Cyber Cities: The Role of Illinois Municipalities in Preventing and Managing Cyberattacks

Monica Pechous
Illinois Local Government Lawyers Association
Writing Competition for Members

15 Dwyer Place
St. Louis, MO 63124
mpechous@kentlaw.iit.edu
(702) 501-0031

Associate Attorney, Tucker Ellis LLP
Juris Doctor, Chicago-Kent College of Law (December 2020)

Monica Pechous works as an associate attorney at Tucker Ellis LLP in St. Louis, Missouri. She received her law degree from Chicago-Kent College of Law in 2020 and her MBA from Southern Illinois University Edwardsville in 2021. She is licensed to practice in both Illinois and Missouri.

I certify that this entry is the original work of the author and has not been previously published.

Cyber Cities: The Role of Illinois Municipalities in Preventing and Managing Cyberattacks

INTRODUCTION

Across the world, millions of people have felt the devastating impacts of the COVID-19 pandemic. In the United States alone, over 50 million people have contracted COVID-19, resulting in 800,000 deaths.[1] One in four patients are afflicted with "long-haul" COVID-19—these patients experience serious and ongoing symptoms for months on end.[2] Aside from public health impacts, the pandemic has also caused a severe economic crisis affecting individuals, corporations, and governments.[3] Data from the United States Census Bureau reveals increased hardship across American households since the onset of the pandemic: millions of people are unemployed and lack the resources to afford necessities like food and rent.[4]

As COVID-19 rages on, governments, corporations, and non-profit organizations have focused on mitigating the impacts of the pandemic within their communities.[5] Notably, local governments have assumed the bulk of the responsibility for promoting public health initiatives, protecting residents, and providing resources to those with the greatest need.[6] Such is especially

---

[1] Centers for Disease Control and Prevention, *Covid Data Tracker Weekly Review*, (Dec. 17, 2021), https://www.cdc.gov/coronavirus/2019-ncov/covid-data/covidview/index.html.
[2] UC Davis Health, *Studies Show Long-Haul COVID-19 Afflicts 1 in 4 COVID-19 Patients, Regardless of Severity*, (Mar. 30, 2021), https://health.ucdavis.edu/newsroom/news/headlines/studies-show-long-haul-covid-19-afflicts-1-in-4-covid-19-patients-regardless-of-severity/2021/03.
[3] Center on Budget and Policy Priorities, *Tracking the COVID-19 Economy's Effects on Food, Housing, and Employment Hardships*, (Nov. 10, 2021), https://www.cbpp.org/research/poverty-and-inequality/tracking-the-covid-19-economys-effects-on-food-housing-and.
[4] *Id.*
[5] Mariana Lameiras & Delfina Soares, *In the Doom of Hope: Local Governments as Key Agents to Respond to the Pandemic*, UNITED NATIONS UNIVERSITY, (Mar. 26, 2021), https://egov.unu.edu/op-eds/local-governments-and-pandemic.
[6] *Id.*

true in Illinois: when the first COVID-19 vaccine became available to the public in December 2020, local health departments across Illinois quickly began to disseminate information about the vaccine, organize vaccine distribution centers, and collect data online from individuals seeking a vaccination appointment.[7] In response to the economic impacts of the pandemic, municipal governments like the City of Chicago began to offer resources online to help residents seeking financial assistance, housing, and food[8]—including a virtual form in which residents could input personal data in order to receive stimulus check payments from the federal CARES Act.[9]

While Illinois local governments have been essential in slowing the spread of COVID-19 and aiding vulnerable populations financially impacted by the pandemic, another threat—aside from the virus itself—looms in the background. By collecting personally identifiable information online to schedule vaccine appointments and offer financial assistance, Illinois local government units have exposed themselves to the threat of cyberattacks—and, in turn, have exposed their residents to data breaches—the consequences of which are innumerable.[10] In recent years, local governments across the United States have increasingly become the target of cyberattacks, in which perpetrators steal data, incapacitate systems, and often demand ransom in exchange for the

---

[7] Dan Petrella et al., *Hope at a Historic Moment: First COVID-19 Vaccinations Scheduled to be Given in Illinois on Tuesday*, CHICAGO TRIBUNE (Dec. 14, 2020), https://www.chicagotribune.com/coronavirus/ct-coronavirus-illinois-chicago-vaccinations-20201215-kdcvoosh6najxonropu26w2ipm-story.html.

[8] City of Chicago, *Coronavirus Response Center*, (last visited Dec. 30, 2021), https://www.chicago.gov/city/en/sites/covid-19/home.html.

[9] City of Chicago, *Business and Employment*, (last visited Dec. 30, 2021), https://www.chicago.gov/city/en/sites/covid-19/home/business-and-employment.html.

[10] Maggie Miller, *Illinois Public Health Agency Website Taken Down by Hackers*, THE HILL, (Mar. 12, 2020), https://thehill.com/policy/cybersecurity/487282-illinois-public-health-agencys-website-taken-down-by-hackers?rl=1.

return of such data and systems.[11] The COVID-19 pandemic has exacerbated the number of cyberattacks on municipalities, as perpetrators recognize an opportunity to collect a large sum of ransom money from a local government—or at the very least, collect the personal data of all residents who used the system.

As municipal use of technology and data continues to expand, commentators have debated whether local governments ought to be liable for the cyberattacks they experience.[12] Local governments typically carry liability insurance specifically for cyberattacks—but increasing rates of cyberattacks have caused insurance premiums to inflate exponentially, making it nearly impossible for smaller municipalities to afford coverage.[13] Those in favor of the removal of municipal liability argue that holding a municipality liable only hurts the taxpayers, as local government funds will be diverted away from fundamental services in order to address liability stemming from the cyberattack.[14] Conversely, many view municipal liability positively, believing that it forces the local government unit to take responsibility for its own cyber security and data protection policies in order to prevent attacks.[15]

This Article contends that removing liability from municipal governments—perhaps temporarily for the duration of the COVID-19 pandemic—is the most effective way to manage cyberattacks. Part I of this Article explains the existing responsibilities of Illinois municipalities

---

[11] KnowBe4, *Whitepaper: The Economic Impact of Cyber Attacks on Municipalities*, (last visited Dec. 29, 2021), https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf.
[12] *See* Illinois Municipal League, *2021 State Legislative Agenda*, (last visited Dec. 29, 2021), https://www.iml.org/file.cfm?key=20298.
[13] Andrea Noble, *Cyber Insurance for Local Governments Costs More, Covers Less*, ROUTE FIFTY, (Nov. 16, 2021), https://www.route-fifty.com/tech-data/2021/11/cyber-insurance-local-governments-costs-more-covers-less/186882/.
[14] *Id.*
[15] KnowBe4, *supra* note 11.

with respect to cyber security and data protection, as well as the privileges and immunities generally afforded to municipalities.[16] Part II describes the onslaught of cyberattacks perpetrated against Illinois municipalities in recent years, with a focus on how the COVID-19 pandemic has attracted growing numbers of cyberattackers.[17] Part III assesses various solutions for combatting cyberattacks on local government systems.[18] Ultimately, Part III contends that the removal of municipal liability for cyberattacks will best serve the interests of the Illinois municipalities and their residents.[19] In such instances, municipal immunity will allow local governments to fully dedicate their limited budgets to resident needs rather than emergent lawsuits—especially in light of the COVID-19 pandemic, which has diminished local government budgets and highlighted community needs more than ever before. However, for best results, such a removal of liability ought to be coupled with increased cyber security requirements within local government units.

I. EXISTING RIGHTS AND RESPONSIBILITIES OF ILLINOIS MUNICIPALITIES

In accordance with the Illinois Constitution, Illinois municipalities have several rights and responsibilities.[20] These rights and responsibilities, supplemented by relevant legislation, comprise the framework under which local governments operate.[21] Additionally, local governments enjoy immunity from legal liability in certain instances.[22]

A. Legislation Relating to Data Privacy and Cyber Security

[16] *See infra*.
[17] *See infra*.
[18] *See infra*.
[19] *Id.*
[20] ILL. CONST. Art. VII (1970) (Local Government).
[21] *See id.*
[22] 745 ILCS 10/1 *et seq*.

With respect to data privacy and cyber security, the Illinois General Assembly has passed several pieces of legislation, each of which contributes to the protection of personally identifiable information while still allowing local governments to obtain and use such information when necessary. Recognizing the inherent vulnerability of internet-based systems, the General Assembly has limited the collection and use of certain types of personally identifiable information.[23] For example, the Identity Protection Act restricts public agencies in their use of social security numbers and imposes restrictions on the collection and retention of such data.[24] While the Act recognizes the legitimate use of social security numbers by local government agencies, it seeks to minimize unauthorized data disclosures by restricting access to sensitive information.[25] Notably, the Act prohibits requiring an individual to "use his or her social security number to access an internet website"—a requirement likely created to minimize the consequences of a cyberattack on a local government website.[26]

Similarly, the Personal Information Protection Act ("PIPA") requires that local government agencies promptly notify all Illinois residents when their personal information has been compromised in a data breach.[27] While PIPA is reactive in nature—requiring local governments to give notice of a data breach once it has already happened, rather than requiring the local government to take steps to prevent the breach—it still protects Illinois residents by ensuring awareness of the breach and offering resources to mitigate the loss of personal information.[28] PIPA requires that local governments provide impacted individuals with contact information for credit

---

[23] Chrissie L. Peterson, *Cyber Liability in the Public Sector*, (May 11, 2017), https://secure.heylroyster.com/_data/files/Seminar_2017/Governmental-I-CLP.pdf.
[24] *Id.*
[25] 5 ILCS 179/1.
[26] *Id.*
[27] 815 ILCS 530/1 *et seq*.
[28] *Id.*

reporting agencies and the Federal Trade Commission to minimize instances of fraud that might result from data breaches.[29] Through its language, PIPA inadvertently encourages local governments to adopt more rigorous internal policies for data protection and cyber security.[30] For example, failure to notify affected Illinois residents in a timely manner is a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act.[31] PIPA's stringent requirements, along with penalties associated with failure to comply with the Act, may act as a deterrent to local government units such that they proactively implement stronger cyber security measures to prevent data breaches in the first place.

B. Municipal Immunity Generally

There are various instances in which Illinois municipal governments enjoy immunity from legal liability.[32] While municipal immunity does not yet clearly extend to liability relating to data breaches or cyberattacks, the most well-known immunity afforded to local governments in Illinois is codified in the Tort Immunity Act.[33] The Tort Immunity Act functions to "protect local public entities and public employees from liability arising from the operation of government."[34] Through the Act, agencies and their employees are granted immunity from liability for injuries occurring on public property, during fire protection and rescue services, and during the provision of medical care, among other things.[35] Despite the complexities of the Tort Immunity Act, it represents a clear

[29] *Id.*
[30] *See id.*
[31] 815 ILCS 530/1 *et seq*.; *see also* 815 ILCS 505/1.
[32] *See* 745 ILCS 10/1 *et seq*.
[33] *Id.*
[34] *Id.*
[35] *Id.*

purpose: local government units ought to be able to freely function without fear of liability interfering with operations and activities.[36]

II. INCREASING RATES OF CYBERATTACKS

Rapid technological advances over the past few decades have resulted in internet- and cloud-based systems becoming commonplace in daily life. Use of technology, databases, and servers has greatly improved the functionality and operations of many organizations—though not without a price. Hackers have capitalized on the increased use of cyber systems, constantly identifying new ways of compromising security, improperly obtaining data, and seeking out financial compensation in exchange for returning access to a system to its rightful owner.[37]

A. Cyberattacks on Local Government Systems

Over time, hackers have identified a particularly attractive target for their attacks: local governments.[38] Cyberattacks on local governments have far-reaching consequences, impacting law enforcement, education, and healthcare services.[39] Such attacks interfere with a municipality's ability to effectively govern, distribute accurate information, and provide necessary services to residents.[40] At best, cyberattacks on local governments are an inconvenience; at worst, they result in loss of funds, personally identifiable information, and governmental control.[41]

---

[36] Brian D. Schwartz, *Tort Immunity in Illinois*, ILLINOIS MUNICIPAL REVIEW, (Aug. 1993), https://www.lib.niu.edu/1993/im930824.html.
[37] KnowB4, *supra* note 11.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

Orchestrated through advanced phishing techniques, perpetrators can surreptitiously gain access to confidential records held by governmental entities.[42] Illinois local governments are no stranger to cyberattacks—in January 2017, Morton School District teachers received a phishing email from a foreign entity representing itself as the district superintendent.[43] The email requested the names, social security numbers and salary information for hundreds of school district employees—which hackers gained access to when a teacher fell victim to the scheme.[44] Despite the loss of sensitive data, the school district emerged from the attack without losing funds.[45] However, in the Quad-Cities in November 2021, at least three local government entities were forced to pay substantial sums of money as ransom to hackers.[46] The hackers, who impersonated vendors the cities worked with, eventually returned system access to the local governments after receiving $115,000 from Rock Island County, $222,000 from LeClaire, and $420,000 from Moline.[47] Despite paying ransom, the municipalities had no way to ensure that the confidential data held within their systems was left untouched.[48]

Unfortunately, as Illinois local governments utilize internet-based systems to combat the COVID-19 pandemic, such governments expose themselves to a greater threat of cyberattacks.[49] While internet-based systems provide greater access to information and ease of use for residents,

---

[42] *Id.*
[43] Chronicle Media, *Morton School District Apparently Hacked by Russians*, TAZEWELL CHRONICLE, (Feb. 2, 2017), https://chronicleillinois.com/news/tazewell-county-news/morton-school-district-apparently-hacked-russians/.
[44] *Id.*
[45] *Id.*
[46] Sarah Watson, *At Least 3 Quad-Cities Municipalities Have Fallen Victim to Cyber Attacks. Experts Say They Are Common, But Can Be Prevented*, QUAD-CITY TIMES, (Nov. 21, 2021), https://qctimes.com/news/local/at-least-3-quad-cities-municipalities-have-fallen-victim-to-cyber-attacks-experts-say-they/article_355e38d1-2b4c-58f7-9eea-1eb0c113584f.html.
[47] *Id.*
[48] *Id.*
[49] Miller, *supra* note 10.

especially during periods of quarantine, these systems are vulnerable to bad actors if not properly secured.[50] In early March 2020, when little was known about the severity and contagion of COVID-19, the Champaign-Urbana Public Health District's website was taken down in a cyberattack.[51] The agency, which serves over 200,000 people, found itself unable to share timely and accurate information about the nascent pandemic.[52] As a result of the ransomware attack, the website was immobilized for nearly two weeks, the agency was required to pay an undisclosed amount of money to regain access to the website, and personally identifiable information of residents was compromised.[53] The agency announced on its Facebook page that its website was down—offering a phone number and email address by which residents could contact the agency with any COVID-19 questions or concerns.[54] However, at such a critical point in the pandemic, loss of website functionality likely contributed to increased spread of the virus due to lack of accessible public health information.[55] Combined with the loss of confidential data, such an incident represents just how disastrous a cyberattack on a local government system can be during times of crisis.[56]

B. Lawsuits Stemming from Cyberattacks

Over the course of the pandemic, Illinois residents have filed lawsuits against private health groups across the state, alleging that such groups negligently maintained their systems and failed

---

[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*

to safeguard the protected health information of users.[57] In November 2021, a class action suit was filed against DuPage Medical Group after 600,000 patients were notified that their protected health information was compromised in a cyberattack.[58] Now, as local governments manage and control a sizeable share of statewide COVID-19 testing and vaccination efforts, many municipalities fear the prospect of being sued if a cyberattack occurred on a municipal system. Similarly, a class action suit was filed in June 2020 against Deloitte Consulting for its failure to secure personally identifiable information within the Illinois unemployment system, causing a data breach affecting 32,483 Illinois residents.[59] The breach resulted in identity theft and fraudulent bank charges for those impacted—a crippling consequence for individuals already financially struggling and out of work due to the pandemic.[60] As municipal governments create online portals for residents to apply for assistance, they may similarly be at risk for cyberattacks and subsequent lawsuits. While no plaintiff has brought such a suit against a local government or its officials yet, the uptick of suits against private groups, coupled with ever-increasing numbers of cyberattacks, are a cause for concern.

III. SOLUTIONS FOR ADDRESSING CYBERATTACKS DURING THE COVID-19 PANDEMIC

When the operative Illinois Constitution was ratified in 1970, technologies taken for granted today—such cell phones and the internet—did not yet exist. Further, delegates to the constitutional convention could not have predicted the magnitude—or the very existence—of the

---

[57] Jill McKeon, *DuPage Medical Group Faces Lawsuit After Cyberattack Impacts 600K*, HEALTH IT SECURITY, (Sept. 8, 2021), https://healthitsecurity.com/news/dupage-medical-group-faces-lawsuit-after-cyberattack-impacts-600k.
[58] *Id.*
[59] Ben Szalinski, *Illinois Unemployment Data Breach Leads to ID Theft, Class-Action Lawsuit Claims*, ILLINOIS POLICY, (June 18, 2020), https://www.illinoispolicy.org/illinois-unemployment-data-breach-leads-to-id-theft-class-action-lawsuit-claims/.
[60] *Id.*

COVID-19 pandemic. Despite the need to modernize the Illinois Constitution to address issues relating to data privacy and cyber security, there is limited support for a constitutional convention today.[61] As such, commentators have generally divided into two camps regarding municipal liability for cyberattacks: one group urges the Illinois General Assembly to grant immunity to municipalities when such attacks occur;[62] the other urges municipalities to take responsibility for such attacks—as well as take preventative measures to minimize the risk of their occurrence.[63] Extenuating circumstances caused by the COVID-19 pandemic complicate the dialogue, as public health initiatives and financial assistance programs necessitate the use of internet-based systems to collect personally identifiable information. Relatedly, the pandemic has caused both taxpayers and local government units to struggle financially, creating contention as to where and how money should be spent.

A. Municipal Responsibility for Cyberattacks

Presently, municipalities shoulder the burden of preventing and managing cyberattacks. As a first line of defense, many municipalities purchase cyber insurance coverage to alleviate costs associated with ransom payments to hackers and liability to impacted residents.[64] However, the heightened threat of cyberattacks has resulted in higher insurance premiums, rising deductibles, and lesser coverage.[65] In Maryland, the cost of cyber insurance for local government entities rose

[61] Ryan Keith, *Quinn: 'Con-Con' Question on Ballot Unfair*, THE STATE JOURNAL REGISTER, (Nov. 5, 2008), https://www.sj-r.com/story/news/2008/11/06/quinn-con-con-question-on/44241298007/ (58% voted "no" to an Illinois constitutional convention).
[62] Illinois Municipal League, *supra* note 12.
[63] KnowBe4, *supra* note 11.
[64] Noble, *supra* note 13.
[65] *Id.*

by 300% in the past year alone.[66] In Missouri, the available limit for cyber security coverage declined from $1 million to $250,000, while deductibles climbed from $5,000 to $25,000.[67]

While cyber insurance is a viable option for some municipalities, including larger entities like the City of Chicago, many of Illinois's nearly 1,300 municipalities lack the resources to afford such coverage. Despite such financial limitations, some commentators believe that responsibility for cyberattacks should remain with local government units. Municipalities already have a responsibility to safeguard confidential information, as evidenced by the Identity Protection Act and Personal Information Protection Act.[68] Accordingly, many argue that local governments should implement stronger data protection and cyber security measures—and if a municipality falls victim to a cyberattack, it should bear responsibility for allowing the attack to occur. A 2017 study by the International City/County Management Association ("ICMA") indicates that most local governments are sorely unprepared for cyberattacks.[69] Of approximately 400 participating local governments, the ICMA report reveals that over half have never developed formal cyber security policies, standards, strategies, or plans.[70] 66.3% have no plan for recovery from breaches, and 66.9% have no cyber security risk management plan at all.[71] It is no surprise that cyberattacks are on the rise as hackers can effortlessly access systems which local governments fail to adequately protect. Proponents of municipal liability for cyberattacks argue that municipalities

---

[66] *Id.*
[67] *Id.*
[68] *See* 5 ILCS 179/1; *see also* 815 ILCS 530/1 *et seq*.
[69] International City/County Management Association, *Cybersecurity: Protecting Local Government Digital Resources*, (May 2017), https://icma.org/sites/default/files/18-038%20Cybersecurity-Report-hyperlinks-small-101617.pdf.
[70] *Id.*
[71] *Id.*

should not be absolved from liability when their inactions and failures likely facilitated the attack to begin with.

B. Proposal to Remove Municipal Liability from Cyberattacks

In response to the debilitating impacts of cyberattacks on local government systems, many commentators argue that municipalities should be immune from liability when such attacks occur. In its 2021 State Legislative Agenda, the Illinois Municipal League, an organization representing the interests of municipalities across the state, offered a proposal to remove municipal liability from cyberattacks.[72] Per the proposal, the IML asserts that "making municipal governments liable does not punish the criminal, instead it punishes the city and its taxpayers."[73] Further, the IML explains that "costs from a liability lawsuit would only put additional financial pressure on a city's budget, threatening the critical government services that taxpayers depend on for their health, safety, and wellbeing."[74]

Municipal immunity is not a foreign concept in Illinois, though it has never been directly applied to incidents linked to cyber security and data privacy protection.[75] However, some commentators draw inspiration from the Illinois Tort Immunity Act as rationale for municipal immunity from liability for cyberattacks.[76] Proponents of removing municipal liability for cyberattacks contend that local governments should be able to collect data and operate cyber systems to provide services for public benefit without fear of a lawsuit. One major benefit of the Tort Immunity Act is its ability to safeguard local government funds; with no risk of a lawsuit for

[72] Illinois Municipal League, *supra* note 12.
[73] *Id.*
[74] *Id.*
[75] *See* 745 ILCS 10/1 *et seq*.
[76] *Id.*

covered incidents, local governments are free to expend resources solely on serving residents, rather than having to set aside large sums of money for potential liability suits.[77] Similarly, municipal immunity from liability for cyberattacks would preserve the resources of local governments, thus allowing those institutions to focus on funding vital services instead.

C. The Impact of COVID-19: Immunity Supplemented by Responsibility

The unprecedented nature of the COVID-19 pandemic has caused lawmakers and constituents alike to view the bounds of law and policy in new and unique ways. COVID-19 has necessitated expanded use of cyber systems to collect health data, schedule vaccination appointments, and offer financial assistance to struggling residents. While permanent municipal immunity from liability for all cyberattacks would afford the greatest benefit to municipalities, the urgency brought on by COVID-19 calls for at least temporary municipal immunity from liability for cyberattacks for the duration of the pandemic. Facing limited funds already, municipal governments should be able to focus on providing fundamental services for residents struggling due to COVID-19, rather than spending taxpayer money on fines and damages associated with liability for a cyberattack. Whether temporary or permanent, the Illinois General Assembly should consider the great success of the Tort Immunity Act in allowing local governments to function effectively without fear of liability.[78]

However, municipal immunity from liability for cyberattacks should be limited in nature: to qualify for such immunity, Illinois municipalities should be required to implement internal cyber security measures to prevent and deter cyberattacks. While some sophisticated cyberattacks may be inevitable, local governments are responsible for taking all reasonable measures to protect

[77] *Id.*
[78] *Id.*

resident data from attack. By requiring Illinois local governments to implement internal cyber security measures, the Illinois General Assembly would bolster the purpose of the Identity Protection Act and the Personal Information Protection Act, as well as minimize instances of cyberattacks.[79] The COVID-19 pandemic has wreaked havoc on countless Illinois residents already; while local governments should not be punished for the criminal actions of hackers, they still have a duty to protect residents and their confidential information, especially during such tumultuous times.

CONCLUSION

In recent years, local governments have faced tremendous pressure caused by both the COVID-19 pandemic and the surge of cyberattacks on local government systems. The convergence of these issues has created the perfect storm for Illinois municipalities, which must provide critical services to residents while being cognizant of the risks associated with use of cyber systems. While existing legislation serves to protect the personally identifiable information of Illinois residents, cyberattacks may still jeopardize such information and result in serious financial losses for local governments. Local government units should be free to govern without fear of liability; as such, the Illinois General Assembly should remove municipal liability for cyberattacks. However, such immunity should be tempered by the requirement of effective internal cyber security policies, ensuring that municipalities remain accountable for the protection of resident data.

[79] *See* 5 ILCS 179/1; *see also* 815 ILCS 530/1 *et seq*.