UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

The Transaction Costs of Municipal Cyber Risk Management

ROWLAND HERBERT-FAULKNER

CLTC WHITE PAPER SERIES

The Transaction Costs of Municipal Cyber Risk Management

ROWLAND HERBERT-FAULKNER

April 2024

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Local governments across the United States face a costly cyberattack epidemic, as ransomware and other attacks threaten to expose citizens' private data and paralyze civic functionality. While a sturdy cybersecurity posture has long been a national defense priority and an industry expectation, local governments represent a uniquely expansive, complex, and novel domain for managing cyber risk. Cities of all sizes are vulnerable to data breaches, financial theft, and denial-of-service attacks, all conducted by seasoned cyber criminals. However, the capacity of cities to prepare for and respond to cyber threats varies widely. That variation is further complicated by the interagency and third-party collaboration often required for effective cyber risk management.

This white paper supports municipal efforts to strengthen cybersecurity posture by identifying the sources of transaction costs associated with municipal cyber risk management. Transaction costs are generally defined as the costs of searching for information, coordination between parties, drawing up and enforcing contracts, and negotiation, all of which are part of managing cyber risk. When such costs are unaccounted for, decision-makers find themselves surprised and unprepared, leading to changes in administrative activities and cost overruns not captured by the initial resource allocations. The guidance and resources provided to city governments by the private sector and federal and state governments are unequivocally essential, but local governments will benefit from knowing what expenditures — especially temporal and financial expenditures — are required to access and leverage cyber risk management resources across all timescales. The guidance serves two functions:

1. To strengthen the security posture of local governments, and
2. To establish a consistent, predictable, well-defined, and equitable cyber risk governance system, which is an implicit effort to reduce transaction costs.

Using semi-structured interviews with local officials, industry professionals, legal experts, and researchers; extensive document analysis of government and industry publications and media reports; and a review of cybersecurity scholarship, I investigate the source, nature, magnitude, and timescale of the cybersecurity transaction costs that municipalities bear.

Three key findings emerge from this research:

- Risk mitigation and risk transfer are the main sources of transaction costs in municipal cyber risk management. Cyberattacks force cities to mitigate future risk through time- and resource-intensive coordination, procurement, and contracting efforts.
- Partnerships with the private sector and third parties are essential, though they drive up transaction costs, especially in terms of contracts and negotiations.
- Municipalities are ill-positioned to transfer cyber risk because of insurer reluctance and product insecurity. Cities struggle to transfer cyber risk because of legacy systems, device insecurity, and extreme caution in the cyberinsurance market.

This analysis of transaction costs in cyber risk management approaches available to municipalities offers insights into what are likely to be core elements of urban technology governance in the future: extensive contracting with private firms, assigning product liability, and interagency collaboration and coordination.

This paper highlights many of the classic challenges associated with governance and related challenges that incur transaction costs. The work is timely; scholars, government officials, and industry experts have a magnifying glass on municipal cybersecurity challenges and are working in earnest to devise governance solutions that cities of all sizes can adopt. These efforts call attention to the future of urban governance in an increasingly digital world. This future will require intricate long-term relationships between the public sector, the private sector, and residents, with cybersecurity essential for the structural integrity of those relationships.

Introduction

"An attacker only has to be right once. Organizations have to be right all the time."
—Former cybersecurity program manager

Cyberattacks on municipalities have become a regular occurrence in recent years. "Incidents involving US local governments happen at a rate of more than 1 per week," according to Brett Callow, a threat analyst with Emsisoft.[1] Cities of all sizes have proven to be lucrative targets for ransomware attackers in particular. In 2018, a cyberattack cost the city of Atlanta $17 million for response, recovery, and remediation. In 2019, a ransomware attack cost the city of Baltimore $5.3 million to respond, in addition to over $14 million in lost revenue because of compromised payment collection systems. In 2023, the hacker group Play Ransomware leaked 10 gigabytes of data that they had stolen from the city of Oakland, California; the costs of the attack have not yet been reported. The impacts of such breaches go beyond the walls of city hall: for example, a resident whose personal information was stolen in the Oakland cyberattack has become a victim of fraud, with close to $50,000 charged to credit cards opened in his name.[2] Despite the increased media coverage of such attacks, not all cyber incidents are detected, and of those that are detected, not all are reported, a reality that underscores the magnitude of the cyber risk challenges local governments face.[3] Legacy hardware and software, along with disparities in personnel risk awareness and capacity to preempt and respond to incidents, have left cities especially vulnerable to cybercrime. Further, municipalities cannot afford any downtime and must restore compromised services as quickly as possible following an attack.

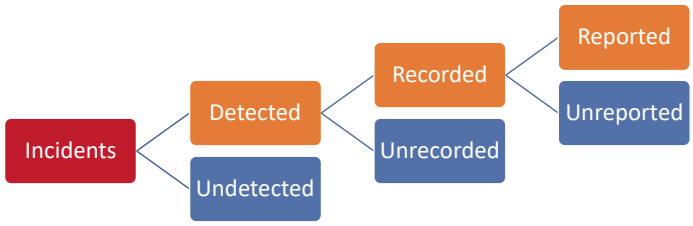

Figure 1. Prevalence and awareness of cyberattacks. See Romanosky (2016) and Kesan et al. (2019).

1 Abrams (2023).
2 Sierra (2023).
3 Romanosky (2016) and Kesan et al. (2019).

While technological advancements have brought greater efficiencies in civic functions such as finance, administration, monitoring, and communications, the ubiquity of digital infrastructure has created an expansive attack surface that renders personal data, operations, finances, and a host of other elements vulnerable. Most local governments require extensive support and preparation to span the gap between their current readiness and response capabilities and those recommended by cybersecurity leaders in industry and the federal government. "Local governments are often priced out of meeting best practices," according to journalist Jule Pattison-Gordon, who authored an article describing the challenges municipalities face when managing cyber risk.[4]

The production costs of tools and services are readily evident on their price tags, but transaction costs often do not become apparent until governance actors start making implementation decisions. Transaction costs are generally defined as the costs of searching for information, coordination between parties, drawing up and enforcing contracts, and negotiation. When unaccounted for, decision-makers find themselves surprised by and unprepared to assume such costs, leading to changes in administrative activities and cost overruns not captured by the initial resource allocations. Improved cyber hygiene, threat monitoring, infrastructure upgrades, IT personnel expansion, and the creation of incident response plans are indeed necessary, but they require preparation on the part of local governments. It is in the preparation and subsequent execution that critical transaction costs are incurred. These costs can complicate and impede the process of implementing the recommendations. Accounting for the full scope of expenditures required for cities that want to upgrade their technological capacity will help inform and position city officials to manage cyber risk.

This report focuses on elucidating the transaction costs borne by municipalities when managing cyber risk. Using semi-structured interviews with local officials, industry professionals, legal experts, and researchers; extensive document analysis of government and industry publications and media reports; and a review of cybersecurity scholarship, I investigate the source, nature, magnitude, and timescale of the cybersecurity transaction costs that municipalities bear. I find that municipalities incur significant transaction costs when mitigating and transferring cyber risk. How these costs are incurred and paid implicate urban governance structures, which have been under pressure to evolve to serve and be served by the potential of big tech.

4 Pattison-Gordon (2022).

RESEARCH BACKGROUND

This study explores the transaction costs that municipalities incur when transferring cyber risk, building upon scholarship on transaction costs, cybersecurity, and federal and industry best practices and recommendations.

Transaction Costs

Transaction costs emerge in the course of locating and coordinating parties and information; contracts and negotiations; inventory and monitoring; and compliance and enforcement.[5] Such costs sometimes emerge unexpectedly and often complicate or thwart implementation processes.[6] Williamson (1981) argues that transaction cost analysis can help identify the most efficient governance structure, especially when deciding to purchase goods and services in the market or produce them in-house. In the context of municipal cybersecurity governance, local governments must collaborate with federal and state agencies (e.g., CISA, National Guard) as well as industry players (e.g., auditors, threat analysts), legal counsel, and insurers. They must also document and report cyberattacks; take out cyberinsurance policies, and negotiate liability and remediate damages in the wake of incidents; and comply with industry and government cybersecurity standards. Managing cyber risk therefore requires a combination of goods and services procurement from the market and changes in organizational behavior, tasks which incur transaction costs. The activities listed above accrue significant costs that can prohibit local governments from implementing best practices.

Table 1. Key Sources of Transaction Costs in Municipal Cyber Risk Management

This table lists the primary sources of transaction costs that city governments face when managing cyber risk, as identified in academic scholarship and government and industry publications, and through my semi-structured interviews with city leaders.

Activity	Transaction Cost Type	Expenditure
Federal and State Grant applications (e.g., State and Local Cyber Security Grant Program, Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program)	Location/coordination	Time
Interagency, intergovernmental, and third-party collaboration	Location/coordination of parties and information	Time, money

5 Niehans (1987), Stavins (1995), Allen (1998), and Whittington (2012).
6 Pressman and Wildavsky (1984).

Legal counsel	Location/coordination of parties and information; Contracts/negotiation	Time, money
Implementing risk management practices	Location/coordination; Monitoring/inventory	Time, money
Insurance	Location/coordination; Contracts; Monitoring/inventory	Money: at least $100k/year for cyberinsurance premiums; assumes requisite security controls are in place; some municipalities self-insure or combine self-insurance with reinsurance
Compliance with and enforcement of government and industry standards	Monitoring/inventory; Record-keeping; Compliance enforcement	Time, money
Audits/testing	Location/coordination; Monitoring/inventory	Time, money: can be free if provided by state or federal government (CISA assessments and vulnerability scans)
Remediation	Location/coordination; Exchange information; Monitoring/inventory; Contracts; Record-keeping	Time, money

In 2020, in response to the increasing frequency of ransomware attacks on state, local, tribal, and territorial (SLTT) organizations and critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released the 2020 Ransomware Guide, which details best practices for ransomware prevention and response.[7] This resource illuminates many of the emergent transaction costs that local governments must take on to maintain and secure their digital systems. The recommendations outlined in the guide are informed by industry best practices and include procedural and technical steps that organizations can take to strengthen their posture against ransomware attacks. These steps include creating a cyber incident response and communications plan; maintaining offline, encrypted data backups; implementing a cybersecurity user awareness and training program; and conducting vulnerability scans. As with most guides and recommendations, however, the costs involved in carrying out these steps — particularly the transaction costs — are not outlined. Yet these recommendations implicitly seek to increase

7 Ransomware Guide (2020).

the capacity of sub-federal entities to economize their transaction costs,[8] thereby improving governance efficiency.

RESEARCH DESIGN

I conducted 20 semi-structured interviews with professionals who are involved in different ways with cybersecurity for municipal governments. Interviewees included municipal IT managers, insurance adjusters, executive search professionals, threat analysts, legal experts, CPAs, auditors, industry and academic researchers, cybersecurity program managers, and CIOs and CISOs.

During the interviews, I asked about the unique cyber risks that local governments face, the role of cyberinsurance in municipal cyber risk management, the financial costs associated with compliance and enforcement, best practices around preparation and response, and intergovernmental and third-party collaboration. I did not record the interviews, but extensive notes were taken and represent partial transcriptions.

Interviewees were recruited through professional and conference organizations, researcher and practitioner networks, and subsequent snowballing.

In addition to the interviews, I reviewed cybersecurity scholarship, federal and state legislation, industry publications, media reports, and local, state, and federal policy documents.

8 Williamson (1981).

Cyber Risk Management Strategies in Practice

Governing amidst uncertainty (often because of information asymmetries and differences in capacities between agents) entails economizing transaction costs through risk management.[9] Risk assessment is the first step in managing risk.[10] However, because cyberattacks on municipalities are a more novel and recent phenomenon, many cities are often surprised into conducting cyber risk assessments only after they have experienced an incident. There are four primary risk management strategies widely discussed in literature and practice: *risk avoidance*, *risk acceptance*, *risk mitigation*, and *risk transfer*. For city governments, risk avoidance is nearly impossible, as the prevalence of cyberattacks on cities of all sizes has shown. City governments are simply too dependent upon digital technologies to avoid cyber risk altogether. Risk acceptance likewise is not sufficient; here, the agent acknowledges the potential for risk, but remains passive. Government and industry leaders agree that cities should expect cyberattacks and should prepare to be resilient when they occur. This paper therefore focuses on *risk mitigation* and *risk transfer* as cyber risk management strategies. The section below discusses each of these two strategies.

RISK MITIGATION

Risk mitigation entails reducing the likelihood or impact of risks by implementing system controls and countermeasures. Mitigation gives rise to most of the transaction costs of municipal cyber risk management.

Self-insuring

Self-insuring has become the primary task of municipalities in cybersecurity governance. In this context, it does not refer to policies issued by an insurer. Cities self-insure by adopting practices that mitigate risk and agreeing to bear the cost of unwanted cyber-related outcomes. The task is multifaceted and involves threat monitoring, adopting an incident response and communications framework, budgeting for emergencies,[11] hiring qualified IT personnel, training personnel on cyber hygiene training, hardware and software upgrades, and creating data back-

9 Macher and Richman (2008) and Terman (2023).
10 Quinn (2023) and NIST Cybersecurity Framework (2024).
11 Pattison-Gordon (2022).

ups. Some municipalities self-insure up to a certain amount and purchase reinsurance for costs beyond; this hybrid model can be cheaper since policyholders assume a greater share of the risk.[12] Two interviewees emphasized the importance of total executive buy-in when pursuing the self-insurance pathway, arguing that risk management appropriations should be binding to ensure that resources are available when needed to protect governance integrity. Self-insurance also includes mitigation, which is discussed below.

Municipalities can mitigate some risk by participating in state and federal programs, which provide monitoring and incident response services, though they require compliance with government and industry standards. For example, Washington State offers free monitoring and security audits to municipalities in exchange for metadata related to threats. In Massachusetts, the state government awards Municipal Cybersecurity Awareness grants to "support local government efforts to improve overall cybersecurity posture through comprehensive online end-user training, evaluation, and threat simulation."[13] At the federal level, the State and Local Cybersecurity Grant Program (SLCGP), State Homeland Security Grant Program, Urban Area Security Initiative (UASI), and the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program are efforts to support municipal cyber risk management. CISA also provides vulnerability scans and employs regional liaison officers to perform network security evaluations, but one interviewee noted that not all communities are aware of this resource and recommended more public awareness efforts. The process of applying for such grants, however, generates search and coordination transaction costs. Several interviewees noted that not all cities' staffs have the time, resources, and knowledge to prepare grant applications. Some cautioned against reliance on grant money for the medium and long term because the availability of grant funds is subject to political forces, recommending that small jurisdictions use the state and federal resources to build a strong enough posture to reduce dependence on those resources. Further, use of grant funds for capital and other purchases is one-time, and sustainment of any procured products must be borne by the jurisdiction itself.

Another governance reality with respect to state-local relationships is that states generally cannot compel cities to share data or adopt state provisions. Nevertheless, higher levels of government have long used strings-attached offerings to unify lower levels of government under desired practices and regulations. For example, the State and Local Cybersecurity Grant Program requires its participants to comply with NIST standards, cyberinsurance requirements, and industry standards, all of which involve data sharing and reporting. Given the rampant cyberattacks

12 Ibid.

13 Massachusetts Municipal Cybersecurity Awareness Grant Program. https://www.mass.gov/info-details/about-the-municipal-cybersecurity-awareness-grant-program

that cities face, desperation has driven many to participate in state and federal programs. One interviewee was keen to note that in some cases, states can force local jurisdictions to adopt service-specific cyber requirements; they offered two examples of state-to-local information transfer: license plate lookup for law enforcement and state-level tax information. To receive such information from the state, a locality must comply with the state's digital security requirements. In other words, information exchanges incur transaction costs; in the case of state-to-local information transfer, localities may have to adopt a different information security protocol.

Administration and Talent Acquisition

Several interviewees remarked that local government CISOs and IT managers often have complex administrative responsibilities related to interagency coordination, funding security initiatives, and regulatory compliance — all of which they must carry out with limited authority and staff. To address these challenges, municipalities incur location and coordination transaction costs, especially with respect to staffing, vendor procurement for audits and testing, monitoring, and administrative decision-making.

Talent acquisition and retention came up repeatedly in interviews. One interviewee, a former local government cybersecurity official, described how municipalities end up paying cybersecurity contractors at private-sector levels, while permanent public-sector positions often pay half as much. The *Baltimore Sun* reported that the IT Director in charge during the 2018 cyberattack on that city was paid $250K per year, a pay cut compared to his compensation at his previous job in sales for Intel.[14] Another interviewee (a managing partner with an executive search firm) reported that executive search firms generally charge clients between 30% and 33.3% of a hired applicant's first year's total compensation (comprising base pay and bonuses). The interviewee also reported that compensation varies according to the region of the country (in this case, the United States).

One interviewee, a corporate officer, noted that organizations can benefit from hiring a firm to manage cyber risks. The vendor may offer bundled services — some of which may not be used by the customer — but the money is better spent on purchasing the package (thereby streamlining the risk management process) rather than piecemeal and ad hoc contracting. Another benefit is that industry vendors must remain current with trends and practices in the threat landscape.

14 Duncan (2019).

Cyber Hygiene Improvements

Humans are the primary gateway to cyberattacks.[15] Workforce training, software and hardware upgrades, regular system audits and testing, and the development and implementation of network security frameworks are central to strengthening the security posture of organizations. Nearly all interviewees stated that local governments overwhelmingly lack the financial resources, knowledge, technology, and qualified personnel to prepare for, monitor, and respond to cyber threats. Auditors and cybersecurity analysts reported "horror stories" of organizations struggling to prepare for security audits, due to a lack of knowledge about cyber hygiene, disjointed legacy hardware and software systems, and lack of compliance with relevant ISO and SOC2 standards. As Chris DeRusha, Federal Chief Information Security Officer in the Office of Management and Budget (OMB), said at Nextgov/FCW's Identity Security Workshop, "Legacy IT modernization is the number one biggest rock that needs to get moved for us to be able to secure our systems."[16]

Two interviewees, both with experience carrying out simulated threat campaigns, noted that organizations with IT specialists who are trained to perform such exercises are able to absorb the cost of that dimension of cybersecurity standards compliance. Local governments that do not have that kind of in-house expertise will rely on federal and state support to finance the audits and testing required for compliance with the best cybersecurity practices.

Software and Hardware Insecurity

Several interviewees pointed to the lack of built-in product security, particularly in legacy infrastructure,[17] emphasizing the scale of security vulnerabilities across all municipalities. Scholars have also brought attention to this deficiency, noting that the lack of built-in product security features stems from vendors' aversion to the increased cost of product development and the consequent delays in market release.[18] Similarly, Li and Liao (2018) note that producers of physical and digital infrastructure lack incentives to design and implement built-in security features. Researchers have explored this weakness in the context of smart city infrastructure, calling out that IoT devices are entry points into city governments' networks, a key security weakness demanding attention.[19] Relatedly, Smith et al. (2021) find no overarching public policy to resolve

15 Nurse et al. (2020).
16 Riotta (2023).
17 DeNardis and Raymond (2017), Habibzadeh et al. (2019), and Vitunskaite et al. (2019).
18 Vitunskaite et al. (2019) and Smith et al. (2021).
19 Kalinin et al. (2021), Habibzadeh et al. (2019), and DeNardis and Raymond (2017).

issues with conflicting design protocols that make up IoT applications, issues that expose IoT users to cybersecurity risks.

The most critical implication of these deficiencies is risk transfer. Product users, be they individuals or organizations, assume the security risks and are often left legally and financially responsible for damages and losses. Vitunskaite et al. (2019) discuss liability assignment issues, noting that manufacturers of faulty or vulnerable products are indemnified and end users are not guaranteed compensation. Furthermore, in cases where third-party products are embedded in the city's infrastructure, the city council must assume responsibility for faults and vulnerabilities. Products end up being more expensive than expected because the procuring authority pays the costs of recovery and remediation in the wake of cyberattacks. The 2018 ransomware attack on Atlanta cost the city $17 million, an estimated $6 million of which paid for security services, software upgrades, and new computers and smartphones.[20]

Each successive device or system that an organization adopts is another potential security risk to which it is connected. Kalinin et al. (2021) succinctly articulate the core of the security challenge of interconnected cyberphysical systems: "Connected devices implement different functions, they have various capabilities and features, they are produced by different manufacturers, and with different versions of hardware and software, they meet different security standards." Managing the interconnectedness of physical and digital systems to contain the scope of threats involves interdepartmental coordination transaction costs. Whether municipalities embark on partial upgrades of legacy infrastructure or complete overhauls of hardware and software, the vendor contracting transaction costs that come with interoperability and the transition between systems emerge rapidly. Cities must also engage in procurement processes that in many cases are fraught with bureaucratic challenges and inefficiencies[21] to locate and purchase cyber infrastructure and services, a time-intensive and expensive endeavor.

RISK TRANSFER

Risk transfer involves shifting risk to a third party. Cyberinsurance is the primary mechanism through which municipalities can transfer cyber risk. ICMA's 2016 survey[22] found that 45% of local governments that responded had purchased cyberinsurance, and 27% of respondents had

20 Deere (2018).
21 Terner (2024) and Casady et al. (2023).
22 ICMA Survey Summary Report (2016).

full coverage. Since that survey, insurers have curtailed their assumption of cyber risk, especially for municipal governments.

Cyberinsurance

Regardless of their professional affiliation, interviewees expressed mixed views on the role of cyberinsurance in managing municipal cyber risk. Some argued that it is unlikely to help local governments because of the reluctance of insurers to cover government entities, given the breadth of their risk profile. Romanosky et al. (2019) found that some cyberinsurance carriers consider governments to be ineligible for coverage, owing to the prevalence of legacy infrastructure that is vulnerable to hacking, poor cyber hygiene, and lack of awareness around cyber risk. Similarly, interviewees and other industry researchers observe that cyberinsurance policy exclusions are increasing, letting insurers off the hook for covering cyber losses and weakening policy holders' capacity to recover from cyberattacks.[23] In addition, product insecurity (instantiated in legacy infrastructure and urban IoT systems) creates an expansive risk profile, making insurers hesitate to offer coverage.

It is widely recognized in government and industry, and among researchers, that cities cannot afford any downtime in administration or service provision. In the wake of the 2018 cyberattack on Atlanta's government, the Department of Watershed Management could not accept online or in-person payments, nor could it process new water meter sales. It is no surprise that in response to ransomware attacks — the prevalence of which has skyrocketed over the last decade — many cities opt to pay ransoms rather than risk prolonged and expensive efforts to deny payments and recover damages. Often, the ransom pales in comparison to the costs of recovery and remediation. For example, in the 2019 ransomware attack on the Baltimore city government, hackers demanded $76,000 worth of bitcoin,[24] but the attack cost the city $18 million in recovery and remediation. Some states have barred local agencies from paying ransoms. In 2022, North Carolina became the first state to ban government entities from paying cyberattack ransoms. The state's chief risk officer within the Department of Information Technology cited data compromise, a lack of guarantee that payment will lead to data recovery, and the incentive for more attacks as reasons not to pay ransoms.[25]

Despite the cost evaluation that city officials face, insurers are wary of covering risks like ransomware attacks because continued ransom payouts incentivize hackers to launch fur-

23 See Wolff (2022).
24 Fernandez et al. (2019).
25 Greig (2022).

ther attacks, a concern acknowledged across all interviews and echoed in existing scholarship and industry reports.[26] Several interviewees reflected on the evolution of the cyberinsurance market, noting that many carriers took on cyber risk as an opportunity to understand the risk profile of cyberphysical systems and expand the market. However, as cyberattacks (and consequently, insurance payouts) became more prevalent, insurers began restricting coverage and requiring potential policyholders to demonstrate progressively higher degrees of self-insurance. Many carriers fear the regressive incentive mentioned earlier, but MacColl et al. (2023) argue that "the conclusion that ransomware operators are deliberately targeting organizations with insurance has been overstated." Relatedly, Wolff (2022) finds that cyberinsurance has not improved cybersecurity or reduced cyberattacks. Despite the reluctance of insurers, some jurisdictions have successfully used their cyberinsurance policies to pay ransoms, such as Lake Park, Florida (2019) and San Bernardino County, California (2023). Insurers now require policyholders to meet several minimum requirements related to personnel, hardware, software, and organizational controls before providing coverage, and the premiums are determined based on the degree of compliance with minimum requirements.[27] One interviewee recommended that cities for which cyberinsurance premiums are prohibitively high should spend one year self-insuring by improving their security controls, thereby reducing future cyberinsurance premiums.

Cyberinsurance industry experts have called for a government backstop to protect insurers from insolvency in the event of a catastrophic cyberattack.[28] Others say that taking out cyberinsurance policies will be required for good organizational standing, regardless of what the policy covers or excludes, because the steps required for policy eligibility are among the federal and industry recommendations for improved cyber hygiene.

In sum, cyberinsurers limit municipalities' ability to transfer cyber risk, leaving the latter to self-insure to varying degrees. As discussed above, the self-insurance pathway is laden with transaction costs, particularly in location and coordination of grants and establishing and negotiating contracts.

26 Several interviewees warned of the federal legal restrictions around paying ransoms to foreign agents, particularly agents from countries against whom the United States has imposed sanctions.

27 Policy details remain confidential; a detailed analysis of municipal cyberinsurance expenditures and coverages is not possible at this time.

28 Bellano (2023).

Governance Considerations

This paper's exploration of transaction costs shows that there is no feasible governance arrangement in which municipalities can independently manage cyber risk. Managing cyber-physical systems at the municipal scale requires extensive contracting between public institutions and private firms; addressing product insecurities and the associated liabilities; federal, state, and local interagency coordination; and navigating dynamic political contexts. The transaction costs for these activities, while high, are unavoidable. However, creating uniformity and predictability for municipalities can lower transaction costs through standardized resource pools and contracting practices, improved device security, and reduced bureaucratic friction.

CONTRACTING WITH THIRD PARTIES

> *"Least of all do we appreciate the geometric growth of interdependencies over time where each negotiation involves a number of participants with decisions to make, whose implications ramify over time."*
>
> —*Pressman and Wildavsky (1984)*

The bulk of cyber risk management resources and capacities are beyond the reach of most municipalities,[29] thereby requiring them to turn to extensive contracting with third-party vendors. As DeNardis and Raymond (2017) write, a central public policy challenge lies in "determining what multistakeholder governance looks like in environments in which private companies make design and governance concerns inside of proprietary technical ecosystems that may not involve government, civil society, or new global institutions." They note that multistakeholder governance that involves "technologically complex infrastructures" will have higher transaction costs.[30] Renegotiations of contracts during their lifecycle also add to transaction costs.[31] The transaction costs associated with contracting (and re-contracting) outside vendors is of critical import to local governments, whose risk profile evolves as their cybersecurity posture strengthens.

Threat monitoring is a key task that municipalities can outsource to third parties. Industry practitioners and researchers all emphasized in their interviews that monitoring is essential

29 Brechbühl et al. (2010).
30 Schomaker and Bauer (2020).
31 Ibid. Also see Klijn and Koppenjan (2016).

for dealing with the impact of cyber risks, and that providing municipalities with the resources to monitor is highly valuable. Diverse non-governmental organizations provide risk mitigation services to municipalities, including the Public Infrastructure Security Cyber Education System (PISCES) and Albert Network Monitoring and Management.

PISCES and Albert

PISCES is a non-profit organization that collaborates with local governments, the private sector, and colleges and universities to provide cybersecurity monitoring to small communities in exchange for threat metadata. The metadata is monitored at the Western Washington University Poulsbo Cyber Range. PISCES also partners with academic institutions to comprehensively train students as cybersecurity analysts for entry into the cyber workforce, using the metadata collected from those public sector networks to provide operational experience with real-time event data in critical infrastructure networks.[32]

Albert is an intrusion detection system for state and local governments that monitors network traffic and sends alerts in response to suspicious activity.[33] The service can be purchased directly from the Center for Internet Security or through federal, state, and local procurement vehicles.[34]

PRODUCT LIABILITY

> *"Government can work to advance legislation to prevent technology manufacturers from disclaiming liability by contract, establishing higher standards of care for software in specific critical infrastructure entities, and driving the development of a safe harbor framework to shield from liability companies that securely develop and maintain their software products and services."*
>
> *—Jen Easterly, CISA Director*

Product security, especially in the context of interconnected smart cities infrastructure, remains a critical area for policy intervention, as policies can be used to promote security-by-design in product development and procurement.[35] Security-by-design must address

32 See https://pisces-intl.org/about/pisces

33 Albert Network Monitoring: Guarding State, Local Governments. https://www.cisecurity.org/insights/blog/albert-network-monitoring-guarding-state-local-governments

34 Procurement Contract Vehicles. https://www.cisecurity.org/services/procurement-contract-vehicles

35 Smith et al. (2021), Vitunskaite et al. (2019), Habibzadeh et al. (2019), and DeNardis and Raymond (2017).

challenges such as user privacy, international security, and issues of interoperability versus enclosure.[36] These issues are technical-legal interactions involving the "explosive growth in IoT-enabled devices and the resulting rapid increase in user data collection."[37] Amidst the lack of policy requiring built-in device security, the multitude of interdependencies between system users, technology producers, and local government officials create a precarious cyber risk profile for cities. The complexity of the digital infrastructure across sectors, and the relationships among actors, can mean that disruptions to the system can have tremendous, far-reaching consequences.[38] As mentioned in the previous section, as the number of interdependencies grows, so do the transaction costs. Moore (2010) writes that "high transaction costs could make designing contracts that assign responsibility infeasible," a key consideration in municipal cyberphysical systems where interoperability between legacy infrastructure and IoT remains an administrative and legal challenge.

Vitunskaite et al. (2019) advocate for the embedding of "security by design across all layers of the [smart city] ecosystem," including firms, supply chains, and the lifecycle of smart city infrastructures. There has also been increased federal attention to reducing device insecurity. In July 2023, the White House released the National Cybersecurity Strategy Implementation Plan. Designed as a living document, the plan offers federal agencies a roadmap for achieving two key goals: addressing the "need for more capable actors in cyberspace to bear more of the responsibility for cybersecurity" and "the need to increase incentives to make investments in long-term resilience."[39] Relatedly, CISA Director Jen Easterly has called for technology providers to prioritize product security over market release and cost concerns and to reduce reliance on security patches. Lastly, federal programs such as the Software Bill of Materials (SBOM) in Executive Order 14028 and the NIST IOT cybersecurity criteria for consumer labeling are designed to mitigate product security risks.[40]

INTERAGENCY COLLABORATION AND COORDINATION

Eric Goldstein, executive assistant director for cybersecurity at CISA, says that government and industry "haven't yet fully manifested that culture of collaboration . . . [meaning] a coequal burden on government to say, 'if we're seeing the leading indicators of an intrusion, we have

36 Smith et al. (2021) and Kalinin et al. (2021).
37 Smith et al. (2021).
38 Vitunskaite et al. (2019).
39 National Cybersecurity Strategy Implementation Plan (2023).
40 Cybersecurity White Paper: EO Response (2022).

got to make that available instantaneously to the private sector,' and the inverse needs to be true as well."[41]

There is broad awareness that effective collaboration between government entities — and between government and industry — is essential for the successful implementation of cyber risk management initiatives. Intergovernmental relationships are part and parcel of cybersecurity governance.[42] Repeated interorganizational partnerships lower transaction costs.[43] There are a multitude of shared and divergent initiatives for managing municipal cyber risk, including the National Association of State Chief Information Officers (NASCIO) recommendations for streamlining federal and state cybersecurity standards compliance protocols,[44] the Department of Homeland Security's effort to harmonize cyber incident reporting to the federal government,[45] and the creation of New York's Joint Security Operations Center (JSOC).[46] Tennessee's Comptroller of the Treasury Office launched its CyberAware program "to help local government officials protect their computer systems and educate their staff about potential cybersecurity threats," recognizing that "many local governments may lack the funding or resources necessary for implementing effective cybersecurity controls."[47] Echoing NASCIO's recommendation, some insurers believe that the federal government should first consult with state insurance regulators to avoid dual regulation,[48] an implicit argument for reducing compliance transaction costs.

Such initiatives mark important steps toward addressing a dynamic, pervasive, and long-term security challenge that affects civic functionality. These initiatives are starting to help capture and manage the broader cybersecurity transaction costs that local governments face.

GEOGRAPHIC AND POLITICAL CONSIDERATIONS

Another governance consideration is that, compared to larger cities, smaller locales are at a financial, technological, and personnel disadvantage, prompting them to rely more heavily on county, state, or federal resources to manage cyber risk. Interviewees recommended that small

41 Kelley (2023).
42 Harknett and Stever (2011).
43 Siemiatycki (2011).
44 NASCIO Advocacy Priorities (2022).
45 Harmonization of Cyber Incident Reporting to the Federal Government. Department of Homeland Security (2023).
46 "Governor Hochul Announces Formation of Joint Security Operations Center to Oversee Cybersecurity Across the State". https://its.ny.gov/press-release/governor-hochul-announces-formation
47 Tennessee Local Government Cybersecurity. https://www.tn.gov/cybersecurity/local-government-cybersecurity.html
48 Bellano (2023).

cities turn to state and federal resources to support readiness and response. However, some states, like Florida[49] and South Dakota, have rejected the provisions of the recently established federal State and Local Cybersecurity Grant Program (SLCGP). Officials in both states called some of the program's compliance requirements "invasive" and "burdensome," and noted that the program is temporary and requires states to provide matching funds.[50] Some interviewees noted that, while a local government may be willing to accept federal assistance, tensions between the state government and Washington, D.C. can create political and bureaucratic obstacles that prevent cities from accessing the resources they need. Four interviewees noted that mistrust between local, state, and federal government agencies has the potential to inhibit intergovernmental collaboration. Changes in administration (and the consequent changes in political priorities), the career and political goals of government officials, and sensitive political relationships were also cited as factors influencing the success or failure of intergovernmental initiatives. Political antipathy between different levels of government and their administrations will continue to complicate the municipal cybersecurity governance landscape.

49 Freed (2023).
50 Greig (2023).

Conclusion

Analysis of transaction costs can reveal the magnitude of the procedural requirements for implementing cyber risk management strategies. The biggest challenge that cities face is a lack of funding for technology upgrades, hiring, and administrative recommendations put forth by government and industry leaders. This compliance-based risk management context supports risk mitigation, but the required coordination, data-sharing, enforcement, and record-keeping tasks incur temporal and financial transaction costs that can impede municipal participation. In addition, compliance alone is insufficient for managing risk. Municipalities also need the resources to secure their assets. Asset protection requires good cyber hygiene, constant threat monitoring, and trained personnel who can adeptly respond to cyber threats. Risk transfer remains an especially difficult challenge for municipalities because of an unfavorable cyberinsurance market and vulnerable infrastructure.

This paper provides insights into the future of urban governance in a digital world. The public and private sectors have always worked together, but their relationship has been subject to scrutiny about legal responsibility, accountability, business interests, and ethics. Many argue that the private sector "is better [than the public sector] at performing complex technical or economic tasks, innovating and adapting to rapid change, including the ability to forsake unsuccessful enterprises."[51] Those in agreement with this view see the public sector as less agile and responsive in the face of rapid social, technological, and economic changes because of bureaucratic red tape.[52] Indeed, the financial and administrative challenges that cities face when upgrading and replacing legacy systems make the digital transformation especially burdensome.

Public-private partnerships (P3s) are a popular governance model lauded for synergizing the combinations of public and private actors and their knowledge and skills,[53] particularly in smart cities initiatives.[54] P3s have also been critiqued for their lack of transparency, high transaction costs, and "a debatable performance in terms of delivering value for money by transferring the right amount of risk to the private sector for the right price."[55] Other private sector-oriented governance models, such as New Public Management and Reinventing Government, have been

51 Nisar (2007); also see Osborne and Plastrik (1997).
52 Osborne and Gaebler (1994) and Warner (2008).
53 Klijn and Teisman (2003).
54 Meijer and Thaens (2021).
55 Hurk and Siemiatycki (2018).

widely critiqued for their assumptions about the normative role of municipal government[56] and their centering of the profit motive vis-à-vis public goods and services.[57] Despite those critiques, the reality of our municipal infrastructure and the threats it faces —compounded by the lack of cybersecurity risk mitigation and risk transfer mechanisms available — necessitates an increased private-sector role in urban governance. Transaction cost analyses will be essential in addressing these points of scrutiny and establishing equitable governance arrangements that specify and support the contributions of all parties involved. Studying the transaction costs of municipal cyber risk management illuminates the procedural requirements for initiating and sustaining the necessary governance relationships between industry and federal, state, and local governments.

56 Savas (2001) and Monstadt (2007).
57 Sagalyn (2011) and Hurk and Siemiatycki (2018).

References

"About the Municipal Cybersecurity Awareness Grant Program." Mass.gov. Accessed March 25, 2024. https://www.mass.gov/info-details/about-the-municipal-cybersecurity-awareness-grant-program.

Abrams, Lawrence. "City of Dallas hit by Royal ransomware attack impacting IT services." BleepingComputer. Last modified May 3, 2023. Accessed March 25, 2024. https://www.bleepingcomputer.com/news/security/city-of-dallas-hit-by-royal-ransomware-attack-impacting-it-services/.

"Albert Network Monitoring: Guarding State, Local Governments." Center for Internet Security. Accessed March 25, 2024. https://www.cisecurity.org/insights/blog/albert-network-monitoring-guarding-state-local-governments.

Allen, Douglas W., Transaction Costs (2000). "Encyclopedia of Law and Economics, Volume I: The History and Methodology of Law and Economics", Bouckaert and De Geest (ed) Edward Elgar, 2000.

Bellano, Anthony. "Industry Sees Need for Federal Cyber Backstop, but What Model is Best?" Best's Review, February 2023, 28-33.

Brechbühl, Hans, Robert Bruce, Scott Dynes, and M. Eric Johnson. 2010. "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy." Information Technology for Development. Informa UK Limited. doi:10.1002/itdj.20096.

Casady, Carter B., Ole Helby Petersen, and Lena Brogaard. 2023. "Public Procurement Failure: The Role of Transaction Costs and Government Capacity in Procurement Cancellations." Public Management Review. Informa UK Limited. doi:10.1080/14719037.2023.2231945.

Cybersecurity and Infrastructure Security Agency, #StopRansomware Guide, Doc. (Sept. 2020).

Deere, Stephen. "CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million." Atlanta Journal-Constitution, August 1, 2018. Accessed March 25, 2024. https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXSoK/.

DeNardis, Laura and Raymond, Mark, The Internet of Things as a Global Policy Frontier (December 10, 2017). UC Davis Law Review, Vol. 51, No. 2, 2017.

Department of Homeland Security. Harmonization of Cyber Incident Reporting to the Federal Government. N.p., 2023.

Duncan, Ian. "Baltimore IT director who was at helm during ransomware attack and city's recovery is on leave." Baltimore Sun, September 10, 2019. Accessed March 25, 2024. https://www.baltimoresun.com/2019/09/10/baltimore-it-director-who-was-at-helm-during-ransomware-attack-and-citys-recovery-is-on-leave/.

Fernandez, Manny, David Sanger, and Marina Trahan Martinez. "Ransomware Attacks Are Testing Resolve of Cities Across America." New York Times, August 22, 2019. Accessed March 25, 2024. https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html.

Freed, Benjamin. "Cyber grant money is beginning to flow, CISA officials say." Statescoop. Last modified February 10, 2023. Accessed March 25, 2024. https://statescoop.com/state-local-cyber-grants-cisa/.

Greig, Jonathan. "All but Florida, South Dakota apply for federal cyber grants allocated by infrastructure bill." The Record. Last modified February 10, 2023. Accessed March 25, 2024. https://therecord.media/all-but-florida-south-dakota-apply-for-federal-cyber-grants-allocated-by-infrastructure-bill

Greig, Jonathan. "An inside look into states' efforts to ban gov't ransomware payments." The Record. Last modified August 22, 2022. Accessed March 25, 2024. https://therecord.media/an-inside-look-into-states-efforts-to-ban-govt-ransomware-payments.

"Governor Hochul Announces Formation of Joint Security Operations Center to Oversee Cybersecurity Across the State." New York State Office of Information Technology Services. Last modified February 22, 2022. Accessed March 25, 2024. https://its.ny.gov/press-release/governor-hochul-announces-formation.

Habibzadeh, Hadi, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, and Tolga Soyata. 2019. "A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities." Sustainable Cities and Society. Elsevier BV. doi:10.1016/j.scs.2019.101660.

Harknett, Richard J., and James A. Stever. "The New Policy World of Cybersecurity." Public Administration Review 71, no. 3 (2011): 455–60. http://www.jstor.org/stable/23017502.

Hurk, Martijn van den, and Matti Siemiatycki. 2018. "Public–Private Partnerships and the Design Process: Consequences for Architects and City Building." International Journal of Urban and Regional Research. Wiley. doi:10.1111/1468-2427.12629.

International City/County Management Association, and University of Maryland, Baltimore County. Cybersecurity 2016 Survey Summary Report of Survey Results. N.p., 2016.

Kalinin, Maxim, Vasiliy Krundyshev, and Peter Zegzhda. 2021. "Cybersecurity Risk Assessment in Smart City Infrastructures." Machines. MDPI AG. doi:10.3390/machines9040078.

Kelley, Alexandra. "Cyber investments aim to paint broader view of digital threats, official says." Nextgov. Last modified October 10, 2023. Accessed March 25, 2024. https://www.nextgov.com/cybersecurity/2023/10/cyber-investments-aim-paint-broader-view-digital-threats-official-says/391088/.

Kesan, Jay P., and Linfeng Zhang. 2021. "An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses." IEEE Transactions on

Emerging Topics in Computing. Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/tetc.2019.2915098.

Klijn, Erik Hans, and Joop Koppenjan. 2016. "The Impact of Contract Characteristics on the Performance of Public–Private Partnerships (PPPs)." Public Money & Management. Informa UK Limited. doi:10.1080/09540962.2016.1206756.

"Local Government Cybersecurity." Tennessee State Government. Accessed March 25, 2024. https://www.tn.gov/cybersecurity/local-government-cybersecurity.html.

Macher, Jeffrey T., and Barak D. Richman. 2008. "Transaction Cost Economics: An Assessment of Empirical Research in the Social Sciences." Business and Politics. Cambridge University Press (CUP). doi:10.2202/1469-3569.1210.

Monstadt, Jochen. 2007. "Urban Governance and the Transition of Energy Systems: Institutional Change and Shifting Energy and Climate Policies in Berlin." International Journal of Urban and Regional Research. Wiley. doi:10.1111/j.1468-2427.2007.00725.x.

National Association of State Chief Information Officers. Memorandum, "Harmonize Disparate Federal Cybersecurity Regulations," 2022.

National Institute of Standards and Technology. 2022. "Cybersecurity White Paper: EO Response." https://doi.org/10.6028/nist.cswp.02042022-2.

National Institute of Standards and Technology. 2024. "The NIST Cybersecurity Framework (CSF) 2.0." doi:10.6028/nist.cswp.29.

Niehans, Jürg. "The New Palgrave: A Dictionary of Economics, Eatwell, J., Milgate, M. ve Newman, P." (1987).

Nisar, Tahir M. 2006. "Risk Management in Public–Private Partnership Contracts." Public Organization Review. Springer Science and Business Media LLC. doi:10.1007/s11115-006-0020-1.

Nurse, Jason R. C., Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese. "The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes." 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2020): 1-8.

Osborne, David, and Ted Gaebler. 1994. "Reinventing Government: How the Entrepreneurial Spirit Is Transforming the Public Sector." London, England: Addison Wesley.

Osborne, David, and Peter Plastrik. 1997. "Banishing Bureaucracy: Five Strategies for Reinventing Government." Boulder, CO: Perseus Books.

Pattison-Gordon, Jule. "Local Governments Seek Other Options Amid Cyber Insurance Woes." Governing. Last modified May 15, 2022. Accessed March 25, 2024. https://www.governing.com/security/local-governments-seek-other-options-amid-cyber-insurance-woes.

Pressman, Jeffrey L., and Aaron Wildavsky. 1984. Implementation: How Great Expectations in Washington Are Dashed in Oakland; Or, Why It's Amazing That Federal Programs Work

at All, This Being a Saga of the Economic Development Administration as Told by Two Sympathetic Observers Who Seek to Build Morals on a Foundation. 3rd ed. Berkeley, CA: University of California Press.

"Procurement Contract Vehicles." Center for Internet Security. Accessed March 25, 2024. https://www.cisecurity.org/services/procurement-contract-vehicles.

Quinn, Stephen. 2023. "Enterprise Impact of Information and Communications Technology Risk:" National Institute of Standards and Technology. doi:10.6028/nist.sp.800-221.

Riotta, Chris. "The White House is developing a 10-year modernization plan to replace legacy IT." Nextgov. Last modified August 15, 2023. Accessed March 25, 2024. https://www.nextgov.com/modernization/2023/08/white-house-developing-10-year-modernization-plan-replace-legacy-it/389438/.

Romanosky, Sasha. 2016. "Examining the Costs and Causes of Cyber Incidents." Journal of Cybersecurity. Oxford University Press (OUP). doi:10.1093/cybsec/tyw001.

Sagalyn, Lynne B. 2011. "Chapter 12. Public-Private Partnerships and Urban Governance: Coordinates and Policy Issues." Global Urbanization. University of Pennsylvania Press. doi:10.9783/9780812204476.191.

Savas, E. S. "Privatization and the New Public Management." Fordham Urban Law Journal 28, no. 5 (2001).

Schomaker, Rahel M., and Christian Bauer. 2020. "Trust and Transaction Costs in Public–Private Partnerships—Theoretical Reflections and Empirical Findings." Public Money & Management. Informa UK Limited. doi:10.1080/09540962.2020.1801882.

Siemiatycki, Matti. 2011. "Public-Private Partnership Networks: Exploring Business-Government Relationships in United Kingdom Transportation Projects." Economic Geography. Wiley. doi:10.1111/j.1944-8287.2011.01115.x.

Sierra, Stephanie. "Man says fraudulent accounts opened, home purchased in his name after city ransomware hack." Eyewitness News ABC 7. Last modified December 27, 2023. Accessed March 25, 2024. https://abc7.com/oakland-california-ransomware-attack-cyber-identity-theft/14228972/.

Smith, Kane J., Gurpreet Dhillon, and Lemuria Carter. 2021. "User Values and the Development of a Cybersecurity Public Policy for the IoT." International Journal of Information Management. Elsevier BV. doi:10.1016/j.ijinfomgt.2020.102123.

Stavins, Robert N. 1995. "Transaction Costs and Tradeable Permits." Journal of Environmental Economics and Management. Elsevier BV. doi:10.1006/jeem.1995.1036.

Terman, Jessica N. 2023. Third-Party Governance: Using Third Parties to Deliver Governmental Goods and Services. New York: Routledge.

The White House. National Cybersecurity Strategy Implementation Plan, 2023. N.p., 2023.

Vitunskaite, Morta, Ying He, Thomas Brandstetter, and Helge Janicke. 2019. "Smart Cities and Cyber Security: Are We There yet? A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership." Computers & Security. Elsevier BV. doi:10.1016/j.cose.2019.02.009.

Warner, Mildred E. "Reversing privatization, rebalancing government reform: Markets, deliberation and planning." Policy and Society 27, no. 2 (2008): 163-174.

"What is PISCES?" PISCES. Accessed March 25, 2024. https://pisces-intl.org/about/pisces.

Whittington, Jan. 2012. "When to Partner for Public Infrastructure?" Journal of the American Planning Association. Informa UK Limited. doi:10.1080/01944363.2012.715510.

Williamson, Oliver E. "The economics of organization: The transaction cost approach." American Journal of Sociology 87, no. 3 (1981): 548-577.

Wolff, Josephine. 2022. "Cyberinsurance Policy." The MIT Press. doi:10.7551/mitpress/13665.001.0001.

Acknowledgments

I would like to thank the following organizations and individuals who provided assistance with this report: The Center for Long-Term Cybersecurity provided generous financial support and professional guidance. Andrew Reddie, PhD., Anne Cleaveland, PhD., Karen Trapenberg Frick, PhD., Lisa Ho, Shanti Corrigan, and Charles Kapelke all kindly provided research guidance and helped connect me with cybersecurity experts. To Mike Hamilton of Critical Insight, your professional experience and feedback played a crucial role in the success of this project. The interviewees shared invaluable information that helped clarify and refine the contours of this effort. I also thank the RSAC Scholars Program for their help in establishing contacts in the cybersecurity community.

About the Author

Rowland Awadagin Herbert-Faulkner is a PhD Candidate in the Department of City and Regional Planning at the University of California, Berkeley. His dissertation research focuses on technology governance at the municipal and regional scales.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley