CYBERSECURITY AND LOCAL GOVERNMENT

DONALD F NORRIS • LAURA K MATECZUN
RICHARD F FORNO

WILEY

Cybersecurity and Local Government

Cybersecurity and Local Government

Donald F. Norris

Laura K. Mateczun

Richard F. Forno

WILEY

This edition first published 2022

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office
The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Norris, Donald F., author. | Mateczun, Laura, author. | Forno, Richard, author.
Title: Cybersecurity and local government / Donald F. Norris, Laura Mateczun, Richard F. Forno.
Description: Hoboken, NJ : John Wiley & Sons, 2022. | Includes bibliographical references and index. | Contents: Why local government cybersecurity? -- What is cybersecurity? -- Cybersecurity 101 for local governments -- What the literature tells us about local government cybersecurity -- Cyberattacks on local government -- Managing local government cybersecurity -- Cybersecurity policies local government s should adopt -- People: The root of the problem -- The NIST Framework demystified -- Cybersecurity law -- Important questions to ask -- The future of local government cybersecurity -- Summary and recommendations.
Identifiers: LCCN 2022004676 (print) | LCCN 2022004677 (ebook) | ISBN 9781119788287 (hardback) | ISBN 9781119788294 (pdf) | ISBN 9781119788300 (epub) | ISBN 9781119788317 (ebook)
Subjects: LCSH: Local government--United States. | Computer security--United States.
Classification: LCC JS331 .N65 2022 (print) | LCC JS331 (ebook) | DDC 320.8/50973--dc23/eng/20220213
LC record available at https://lccn.loc.gov/2022004676
LC ebook record available at https://lccn.loc.gov/2022004677

Cover image: Images courtesy of Siemens Energy
Cover design by Wiley

Set in 9.5/12.5pt STIXTwoText by Integra Software Services Pvt. Ltd, Pondicherry, India

Dedication

This book is dedicated to the officials, staff, and volunteers working cybersecurity in local governments across the USA and around the world. Theirs is one of the most important jobs in local government (really, in almost all organizations) today. And in their case, it's often a thankless task played out in an especially challenging environment. They have our deepest appreciation, respect, and thanks!

Contents

Preface

The highest purpose of any government is to ensure the safety, security, and well-being of its citizens. From providing day-to-day services like business licenses, utilities, emergency services, and processing tax payments, to ensuring an effective response to weather events, disasters, or (hopefully) one-off existential events like the COVID-19 pandemic, local governments truly are at the center of it all. So the old adage that "all politics is local" certainly rings true.

The innovations and conveniences of internet technologies, along with the evolving expectations of a networked society and workplace since the 1990s, has led to a reliance on information technology in nearly every facet of modern life. These tools and platforms have permeated our society, including how local governments operate internally and provide external services to their communities. Yet hardly a day goes by without news reports about how local governments were victimized, if not crippled, by cyberattacks launched by criminals or international adversaries. Therefore, ensuring the ability of government to function and deliver services to its citizens in an available, secure, and trusted manner is more important than ever. In other words, regardless of whether you're an elected leader, senior manager, or rank-and-file employee within local government, the importance of implementing and maintaining strong cybersecurity measures and practices within your purview cannot be overstated.

But providing effective cybersecurity isn't an easy task for any type of organization, and local governments, as political creatures, have unique attributes that can make this process even more challenging. *Cybersecurity and Local Government* is intended to help these often beleaguered local government officials enhance, or in some cases, *establish*, the necessary measures to protect their information systems and preserve their ability to continue delivering services to their communities.

To accomplish this, we begin by discussing the need for cybersecurity and why it's a particularly important concern for local governments. While ongoing news headlines about cities held hostage by ransomware are easy to point at to illustrate the severity of this issue and need for strong local government cybersecurity, as researchers we are required to base analysis upon data and other reputable evidence. Thus, much of *Cybersecurity and Local Government* centers around the findings of two separate nationwide surveys (conducted in 2016 and 2020) of local government IT and cybersecurity leaders. This deep-dive into America's grassroots provided a useful and realistic

understanding of America's local government cybersecurity – or lack thereof – upon which we could then base recommendations on. **Sadly, in several ways, it's not a pretty picture.**

After confirming the tenuous state of local government cybersecurity in the US, the logical follow-on question is: what can be done to improve things? We answer that by offering multiple recommendations based on current and time-proven industry best practices for local government officials to consider implementing. In doing so, we emphasize that from budgets, staffing, and political considerations to policies, procedures, and training, local government cybersecurity is a complex and nuanced issue and one that technology alone can't remedy. Indeed, we devote an entire chapter presenting people as the root of most cybersecurity problems.

While much of the book tends to be retrospective and focuses on things from the past, we conclude *Cybersecurity and Local Government* by looking into the future. What are the trends in technology most likely to present cybersecurity concerns for networked organizations like local governments? How will the threat landscape change? And of course, how can local governments adapt their cybersecurity thinking to reflect shifts in society due to COVID-19, such as remote work and providing expanded online citizen services? While we certainly don't claim to have all the answers – or indeed know all the questions – we are convinced that *Cybersecurity and Local Government* provides local government readers a solid resource to consult when they are looking to establish or enhance their respective cybersecurity programs.

Twenty years after the internet revolutionized the world, it's unfortunate that any modern organization – and especially local governments – still needs to be advised about implementing effective cybersecurity. While cybersecurity professionals may find this a distressing reality, upon closer reflection, this itself may be a useful lesson in cybersecurity for everyone: no matter how fast the world moves, or how complex the issues at hand, the protection of information and information resources is a necessary enabler of modern society. This is especially true for local governments and their ability to provide trusted services to their local communities.

- Don, Laura, and Rick

About the Authors

Donald F. Norris, PhD, is Professor Emeritus of Public Policy at the University of Maryland, Baltimore County. He retired from UMBC in 2017 after serving twenty-seven years as Director of the Maryland Institute for Policy Analysis and Research and ten years as Director of the UMBC School of Public Policy. His fields of study include: (1) public management, where he specializes in information technology in governmental organizations, including e-government and cybersecurity; and (2) urban affairs broadly, but with specific attention to metropolitan governance. Dr. Norris has published seven books, thirty-seven articles in refereed journals, twenty-five chapters in books, and fourteen papers in refereed conference proceedings. His most recent scholarly works appeared in *Public Administration Review* in 2019 and the *Journal of Urban Affairs* in 2020 (online) and 2021 (in print). The data for these papers came from the first nationwide survey of local government cybersecurity and was conducted by UMBC scholars in partnership with the International City/County Management Association (ICMA). Dr. Norris received a BS in history from the University of Memphis and an MA and a PhD in political science from University of Virginia. He can be reached at: norris@umbc.edu.

Laura K. Mateczun, JD, is a PhD student in the School of Public Policy at the University of Maryland, Baltimore County where she is writing her dissertation on local government cybersecurity. She received a Graduate Certificate in Cybersecurity Strategy and Policy from UMBC in 2021. She has also co-authored four peer-reviewed articles based on the results of the first-ever nationwide survey on local government cybersecurity. Her policy interests are interdisciplinary in nature and span fields from public management to criminal justice and cybersecurity. She is a 2014 graduate of the University of Maryland, Francis King Carey School of Law and is a member of the Maryland Bar. Laura received a BA in public policy and political science from St. Mary's College of Maryland in 2011. She can be reached at: lam6@umbc.edu.

Richard F. Forno, PhD, is a principal lecturer in the UMBC Department of Computer Science and Electrical Engineering, where he directs the UMBC Graduate Cybersecurity Program and serves as the assistant director of UMBC's Center for Cybersecurity. His twenty-year career in operational cybersecurity before academia spans the government, military, and private sectors in both technical and management roles, including helping

to build a formal cybersecurity program for the US House of Representatives, serving as the first Chief Security Officer for Network Solutions (then, the global center of the internet DNS system), consulting to Fortune 100 companies, and more. Dr. Forno holds degrees in international relations from American University and Salve Regina University, and is a graduate of Valley Forge Military College and the United States Naval War College. His doctoral research at Curtin University of Technology explored the complex nature of security informatics and risk communication for internet-based organizations, and as one of the early thought leaders on cyberwarfare, he continues to research, write, and speak about resiliency and the influence of internet technology upon global society. He can be reached at: rforno@umbc.edu

1

Why Local Government Cybersecurity?

This book begins with a simple question: why examine cybersecurity among America's local (or grassroots) governments? What's so special about these organizations that they deserve scrutiny? They are, after all, just organizations, and most, if not all organizations have certain similarities, especially the need to maintain effective levels of cybersecurity.

The need for cybersecurity is demonstrated every day and is a common staple in the popular media. And local governments do not differ much, if any, in the need for cybersecurity from organizations such as Microsoft, Target, Home Depot, JPMorgan Chase, the White House, or many others. The similarity to which readers should be aware is that *all* of these organizations have been successfully hacked...as has a growing number of local governments.

1.1 Most Important Reason

Perhaps the most important reason that cybersecurity among local governments warrants our attention is that these governments are increasingly targets of cybercriminals and are under constant, or nearly constant, attack (Norris et al., 2018, 2019, 2020). Moreover, aside from relatively few studies, little is known about the specific vulnerabilities, exposures, practices, and shortcoming of local governments in this matter – yet every local government cybersecurity official who one of the authors (Norris) helped interview in 2013 agreed that their governments were under constant attack. Among local governments responding to a survey that two of the authors (Norris and Mateczun) helped conduct in 2016, 28 percent reported being attacked at least hourly or more frequently, and 19 percent said at least once a day (for a total of 47 percent of all respondents). What is really troubling, however, is that more than a quarter (nearly 28 percent) said that they *did not know how frequently they were being attacked* (Norris et al., 2019).

Among local government Chief Information Security Officers (CISOs) responding to a 2020 survey of mainly large US local governments, 57 percent said that they were under attack constantly, 29 percent said at least hourly, and 14 percent said daily (Norris, 2021). Last, the frequency and severity of cyberattacks against local governments is expected to continue to grow, not to abate, because these governments have become favorite targets of cybercriminals. A reason for this undesirable outcome is that while many

Cybersecurity and Local Government, First Edition. Donald F. Norris, Laura K. Mateczun and Richard F. Forno.

organizations, on average, typically do a poor job with cybersecurity, local governments do it even more poorly.

1.2 Additional Reasons

There are other reasons to be concerned about cybersecurity among local governments. The first is the sheer number of American local governments. As of the 2017 Census of Governments, there were 90,074 units of local government, of which 38,779 are general purpose governments, including 3031 counties, 19,519 municipalities and 16,360 towns and townships. There were also 38,542 special districts, most of which are single purpose districts providing such services as fire protection (5975), potable water (3593), drainage/flood control (3344), etc. Last, there were 12,754 independent public school districts (US Census Bureau, 2017). Taken together, this represents a *lot* of governments, especially considering that there are only 50 states and one federal government in the US.

A related point is that most general purpose (municipalities, counties, townships) local governments in the US are small. Around three-quarters of the nation's incorporated places had fewer than 5000 residents in 2020 (Toukabri and Medina, 2020). Moreover, the great majority of American cities (78 percent) have populations of 10,000 or less (ICMA, 2013). This does not include the 12,801 municipalities with populations of less than 2500, which constituted 47 percent of all cities in 2017 (Miller, 2018; see also Chapter 13). And, because of their size, small local governments are faced with budgetary constraints not typically experienced by large local governments like those of big cities and counties. This is one reason smaller local governments are unable to to fund adequate levels of cybersecurity. See Table 1.1 that shows the dramatic differences in municipalities by population, with the vast majority (80 percent) having populations of 10,000 or less, not including the number with fewer than 2500 inhabitants (ICMA, 2015). The distribution of county governments is somewhat similar, although not quite as skewed toward those with very small populations.

Except for the smallest among them, local governments operate information technology (IT) systems that are critical to their ability to function and to provide services to their residents. Cumulatively, they spend billions of dollars each year to support their IT systems. One estimate placed state and local government spending on information technology at over $109 billion per year (GovDataDownload, 2019).

Second, local governments provide essential, often critical public services to their residents and visitors. Consider the following and their importance to the daily lives of everyone involved: public safety (police and fire especially), the courts, election systems, emergency medical services, water provision and wastewater collection and treatment, and emergency and disaster management. Disrupting any of these services or shutting them down altogether would produce serious consequences for local governments. Modern cybercriminals know this and target local governments to steal from them and/or impede their ability to function. As of this book's writing, September of 2021,[1] the

Table 1.1 Cumulative distribution of US municipalities (over 2500) and counties (all).

Municipalities		Counties	
Over 1 Million	9	Over 1 Million	33
500,000 to 1 Million	25	500,000 to 1 Million	73
250,000 to 499,999	42	250,000 to 499,999	124
100,000 to 249,999	208	100,000 to 249,999	296
50,000 to 99,999	486	50,000 to 99,999	390
25,000 to 49,999	888	25,000 to 49,999	614
10,000 to 24,999	1939	10,000 to 24,999	828
5,000 to 9,999	1934	5000 to 9999	379
2500 to 4,999	1993	2500 to 4999	164
		Under 2500	130
Total	7524		3031

Source: ICMA (2013). The Municipal Yearbook 2013. Tables 2 and 3, pp. xii and xv.

most recent trend in cyberattacks against local governments involves ransomware. Such attacks are when a cybercriminal obtains access to a local government IT system, locks it down, encrypts its data, and demands payment (ransom, often in the form of cryptocurrency) for the promised return the IT system and its data to the local government unharmed.[2]

In 2018 and 2019, respectively, Atlanta, Georgia and Baltimore, Maryland were victims of ransomware attacks that, among other things, caused considerable disruption of their ability to perform basic functions and provide public services. (Brief discussions of the incidents in Atlanta and Baltimore appear later in this chapter.)

A third reason to examine cybersecurity among America's local governments is that they receive, utilize, and store volumes of sensitive information, especially personally identifiable information (PII) such as names, addresses, drivers' license numbers, credit card numbers, social security numbers, tax records, and medical information. Such information is valuable to cybercriminals and obtaining it is often the purpose of cyberattacks. In fact, over the past few years, numerous local governments have reported that they lost at least some of their PII as a result of data breaches and subsequent information exfiltration. In some cases, they were threatened with the data being released (or destroyed) unless they paid a ransom.

As noted earlier, in many ways local governments are quite similar to other types of organizations in both the public and private sectors. True enough, but they also have characteristics that set them apart in ways that challenge their ability to provide high levels of cybersecurity. This represents the fourth reason for this book's direct focus on local government cybersecurity.

These characteristics include but are not limited to the fact that local governments are *public* entities that provide *public* services; they are subject to politics in ways that private

sector entities are not; their structure is often federated; there is never enough money in a local government's budget to cover all needs (real and perceived); and finally their residents are essentially their owners. We will address each of these characteristics briefly below.

Local governments are *public* entities that provide *public* services. This means that the "bottom line" is not quarterly or annual profits and maximizing shareholder returns, but rather the delivery of a wide variety of services such as those noted above and others. Few private sector businesses have as wide a span of responsibilities. And, within local governments, each separate function or service competes with all the rest for attention, funding, and cybersecurity.

This is where politics (both the good, the bad, and the ugly) comes in. Decision-making in local governments involves small "p" politics (so to speak) in the sense of choosing among available and fundable alternatives. One hopes that such decision-making is a more or less rational process, and that it is driven by evidence and objective analysis. Unfortunately, decisions in local government are often also driven by large "P" politics. Here, the interests of the chief elected officials and the elected councilors may clash because of political party, ideology, or electoral interests, having little to do with what is best for the city or county at that moment or in the future. Certainly, there is politics in private firms, but at the end of the day firms measure success by the financial bottom line. Local governments have no such simple metric, and each official has his or her own view of success, often involving what is politically convenient for the official. This means that the calculations made by officials when choosing among alternatives (small "p") are often colored by large "P" factors.

The structure of local governments is typically federated among executive, legislative, and judicial branches (although courts play a more limited role in local government administration than at the state and federal levels). In a private business, what the CEO, board chairman, or owner of a firm decides is final and employees must abide by that decision or policy. This not to say that there may be spirited discussion and debate within the organization, but it is those leaders' sole responsibility to make the decision. By contrast, in local governments, even those with structurally powerful elected executives, decisions often are made by parties in least two different and often competing branches of government (and a third if the courts are involved). In mayor-council cities, these are the mayor and city council. In council-manager cities, the chief decision-maker for city administration is the city manager, but he or she must act within the bounds of policy adopted by the city council. And council members often have differing views regarding alternative policies and courses of administration. This makes for a decision-making process in the public sector that is very different from that of the private sector (e.g., Allison, 1983).

Additionally, there is never enough money in a local government's budget to cover all needs (real and perceived) throughout the organization. Indeed, lack of adequate funding is nearly always the number one complaint heard from Chief Information Officers (CIOs) and CISOs (Norris et al., 2019, 2020). This is almost certainly true of many private sector businesses as well, but few of them have as many different and competing functions to perform and services to provide as local government. To give a perhaps overly simplistic example, General Motors builds cars, and GM dealerships sell cars and repair cars. Yet both singularly focus all of their efforts on cars.

Cumulatively, these characteristics mean that providing high levels of cybersecurity in local governments is more complex and more difficult than in private sector organizations. They also provide good reasons to closely examine local government cybersecurity and to provide recommendations to help improve it (as this book does).

Fifth, cybercriminals have become increasingly successful in hacking both private and public sector organizations in recent years. Among many others, these have included in the private sector: Home Depot, Target, JPMorgan Chase, AT&T, Yahoo, eBay, Google, Anthem, Equifax, SolarWinds, Microsoft, and others. In the federal government: the Office of Personnel Management (OPM), US Central Command, the US Postal Service, the White House, the National Oceanic and Atmospheric Administration (NOAA), and others. Among local governments: the cities of Atlanta, Baltimore, Dallas, and New Orleans, the city and county governments of Durham, NC, and many more. A simple scan of daily headlines continues to demonstrate that all types of organizations from the government and private sector remain under active cyberattack.

Sixth, cyberattacks are deployed not only by individuals and organizations, but also by nation-states and their surrogates and by transnational, non-state actors such as terrorists. One of the clearest and most frightening examples is the ongoing "meddling" in US elections by the Russian government. Here, American intelligence agencies have unanimously concluded that hackers under the control and by the direction of the Russian government interfered in the 2016 American presidential election with the intent of helping Donald Trump, the Republican nominee, become president. Indeed, since 2016, American intelligence agencies continue to identify active Russian efforts to use cyberattacks (e.g., hacking) in supporting traditional influence activities such as misinformation and disinformation intended to interfere with America's domestic elections.

Hacking by nation-states also reaches down to the local government level. In the ransomware attack in March of 2020 against the city and county governments of Durham, NC, cybercriminals deployed malware of Russian origin. According to the North Carolina State Bureau of Investigations, the attack was the work of Russian hackers using the Ryuk malware delivered via phishing emails (Ropek, 2020). This is the same malware that took down the City of New Orleans IT system in 2019.

Seventh, cyberattacks are very costly to the US and world economies. Cybersecurity Ventures estimates that by 2025 the annual cost of data breaches will reach $10.5 trillion worldwide, up from $3 trillion in 2015, and would represent the greatest transfer of economic wealth in history (Morgan, 2020). As discussed below, the attacks on Atlanta and Baltimore cost those cities at least $17 and $18 million, respectively, not including the cost of lost productivity. These are only two of many local governments that have experienced breaches recently. Expect more to be similarly impacted in coming years.

Eighth, The Internet of Things (IoT), also called "cyber-physical systems," is a rapidly expanding phenomenon that introduces new vulnerabilities and risks for local governments. In many cases, this is evidenced through initiatives aimed at creating "smart cities" that deploy internet-connected devices to sense, collect, and share data and in some cases, directly control physical systems, for improved monitoring and management of assets and resources. To provide a sense of the enormity of the IoT, the research firm Statistica estimated that there would be 13.8 billion IoT and non-IoT devices connected to the internet in 2021. This was expected to more than double to

30.9 billion by 2025 (2021). By contrast, just a few years ago, a typical US household with broadband internet service had one or two computers connected. According to one source, in 2020 such homes had a Wi-Fi router connecting 12 devices that include computers, televisions, thermostats and smoke alarms, security cameras and smart speakers like Amazon Echo, which is expected to increase to 20 by 2025 (Parks Associates, 2020).

Local governments increasingly use IoT devices to better support their services, such as monitoring traffic and parking, detecting rubbish levels in trash receptacles, smart meters, and security cameras. Moreover, as they increasingly manage "smart" cyber-physical systems, such as wastewater, electricity, etc., the consequences of poor defense are more than just data breaches or system failures – they now include physical harm and damage to the community.

For local governments, the spread of IoT devices greatly increases the "attack surface" that makes them vulnerable to cybersecurity threats.[3] This attack surface was expanded significantly with local government employees working from home during the COVID-19 pandemic of 2020–2022. Moreover, the set of IoT devices and cyber-physical systems may be large and very heterogeneous, with different manufacturers, capabilities, and interfaces. The result is an environment that is inherently difficult to monitor and update as new security vulnerabilities are discovered.

One prominent risk is that some IoT devices could be infected and used to launch Distributed Denial of Service (DDoS) attacks on internet services and sites. For example, in 2016 the Mirai Botnet compromised as many as 600,000 IoT devices and used these to attack and disable several popular internet sites (Antonakakis et al., 2017). Other risks are that such devices can be disabled, have their sensor data stolen or modified, or have their activator functions used inappropriately that could result in damage. Before incorporating IoT technologies, local governments must understand and plan for the additional security risks they introduce by developing and supporting policies that will protect them from current and future threats.[4]

Ninth, the expanded attack surface arising from the shift to working from home is yet another reason local government cybersecurity warrants attention. Working from home strains computer networks and poses additional risks such as the use of insecure Wi-Fi networks and the use of personal devices when working with sensitive information. COVID-19 and other disasters bring a surge of phishing attacks, often bearing ransomware, and these only become worse with the enlarged attack surface from working at home. Cybercriminals take advantage of both the trends of the day and the human element of cybersecurity.

Cybersecurity officials are mission enablers regardless of the type of organization for which they work. For local governments in times of disaster, this means cyber staff must preserve the use of technology, protect the organization's information assets wherever they might be located, and help to provide the continuous operational capability for the many critical functions of the organization that rely on technology. Their focus also needs to be on resilience during disaster, which means not only the ability to prevent a cyberattack and, if necessary, to stop a successful one, but also to recover from it while continuing critical operations in as normal a manner as possible.

Finally, as discussed elsewhere in this book, there is an enormous gap in the scholarly and professional publications on the subject of local government cybersecurity. Indeed, the extensive literature review conducted in preparation for this book identified only 14 articles about local government cybersecurity in peer-reviewed journals in the social sciences and computer science between 2000 and summer 2021 – a problem that may begin to be at least partly rectified with this book (Appendix 1.1). Likewise, this search found very few works in the professional literature directly discussing local government cybersecurity. This said, many works from the professional world are relevant to local governments, especially those that discuss common cybersecurity problems and best cybersecurity practices.

1.3 Case Studies

This chapter next examines two cases of notable instances of local governments that were successfully hacked, including Baltimore, MD and Atlanta, GA. These examples were selected to demonstrate the current state of local government cybersecurity and the impact that a successful cyberattack can have upon local communities that are not properly prepared for them.

Case 1.1 Atlanta and the Two Iranians

Atlanta, GA, a city with a population of nearly 500,000 in a metropolitan area of almost 6 million has the distinction of being hacked, according to the US Justice Department which indicted them, by two Iranians (Deere, 2018c). Although the nationality of the hackers mattered little to Atlanta officials and residents at the time, that the city's computer system had been taken down in a ransomware attack mattered significantly. The attack occurred, or rather, was discovered, on March 22, 2018, although it could have been going on much longer.

Atlanta's attackers used a ransomware known as SamSam in a "brute force" attack against the city's IT system (Colorado Computer Support (CCS), 2018). In such an attack, the attacker repeatedly runs passwords against elements of an IT system until it finds a match and, upon successfully logging into the network, inserts the malware into the system. These attacks can occur over weeks or even months. Unfortunately, whatever method is employed, attackers often succeed, get into a target's system, remain there doing their damage until detected and removed.

The city initially reported that the attack had taken down the municipal court system, the city's email, water, and traffic ticket payment systems, and Wi-Fi at Hartsfield-Jackson International Airport (Blinder and Perlroth, 2018). Dashboard camera videos from police cars were destroyed (Freed, 2019). Later, officials discovered that financial, customer relationship management, and service desk systems were affected along with the data associated with them, and several years' worth of officials' and employees' correspondence had been lost (Freed, 2019). The attackers

demanded a ransom in Bitcoin equal to about $51,000, but the city chose not to pay and instead began to remove the malware and get their systems back up and running again. No small task, it turned out.

In April, the city paid $2.7 million for contracts with cybersecurity and communications firms to assist in their recovery efforts (Deere, 2018a). Over time, the city's estimated recovery costs were $9.5 million (Kearney, 2018), and, later still, the full cost of the recovery, not including lost city productivity, was estimated to be $17 million (Deere, 2018b). However, by June of 2018, about one-third of software programs the city relied on still were partly or completely unusable. And, as much as a year later, the city's systems were not fully restored, and the city was still in the process of improving its cybersecurity program (Freed, 2019).

What went so wrong in Atlanta? The answer appears to be at once simple and complex. The simple part is found in three reports on the city IT system from the city auditor. These reports, dated 2010, 2014, and 2018, found numerous weaknesses and vulnerabilities in Atlanta's IT system, including up to 2000 "severe vulnerabilities" discovered by monthly vulnerability scans. Many of the vulnerabilities identified were *over a year old* and the report found "no evidence of mitigation of the underlying issues" (Deere, 2018b). The final report also found evidence of "ad hoc and undocumented [security] processes," and almost 100 servers using a version of Windows that Microsoft no longer supported (Freed, 2019). These findings are damning and strongly suggest that Atlanta's IT department was guilty of both IT and cybersecurity malpractice. Indeed, one cybersecurity expert suggested as much by saying that negligence was likely involved (Deere & Klepal, 2018)

The complex part, which at least partially excuses the IT department, is found in the then new mayor's acknowledgement that cybersecurity had not been a city priority. Clearly, the auditor's reports had not gained traction with city elected officials and top management or their findings would have been taken seriously and efforts necessary to fix a demonstrably broken and vulnerable IT system would have been underway. Making such efforts, however, is not simple for local governments. Cybersecurity is expensive and competes with many other needs, both real and perceived. To complicate matters, local governments never have enough money to meet all needs and must choose which ones are funded, especially in times of severe economic downturns (such as the great recession of 2007–2009 and the brief COVID-19 recession of 2020). This is where politics (or making choices in order to govern) gets involved and often makes a complex situation even more confusing. Not to mention, politicians almost always favor funding of highly visible things like education, public safety, and other needs than things like cybersecurity that no one ever sees; that is, until there is a cybersecurity incident with its corresponding cost, chaos, and adverse media publicity.

Case 1.2 Baltimore and Robbinhood

Baltimore, MD, a city with a population of 600,000 residents in a metropolitan area of 2.7 million, has the distinctly undesirable reputation of having been successfully attacked twice in as many years, 2018 and 2019. The 2018 incident occurred on March 25 and involved a ransomware attack on and takedown of the city's Computer Assisted Dispatch (CAD) system that supports Baltimore's 911 emergency dispatch and 311 non-emergency phone systems. During this incident, city IT and cybersecurity staff were able to identify the problem quickly and, according to the city's CIO, Frank Johnson, "isolate and take offline the affected server, thus mitigating the threat" (Rector, 2018a). The system was restored in less than 24 hours. The city later revealed that the incident occurred because staff were working on part of the IT system and had misconfigured a firewall accidentally and exposed a port (an opening to the internet) for 24 hours. Consequently, the attackers found the opening they needed and managed to enter the city's network (Rector, 2018b).

Apparently, however, Baltimore did not learn much from this experience – or, at least, did not learn enough from it – because on May 7, 2019, the city was attacked again and with far greater consequence and cost. Baltimore's IT system was attacked by as yet unknown cybercriminals using the Robbinhood ransomware, which had successfully penetrated the city of Greenville, NC, a month earlier (Duncan and Zhang, 2019).

This time, the attackers took over and encrypted nearly all of Baltimore's data infrastructure, demanded a ransom of 13 Bitcoin (at the time, around $76,000) to release the hostage's systems and data. The city refused to negotiate, and it took months before their systems were fully up and running again. During this time, several city services were either fully or partially disabled, including water billing (which was not fully functional for several months), property tax collection, parking ticket payments, and the city's government email and voice mail systems. Real property sales were interrupted for several weeks because the system that handled property transfers was offline as well (Chokshi, 2019; Gallagher, 2019)

Of course, as with any high-profile cybersecurity incident, there is the embarrassment factor to contend with. How could this attack have occurred just after the one in 2018? Were no lessons learned? It turns out that apparently few if any were. For example, Baltimore had a great opportunity to buy cybersecurity insurance in the aftermath of the 911 attack. It did not. This is unfortunate for at least two reasons. First, in the process of applying for cybersecurity insurance, the city almost certainly would have had to conduct a vulnerability analysis to qualify for coverage. Such an analysis might have found the exact weakness that permitted the attack to succeed. According to cybersecurity expert Herb Lin of Stanford University, if Baltimore had installed a simple patch for Windows that Microsoft made available in 2017, this entire episode could have been prevented (Ropek, 2019). Second, the cyber insurance could have covered at least some of the estimated $18 million that the attack cost the city.

What enabled this attack to be successful? First, for years the city had underinvested in cybersecurity. The CIO had warned city officials months earlier to purchase cybersecurity insurance and also that its IT system was essentially a disaster waiting to happen due to a lack of adequate funding and lack of cybersecurity training of employees (Duncan and Zhang, 2019; Gallagher, 2019). Of course, the CIO was placed "on leave" (or fired), some think, made a scapegoat over this incident since someone had to be publicly held responsible and it certainly couldn't be any of the city's elected officials.

Next, Baltimore's IT system consisted largely of old technology that was improperly managed and underfunded. According to a knowledgeable local observer, technology writer Sean Gallagher, Baltimore's IT system consisted of "a dangerously ill-prepared, kludged together municipal IT system" with a "chaotic jumble of operating systems," whose IT staff were "overworked, underpaid…[and] dramatically underfunded" (Shen, 2019). Gallagher also noted that the "city does not have a full handle on its vulnerability management and patch management and keeping up to date with things." There were also reports about how Baltimore needed to send IT staff personally to each computer because the city had no way of providing updates to systems from a central location (Duncan & Zhang, 2018). If these observations are true, and there is little reason to believe otherwise, then it was only a matter of time before a serious incident occurred.

Case 2.1 Lessons from Atlanta and Baltimore: In retrospect, successful cyberattacks like these are not terribly surprising. This is, in part, because many, if not most local government officials do not fully or even substantially understand the need for cybersecurity. Nor do these officials provide adequate funding for cybersecurity (Norris et al., 2020). This seems to have been abundantly true in Atlanta and Baltimore: both cities experienced ransomware attacks, both attacks took down important city services, both were costly in terms of recovery, both cities had a history of under-investing in already vulnerable IT systems, and both attacks brought considerable municipal embarrassment.

The primary lessons that should be drawn here are that local government officials must fully understand the need for and provide adequate direction and funding for high levels of cybersecurity. Failure to do so will result in similar outcomes just about every time.

1.4 Conclusion

In addition to the reasons discussed earlier in this chapter, the Atlanta and Baltimore examples should demonstrate clearly why it is crucial that local governments and the officials leading them understand the many cybersecurity issues they face. Failure to do so places their communities at increased risk of experiencing likely preventable cybersecurity problems.

This understanding should, at a minimum, encompass the cyberthreats that these governments face, the actions they should take to protect their information assets from attack, and to mitigate the damage after successful attacks, the gap between those actions and the need for high levels of cybersecurity at the grassroots and, finally, the barriers that these governments encounter when deploying cybersecurity. Understanding these issues will enable local officials not only to see why cybersecurity is crucial to their governments' digital well-being but will help ensure that cybersecurity has their full support and is adequately funded and properly managed.

Appendix 1.1 Local Government Cybersecurity Articles in Peer-Reviewed Journals from 2000 to mid-2021

Article	Topic
Surveys and Focus Groups	
(Hatcher et al., 2020)	Survey of public officials in US cities of cybersecurity strategic plans, support for those plans, types of cybersecurity policies implemented, and resources needed for cybersecurity planning
(Norris et al., 2020)[2]	Nationwide survey of US local government cybersecurity management
(Norris et al., 2019)[2]	Nationwide survey of cyberattacks against US local governments
(Norris et al., 2018)	Focus group of local government IT and cybersecurity leaders in one US state on cyberattacks and cybersecurity management
(Caruson et al., 2012)	Survey of local government officials in Florida, examining the relationship between agency size and various cybersecurity issues
(MacManus et al., 2012)	Survey of local government officials in Florida, measuring cross-pressure between transparency and privacy
Smart Cities	
(Ali et al., 2020)	Exploration of critical factors of information security requirements of cloud services within the Australian regional and local government context
(Habibzadeh et al., 2019)	A survey of cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities
(Vitunskaite et al., 2019)[1]	A comparative case study of Barcelona, Singapore, and London smart cities governance models, security measures, technical standards, and third party management based on 93 security standards and guidance
Case Study	
(Phin et al., 2020)[1]	Case study evaluation of a Malaysian local government organization for the physical security components of its IT department

(*Continued*)

Article	Topic
Frameworks	
(Falco et al., 2019)	A cyber negotiation framework to help defend urban critical infrastructure against cyber risks and bolster resilience
(Ibrahim et al., 2018)[1]	Case study evaluation of a local government organization in Western Australia using the NIST Cybersecurity Framework
Economic Techniques	
(Kesan & Zhang, 2019)[1]	Uses linear models to understand the relationship between local government budgets, IT expenditures, and cyber losses
(Li & Liao, 2018)	Study of alternative economic solutions to the cybersecurity threat of smart cities

[1]Indicates article was published in a computer science journal.
[2]Indicates article is discussed in depth in Chapters 5, and 6.

Notes

1 The authors completed the manuscript for this book at the end of September 2021. All further references to when the book will simply state: "As of this writing." to mean that date.
2 Promises that are not always kept!
3 For cybersecurity purposes, an attack surface consists of the totality of the points in an information system that is vulnerable to attack.
4 Many thanks to our UMBC colleague Professor Tim Finin, who wrote this section on the IoT for a paper he and Professor Anupam Joshi co-authored with two of the co-authors of this book (Norris and Mateczun).

References

Ali, O., Shrestha, A., Chatfield, A., and Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1), https://www.sciencedirect.com/science/article/pii/S0740624X19300231

Allison, G.T. (1983). Public and private management: Are they fundamentally alike in all unimportant respects? In J.M. Shafritz and A.C. Hyde (Eds.) *Classics of Public Administration*. Wadsworth Cengage Learning.

Antonakakis, M., April, T., Bailey, M., et al., (2017). *Understanding the Mirai Botnet*. A paper included in the Proceedings of the 26th USENIX Security Symposium August 16–18, Vancouver, BC, Canada.

Blinder, A. and Perlroth, N. (2018, March 27). *Cyberattack Hobbles Atlanta, and Security Experts Shudder*. New York Times. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Caruson, K., MacManus, S.A., and McPhee, B.D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Homeland Security & Emergency Management*, 9(2), 1–22. https://www.degruyter.com/document/doi/10.1515/jhsem-2012-0003/html

Chokshi, N. (2019, May 22). *Hackers are holding Baltimore hostage: How they struck an what's next*. New York Times. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

Colorado Computer Support (CCS) (2018). *The City of Atlanta held hostage by cybercriminals*. https://www.coloradosupport.com/the-city-of-atlanta-held-hostage-by-cybercriminals

Deere, S. (2018a, April 12). *Cost of City of Atlanta's cyber attack: 2.7 million and rising*. Atlanta Journal-Constitution. (Accessed March 20, 2020). https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI

Deere, S. (2018b, August 1). *Confidential report: Atlanta's cyber attack could cost taxpayers $17 million*. Atlanta Journal-Constitution. https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K

Deere, S. (2018c, November 28). *Feds: Iranians let cyberattack against Atlanta, other US entities*. Atlanta Journal-Constitution. https://www.ajc.com/news/local-govt–politics/feds-iranians-led-cyberattack-against-atlanta-other-entities/xrLAyAwDroBvVGhp9bODyO

Deere, S. and Klepal, D. (2018, March 29). *Emails show Atlanta received multiple alerts about cyber threats*. Atlanta Journal-Constitution. https://www.ajc.com/news/local-govt–politics/emails-show-atlanta-received-multiple-alerts-about-cyber-threats/xbFP3eVt3Eq72lw5UqjIFP

Duncan, I., and Zhang, C. (2018, May 17). *Analysis of ransomware used in Baltimore attack indicates hackers needed "unfettered access" to city computers*. Baltimore Sun. https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html

Duncan, I. and Zhang, C. (2019, May 17). *Analysis of ransomware used in Baltimore attack indicates hackers needed "unfettered access" to city computers*. Baltimore Sun. https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html

Falco, G., Noriega, A., and Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. *Journal of Cyber Policy*, 4(1), https://doi.org/10.1080/23738871.2019.1586969

Freed, B. (2019, March 22). *One year after Atlanta's ransomware attack, the city says it's transforming its technology*. Statescoop. (Accessed April 15, 2020). https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology

Gallagher, S. (2019, May 20). *Baltimore ransomware nightmare could last weeks more, with big consequences*. Ars Technica. https://arstechnica.com/information-technology/2019/05/baltimore-ransomware-nightmare-could-last-weeks-more-with-big-consequences

GovDataDownload (2019, March 26). *State and local government sees an uptick in IT spending; Cybersecurity remains top focus*. https://govdatadownload.netapp.com/2019/03/state-local-government-sees-uptick-it-spending-cybersecurity-remains-top-focus/#.YVJQWNNKjOQ

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., et al., (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities.