypotheses. I assess that quantitative findings provide limited support for a hypothesis if I found a bivariate relationship between the variables of interest, but the relevant finding was not statistically significant in multivariate models. If some experts provided insight consistent with the hypothesis but it was not discussed sufficiently to be considered a theme, the support for the expectation from qualitative findings was assessed as limited. For some of the hypotheses related to which the support from my findings was limited, I conclude that the relationship is more nuanced than accounted for by my expectation. Quantitative findings were assessed as providing moderate support if I found a bivariate consistent relationship and a statistically significant finding relevant to the hypothesis in at least one multivariate model. Qualitative findings were assessed as moderate evidence if I identified a theme consistent with the expectation, but the theme was referenced by fewer than half of the interview respondents. I assessed quantitative findings as providing strong support if there was a statistically significant finding supporting the hypothesis across all relevant tests. Qualitative findings were assessed as providing strong support if most of the experts provided insight consistent with the prediction. Finally, quantitative findings were assessed as providing evidence to the contrary of the hypothesis if I found a statistically significant bivariate relationship in my sample between the variables of interest in the opposite direction of that which was predicted. While additional research is needed to confirm each of my findings, I am more confident about those for which the evidence was assessed as moderate to strong.

Based on limited support from quantitative research and strong support qualitative research, I conclude that the financial resources of local election offices seem to influence cybersecurity preparedness because financial resources are needed to hire staff, and particularly

to hire staff with expertise in IT or cybersecurity. Future research should further explore this relationship and investigate whether financial resources only matter because they are related to human resources or there are additional reasons for which financial resources influence the cybersecurity preparedness of local election administration offices. I conclude that the professional experience of local election officials in election administration may influence the cybersecurity preparedness of local election offices. Additional research should explore this relationship by considering the influence of factors such as years of experience, certifications, and academic degrees of both election officials and their election administration staff on the cybersecurity preparedness of an office. Similarly, based on limited evidence, I conclude the size of an office's total election administration staff may influence cybersecurity preparedness. My findings provide stronger evidence that staff who specialize in IT are important. I conclude that the number of IT specialists employed by a local election office tends to influence its cybersecurity preparedness. Future studies should investigate potential nuance in this relationship by investigating the impacts of not just the quantity of IT staff but also the qualifications of IT staff on an office's cybersecurity posture. My findings did not provide any evidence that the level of education of the local election official or the geographic location of the office influences cybersecurity preparedness.

Based on limited to moderate evidence, I conclude that a jurisdiction's population size seems to influence the cybersecurity of the local election office because population size is related to resource allocation for the office. Related to the rest of the jurisdiction-level hypotheses, my findings either provide inadequate evidence to make a conclusion related to the expectation, or my findings provide evidence which contradicts my expectation. Additional research is needed to explore whether and how characteristics of the population served by a local election

administration office influence the preparedness of the office. I found no evidence that whether a local jurisdiction is urban or rural impacts the cybersecurity preparedness of the election administration office. I found no evidence that the median income or the age of the jurisdiction's residents influence cybersecurity preparedness for election offices. I conclude, based on limited support, that election offices in local jurisdictions with lower percentages of high school graduates may tend to be more compliant with cybersecurity recommendations. I failed to link this finding to a logical explanation. I also conclude that election administration offices may tend to be more cybersecurity compliant as their jurisdictions' populations have higher levels of diversity related to race, ethnicity, and language. This conclusion may be related, at least in part, to jurisdiction size and therefore resource availability. However, future research is needed to explore whether and why the demographic diversity of local jurisdictions influences the cybersecurity preparedness of election offices.

Related to intergovernmental partnerships, based on support from qualitative findings, I conclude that receiving information and other support from the state election office, DHS/CISA, the EI-ISAC, local IT departments, and other network partners seems to influence the cybersecurity preparedness of local election administration offices. My quantitative findings provide additional evidence that partnerships within local government may be important. Due to inadequate variation within the sample, the quantitative findings did not provide evidence related to the estimated influence of any of the other intergovernmental partnerships which were considered. Future research should explore additional nuance related to the coordination of local election offices with outside partners on cybersecurity. The most important partnerships probably vary based on the state and local jurisdiction. For example, local jurisdictions in one state may receive extensive direct cybersecurity assistance from the office of their state's CEO, while a

local jurisdiction in another state may rely on DHS/CISA to provide services not available from their state government.

I found no evidence linking the institutional structure of the local election authority to cybersecurity preparedness. Related to the technology use of the office, while I found no evidence linking the use of DRE machines to cybersecurity preparedness, I found strong evidence linking the use of e-pollbooks to cybersecurity preparedness. Across all relevant quantitative models, the use of e-pollbooks in a local jurisdiction was the strongest predictor of the cybersecurity preparedness of a local election administration office.

Summary of Key Conclusions and Grounded Theory

The key finding that stood out across both the quantitative and qualitative elements of this study is that the human resources of local election administration offices seem to influence their cybersecurity preparedness. In-house IT expertise seems to matter, and it seems to be lacking for many local election offices. Experts suggest that receiving cybersecurity guidance from the state government and the federal government may help fill this gap, but it remains difficult for local election offices to implement recommendations if they lack the necessary expertise. Therefore, local election offices are often reliant on outside partners to implement cybersecurity measures for them.

My findings suggest other factors also matter. The technology use of local election offices appears to be strongly related to cybersecurity preparedness. Specifically, the use of e-pollbooks in local election jurisdictions was strongly related to the reported cybersecurity preparedness of the sample of local election offices I studied. Why e-pollbook use seems to be

particularly influential needs further study. It is possible this variable is a proxy for something else such as IT sophistication, cybersecurity risk, or a combination of both.

Financial resources also seem to be at least moderately important to the cybersecurity preparedness of local election offices. However, my findings suggest it is not as simple as local election officials being able to buy a better cybersecurity posture through the purchase of products and services. The effects of money on the cybersecurity preparedness of local election offices appears to be more nuanced than that. Money seems to be influential, at least in part, because more money leads to more staff and more qualified staff.

My findings suggest that election administration expertise within a local election office may also influence its cybersecurity preparedness. Although the variable for the professional experience of local election officials, measured as whether they have a professional election administration certification, was not significant at the 95 percent confidence level in any multivariate models, my overall quantitative analysis suggests it may be an influential factor. Local election administrators having a professional certification has a bivariate relationship with cybersecurity compliance, and the relationship between this variable and other independent variables likely affected my ability to observe its impact in the multivariate models. This is factor should be considered in future research.

Another important finding is that there are many interdependencies in the intergovernmental network surrounding election cybersecurity. Local governments, state governments, the federal government, vendors, and non-profit organizations all appear to play an important though sometimes overlapping role. My findings suggest local election administration offices are heavily reliant on state government when it comes to cybersecurity. My analysis also

suggests that receiving IT support from outside entities within the local government structure is related to compliance with more cybersecurity best practices. The experts I interviewed argued that accepting assistance from government partners, and sometimes vendors and non-profit organizations, improves the cybersecurity preparedness of local election offices simply because local election officials do not have the capacity to handle cybersecurity on their own.

This study suggests there is more reliance on partners than coordination with partners from local election administrators when it comes to cybersecurity. Based on the conclusions of intergovernmental relations scholars, this lack of leadership and control of this issue on the part of local election administrators may negatively impact implementation. Further detail on how local election officials coordinate with partners and how their coordination style impacts the cybersecurity preparedness of local election administration offices is an important area for further study.

Finally, my findings suggest that the most basic of cybersecurity practices are among the most important for local election administration offices. Further, there is room for growth among local election offices related to implementing the basics. Though most of the local election administrators in the sample reported compliance with most of the basic cybersecurity practices about which they were asked, there was still some variation in reported compliance. Experts reported during interviews that just the basics will go a long way toward protecting local election offices and the systems they control from the most common threats but that many offices have not yet implemented all of the basics. This suggests that improving the cybersecurity preparedness of local election administration offices is not as unattainable a goal as it may seem. Though additional expertise is needed within local election offices, it may be that these offices need someone who understands the basics of cybersecurity, who is able to interpret cybersecurity

recommendations, and who can oversee the implementation of simple steps such as updating software, installing anti-virus software, and implementing two-factor authentication. It does not seem to be the case that all local election administration offices are in need of advanced cybersecurity engineers.

In summary, this study provides strong evidence that access to IT expertise is important for local election administrators when implementing ongoing cybersecurity programs. This is consistent with the findings of prior research related to local government IT and cybersecurity capacity (e.g., Kim and Bretschneider 2004; Norris et al. 2018). My findings suggest that having in-house IT staff may be particularly beneficial but that local election administrators can fill gaps by bringing in outside partners to help. This finding is consistent with Honadle's (2004) claim that the acceptance of assistance from higher levels of government is important to local government capacity. According to my findings, most local election offices receive cybersecurity support from their state election office. Working with additional partners such as DHS/CISA, the EI-ISAC, local government IT departments, vendors, non-profit organizations, and other state and federal government agencies to receive cybersecurity assessments, services, information, and other resources seems to help local election administrators improve the cybersecurity preparedness of their office.

I developed a grounded theory from the empirical observations and iterative analysis in this study. This grounded theory can be used as a starting point for future research. Following the recommendation of Glaser and Strauss (1967), this theory is not an attempt to provide a perfect description of the cybersecurity preparedness of local election administration offices. Rather, my aim is to account for most of the relevant factors and behavior.

My grounded theory is that there is a digital and cybersecurity divide impacting local election administration offices that is influenced by the resource availability of the offices. The most important resource for local election offices related to cybersecurity preparedness is having staff with IT expertise. My theory is that the presence of IT specialists within a local election administration office will influence the office's IT sophistication and cybersecurity preparedness because IT specialists know how to manage IT as well as interpret cyber threat information, assess cybersecurity risk, implement security controls, detect cyber threats and incidents, respond to incidents, and recover from incidents on an ongoing basis. They have IT and cybersecurity expertise that most local election administrators do not have. However, most local election entities lack in-house IT experts. Therefore, I further theorize that the cybersecurity preparedness of local election administration offices which lack in-house IT specialists is influenced by the degree to which the local election administrators access IT and cybersecurity expertise through outside partnerships. Outside specialists can help local election officials understand threat information, assess risk, implement controls, detect threats and incidents, respond to incidents, and recover from incidents. Support from outside partners is likely to be less consistent than in-house support, but outside partners can help fill gaps in capacity that exist within local election offices. Further, receiving assistance from outside partners is likely to influence cybersecurity preparedness even when in-house experts are present simply because the outside partners can add additional capacity and fill remaining gaps. While financial resources seem to be impactful in that budgets influence staffing, human resources tend to be more influential than financial resources on the cybersecurity preparedness of local election administration offices. Beyond just IT staff, having more election administration staff and having a local election official with more experience in the field may tend to have an influence on the cybersecurity preparedness of local

election administration offices. Having a larger staff may reduce the extent to which time constraints are a barrier to cybersecurity preparedness. More staff also means more individuals are available to coordinate with partners. The election administration experience of a local election office's staff is likely influential because more experienced local election administrators probably tend to have a better understanding than less experienced administrators of the election-specific IT systems which must be protected. The extent to which local election officials have developed relationships with intergovernmental partners is likely also influenced by their experience in the field.

Because few of the factors explored by this research are specific to election administration, this theory may apply broadly to local government entities. Its applicability to cybersecurity preparedness for other types of local government entities which tend face cyber threats, such as school districts and courts, in addition to local election offices should be considered by future research.

Implications for Policy Makers and Administrative Leaders

As this research is exploratory, it should not be used as the sole basis for policy decisions. Rather, the grounded theory presented in the previous section should be used to inform future research which could then inform policy decisions. There are some key takeaways, however, that decision makers may choose to consider alongside other evidence.

Many local election administrators are facing shortages of the resources they need to improve their cybersecurity risk posture. For example, of the fifty local election administration offices in my sample, twenty-two reported that they do not have any IT specialists on their staff. While local election officials need resources to improve their cybersecurity preparedness, money

alone does not seem to buy solutions. Local election offices need access to experts who can oversee and implement their cybersecurity programs on an ongoing basis.

Thought leaders should consider how to recruit more cybersecurity experts into the field and how to ensure local election administrators have direct and ongoing access to cybersecurity experts. Recruitment of IT and cybersecurity experts can be challenging for large organizations as the nation faces a cybersecurity workforce shortage. It is even more challenging for local government entities who cannot compete with the federal government or the private sector on compensation. Solutions may include programs which use creative methods, such as scholarship offers or an appeal to one's sense of service or patriotism, to recruit cybersecurity talent to work for local government on assignment. Such programs exist on a limited basis[28], and their effectiveness should be studied and considered. Other programs, such as state cyber navigator programs, through which state governments can provide direct and ongoing cybersecurity support to local governments, should also be considered. Another potential innovation, which was proposed by an interview respondent, is a model where IT experts are hired, funded, and shared across multiple local jurisdictions or local government entities. Overall, my findings suggest that while accepting services and guidance provided by the federal or state government can help local election officials improve the cybersecurity preparedness of their offices, building capacity and gaining expertise within the local election offices is also important and is likely to lead to further improvement.

Additionally, the entities serving as partners to local election administration offices related to cybersecurity should consider whether the complete reliance of the local offices on their support is ideal. One respondent, for example, expressed concern that election officials who

[28] An example is CyberCorps: Scholarship for Service: https://www.sfs.opm.gov/.

rely on consultants to manage their post-election audits may not know how to manage the audits on their own once the consultants have moved on to another jurisdiction. Another respondent expressed concern that many local election offices who rely on the same vendors for cybersecurity services will not receive the incident response services they need if a widespread incident effects several customers of the same company. Another interviewee suggested that some deficits in cybersecurity preparedness among local election offices may be due to local election offices relying heavily on the state election office, while the state office is more focused on protecting their own systems than providing support to local election officials.

In addition to providing support services, partners should consider how they can help local election administration offices build internal capacity and expertise so they can independently assess and manage their own cybersecurity risk, at least on a basic level. Because recruiting IT specialists to service the more than eight thousand local election jurisdictions in the United States is unlikely to ever occur with one hundred percent success, training current election administrators on how to implement the most basic and most efficient cybersecurity practices themselves may be an important step. Partners should consider expanding training opportunities and should consider how to craft training in a way that may help local election officials become more self-sufficient related to implementing basic cyber hygiene steps throughout their local election office and for its staff, systems, and processes.

Limitations

There are several limitations to this study which limit the strength of the evidence it provides. These limitations should be considered relevant to the findings. First, all of the findings rely on the analysis of subjective responses. An original survey and expert interviews were used

to collect data. A strength of these methods is that they allow for the collection of primary data. A weakness is that the data are subjective, and response bias is possible.

Next, the quantitative analysis was based on a small, non-random sample. Only fifty of the over eight thousand local election administration offices in the United States are represented in the sample. Further, I suspect that local election offices with above average cybersecurity maturity were more likely to participate than others. This means the sample is not representative.

An additional limitation is the potential of omitted variable bias. Because there was not lot of prior research or an established theory to test, I used contributions from several different areas of literature to construct an analytic framework. Therefore, it is difficult to gauge whether my models accounted for all relevant variables. The omission of substantively important variables biases results. As more research is conducted in this area, researchers will be able to create models based on more informed theory which will reduce the likelihood of omitted variable bias. My grounded theory provides a starting point.

Finally, this research design did not produce strong enough evidence to make assertions about causality. This is not a surprise as the study is exploratory, but it is a limitation. While all research has limitations, future research in this area should incorporate different research methods in order to not have the same limitations to this study and add to our understanding of the topic.

Directions for Future Research

Based on my research findings and limitations, I have identified several topics ripe for further investigation. First, future research should test the relationships between key variables identified by this study and the cybersecurity preparedness of local election administration

offices using a larger and different sample. If using survey research, allowing for anonymity is likely to result in a better response rate. Further tests are needed to confirm the influence of IT staff on the cybersecurity preparedness of local election administration offices. Additional studies should consider not just the quantity of IT staff but also the quality through considering factors like years of experience, cybersecurity-specific expertise, and whether IT employees have relevant degrees or certifications. Future studies should additionally consider the impacts of budget, intergovernmental partnerships, and the professional experience of local election officials and their staff on local election office cybersecurity preparedness.

The impacts of the demographic characteristics of the population of local jurisdictions on the cybersecurity preparedness of election offices should also be further studied. This research suggests local election offices which serve a more diverse population tend to be more compliant with cybersecurity recommendations. Additional investigation is needed to understand why this may be the case, as a causal mechanism is not obvious. Future quantitative studies should also consider whether additional variables need to be considered.

A second area for future research is to consider whether there is a broader cybersecurity divide for local government and whether the same factors which influence cybersecurity preparedness for local election offices apply to other local government entities. Cybersecurity is a relevant issue for all local government entities who all have become a target for cyber-attacks. As resource shortages and capacity challenges are not limited to election administration offices, it is likely that the impact of these challenges on cybersecurity implementation applies broadly across local government.

An additional direction for future research, which is needed to further understand this topic, is a series of qualitative case studies. This approach may help us further understand the causal mechanism between the concepts I identified as potentially important because it would allow researchers to trace processes. For example, this study provides evidence that intergovernmental relationships are important to the cybersecurity preparedness of local election offices. My findings suggest that one reason intergovernmental relationships may influence cybersecurity preparedness is because partners can help local election offices fill gaps in technical expertise. Qualitative case studies may allow us to understand more about how and why they are important by allowing us to observe how one thing leads to another. Case studies would also allow for further study of the nature of the relationships. For example, certain behaviors or power dynamics within intergovernmental relationships may have a different impact than others. A comparative case study approach would allow researchers to explore how local election offices with different internal characteristics and different partnerships may or may not have different levels of cybersecurity preparedness.

Another direction is further investigation of the evolving roles of other layers of government in election cybersecurity. This study has an intentional focus on local election administration offices because these are the entities primarily responsible for the administration of elections in the United States. My findings suggest, however, that the state election office plays a disproportionately large role in election cybersecurity compared to other aspects of election administration. Further, the federal government appears to be more involved in election cybersecurity than in other aspects of election administration. Hale et al. (2015) describe how the role of state governments in election administration evolved after the NVRA, and the role of the federal government increased post-HAVA. Research to consider how the events surrounding the

2016 election, the critical infrastructure designation, and an influx of federal grant money at the state-level may have led to potential changes in election administration roles is warranted.

Future studies should also consider the impact of policymakers and policy. This study predominantly considers administrative capacity and the actions of public administrators, but Derthick (1990) argues policy makers often impact administrative performance. As several state legislatures have enacted election cybersecurity laws since 2016 (NSCL 2019), exploring the potential impact of these laws on the cybersecurity preparedness of election administration offices is another important direction for investigation. Studies to consider the impacts of policymakers and policy should explore whether partisanship influences election cybersecurity. While none of the experts interviewed for this study mentioned partisanship in relation to the cybersecurity preparedness of local election offices, a partisan debate over election security has emerged in the US Congress. It is possible the partisanship surrounding this issue on the national stage will have state and local impacts.

Another relevant approach is further studying this topic through the lens of public sector emergency management. The emergency management literature broadly argues that coordination problems and blurred boundaries lead to deficient preparedness for and response to emergencies (e.g. Schneider 2008). My findings suggest that who is in charge of securing election systems is not always clear. Future research should explore whether and how this impacts cybersecurity preparedness and particularly how it has impacted the response to cyber incidents.

The emergency management literature also suggests that one type of emergency can distract from others, leading to degraded government attention (Birkland and Waterman 2008). The 2020 election cycle was largely seen as a testing ground for how far election cybersecurity

efforts have come since 2016. However, election administrators and the federal government are facing another crisis in the midst of the 2020 elections – a global pandemic. Post-2020 research should consider how being forced to respond to COVID-19 impacted the government's attention to ongoing election cybersecurity efforts. This research should consider impacts related to all of the important players within the intergovernmental network and how shifting focuses at one level may have an impact on intergovernmental partners. For example, if the federal government is broadly are distracted by COVID-19 response, will the availability of cybersecurity services to local election administration offices decrease? If so, how will that decrease impact cybersecurity preparedness at the local level?

Finally, another important area for future research is program evaluation. There are currently programs being implemented at the local, state, and federal level aimed at addressing the cybersecurity deficiencies of local election administration offices. For example, several states have implemented cyber navigator programs through which cybersecurity experts are hired by state government to assist local governments. Because these programs attempt to fill some of the gaps identified by this research, their impact on the cybersecurity preparedness of local election administration offices should be studied.

Contributions

This study makes several contributions to the literature. First, it provides preliminary evidence that a cybersecurity divide among US local government entities exists. It also appears that cybersecurity and the use of digital IT are related for local election offices. This suggests that a local government cybersecurity divide may be related to a local government digital divide. This builds onto research which claims there is an organizational digital divide (e.g. Iacovou et

al. 1995, McNutt 2008; Riggins and Dewan 2008) by providing preliminary evidence that both a digital divide and cybersecurity divide exist for local government entities. While there has been extensive research on the digital divide and substantial research on local government capacity, this study attempts to build a bridge between the two. More specifically, my findings suggest that human resources and particularly the extent to which local government entities employ IT experts may be among the most important influences on the cybersecurity divide. This evidence supports some of the findings of studies focused on the IT and cybersecurity capacity of local government (e.g., Kim and Bretschneider 2004; Norris et al. 2018). Overall, my study and grounded theory lay a foundation for future research of the local government cybersecurity divide and its causes.

Additionally, this study contributes to our understanding of the intergovernmental network which exists around the issue of US election cybersecurity. Hale et al. (2015) provided a detailed description of the intergovernmental network around election administration which has local government at the center. My research suggests the network may look and operate differently when it comes to election security. Specifically, my findings suggest state and federal government agencies play an outsized role in election cybersecurity compared to other aspects of election administration. One explanation may be that while local election administrators are the experts on election administration, they lack the levels of cybersecurity expertise that exist within other levels of government and supporting third-party organizations. My analysis of the intergovernmental relationships of local election administrators related to cybersecurity provides support to the conclusions of local government capacity and intergovernmental relations studies, which suggest that accepting assistance and information from outside entities can help local public administrators improve implementation (e.g., Hale 2011; Honadle 2001). My findings

raise questions over how the apparent lack of control of many local election administration offices over their own cybersecurity efforts may impact the results of these efforts.

Finally, this study offers a measure of the cybersecurity preparedness of local election administration offices which could be applied to other studies. My measure is based on a systematic qualitative analysis of the cybersecurity practices recommended for election administration offices by several well-respected organizations and federal agencies within the election security space. While additional entities have released best practice guides on election cybersecurity since the time this measurement was constructed, other scholars could simply review those recommendations to gauge their consistency with the thirteen concepts I identified and included in my measure. Alternatively, they could use my method of constructing the variable to conduct a systematic review of updated guidance.

In summary, this study accomplished the goals of exploratory research. I pieced together empirical insight from multiple areas of public administration research to build an analytic framework for a research question related to which prior research is extremely limited. I used research contributions from a range of literature to generate two series of specific hypotheses to conduct preliminary analysis of relationships between the cybersecurity preparedness of local election offices and the potential influences I identified based on the literature. I also generated a broad research expectation to explore the cybersecurity preparedness of local election administration offices and the role of their intergovernmental partners related to election cybersecurity through qualitative analysis. I collected primary and secondary data through an original survey and interviews of experts. I conducted quantitative and qualitative data analysis and made broad conclusions addressing factors which seem to influence cybersecurity preparedness for local election administration offices and describing the intergovernmental

partners on which local election officials rely for cybersecurity support. The conclusions of this study were used to produce grounded theory which can inform the progression of this timely and important line of inquiry.

References

Agranoff, Robert and Michael McGuire. 2003. *Collaborative Public Management: New Strategies for Local Governments.* Washington: Georgetown University Press.

Anderson, Monica. 2017. Digital Divide Persists Even as Lower-income Americans Make Gains in Tech Adoption. *Pew Research Center.*

Anderson, Monica and Andrew Perrin. 2017. Disabled Americans are less likely to use technology. *Pew Research Center.*

Belfer Center for Science and International Affairs, Harvard Kennedy School. 2018. The State and Local Election Cybersecurity Playbook.

Birkland, Tom A. 2009. Disasters, Catastrophes, and Policy Failure in the Homeland Security Era. *Review of Policy Research* 26(4), 423–438.

Birkland, Tom and Sarah Waterman. 2008. Is Federalism the Reason for Policy Failure in Hurricane Katrina? *Publius* 38(4), 692–714.

Bratton, Michael, Robert Mattes, and E. Gyimah-Boadi. 2005. *Public Opinion, Democracy, and Market Reform in Africa.* Cambridge: Cambridge University Press.

Brown, Mitchell and Kathleen Hale. *Applied Research Methods in Public and Nonprofit Organizations.* San Francisco: John Wiley & Sons.

Brown, Mitchell, Lindsey Forson, Kathleen Hale, Ryan Williamson, and Bob Smith. 2020. Capacity to Address Natural and Man-made Vulnerabilities: The Administrative Structure of U.S. Election System Security. *Election Law Journal* 19, no. 2.

Center for Internet Security (CIS). 2018. CIS Controls. Version 7.

Center for Internet Security (CIS). 2018. A Handbook for Election Infrastructure Security.

Center for Internet Security (CIS) website. 2020. Available from https://www.cisecurity.org/ei-isac/.

Claassen, Ryan L., David B. Magleby, J. Quin Monson, and Kelly D. Patterson. 2013. Voter Confidence and the Election-Day Voting Experience. *Political Behavior* 35, no. 2.

Comfort, Louise K., Arjen Boin, and Chris C. Demchak. 2010. *Designing Resilience: Preparing for Extreme Events.* Pittsburgh: University of Pittsburgh Press.

Comfort, Louise K., William L. Waugh, and Beverly A. Ciglar. 2012. Emergency Management Research and Practice in Public Administration: Emergence, Evolution, Expansion, and Future Directions. *Public Administration Review* 72, no. 4.

Cybersecurity and Infrastructure Security Agency (CISA). 2019. Security Tip (ST04-001): What is Cybersecurity?. Available from: https://us-cert.cisa.gov/ncas/tips/ST04-001.

Cybersecurity and Infrastructure Security Agency (CISA), Multi-State Sharing and Analysis Center (MS-ISAC), National Governors Association (NGA), and National Association of State Chief Information Officers (NASCIO). 2019. CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks: Take the First Three Steps to Resilience Against Ransomware for State and Local Partners.

Derthick, Martha. 1990. *Agency Under Stress: The Social Security Administration in American Government.* Washington: The Brookings Institute.

Election Center. 2016. Elections Security Checklist.

Election Infrastructure Subsector Coordinating Council (EISCC). 2017. EISCC Charter. Volume 1.0

Election Infrastructure Subsector Government Coordinating Council (EIS GCC). 2020. Statement from EIS GCC on Ongoing Efforts to Protect 2020 Elections.

Election Infrastructure Subsector Government Coordinating Council (EIS GCC). 2017. EIS GCC Charter.

Essex, Aleksander. 2017. Detecting the Detectable: Unintended Consequences of Cryptographic Election Verification. *IEEE Computer and Reliability Societies* (May/June).

Gallagher, Sean. 2019. DHS, FBI say election systems in all 50 states were targeted in 2016. *Ars Technica.*

Gargan, John J. 1981. Consideration of Local Government Capacity. *Public Administration Review* 41, no. 6.

Glaser, Barney G. and Anslem L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Chicago: Aldine Publishing Company.

Hale, Kathleen. 2011. *How Information Matters: Networks and Public Policy Innovation.* Washington: Georgetown University Press.

Hale, Kathleen and Christa Slaton. 2008. Building Capacity in Election Administration: Responses to Complexity and Interdependence. Public Administration Review 68 (839–849).

Hale, Kathleen and Mitchell Brown. 2013. Adopting, Adapting, and Opting Out: State Response to Federal Voting System Guidelines. *Publius* 43 no. 3, 428–451.

Hale, Kathleen and Mitchell Brown. 2020. *How We Vote: Innovations in American Elections.* Washington: Georgetown University Press.

Hale, Kathleen, Robert Montjoy, and Mitchell Brown. 2015. *Administering Elections: How American Elections Work.* London: Palgrave-MacMillan.

Honadle, Beth Walter. 2001. Theoretical and Practical Issues of Local Government Capacity in an Era of Devolution. *The Journal of Regional Analysis and Policy* 31, no 1.

Iacovou, Charalambos L., Izak Benbasat, and Albert S. Dexter. 1995. Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *MIS Quarterly*, no. 194: 465-485.

Kellstedt, Paul M. and Guy D. Whitten. 2013. *The Fundamentals of Political Science Research.* New York: Cambridge University Press.

Kettl, Donald F. 2000. The Transformation of Governance: Globalization, Devolution, and the Role of Government. *Public Administration Review* 60, no. 6.

Kettl, Donald F. 2006. Managing Boundaries in American Administration: The Collaboration Imperative. *Public Administration Review* (December).

Kim, Hyun Joon and Stuart Bretschneider. 2004. Local Government Information Technology Capacity: An Exploratory Theory. *Proceedings of the 37th Hawaii International Conference on System Sciences.*

Kohut, Andrew. 2017. Public Concern About the Vote Count and Uncertainty About Electronic Voting Machines. *Pew Research Center.*

Lewis-Beck, Michael. 1980. *Applied Regression: An Introduction.* Newbury Park: Sage Publications.

McNutt, John. 2008. Advocacy Organizations and the Organizational Digital Divide. Currents: Scholarship in the Human Services 7, no. 2.

Milward, H. Brinton and Keith Provan. 2000. Governing the Hollow State. *Journal of Public Administration Research and Theory* 10, no. 1: 359–380.

Moher, Ester, Jeremy Clark, and Aleksander Essex. 2014. Diffusion of Voter Responsibility: Potential Failings of E2E Voter Receipt Checking. USENIX Journal of Election Technology and Systems (JETS) 3, no. 1.

Morley, Michael and Franita Tolsen. 2018. Interpretation: Elections Clause. The Constitution Center: https://constitutioncenter.org/interactive-constitution/interpretations/elections-clause-morley-tolson.

Mossberger, Karen, Caroline J. Tolbert, and William W. Franko. 2012. *Digital Cities: The Internet and the Geography of Opportunity.* Oxford: Oxford University Press.

Mueller, Robert S. 2019. Report on the Investigation into the Russian Interference in the 2016 Presidential Election. Volume 1.

National Association of Secretaries of State (NASS). 2017. NASS Statement on Critical Infrastructure Designation for Elections.

National Association of Secretaries of State (NASS). 2019. Issue Briefing: Securing Elections Against Cyber Threats.

National Association of Secretaries of State (NASS). 2020. NASS Resolution on Principles for Federal Assistance in Funding of Elections.

National Conference of State Legislatures (NCSL). 2020. State Elections Legislation Database. Available from https://www.ncsl.org/research/elections-and-campaigns/elections-legislation-database.aspx.

National Institute of Standards and Technology (NIST). 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.

Norris, Donald F., Laura Mateczun, Anupam Joshi, and Tim Finin. 2018. Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security. *Journal of Homeland Security and Emergency Management* 15, no. 3.

Perrin, Andrew. 2017. Smartphones help blacks, Hispanics bridge some – but not all – digital gaps with whites. *Pew Research Center.*

Perrin, Andrew. 2017. Digital gap between rural and nonrural America persists. *Pew Research Center*.

Riggins, Frederick J. and Dewan, Sanjeev. 2008. The Digital Divide: Current and Future Research Directions. *Journal of the Association for Information Systems* 6: no. 12, Article 4.

Rogers, Everett M. 1995. *Diffusion of Innovations*, New York, NY: Free Press.

Ruxton, Megan M. and Kyle L. Saunders. 2016. Declining Trust and Efficacy and Its Role in Political Participation in *Why Don't Americans Vote?: Causes and Consequences,* ed. King, Bridgett A., and Kathleen Hale, 1 - 10. Santa Barbara: AB-CLIO.

Schneider, Saundra. 2008. Who's to Blame? (Mis) perceptions of the Intergovernmental Response to Disasters. *Publius* 38, no. 4.

Select Committee on Intelligence of the United States Senate ("Senate Intelligence Committee"). 2019-2020. Report on Russian Active Measures Campaigns and Interference in the 2016 US Election. Volumes 1 – 4.

United States Department of Homeland Security (DHS). 2017. Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.

United States Department of Homeland Security (DHS). 2018. Secretary Nielsen Statement on President Trump's Election Security Executive Order.

United States Department of Homeland Security (DHS). 2019. Testimony, Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security for a Hearing on Securing U.S. Election Infrastructure and Protecting Political Discourse before the US House of Representatives Committee on Oversight and Reform.

United States Department of Homeland Security (DHS) website. 2020. Available from https://www.cisa.gov/election-security.

United States Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI). 2016. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security.

United States Election Assistance Commission (EAC) website. 2017. Starting Point: U.S. Election Systems as Critical Infrastructure.

United States Election Assistance Commission (EAC) website. 2018. Available from https://www.eac.gov/.

Wright, Deil (1974). "Intergovernmental Relations: an Analytical Overview." *The Annals of the American Academy of Political and Social Science* 416, no. 1: 1-16.

Table 1. Independent Variable Data Sources

Variable	Measure	Source - Secondary	Source - Survey
Budget	Reported election administration budget for previous fiscal year		✔
Rural	US Census Bureau – ordinal measure (urban, somewhat urban, not urban)	✔	
Education of LEO	Reported highest degree of LEO		✔
Professional Experience	LEO professional certificate, reported		✔
IT Staff	Reported number of IT specialists		✔
Total Staff	Reported total election administration staff		✔
Income - jurisdiction level	US Census Bureau - Median income	✔	
Education - jurisdiction level	US Census Bureau - Percent high school graduate or higher	✔	
	US Census Bureau - Percent bachelor's degree or higher	✔	
Population - jurisdiction level	US Census Bureau - Number of persons	✔	
Language - jurisdiction level	US Census Bureau - Percent speak a language other than English	✔	
Age – jurisdiction level	US Census Bureau - Median age	✔	
	US Census Bureau – Percent 65 or older	✔	
Race - jurisdiction level	US Census Bureau - Percent Non-white	✔	
	US Census Bureau - Percent Black	✔	
Ethnicity - jurisdiction level	US Census Bureau - Percent Hispanic	✔	
LEO Structure	Single individual, board, or divided duties (Hale et al. 2015)	✔	
DRE	Yes or no		✔
Electronic Pollbook	Yes or no		✔
Registered Voters	Number of registered voters according to state CEO website	✔	

Table 2. Construction of Dependent Variable

	Belfer Center[29]	CIS[30]	EAC[31]	Election Center[32]	NIST[33]
Access Control	Limit the number of people with access to the system. Restrict what each user is authorized to do. Quickly remove those who no longer need access.	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Only authorized personnel should have access to the voter registration database."	Are only authorized personnel granted access to software? Do you have a network access control system that controls user access permission levels?	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Anti-Virus	Ensure that your systems have the most updated antivirus software.	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Run and update anti-virus software to protect election night reporting systems.	Do you have anti-virus software installed to detect 'Advanced Persistent Threats?'	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

[29] All items in this column are paraphrased or directly quoted from the Belfer Center.

[30] All items in this column are paraphrased or directly quoted from the CIS.

[31] All items in this column are paraphrased or directly quoted from the EAC.

[32] All items in this column are paraphrased or directly quoted from the Election Center.

[33] All items in this column are paraphrased or directly quoted from the NIST.

Cyber-hygiene Training	Issue guidance about the necessity of applying cybersecurity standards, stressing the importance of cybersecurity for staff by personally introducing orientations and trainings, and following up with operations personnel on a regular basis about the implementation of improved cybersecurity protections.	For all functional roles in the organization, identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	Conduct training and exercises related to managing IT and election systems.	---	Personnel and partners are provided cybersecurity awareness education and are trained to perform cybersecurity duties consistent with related policies, procedures, and agreements.
Data Back-ups	Backups should be regularly performed, either through automation or as part of a scheduled manual process; backups should be read-only once created to prevent data corruption; and backups should be regularly tested by performing a complete restore from backed-up data.	Ensure that all system data is automatically backed up on a regular basis.	The [voter registration] database should be backed up routinely. If any unexpected modifications to the data were to occur, the database could be restored to the last known state… The ability to perform backups and restores should be tested and validated.	Is there a backup for the loss of data from election equipment damage?	Backups of information are conducted, maintained, and tested.
Encryption	Implement an encryption plan for data 'at-rest' and 'in-transit.'	Protection of data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention	Related to voter registration systems, encryption should be used throughout, including but not limited to encrypting the database, server,	Do you employ encryption standards for all data – specifically personally identifiable information?	Information and records (data) are managed consistent with organization's risk strategy to protect the confidentiality, integrity, and

		techniques.	backups, any files used for distribution, all data transmission and communication.		availability of information. Data at-rest and data in-transit are protected.
Firewalls	Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the Internet.	Implement firewalls to protect networks and applications.	Use firewalls to protect election night reporting systems and the voter registration system.	Is the software platform protected by a firewall?	Network activity is protected.
Intrusion Detection	Automated forms of data monitoring are critical for detecting anomalies and highlighting when manipulation or intrusion occurs.	Deploy network-based Intrusion Detection Systems sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	For both voter registration systems and election night reporting systems, use an intrusion detection system and monitor the incoming and outgoing traffic for signs of irregularities.	Does the software log multiple log-in attempts, increased data traffic, and/or volume of data transmitted?	Anomalous activity is detected and the potential impact of events is understood.
Inventory	Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs. Map how other	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	---	Have you defined your inventory of critical election systems? Do you have a complete map of your network and all its interconnections both within your organization and with outside entities?	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with relative importance to organizational objectives and the

	systems connect to the VRDB.				organization's risk strategy.
Two-factor Authentication	Require two-factor authentication to log into the voter registration database, email accounts, social media accounts, the vote tally system device, the ENR system, and any other official accounts or systems.	Require multi-factor authentication for access to all user accounts, networks, and devices.	Enable two-factor authentication for the uploading of results and remote administration of the ENR.	---	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
Passwords	Require strong passwords not only for official systems and accounts but also for key officials' private email and social media accounts. For your passwords, create SomethingReallyLongLikeThisString, not something really short like Th1$.	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system." Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	Encourage the use of strong passwords and proper password management.	Is your network password-protected? Do you provide administrative passwords only to employees with a clearly defined 'need to know/edit' status? Do you change critical system passwords regularly?"	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
Risk & Vulnerability Testing	RVAs can include penetration testing, vulnerability scanning and testing, database and operating systems scans,	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with	Use software to identify security vulnerabilities on systems deployed in a network. Regular vulnerability scans of the ENR and other systems on the same	Do you regularly conduct vulnerability and intrusion testing on your network?	Vulnerability scans are performed.

	Web application scanning and testing, and several other services.	elevated rights on the system being tested.	network can often find points of weakness.		
Security Patches	Follow all applicable guidance for patching and software updates.	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	Outdated software is the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available.	Do you ensure that servers, PCs, and laptops are encrypted or updated with the most current security patches?	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Vendor Management	Require vendors to make security a priority.	Election offices should require documentation of cybersecurity processes from vendors and should assess contracted supply chains.	Have a vendor management strategy.	Do your vendors and partners have a strong commitment to network security?	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners

Table 3. Compliance with Cybersecurity Concepts – Modal Responses

Cybersecurity Concepts	n	Modal Response
Access Control	50	Yes (39)
Anti-Virus	50	Yes (45)
Cyber-Hygiene Training	50	Yes (36)
Data Back-ups	50	Yes (30)
Encryption	50	Yes (22)
Firewall	50	Yes (49)
Intrusion Detection	50	Yes (27)
Inventory	50	Yes (41)
Two-factor Authentication	50	Yes (27)
Passwords	50	Yes (35)
Risk & Vulnerability Assessments	50	Yes (36)
Security Patching	50	Yes (35)
Vendor Management	50	No (31)

Table 4. Univariate Statistics Describing Local Election Offices – Mean and Standard Deviation

Variable	n	Mean	Standard Deviation
Cybersecurity Compliance	50	69.2	19.68
Reported Budget	50	1,472,996	4,596,501
Number of IT Staff	50	1.28	1.96
Total Staff	50	8.14	15.84

Table 5. Univariate Statistics Describing Local Election Offices – Median and Quantiles

	----------Quantiles----------				
Variable	Min.	25%	Median	75%	Max.
Cybersecurity Compliance	23.08	61.54	69.62	84.62	100
Reported Budget	700	35,000	183,636.5	742,000	30,000,000
Rural	0	0	1	2	2
LEO Education	1	2	3	3	5
Number of IT Staff	0	0	1	2	10
Total Staff	1	2	4	6	100

Table 6. Univariate Statistics Describing Local Election Jurisdictions – Mean and Standard Deviation

Variable	n	Mean	Standard Deviation
Median Income	50	57,569.5	15,893.75
Percent High School plus	50	88.67	4.72
Percent Bachelor plus	50	27.71	11.42
Population	50	279,996.7	794,635.6
Percent Other Language	50	13.49	11.07
Median Age	50	40.56	5.62
Percent 65older	50	17.5	4.68
Percent Nonwhite	50	17.82	12.03
Percent Black	50	6.31	7.82
Percent Hispanic	50	13.23	12.64
Registered Voters	50	142,650.1	301,892.2

Table 7. Univariate Statistics Describing Local Election Jurisdictions – Median and Quantiles

		----------Quantiles----------				
Variable	n	Min.	25%	Median	75%	Max.
Rural	50	0	0	1	2	2
Median Income	50	30,298	44,865	56,728.5	63,926	108,828
Percent High School plus	50	77.5	85.7	89.2	91.8	97.4
Percent Bachelor plus	50	12.3	17.8	23.95	35.5	61.3
Population	50	732	13,120	47,572	194,174	5,238,541
Percent Other Language	50	.2	5.5	9.05	18.7	37.7
Median Age	50	24.5	37.3	40.2	44.4	55.3
Percent 65older	50	7.2	14.6	17.3	19.3	32.2
Percent Nonwhite	50	1.9	8	15.7	27	47.3
Percent Black	50	0	.8	2.55	9	31.6
Percent Hispanic	50	.4	4	8.65	20.5	55.6
Registered Voters	50	658	6,666	31,099.5	130,359	1,570,127

Table 8. Modal Categories of Categorical Variables

Variable	n	Modal Category
Certification	50	No (32)
Local Structure	50	Single LEO (22)
DRE	50	No (35)
E Pollbook	50	Yes (27)
EI-ISAC	50	Yes (38)
DHS	50	Yes (40)
State Training	50	Yes (46)
Local Support	50	Yes (36)

Table 9. Correlation with Cybersecurity Preparedness

	Cybersecurity Compliance
Rural	-0.1936
Reported Budget	0.2888*
LEO Education	0.0280
Number of IT Staff	0.4206*
Total Staff	0.3576*
Median Income	-0.0065
Percent High School plus	-0.2861*
Percent Bachelor plus	-0.0788
Registered Voters	0.3163*
Percent Other Language	0.3303*
Median Age	-0.1016
Percent 65older	0.0240
Percent Nonwhite	0.3439*
Percent Black	0.3393*
Percent Hispanic	0.2801*

* $p<.05$

Table 10. Difference of Mean Cybersecurity Preparedness Scores

	Mean – no	Mean – yes	Difference	T-Statistic
Certificate	63.4513	78.5272	15.0759	-2.7519*
DRE	69.1669	68.2060	.9609	.1557
E Pollbook	59.1830	77.1378	17.9547	-3.5546*
EI-ISAC	65.3558	69.9910	4.6352	-0.7032
DHS	61.5390	70.7135	9.1745	-1.3203
State Training	57.6925	69.8513	12.1588	-1.1827
Local Support	59.8900	72.3742	12.4842	-2.0674*

* $p<.05$

Table 11. Estimated Influence of Office Characteristics on Cybersecurity Preparedness

	Model A	Model B	Model C	Model D	Model E	Model F
IT Staff	4.2512* (1.3236)					
Reported Budget		.000001* (.0000005)				
Certificate			15.0760* (5.4784)			
LEO Education				.5178 (2.6726)		
Staff Total					.4471* (.1685)	
Rural						-4.7672 (3.4874)
Constant	63.437* (3.0757)	67.046* (2.8474)	63.451* (3.2871)	67.532* (7.5023)	65.239* (2.9774)	73.264* (4.2426)
R^2	.1769	.0834	.1363	.0008	.1279	.0375

Bivariate OLS Regression Models
Standard errors in parentheses, *p<.05

Table 12. Estimated Influence of Jurisdiction Characteristics on Cybersecurity Preparedness

	Model G	Model H	Model I	Model J	Model K	Model L	Model M	Model N
Median Income	-.000008 (.0002)							
High-School		-1.200 * (.5803)						
Registered Voters			.00002* (.000009)					
Other Language				.5908* (.2437)				
Rural					-4.7672 (3.4874)			
Senior Population						.1016 (.6110)		
Not White							.5663* (.2232)	
Hispanic								.4389* (.2171)
Constant	69.34* (10.73)	175.31* (51.53)	65.92* (2.974)	60.91* (4.23)	73.26* (4.24)	67.10* (11.06)	58.79* (4.78)	63.07* (3.95)
R^2	.0000	.0818	.1000	.1091	.0375	.0006	.1183	.0785

Bivariate OLS Regression Models
Standard error in parentheses, *p<.05

Table 13. Estimated Influence of Technology Use and Partnerships on Cybersecurity Preparedness

	Model O	Model P	Model Q	Model R	Model S	Model T	Model U
DRE	-.9609 (6.1729)						
Electronic Pollbooks		17.9547* (5.0512)					
Local Structure Board			6.6304 (6.9834)				
Local Structure Combo			5.899 (6.6846)				
EI-ISAC				4.6352 (6.5913)			
DHS					9.1745 (6.9487)		
State Training						12.1588 (10.2809)	
Local Support							12.4842* (6.0387)
Constant	69.167* (3.3810)	59.183* (3.7118)	65.385* (4.2562)	65.356* (5.7461)	61.539* (6.2151)	57.693* (10.2809)	59.89* (5.89)
R^2	.0005	.2084	.0251	.4853	.0350	.0283	.0441

Bivariate OLS Regression Models
Standard errors in parentheses, *p<.05

Table 14. Estimated Influences on Local Election Office Cybersecurity Preparedness

	Model V	Model W	Model X	Model Y	Model Z
Budget	-.000001 (.000001)	-.000001 (.000001)	-----	-----	-----
Rural	-3.5460 (3.69818)	-.1.6140 (4.0581)	-2.1037 (6.5621)	-1.7155 (4.1809)	-----
LEO Education	-5.5052 (2.8730)	-6.0588 (3.0490)	-5.7158 (2.9192)	-5.8172 (3.1047)	-----
Certification	9.8249 (5.9795)	2.8559 (6.9080)	4.4473 (6.5621)	9.0347 (6.6891)	3.6589 (5.8129)
IT Staff	5.2865* (2.5908)	1.9630 (3.200)	2.5546 (1.6412)	4.0986* (1.6116)	1.4096 (1.5056)
Staff Total	.1976 (.4636)	.5164 (.5173)	-----	------	-----
Electronic Pollbooks		17.2414* (7.3664)	16.9206* (6.9129)	-----	12.9691* (5.6581)
DRE		-2.4971 (6.1331)	-3.8990 (5.8214)	-.5869 (6.0253)	-----
Racial Diversity		.4468 (.3076)	.3516 (.2858)	.2264 (.2991)	.2990 (.2312)
Local Structure Board		-4.1651 (8.4364)	-.6701 (7.5893)	5.0495 (7.6802)	-----
Local Structure Combo		-4.6735 (7.6813)	-1.5476 (6.7920)	2.4971 (7.0072)	-----
EI-ISAC		-8.0388 (7.7987)	-8.2641 (7.5154)	-.7995 (7.3060)	-----
DHS		4.6446 (8.6379)	1.9246 (6.9362)	2.8417 (7.3669)	-----
State Training		-6.5806 (7.7987)	-----	-----	-----
Local Support		9.3784 (8.6380)	6.0151 (5.8812)	4.9673 (6.23900	8.5695 (5.4321)
Constant	76.2596* (9.4257)	68.43* (14.952)	67.62* (12.465)	65.9213* (13.2374)	47.2567* (5.7951)
Adj. R^2	.2100	.2402	.2723	.1767	.2882

Multivariate OLS Regression Models, Standard errors in parentheses, *p<.05

Table 15. Definitions of Qualitative Themes

Theme	Definition
Critical Infrastructure	Respondents refers to elections as critical infrastructure of the United States or to the nation-state threat that requires a whole-of-government response.
Cyber Hygiene	Respondent refers to basic cyber hygiene best practices that are or should be conducted by LEOs. Two-factor authentication was the one most frequently mentioned.
DHS/CISA	Respondent refers to the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security (DHS) or to DHS broadly as a partner for LEOs related to cybersecurity.
Federal Partners	Respondent refers to a federal agency other than DHS as a partner for LEOs related to cybersecurity. The EAC was the one most frequently mentioned. This also includes broad mentions of federal partners.
Incident Response Plans	Respondent refers to the creation or exercise of an incident response plan by LEOs.
Information Sharing	Respondent refers to LEOs sharing (and receiving) information within the intergovernmental network through the EI-ISAC, the MS-ISAC, the EIS-GCC, or generally.
LEO Responsible	Respondent suggests LEOs have primary responsibility for US election cybersecurity.
Local IT	Respondent refers to LEOs work with the IT department within their county or municipal government or the need for such coordination.
Need for Additional Funding	Respondent refers to LEO's funding shortfalls or need for additional funds for cybersecurity.
Need for Improvement	Respondent refers to the need for improvement among LEOs in cybersecurity practices. Note: most references to a need for improvement suggest LEOs are trying but resource shortages are a barrier. Some references suggest LEOs need to realize this is a real threat and take ownership of the issue.

Need for IT Staff/Expertise	Respondent refers to the lack of IT staff or expertise within a local election office or the need for in-house IT staff.
Non-Governmental Partners	Respondent refers to LEOs receiving cybersecurity-related assistance from non-governmental partners including professional associations, other non-profits, and for-profit companies or the importance of receiving such assistance. Note: from for-profit companies, free services/resources are included here. Paid services are included in the "vendors" theme.
Owner/Operator Responsible	Respondent refers to the owner and/or operator of a specific IT system as having primary responsibility to protect it. This can include LEOs, state CEOs, local IT, or vendors.
Procedural Controls	Respondent refers to non-technical controls that can help protect elections from threats to their integrity (including cyber threats and routine operational issues) such as maintaining chain of custody and logic & accuracy tests. Note: All references suggest LEOs do these things regularly and/or that they are well-versed in these controls.
Shared Responsibility	Respondent refers to US election cybersecurity as a shared responsibility. References include some mixture of LEOs, state CEOs, the federal government, and vendors.
State CEO	Respondent refers to LEOs work with the office of their state chief election official on cybersecurity or the need for such coordination. This includes support from a state cyber navigator program.
State Partners	Respondent refers to a state government entity other than the office of the state CEO as a partner for LEOs related to cybersecurity. The State CIO and the National Guard were most frequently mentioned. This also includes broad mentions of state partners.
Time Constraints	Respondent refers to time constraints as a challenge for LEOs that may hinder cybersecurity preparedness.
Training	Respondent refers to participation in cybersecurity-related training for LEOs and their staff or the need for training.
Use of Federal Grants	Respondent refers to use of existing federal grant funds for election security.

Variation	Respondent refers to the variation in local election office both in terms of cybersecurity practices and seemingly related characteristics. The most common mention was variation in jurisdiction size as a factor affecting cybersecurity preparedness.
Vendors	Respondent refers to LEOs work with their vendors on IT or cybersecurity or the need for such coordination. In some cases, this includes mentions of LEOs being too reliant on vendors. This includes mentions of technology providers, IT providers, and cybersecurity providers.

Table 16. Qualitative Themes in Order of Prevalence

All Respondents	Non-Profit Respondents	Federal Respondents	State Respondents
State CEO	State CEO	State CEO	Information Sharing
Need for IT Staff/Expertise	Need for IT Staff/Expertise	Need for IT Staff/Expertise	State CEO
DHS/CISA	DHS/CISA	Information Sharing	DHS/CISA
Information Sharing	Cyber Hygiene	Need for Additional Funding	Cyber Hygiene
Cyber Hygiene	NGO Partners	DHS/CISA	Training
NGO Partners	Training	Owner/Operator Responsible	Need for IT Staff/Expertise
Need for Additional Funding	Shared Responsibility	Vendors	NGO Partners
Training	Federal Partners	Local IT	Need for Additional Funding
Shared Responsibility	Procedural Controls	Cyber Hygiene	Owner/Operator Responsible
Owner/Operator Responsible	Need for Additional Funding	NGO Partners	Shared Responsibility
Federal Partners	Owner/Operator Responsible	Shared Responsibility	Variation
Vendors	State Partners	Federal Partners	Need for Improvement
State Partners	Time Constraints	Variation	State Partners
Local IT	Information Sharing	Need for Improvement	Procedural Controls
Procedural Controls	Vendors	LEO Responsibility	Federal Partners
Variation	Local IT	Use of Federal Grants	Vendors
Need for Improvement	Variation	Training	Local IT
LEO Responsible	Need for Improvement	State Partners	LEO Responsible
Time Constraints	LEO Responsible	Time Constraints	Time Constraints
Use of Federal Grants	Incident Response Plans	Incident Response Plans	Use of Federal Grants
Incident Response Plans	Critical Infrastructure	Critical Infrastructure	Incident Response Plans
Critical Infrastructure	Use of Federal Grants	Procedural Controls	Critical Infrastructure

Table 17. Qualitative Findings – Responsibilities and Partnerships

	NGO	LEO Primary	Critical Infrastructure	Owner/ Operator	Shared Responsibility	Federal Grant Use	DHS/ CISA	Local IT	Federal Partners	State Partners	State CEO	Vendors
All	●	◉	○	◉	◉	○	●	◉	◉	◉	●	◉
Non-Profit	●	◉	◉	◉	●	○	●	◉	●	◉	●	◉
Federal	◉	◉	◉	●	◉	◉	●	●	◉	◉	●	●
State	◉	○	○	◉	◉	○	●	○	○	◉	●	○

KEY:
- ● = At least two-thirds of respondents discussed theme
- ◉ = Greater than one-third but fewer than two-thirds of respondents discussed theme
- ○ = Up to or exactly one-third of respondents discussed theme

Table 18. Qualitative Findings – Resources and Practices of Local Offices

	Cyber Hygiene	Incident Response	Information Sharing	Funding Needs	Need to Improve	IT Needs	Procedural Controls	Time Constraints	Training	Variation
All	●	○	●	●	◉	●	◉	◉	●	◉
Non-Profit	●	◉	◉	◉	◉	●	●	◉	●	◉
Federal	◉	◉	●	●	◉	●	○	◉	●	◉
State	●	○	●	◉	◉	◉	◉	○	●	◉

KEY:
- ● = At least two-thirds of respondents discussed theme
- ◉ = Greater than one-third but fewer than two-thirds of respondents discussed theme
- ○ = Up to or exactly one-third of respondents discussed theme

Table 19. Qualitative Findings by Question and Respondent Type

	Primary Responsibility	Currently Doing	Top Priorities	Key Partners	Greatest Challenge
Non-Profit Experts	There is a shared and/or split responsibility because the owners and operators of individual systems have primary responsibility over their system. There is a role for the federal government.	LEOs are getting training.	LEOs should develop partnerships with those they can call on for help, if needed.	The state election office is most important, followed by DHS/CISA.	Lack of resources (human resources/expertise and money)
Federal Experts	There is a shared and/or split responsibility because the owners and operators of individual systems have primary responsibility over their system.	LEOs are working with government partners and the EI-ISAC to make use of available of resources and information.	LEOs should build their awareness about existing threats, common risks and vulnerabilities, and available resources.	Their state election office, followed by their federal partners, followed by their vendors.	Lack of resources (human resources/expertise and money)
State Experts	There is a shared and/or split responsibility because the owners and operators of individual systems have primary responsibility over their system.	Most LEOs are relying on outside entities (the state government/state election office, local government IT, and vendors) to provide cybersecurity.	None	Their state election office, followed by CISA and the EI-ISAC/MS-ISAC.	Lack of resources (human resources/expertise and money) and lack of awareness
All Experts	There is a shared and/or split responsibility because the owners and operators of individual systems have primary responsibility over their system.	LEOs are working with government partners and the EI-ISAC to make use of available of resources and information.	Develop trusted partnerships and utilize resources available from partners.	The state election office is most important, followed by DHS/CISA.	Lack of resources (human resources/expertise and money)

Table 20. Evaluation of Findings by Hypothesis

Hypothesis or Research Expectation	Quantitative Assessment	Qualitative Assessment	Conclusion
Local Election Office Characteristics			
Office-level Financial Resources	Limited Support	Strong Support	The financial resources of local election offices seem to influence their cybersecurity preparedness because they need financial resources to hire staff and particularly staff with IT/cybersecurity expertise.
Office-level Geography	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that geographic location (urban versus rural) influences the cybersecurity preparedness of local election offices.
Office-level Education Hypothesis	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that a local election official's level of education influences the cybersecurity preparedness of local election offices.
Office-level Professional Experience	Limited Support	Limited Support	The professional experience of local election officials may influence the cybersecurity preparedness of local election offices.
Office-level Expertise	Moderate Support	Strong Support	The number of IT specialists employed by a local election office seems to influence cybersecurity preparedness.
Office-level Size	Limited Support	Moderate Support	The total number of election administration staff may influence the cybersecurity preparedness of local election offices.
Jurisdiction Characteristics			
Jurisdiction-level Geography	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that the geography of a jurisdiction (urban versus rural) influences the cybersecurity preparedness of local election offices.
Jurisdiction-level Resources	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that the median income of a jurisdiction's residents influences the cybersecurity preparedness of local election offices.

Jurisdiction-level Education	Evidence to the Contrary	Inadequate Evidence	Local election offices in jurisdictions with lower percentages of high school educated residents may tend to be more compliant with cybersecurity recommendations.
Jurisdiction-level Population Size	Limited Support	Moderate Support	The population size of a local jurisdiction seems to influence the cybersecurity preparedness of local election offices because the office's levels of resources (human and financial) is linked to the size of the jurisdiction's population.
Jurisdiction-level Language	Evidence to the Contrary	Inadequate Evidence	Local election offices in jurisdictions with higher levels of language diversity may tend to be more compliant with cybersecurity recommendations.
Jurisdiction-level Age	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that the age of a jurisdiction's residents influences the cybersecurity preparedness of local election offices.
Jurisdictional-level Race	Evidence to the Contrary	Inadequate Evidence	Local election offices in jurisdictions with higher levels of racial diversity may tend to be more compliant with cybersecurity recommendations.
Jurisdiction-level Ethnicity	Evidence to the Contrary	Inadequate Evidence	Local election offices in jurisdictions with higher levels of ethnic diversity may tend to be more compliant with cybersecurity recommendations.
Partnerships			
State CEO	Inadequate Evidence	Strong Support	Receiving support from the office of the state CEO seems to be essential to cybersecurity preparedness for local election offices.
DHS/CISA	Inadequate Evidence	Strong Support	Receiving support from DHS/CISA seems to influence cybersecurity preparedness for local election offices.
EI-ISAC	Inadequate Evidence	Strong Support	Being a member of the EI-ISAC seems to influence cybersecurity preparedness for local election offices.
Local IT	Limited Support	Moderate Support	Coordination with local IT seems to influence cybersecurity preparedness for local election offices.

Controls

Institutional Structure	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that the institutional structure of the local election authority influences the cybersecurity preparedness of local election offices.
DRE Use	Inadequate Evidence	Inadequate Evidence	My findings do not provide evidence that the use of DRE systems is related to the cybersecurity preparedness of local election offices.
E-Pollbook Use	Strong Support	Inadequate Evidence	Local election offices which deploy the use of e-pollbooks tend to be more compliant with cybersecurity recommendations.

Figure 1. Analytic Framework for Exploring Influences on Local Election Administration Office Cybersecurity Preparedness

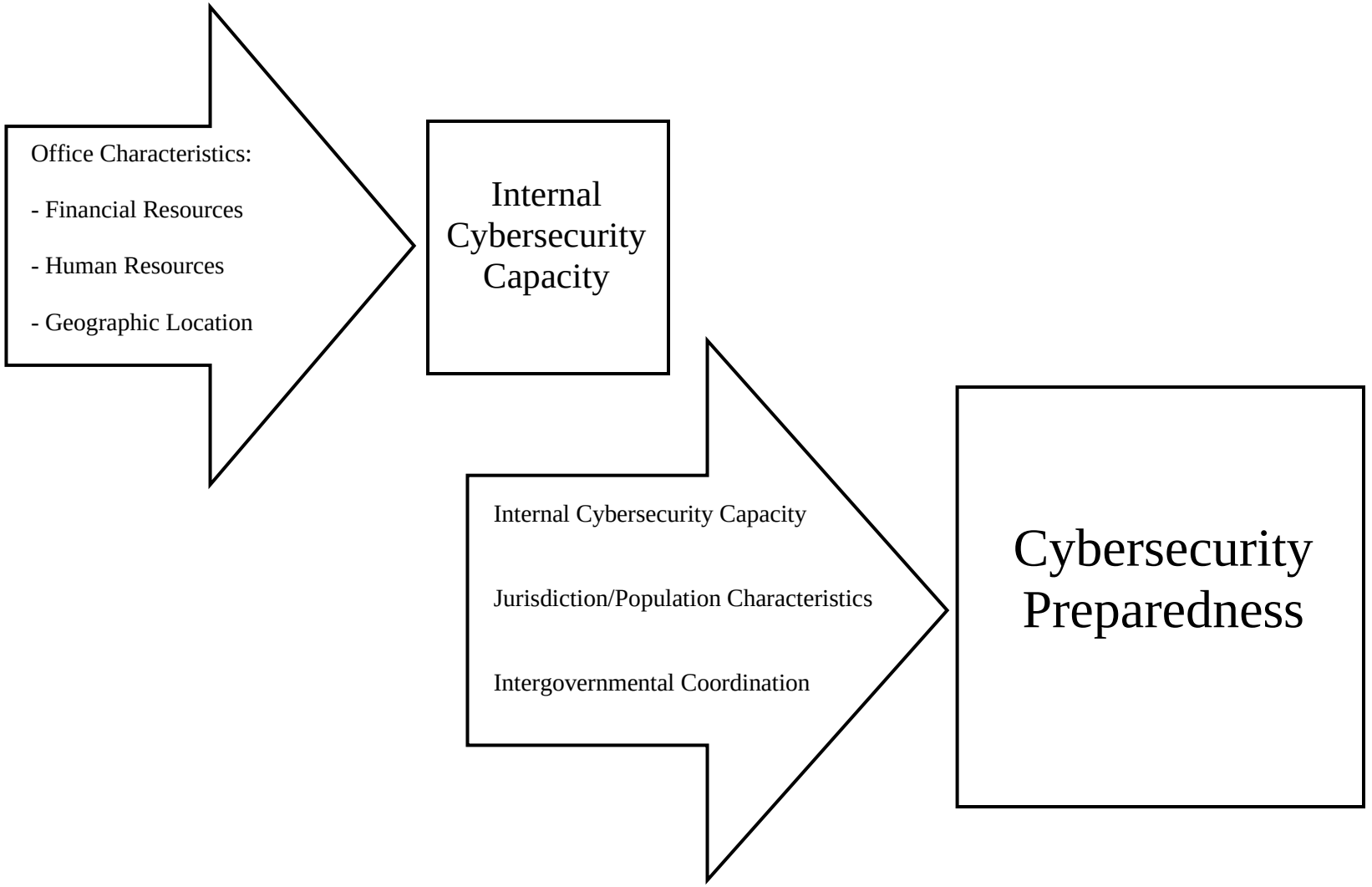


Figure 2. A Local Election Office's Cybersecurity Intergovernmental Network

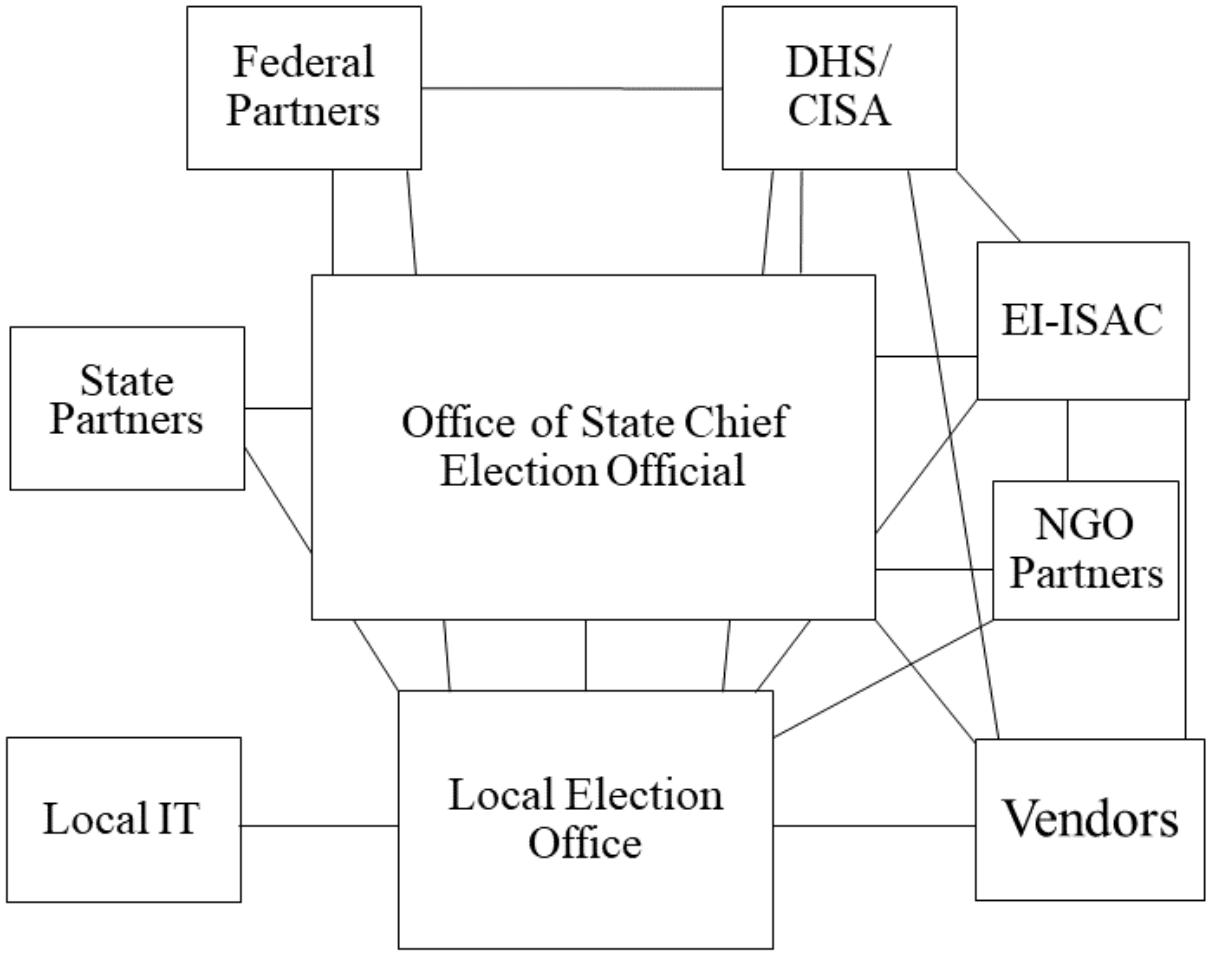
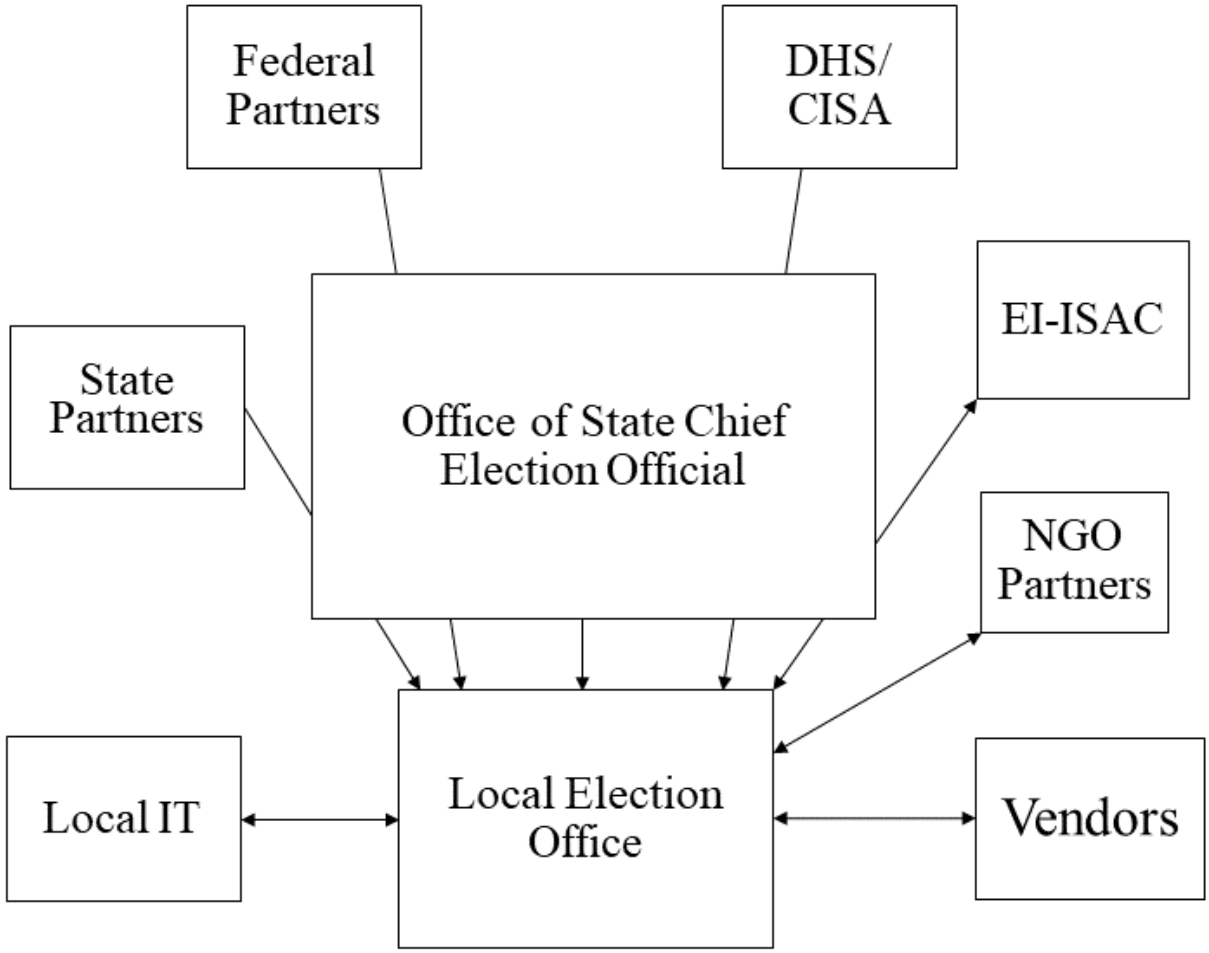


Figure 3. Information Flow between Local Election Administration Offices and Partners



Appendix 1. Survey Instrument

Survey Request Email Script

Dear Election Official,

I am a doctoral candidate in the Department of Political Science at Auburn University. I would like to invite you to participate in my research study about the election cybersecurity practices of local election administration offices. The purpose is to identify challenges and opportunities for local election administrators related to cybersecurity.

You may participate if you are the person responsible for the administration of elections or the head of information technology for election administration in your office and you are age 19 or older.

Participants will complete an online survey which will take approximately 30 minutes. The link to the survey is at the end of this email.

There are no guaranteed direct benefits to you for participating in this study. All respondents will be entered into a raffle to win a $100 Amazon gift card. The benefit to the researchers is the opportunity to produce findings which could inform important policy and budgetary decisions related to election cybersecurity.

The information collected from the survey may be used in my doctoral dissertation, but information which identifies your office as a participant will not be included in the dissertation or any publicly accessible documents.

The only risk related to participating in this study is the potential loss of confidentiality. To minimize this risk, we will take several steps to secure information which identifies your

office. The survey will be administered through the Auburn University Qualtrics account. Your direct survey responses will be protected by two-factor authentication. The name of the survey respondent will not be collected. In data files, all identifying information related to your office will be stored separately from survey responses. The data file containing information which identifies your office will be stored on a USB flash drive in a locked cabinet in a locked office on the Auburn University campus.

If you would like to know more information about this study, please see the attached information letter. If you decide to participate after reading the letter, you can access the survey from the link below or the link in the letter.

If you have any questions, please contact me at lmf0012@auburn.edu or 904-687-9387 or my advisor, Dr. Mitchell Brown, at brown11@auburn.edu.

Thank you so much for your time and consideration.

Link to survey: https://auburn.qualtrics.com/jfe/form/SV_8qwD8KkCEhjpmcZ

Sincerely,

Lindsey Forson, PhD Candidate – Auburn University

Survey Follow-up Request Email Script

Dear Election Official,

I am a doctoral candidate in the Department of Political Science at Auburn University. I'm writing to invite you again to participate in my research study about the election

cybersecurity practices of local election administration offices. The purpose is to identify challenges and opportunities for local election administrators related to cybersecurity. You may participate if you are an election official or an IT professional for the election administration office in your jurisdiction, and you are age 19 or older.

Participants will complete an online survey which takes approximately 15 minutes to complete, on average. There are no guaranteed direct benefits to you for participating in this study. All respondents will be entered into a raffle to win a $100 Amazon gift card. The benefit to the researchers is the opportunity to produce findings which could inform important policy and budgetary decisions related to election cybersecurity.

The information obtained from the survey may be used in my doctoral dissertation, but the information which identifies your office as a participant will not be included in the dissertation or any publicly accessible documents.

The only risk related to participating in this study is the potential loss of confidentiality, as some level of this risk always exists when identifying information is collected. However, to minimize this risk, we will take several steps to secure information which identifies your office. The survey will be administered through the Auburn University Qualtrics account. Your direct survey responses will be protected by two-factor authentication. The name of the survey respondent will not be collected. In data files, identifying information related to your office will be stored separately from survey responses. The data file containing information which identifies your office will be stored on a USB flash drive in a locked cabinet in a locked office on the Auburn University campus.

If you would like to know more information about this study, please see the attached information letter. If you decide to participate, you can access the survey from the link below or the link in the letter. The survey will remain open through December 31, 2019.

If you have any questions, please do not hesitate to contact me at 904-687-9387 or lmf0012@auburn.edu or my advisor, Dr. Mitchell Brown, at brown11@auburn.edu. Thank you for your consideration.

LINK TO SURVEY: https://auburn.qualtrics.com/jfe/form/SV_8qwD8KkCEhjpmcZ

Sincerely,

Lindsey Forson, PhD Candidate, Auburn University

Survey Introduction

Thank you for participating! By responding to this survey, you are providing consent for your responses to be used in my research. Please remember that your identifying material will not be published. All responses included in my dissertation or any subsequent publications will be confidential.

Survey Questions

Section 1 – Overview

1. What is the name of your office?
2. In what state is your office located?

3. What do you believe is the single most important task a local election administration office can complete to protect the election systems they manage from cyber threats?
4. Do you believe the cybersecurity of US election systems is a legitimate concern?

   Response Choices: Yes, No
5. Do believe there is a risk of cyber attack to your office?

   Response Choices: Yes, No
6. Who within the US government do you believe should be primarily responsible for securing US election systems?

   Response Choices: Local governments, State governments, Federal government, A combination of local and state governments, A combination of state governments and the federal government, A combination of local governments and the federal government, A combination of all three, Other
7. In the past three years, have you or has anyone in your office completed cybersecurity or cyber-hygiene training provided by your state election office?

   Response Choices: Yes, No
8. In the past three years, has your office received any direct cybersecurity support from your state election office?

   Response Choices: Yes, No
9. Has your office received any election cybersecurity support from the US Department of Homeland Security?

   Response Choices: Yes, No

10. Does your office receive election cybersecurity support from outside offices or entities within your local government?

    Response Choices: Yes, No

11. Is your office a member of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)?

    Response Choices: Yes, No

12. In the past three years, has your office participated in a Tabletop Exercise (TTX)?

    Response Choices: Yes, No

13. Please list any other organizations (governmental or non-governmental) that your office works with on election cybersecurity efforts.

Section 2 – Cybersecurity Practices

The next section of this survey will ask whether your office completes specific cybersecurity practices. For each cybersecurity practice about which you are asked, please answer to the best of your knowledge whether your office completes the task as a measure of securing some type of election-related system. For the purposes of this survey, "election system" means any system related to administering elections including, but not limited to, voter registration systems, vote casting systems, vote counting systems, and reporting systems. Comment space is available if you would like to clarify or further explain your answer. Leaving a comment is not required. (This list of cybersecurity practices is not intended to be exhaustive.)

14. Does your office have a documented inventory of critical election systems under its control?

Response Choices: Yes, No, N/A, Optional Comment

15. Does your office provide (either directly or through a third-party) and require cyber-hygiene training for all individuals with access to critical election systems?

    Response Choices: Yes, No, N/A, Optional Comment

16. Does your office have a policy prescribing who has what level(s) of access to all critical election systems?

    Response Choices: Yes, No, N/A, Optional Comment

17. Do you have an office policy which requires robust passwords for access to all user accounts, applications, and devices?

    Response Choices: Yes, No, N/A, Optional Comment

18. Do you have an office policy which requires two-factor or multi-factor authentication for access to all user accounts, applications, and devices?

    Response Choices: Yes, No, N/A, Optional Comment

19. Are vulnerability tests run on your network and all connected systems at some regular interval?

    Response Choices: Yes, No, N/A, Optional Comment

20. Does your office implement encryption standards for all data at-rest and in-transit?

    Response Choices: Yes, No, N/A, Optional Comment

21. Is there a firewall protecting your network and all election-related applications?

    Response Choices: Yes, No, N/A, Optional Comment

22. Do your relevant critical election systems have anti-virus software?

    Response Choices: Yes, No, N/A, Optional Comment

23. Is anti-virus software regularly updated by your office?

Response Choices: Yes, No, N/A, Optional Comment

24. Does your office back up all critical election data, including voter registration data, at least weekly?

    Response Choices: Yes, No, N/A, Optional Comment

25. Does your office back up all critical election data, including voter registration data, daily?

    Response Choices: Yes, No, N/A, Optional Comment

26. Is all software used by your office regularly updated with the latest patches?

    Response Choices: Yes, No, N/A, Optional Comment

27. Do you have procedures for ensuring you are aware of necessary software patches?

    Response Choices: Yes, No, N/A, Optional Comment

28. Is there an intrusion detection system on your network?

    Response Choices: Yes, No, N/A, Optional Comment

29. Does your office require all of your election-related vendors to provide written documentation of their cybersecurity processes?

    Response Choices: Yes, No, N/A, Optional Comment

Section 3 – General Office Information

Please answer the following demographic questions about your office, your staff, and yourself to the best of your knowledge:

27. About how many registered voters does your office serve?

28. During your last fiscal year, what was your total budget for administering elections?

29. How many total staff members within your office work on election administration?

30. How many IT specialists are on your staff who work on election administration or election-related systems as at least part of their job?

31. What is your highest educational degree attained?

Response Choices: High School diploma, Bachelor's Degree, Masters Degree, Higher than Masters Degree, Other

32. Do you have a professional election administration certification (e.g. CERA; CEA)?

Response Choices: Yes, No

34. Are Direct Electronic Recording (DRE) machines used in your jurisdiction?

Response Choices: Yes, Sometimes, No

35. Do the voting methods used in your jurisdiction create a voter verifiable paper trail?

Response Choices: Yes, Sometimes, No

36. Are e-pollbooks used in your jurisdiction?

Response Choices: Yes, Sometimes, No

37. Is there anything else you would like to share

Appendix 2. Description of Variables

Cybersecurity Compliance is the dependent variable. It is a measure of the percentage of applicable cybersecurity concept which a jurisdiction reported completing all tasks.

Rural is an ordinal measure of jurisdiction's most recent classification by the US Census Bureau as urban (0), somewhat urban (1), or not urban (2).

Population is the population of the local jurisdiction according to the US Census Bureau.

Median Age is the median age of the local jurisdiction according to the US Census Bureau.

Percent 65older is the percent of the local jurisdiction's population that is age 65 or older according to the US Census Bureau.

Percent High School plus is the percent of the local jurisdiction's population that has completed high school or higher according to the US Census Bureau.

Percent Bachelor plus is the percent of the local jurisdiction's population that has completed a bachelor's degree or higher according to the US Census Bureau.

Median Income is the median income of the local jurisdiction according to the US Census Bureau.

Percent Nonwhite is the percent of the local jurisdiction's population that is a race other than white according to the US Census Bureau.

Percent Black is the percent of the local jurisdiction's population that is black according to the US Census Bureau.

Percent Hispanic is the percent of the local jurisdiction's population that is Hispanic according to the US Census Bureau.

Percent Other Language is the percent of the local jurisdiction's population that speaks a language other than English in the home according to the US Census Bureau.

Registered Voters is the number of registered voters in the local jurisdiction according the jurisdiction's election office or the state chief election official's office.

LEO Education is the highest level of education completed by the local election official as reported on the survey.

Certification is a dichotomous measure of whether the local election official has an election administration professional certification as reported on the survey.

Number of IT Staff is the number of information technology (IT) staff employed by the local election office as reported on the survey.

Total Staff is the number of employees of the local election office as reported on the survey.

Reported Budget is the total elections budget of the last fiscal year of the local election office as reported on the survey.

Local Structure is a categorical measure of the local government institutional structure for election administration according to Hale et al. 2015.

DRE is a dichotomous measure of whether direct recording electronic voting machines are in use in the local jurisdiction as reported on the survey.

E Pollbooks is a dichotomous measure of whether electronic pollbooks are in use in the local jurisdiction as reported on the survey.

EI-ISAC is a dichotomous measure of whether a local jurisdiction is a member of the Elections Infrastructure Sharing and Analysis Center (EI-ISAC) according to the membership roster on the EI-ISAC's website.

Appendix 3. Interview Instrument

Interview Request Email Script

Dear [Name],

I am a doctoral candidate in the Department of Political Science at Auburn University. I'm writing to invite you to participate in my research study about the election cybersecurity practices of local election administration offices. The purpose is to identify challenges and opportunities for local election administrators related to cybersecurity. You may participate if you are age 19 or older.

Participants will be asked to participate in an interview which will last approximately 15 minutes. There are no direct benefits to you for participating in this study. The benefit to the researchers is the opportunity to produce findings which could inform important policy and budgetary decisions related to election cybersecurity.

The only risk related to participating in this study is the potential loss of confidentiality. To minimize this risk, we will not record your name or affiliation anywhere other than on the consent form. The consent form will be stored in a locked cabinet in a locked office on the Auburn University campus. The information obtained from the interview may be used in my doctoral dissertation, but information which identifies you as a participant will not be recorded with your responses and will not be included in the dissertation or any publicly accessible documents. I will record responses by taking notes during the interview.

If you would like to know more information about this study, please see the attached consent form. If you decide to participate after reading the form, please respond to this email so that we can arrange the time and location of the interview.

If you have any questions, please contact me (lmf0012@auburn.edu or 904-687-9387) or my advisor, Dr. Mitchell Brown, at brown11@auburn.edu.

Thank you for your consideration.

Sincerely,

Lindsey Forson, PhD Candidate – Auburn University

Interview Introduction

Good morning/afternoon/evening! Thank you very much for agreeing to participate in my study regarding the cybersecurity practices of local election administration and related opportunities and challenges. Please answer the following questions to the best of your knowledge and allowance. We are not strictly bound by the questions, so please feel free to share additional information. We should be able to complete the interview in about 15 minutes.

Please remember that your responses will remain confidential. Further, I will not reveal in any public materials the names of individuals who were interviewed. I will only describe the types of roles and positions of the interviewees in general. All identifying information will be securely stored and will not be included in publicly accessible data or articles. Do you have any questions before we begin? Okay, let's get started.

Interview Questions

1. Please explain your role in protecting elections from cyber threats.
2. Who do you believe has primary responsibility for election cybersecurity in the US?
3. What are local election administrators doing to protect elections from cyber threats?
4. What are the most important things a local election administrator can do to protect the election systems they manage from cyber threats?
5. Who are the key partners in election cybersecurity for local election administrators?
6. What are the biggest challenges for local election administrators?
7. Is there anything else you would like to add?