Local Government Officials Guide to Cybersecurity

Cybersecurity Essentials for Local Leaders

2025

OCTOBER 2025

Prepared by

Local Government Cybersecurity Alliance (LGCA)

Acknowledgements

The *Local Government Officials Guide to Cybersecurity (LGOGC)* is the result of a collaborative effort by the Local Government Cybersecurity Alliance (LGCA) national working group composed of cybersecurity professionals, local government officials, and dedicated public and private sector partners. We extend our deepest gratitude to all those who contributed their time, expertise, and insight to this initiative.

This guide would not have been possible without the invaluable input of practitioners on the front lines of local governance and cybersecurity. Their lived experience, practical knowledge, and shared commitment to securing public services shaped every aspect of this resource.

Editors & Project Managers

Donald E. Hester, Cybersecurity Professional with Over 30 Years of FSLTT Experience

Ron Puccinelli, Director, Applications Development, South Carolina Department of Motor Vehicles

Elisabeth Dubois, Ph.D., Cyber Risk Specialist, NYMIR Division, Wright Public Entity; Adjunct Professor, Department of Cybersecurity, University of Albany, NY

Veronica Mitchell, Cybersecurity Professional with Over 20 Years of Experience

Ron Tosto, CEO, Servadus

Contributors (in alphabetical order)

Douglas Alessio, Assistant City Manager/ Administrative Services Director, City of Orinda

Bryce Carter, CISO, City of Arlington, TX

John C. Carter, IT Director, City of Cottonwood, AZ

Jessica Contreras, CIO, City of Encinitas

Meghan Cook, Director, Cyber Incident Response Team (CIRT); Assistant Director, Office of Counter Terrorism (OCT)

Chris Covino, Senior Researcher, Institute for AI Policy and Strategy (IAPS)

Gerry Delgado, IT Director, City of Kingman, AZ

Robert De Roeck, MSCIA, CISSP, Principal IT Training Specialist, Indiana University

Fadi Fadhil, Field Chief Information Officer/ Director of Field Strategy, Palo Alto Networks

Cesar Gamez, Information Security Administrator, City of Roseville, CA

Sonja Gonzalez, CITO, New Hampshire Retirement System

Glenn Grandis, Council Member, City of Fountain Valley, CA

John A Green, Data Analyst IV, Texas Workforce Commission

Chris Hanna, IT Security Manager, Port of Oakland, CA

Casey Hiatt, Information Systems & Technology Manager, Midpeninsula Open Space District, CA

Larry D Hobbs, Security and Compliance Specialist II, North Carolina Department of IT

Christopher Jackson, CISM, Silicon Valley Power

Harsh Jadhav, CPA, CISA, CITP, CISM, CRISC, CFE, Chief Audit Executive; Alameda County Employees Retirement Association

Tom Kalinoski Ed.D., Director of Technology and Operations, Colonial Intermediate Unit 20

Mark Kirkendall, IT Security Manager, Calaveras County, CA

Jim Lewis, City Manager, City of Atascadero, CA

Thomas MacLellan, Director, Government Affairs and Strategy for SLED, Palo Alto Networks

Hendra Gunawan, CISO, Los Angeles County Sheriff's Department, CA

Michael Makstman, CISO/ Head of Department of Technology, City and County of San Francisco

Laura Mateczun, Ph.D., Associate Director of Digital Trust, University of Maryland, Baltimore County, MD

Abdeslam Mazouz, CISO, City of Minneapolis, MN

James Meece, CISO, Louisville Metro Government, KY

Matt Milne, City of Los Angeles, CA

Edwin Miranda, CISO, City of Newark, CA

Donald Norris, PhD, Professor Emeritus, University of Maryland, Baltimore County, MD

Christopher Paidhrin, CISO, City of Portland, OR

Tom Pelster, CIO, PRISM

Timothy Renick, Director of Information and Communication Systems, City of Carmel, IN

Ernesto Smith, Information Technology Manager, City of Vernon, CA

Owen Sterzl, IT Program Administrator, Midpeninsula Open Space District, CA

Art Thompson, CIO, City of Detroit, MI

Brandon Welch, Managing Director, Incident Response & Managed Detection Response Business Development, Ankura

Nathan Wiebe, CISO/DCIO, Contra Costa County, CA

Disclaimers

Professional and Liability Disclaimer

The Local Government Officials Guide to Cybersecurity (LGOGC) is provided strictly for informational and educational purposes only. It represents a collaborative synthesis of expert insights and practical experiences from the Local Government Cybersecurity Alliance (LGCA) national working group.

This guide does not constitute professional legal, technical, or specific security advice. Local governments and officials must consult with qualified legal counsel and certified cybersecurity professionals to address their specific circumstances, unique technical infrastructure, and current legal/regulatory requirements.

- No Warranty: The LGCA, its contributors, editors, project managers, and affiliated organizations (including public and private sector partners) make no warranties or representations, express or implied, regarding the accuracy, completeness, currency, or applicability of any information contained herein. The LGCA expressly disclaims all liability for any errors, omissions, or for any actions taken or not taken based on the contents of this guide.
- Limitation of Liability: Use of this guide is solely at the user's own risk. The LGCA and its members shall not be liable for any direct, indirect, incidental, consequential, special, or exemplary damages arising from or in connection with the use or misuse of the information provided herein.

Views Expressed and Organizational Disclaimer

The views and opinions presented in the LGOGC are those of the contributing LGCA working group members only and do not necessarily represent the official views, policies, or opinions of their respective employers, other authors, institutions, or organizations.

The inclusion of individuals, their professional titles, or their organizational affiliations in the acknowledgements does not constitute an official endorsement of this guide by those organizations. Contributors participated in an individual capacity or in a role dedicated to advancing public sector cybersecurity.

The views or opinions expressed are not intended to discriminate against or malign any person, religion, ethnic group, club, organization, company, or Nation-State.

External Links Disclaimer

This guide may contain links to third-party websites, services, and resources that we believe may be useful to you. These links are provided for convenience and informational purposes only. When you leave this guide's content and click on an external link, you are subject to the policies of that new site.

We make no representations or warranty of any kind, express or implied, regarding the accuracy, availability, completeness, reliability, freedom from malware, or validity of any external links. We do not endorse or guarantee the content, views, or opinions represented by any third parties, nor do we assume responsibility for any information or service offered by external websites. We are not responsible for monitoring or facilitating any transactions between you and any third party.

Forward

By Elisabeth Dubois & Donald Hester, Creators of the Local Government Cybersecurity Alliance

We've seen the incredible pace of digital change in your communities. Online permitting, cloud-based utilities, smart infrastructure, and artificial intelligence (AI) are designed to make life better, yet this progress comes with a severe and rapidly escalating cost: cyber risk.

As cybersecurity advisors and public safety professionals, we don't just read the statistics—we sit across the table from the dedicated leaders in town halls and county courthouses. We see the anxiety when a town board struggles to decipher a technical risk assessment, or when a city official has to sign off on a million-dollar security budget request they barely understand.

> The numbers are grim: in 2024, the average cost to recover from a public sector incident reached nearly $3 million, and agencies were left with systems down for weeks. We are seeing essential services—from emergency response to water management—being disrupted, sensitive citizen data compromised, and public trust eroding.

This crisis has fundamentally changed the conversation. Cybersecurity is no longer an IT issue; it is a strategic, fiduciary, and enterprise-level risk. It requires the immediate and sustained engagement of elected and appointed officials—mayors, councilmembers, supervisors, county executives, and administrators—who are ultimately accountable for safeguarding public assets and ensuring service continuity.

While large municipalities may employ a dedicated Chief Information Security Officer (CISO) and robust security teams, the vast majority of local governments—from small towns to rural counties—do not have the resources to hire or retain high-level, strategic cybersecurity personnel. Often, the entire IT function is managed by one or two individuals responsible for everything.

This creates a painful and dangerous disconnect:

1. Risk Exposure: Your cyber risk is identical to that of a large organization.
2. Governance Capacity: You lack a dedicated expert to clearly translate technical threats into business terms, forcing you to make crucial decisions using complicated jargon instead of clear policy language.

Leaders are left with ultimate legal and financial accountability but lack the "decoder ring" to understand what they are signing. This often leads to decision paralysis or, worse, underfunding crucial protections.

This Local Government Officials Guide to Cybersecurity (LGOGC) was created by the Local Government Cybersecurity Alliance (LGCA) to bridge this critical governance gap. We know that non-technical leaders don't need another technical manual. They need a roadmap built by their peers, specifically designed for resource-constrained environments.

This guide provides that clarity. It cuts through the jargon and equips you with the five Core Principles of effective governance—from integrating Enterprise Risk into your strategy to ensuring proper Oversight and Budget Allocation. It offers a framework to ask the right questions, make informed decisions, and transform cybersecurity from a technical vulnerability into a pillar of organizational resilience.

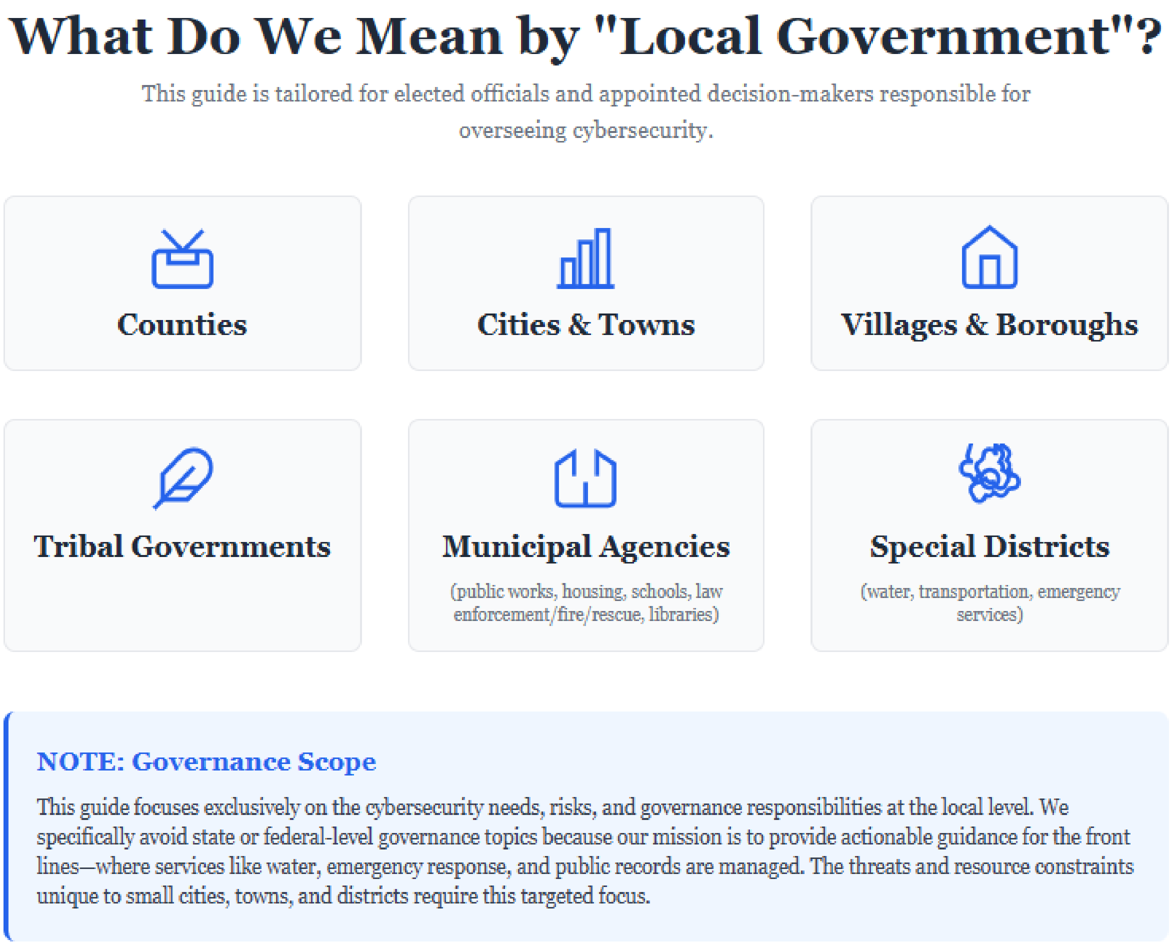
Your commitment to protecting public services is vital. By championing the principles in this guide, you will not only defend your community from today's threats but also secure the foundation for a trustworthy and innovative digital future.

Executive Summary

Local governments are increasingly embracing digital technologies to enhance service delivery, improve operational efficiency, and strengthen engagement with the public. From online permitting platforms to cloud-based utilities and smart infrastructure, these innovations create opportunities to serve communities more effectively. However, this transformation also introduces escalating cybersecurity risks—ranging from ransomware, phishing, and insider threats to sophisticated non-malware attacks—that can compromise sensitive data, disrupt essential services, and erode public trust.

Cybersecurity is no longer simply an IT issue. It is a strategic, enterprise-level risk that intersects with legal, financial, operational, and reputational considerations. As such, it requires active attention and engagement from elected and appointed leaders at every level of local government. From small rural towns to large urban counties, decision-makers must now treat cybersecurity as integral to their broader mission of ensuring public safety, safeguarding taxpayer dollars, and maintaining the continuity of essential services.

The Local Government Officials Guide to Cybersecurity (LGOGC) was created to meet this critical need. It is specifically tailored for non-technical decision-makers—mayors, supervisors, city and county executives, councilmembers, and appointed administrators—who hold ultimate accountability for their municipality's cybersecurity posture.



What Do We Mean by "Local Government"?

This guide is tailored for elected officials and appointed decision-makers responsible for overseeing cybersecurity.

Counties

Cities & Towns

Villages & Boroughs

Tribal Governments

Municipal Agencies

(public works, housing, schools, law enforcement/fire/rescue, libraries)

Special Districts

(water, transportation, emergency services)

NOTE: Governance Scope

This guide focuses exclusively on the cybersecurity needs, risks, and governance responsibilities at the local level. We specifically avoid state or federal-level governance topics because our mission is to provide actionable guidance for the front lines—where services like water, emergency response, and public records are managed. The threats and resource constraints unique to small cities, towns, and districts require this targeted focus.

Purpose of the Guide

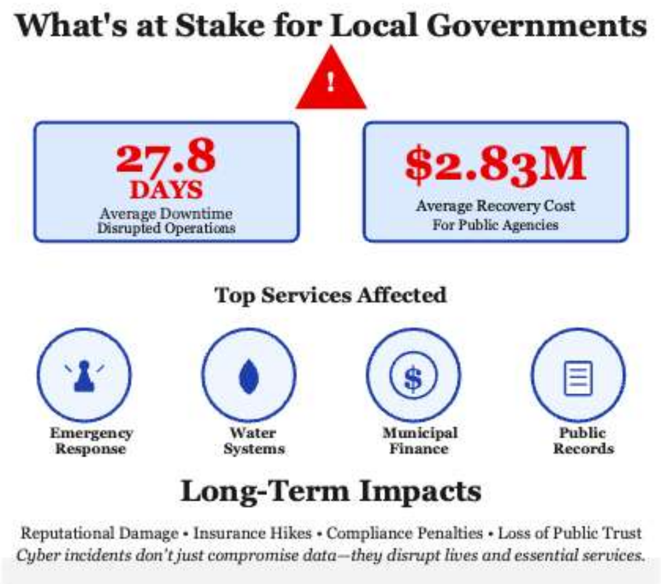
The LGOGC is designed to help local leaders navigate the complex and evolving cyber threat landscape with clarity and confidence. It provides a high-level framework for understanding cyber risks, implementing governance strategies, and building organizational resilience. Rather than turning officials into technical experts, the guide focuses on practical, actionable strategies that integrate cybersecurity into decision-making, planning, and organizational culture.

> Tailored specifically for non-technical decision-makers—mayors, supervisors, councilmembers, trustees, and other elected or appointed municipal officials (collectively referred to in this guide as the 'Board')—the guide provides a high-level framework for understanding cyber risks and implementing governance strategies that improve cyber resilience.

Specifically, the guide equips leaders to:

- Ask the right questions of staff, vendors, and service providers to ensure risks are understood and addressed.
- Understand policy, legal, and budget considerations essential to sustaining an effective cybersecurity program.
- Learn from peer case studies and real-world best practices, highlighting successes and lessons learned across municipalities.
- Take immediate, achievable steps to reduce cyber risk and strengthen organizational resilience.

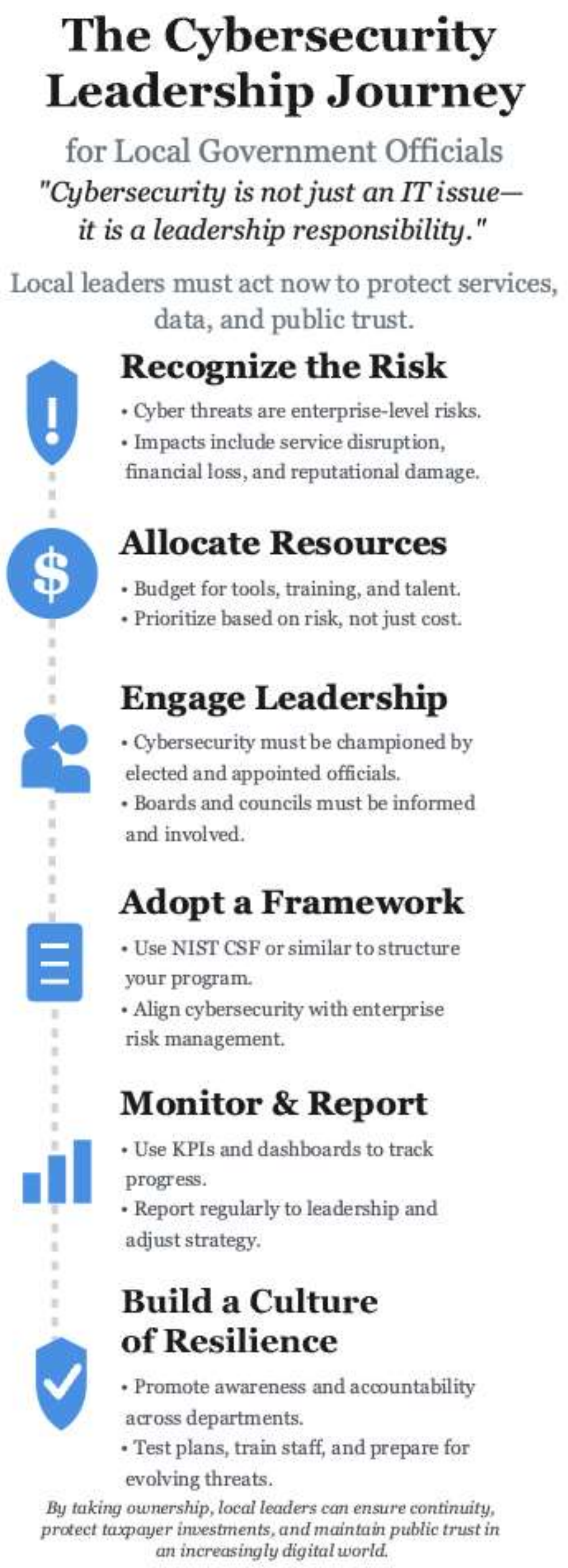
For leaders seeking more detailed guidance, technical best practices, and extended case studies, a wide range of supplemental materials, tools, and learning opportunities are available through the Local Government Cybersecurity Alliance website. These resources enable officials and staff to dive deeper into specific areas of concern, connect with peer communities, and access evolving content that reflects the latest trends, threats, and regulatory considerations.


What's at Stake for Local Governments
!
27.8
DAYS
Average Downtime
Disrupted Operations
$2.83M
Average Recovery Cost
For Public Agencies
Top Services Affected
$
Emergency Response
Water Systems
Municipal Finance
Public Records
Long-Term Impacts
Reputational Damage • Insurance Hikes • Compliance Penalties • Loss of Public Trust
Cyber incidents don't just compromise data—they disrupt lives and essential services.

Why Cybersecurity Matters Now

Cyberattacks targeting local governments have surged in frequency, sophistication, and impact. Threats like ransomware, phishing, and advanced non-malware attacks can disrupt critical services—emergency response, water utilities, waste management, public health, and more. In 2024, the average downtime following a ransomware incident was 27.8 days [1] and the average cost to recover from a cyber incident for public agencies reached $2.83 million, more than double the previous year [2].

The implications extend beyond financial loss: cyber incidents can degrade public trust, increase insurance premiums, lower bond ratings, and expose sensitive citizen data. Cybersecurity is therefore an enterprise-level risk, intersecting with legal, operational, and reputational considerations. In today's interconnected, digital-first environment, governance and leadership engagement are no longer optional—they are essential.



The Cybersecurity Leadership Journey

for Local Government Officials

"Cybersecurity is not just an IT issue—it is a leadership responsibility."

Local leaders must act now to protect services, data, and public trust.

Recognize the Risk

- Cyber threats are enterprise-level risks.
- Impacts include service disruption, financial loss, and reputational damage.

Allocate Resources

- Budget for tools, training, and talent.
- Prioritize based on risk, not just cost.

Engage Leadership

- Cybersecurity must be championed by elected and appointed officials.
- Boards and councils must be informed and involved.

Adopt a Framework

- Use NIST CSF or similar to structure your program.
- Align cybersecurity with enterprise risk management.

Monitor & Report

- Use KPIs and dashboards to track progress.
- Report regularly to leadership and adjust strategy.

Build a Culture of Resilience

- Promote awareness and accountability across departments.
- Test plans, train staff, and prepare for evolving threats.

By taking ownership, local leaders can ensure continuity, protect taxpayer investments, and maintain public trust in an increasingly digital world.

Cybersecurity as Governance Responsibility

Local government leaders have a fiduciary duty to protect public assets, ensure service continuity, and uphold public trust. In the digital age, this duty includes governing cybersecurity as a strategic priority. Cyber threats are enterprise-wide risks that require leadership engagement, policy alignment, and sustained oversight.

As cybersecurity programs mature, governance becomes increasingly important. Reflecting this, NIST elevated governance in its updated Cybersecurity Framework (CSF 2.0) by adding a dedicated Govern Function, signaling that governance is a central pillar of effective cyber risk management, not a peripheral consideration. Leaders must set the tone at the top, embedding cybersecurity into decision-making, organizational culture, and long-term planning.

This guide outlines five core governance areas that local officials must address to build a resilient cybersecurity posture:

1. **Enterprise Risk** - Cybersecurity must be integrated into the organization's overall risk management strategy. Like financial or operational risks, cyber threats can disrupt essential services, damage public confidence, and generate costs ranging from negligible to millions of dollars. Leaders must treat cyber risk as a top-tier enterprise concern and recognize it as a form of financial risk requiring board-level attention.
2. **Assign Budget** - Cybersecurity requires sustained investment. Leaders must ensure that budgets reflect the true cost of managing cyber risk—including staffing, tools, training, and insurance. Funding decisions should

be risk-informed, forward-looking, and aligned with organizational priorities, not just reactive to immediate needs.

3. **Oversight** - Boards and councils must actively oversee cybersecurity efforts. This includes receiving regular briefings, reviewing risk reports, and ensuring that leadership is accountable for implementing and maintaining effective cybersecurity practices. Oversight should be structured, ongoing, and informed by clear performance metrics.
4. **Framework** - Adopting a recognized cybersecurity framework—such as the NIST Cybersecurity Framework—provides structure, consistency, and a common language for managing cyber risk. Frameworks help align cybersecurity with broader governance, compliance, and enterprise risk management efforts. The addition of the Govern Function in CSF 2.0 further highlights the leadership responsibilities in establishing roles, responsibilities, and accountability mechanisms.
5. **Monitor & Report** - Cybersecurity is a continuous process. Leaders must monitor progress, track key performance indicators, and ensure that reporting is clear, actionable, and aligned with strategic goals. Effective reporting enables informed decision-making and accountability, while reinforcing cybersecurity as a governance—not just technical—responsibility.

A Roadmap to Cyber Resilience

The LGOGC does not aim to make public officials technical experts. Rather, it provides a high-level framework for understanding and addressing cybersecurity risks with clarity, confidence, and foresight. Through best practices, case studies, and practical tools, this guide helps leaders:

- Make informed decisions about policy, procurement, and investments.
- Allocate resources effectively to reduce exposure.
- Build a culture of security and resilience across departments.
- Anticipate and manage emerging risks, including those from disruptive technologies like AI, IoT, and cloud innovations.

By championing cybersecurity from the top, local officials can protect their communities from today's threats while laying the foundation for secure, innovative, and trustworthy digital government services in the future.

> Cybersecurity is now a leadership issue. With knowledge, engagement, and commitment, local government officials can transform it from a point of vulnerability into a pillar of public trust and operational strength.

Table of Contents

Acknowledgements 2

Forward 4

Executive Summary 5

Table of Contents 10

Section 1 - The Scope of Cybersecurity 12

Section 2 - Understanding Operational vs. Strategic Cybersecurity 19

Section 3 - Addressing Cyber Risk with Enterprise Risk Management 23

Section 4 –Cybersecurity Governance Principles for Local Officials 28

Principle 1- Enterprise Risk 29

Moving cybersecurity beyond the IT closet. This section explains how to define cyber threats as organizational risk and integrate security planning directly into the local government's overall strategic and financial decision-making process.

Principle 2 - Assign Budget 35

Guidance on ensuring sufficient, risk-based funding for cybersecurity. Learn how to correlate budget requests with specific, quantifiable risks to secure the resources needed to reduce threats to a manageable level.

Principle 3 - Oversight 40

Establishing the governance structure for security. This section details how to foster a strong cyber culture, improve staff literacy, set clear expectations for the entire organization, and embed accountability into daily operations.

Principle 4 - Framework 44

Guidance on selecting an appropriate cybersecurity framework (e.g., NIST, CIS). This section covers how to choose the right standard, map security responsibilities across departments, and ensure systematic adherence to best practices.

Principle 5 - Monitor & Report 48

Ensuring officials receive the right information at the right time. This section focuses on creating clear, concise reporting and metrics that are sufficient for executive decision-making, allowing leaders to track progress and manage evolving threats effectively.

Conclusion 51

References 52

Section 1 - The Scope of Cybersecurity

Section 1 - The Scope of Cybersecurity

The Growing Cyber Threat Landscape

Local governments across the U.S. are responsible for delivering essential public services and safeguarding vast amounts of sensitive data. With over 90,000 municipal entities managing everything from Social Security numbers and medical records to emergency dispatch and water treatment systems, the stakes are high. When these systems are compromised, the consequences can be immediate and severe—ranging from stolen data to halted public services.

Cyberattacks on municipalities are no longer rare—they're escalating in both frequency and impact. Between 2022 and 2023, thousands of cyber-attacks targeted U.S. local governments, which is expected to future years [3]. Many of these incidents go unreported, and a growing number are aimed at emergency communications, dispatch centers, and water infrastructure [4]. Research shows that many local governments operate under constant or near-constant attack, often without the resources, training, or policies needed to respond effectively.

High-profile breaches like the SolarWinds supply chain attack have further exposed the interconnectedness—and vulnerability—of public systems at every level. These are not just technical failures; they are crises of trust, safety, and stability. A single breach can paralyze government operations, endanger public health, and erode public confidence in democratic institutions.

Case Snapshots: Cyber Incidents and Their Impact

Location & Date	**Incident Details**	**Services Disrupted**	**Recovery Time**	**Estimated Cost**
Hoboken, NJ (Nov 2024)	Ransomware shut down digital services, closed City Hall, and suspended court operations.	City Hall, Municipal Court, Online Services	Several weeks	Not disclosed
White Lake Twp, MI (Nov 2024)	Cyberattack compromised a $35M civic center project transaction.	Financial operations, project planning	Ongoing	Not disclosed
Suffolk County, NY (2022)	Ransomware disrupted police dispatch, payments, and public records; 470,000+ residents affected.	Emergency services, payments, records access	Months	$25+ million
Oldsmar, FL (2021)	Hacker remotely accessed water treatment controls, attempting to poison water supply.	Water treatment system	Immediate response	Minimal (averted)
Washington D.C. PD (2021)	Babuk ransomware leaked sensitive officer data including SSNs and psychological evaluations.	Internal police systems, personnel data	Weeks	Not disclosed
Baltimore, MD (2019)	RobbinHood ransomware froze city systems due to unpatched software.	Billing, email, city services	Months	$18 million

Key Steps for Cybersecurity Readiness in Municipalities

1. **UNDERSTAND CYBER RISKS** Begin by identifying cybersecurity as a top priority. Recognize the types of threats your municipality may face, from phishing attacks to ransomware, and assess your current vulnerabilities.

2. **GRASP THE POTENTIAL IMPACTS** Evaluate how cyber threats could affect your operations, data integrity, public trust, and service delivery. Understanding the consequences helps prioritize your response.

3. **RECOGNIZE THE NEED TO MITIGATE THREATS** Acknowledge that proactive measures are essential. This includes implementing security protocols, updating systems, training staff, and preparing incident response plans.

4. **INFORM DECISION-MAKERS** Ensure that leadership and policymakers have access to clear, actionable information. This empowers them to make informed decisions about cybersecurity investments, policies, and emergency planning.

Cybersecurity as a Strategic, Enterprise-Level Concern

Cybersecurity today is no longer confined to the domain of IT departments. For local governments, it is a core strategic concern—impacting service continuity, financial integrity, legal liability, and public trust. Effective cybersecurity governance requires a shift in perspective: from viewing security as a technical function to recognizing it as an enterprise-wide risk that demands leadership attention at the highest levels.

Access our Cyber Community Forum for Local Government, to explore best practices and resources from federal, state, local, public, and private organizations.

Understanding Risk in the Digital Age

As municipalities expand digital services—such as e-permitting, online tax payments, emergency alerts, and citizen portals—they also expand their exposure to cyber threats. Ransomware attacks, vendor vulnerabilities, phishing campaigns, and insider threats can all cause serious operational disruptions, financial loss, and reputational damage.

Governance-minded leaders must recognize that technology is both an enabler and a risk factor. Framing cybersecurity within an enterprise governance structure ensures that decision-making includes both innovation potential and risk exposure—supporting balanced, forward-looking leadership.

Find additional resources to help you break down cybersecurity risks, identify the bad actors involved, understand their methods (threat vectors) and motivations.

Governance as a Foundation for Cyber Resilience

Governance is the cornerstone of building cyber resilience. As cybersecurity programs mature, governance becomes increasingly important—not just for technical oversight but for ensuring that cybersecurity is treated as a strategic, enterprise-wide priority. Recognizing this, NIST added a dedicated Govern Function in its updated Cybersecurity Framework (CSF 2.0), underscoring that governance is a central pillar of effective cyber risk management.

One essential model for supporting this shift is the Enterprise Governance of Information and Technology (EGIT) framework. EGIT enables local governments to align technology investments and digital service delivery with broader goals such as resilience, transparency, and citizen trust—while managing the risks that accompany operating in a digital-first environment.

Alternatives to a Dedicated CISO

Many smaller local governments can't afford a full-time CISO, but strong cybersecurity is still achievable!

Virtual CISO (vCISO) Services

- Expert strategic guidance, part-time.
- Access high-level oversight and compliance without full-time cost.

Leveraging Existing IT Leadership

- Assign cyber duties to your CIO/IT Director.
- Balance operations with strategy; bring in consultants for specialized risks.

Cybersecurity Task Forces or Committees

- Cross-departmental team (IT, Legal, Risk, Compliance).
- Share governance, review policies, prioritize risks, prepare for incidents.

Collaborate with State or Regional Governments

- Connect with state-level cyber training and advisory services.
- Pool resources, gain expertise, stay ahead of threats.
- Share resources, knowledge, and best practices with neighbors.
- Amplify capabilities, build collective resilience.

Consultants and Managed Security Service Providers (MSSPs)

- External experts for planning; MSSPs for monitoring/ response.
- Maintain oversight, get specialized operational management.

Cybersecurity Training for Officials and Staff

- Educate officials, administrators, and key personnel.
- Build strong leadership, foster a security-conscious culture.

Rather than treating cybersecurity as an isolated IT concern, EGIT positions it within the broader governance structure, linking it to financial stewardship, operational continuity, and legal compliance.

At its core, EGIT emphasizes two interdependent responsibilities:

- **Delivering value** to the public through the effective use of data and digital tools.
- **Managing risk**—including cybersecurity—as an integral part of governance.

This risk management dimension is critical. Cyber incidents can have wide-ranging impacts, from negligible operational disruptions to multimillion-dollar losses. They can compromise essential services, erode public trust, and expose municipalities to legal and financial liabilities. For this reason, cyber risk must be treated as a financial and governance issue at the highest level—requiring sustained leadership engagement, clear accountability structures, and risk-informed decision-making.

Local governments can explore how to apply EGIT principles through example governance models designed to support strategic alignment across departments. By embedding governance into cybersecurity programs, municipalities ensure that cybersecurity is not just a technical safeguard, but a fundamental component of enterprise risk management and public trust.

Risk-Informed Leadership Decision-Making

Local leaders make complex decisions every day—balancing service improvements, constituent expectations, cost efficiencies, and risk. EGIT provides a structure for bringing cybersecurity into these conversations, equipping officials to ask the right questions and weigh trade-offs with clarity.

Consider a city exploring a cloud-based solution for managing resident data. A governance-aligned approach ensures that cybersecurity leaders participate in the evaluation—highlighting issues such as third-party risk, compliance requirements, and long-term data integrity. This risk-informed lens allows for decisions that reflect not just efficiency, but security and sustainability.

To help local officials frame these discussions constructively, use our Cybersecurity Questions for Decision-Makers Checklist.

Promoting Transparency and Accountability

Elected and appointed officials have a fiduciary duty to demonstrate responsible stewardship of public assets—including digital infrastructure. A strong governance model supports transparency through regular reporting, public engagement, and clear oversight structures.

Establishing and communicating cybersecurity priorities not only helps leaders stay informed and accountable, but also signals to the public that risk is being taken seriously. Transparent governance builds confidence that local governments are protecting sensitive data, managing taxpayer-funded systems responsibly, and preparing for emerging threats.

Embedding Cybersecurity in Public Service Delivery

Cybersecurity is not a peripheral technical concern—it is central to the reliability, integrity, and trustworthiness of essential government services. From online permitting systems and utility management platforms to emergency response and public health reporting, every digital service depends on resilient, secure infrastructure. Local officials must ensure that cybersecurity is proactively integrated into the planning, procurement, and delivery of public-facing systems, rather than addressed as an afterthought.

Effective integration requires a culture of cross-departmental collaboration and shared responsibility. IT, legal, risk management, finance, and operational units must coordinate to assess threats, prioritize protections, and implement safeguards. Leadership accountability is critical: executives and governing boards must set expectations, allocate resources, and maintain oversight, ensuring cybersecurity aligns with organizational objectives and enterprise risk management priorities.

Embedding cybersecurity into service delivery transforms it from a potential obstacle into a strategic enabler. When security considerations are included from the outset:

- Digital services become more reliable, reducing downtime and service interruptions.
- Equity in access is supported, protecting sensitive data while ensuring all residents can benefit from digital programs.
- Public trust is reinforced, as residents gain confidence that government systems are secure, transparent, and responsive.

Moreover, cybersecurity enhances operational resilience. By anticipating risks and implementing proactive safeguards, municipalities can sustain essential services even in the face of attacks, system failures, or emerging threats. This approach shifts cybersecurity from a reactive, technical function to a strategic element of public service delivery, integrated into the mission of serving and protecting the community.

The Role of the Chief Information Security Officer (CISO)

In any organization, including local governments, the Chief Information Security Officer (CISO) plays a vital role in guiding cybersecurity strategy and risk management. The CISO leads efforts to develop, implement, and oversee cybersecurity policies focused on governance, risk management, and regulatory compliance. This leadership ensures that cyber risks are managed proactively—protecting sensitive data, essential services, and public trust.

For local governments, where critical infrastructure, public-facing services, and resident data converge, the CISO's role is especially important. The CISO helps align cybersecurity practices with the community's expectations and the government's broader mission, reinforcing resilience and accountability.

A well-functioning CISO works closely with key departments such as legal, risk management, compliance, and physical security. This holistic coordination enables the identification of complex vulnerabilities spanning multiple domains and supports the development of comprehensive strategies to protect municipal assets. Beyond technical safeguards, the CISO also champions cybersecurity awareness—cultivating a culture where staff understand risks and adopt safe practices.

Equally important is the CISO's reporting structure. Unlike the Chief Information Officer (CIO), whose focus is typically on technology service delivery and operations, the CISO has a broader mandate that spans enterprise risk, legal compliance, and governance. For this reason, best practice is to align the CISO role with enterprise risk management or governance functions, rather than placing it solely under IT. This distinction ensures that cybersecurity is positioned as an enterprise-wide concern, not just a technical issue.

To fulfill this role effectively, the CISO must also have direct and unfiltered access to executive leadership, councils, and boards. Local officials have a fiduciary responsibility to establish the organization's cyber risk tolerance, which requires accurate, unbiased information directly from the CISO. Without this access, decisions may be shaped by operational or budgetary priorities that fail to capture the full scope of cyber risk.

The importance of reporting structure is underscored by findings from the 2020 ICMA Local Government Cybersecurity Survey, which showed that municipalities where the CISO reports directly to top elected or appointed officials—such as mayors, councils, or boards—demonstrate stronger cybersecurity prioritization throughout the organization [5]. Elevating the CISO in this way reframes cybersecurity as a strategic enterprise risk, rather than a subset of IT.

Emerging threats illustrate why this distinction matters. For example, deep fake campaigns targeting public officials create reputational and operational risks that extend far beyond the CIO's traditional scope of responsibility. These are governance and trust issues at their core, underscoring why the CISO must be positioned to inform leaders directly.

In short, the CISO's role is not only technical but fundamentally tied to governance, fiduciary duty, and public trust. Ensuring that the CISO has independence, authority, and access to decision-makers is essential for embedding cybersecurity into the foundation of resilient local government operations.

Clarifying Roles: IT vs. Cybersecurity

Strong governance depends on clear role definitions. While IT departments implement and support technology systems, cybersecurity functions should remain operationally distinct—

focused on protecting critical data, systems, and infrastructure. This separation allows cybersecurity professionals to assess risk independently of budget pressures or project timelines.

Cybersecurity is broader than traditional IT. Traditional IT focuses on technology service delivery and related risks, while cybersecurity spans operational technology (OT), legal compliance, financial risk, and enterprise risk management. It has cross-domain impacts: legal, risk management, and finance functions all intersect with cybersecurity. Importantly, cyber incidents can have major financial implications—from negligible costs to millions of dollars—so cyber risk must be treated as financial risk at the governance level.

For example, if a new online permitting platform is launched, IT may focus on functionality and uptime, while cybersecurity leads ensure that sensitive personal data is encrypted, access is tightly controlled, and third-party risks are assessed. This division of responsibilities helps prevent compromises in security due to operational urgency.

For comprehensive guidance on defining and structuring IT and cybersecurity roles, refer to our resource center.

Section 2 - Understanding Operational vs. Strategic Cybersecurity

Section 2 - Understanding Operational vs. Strategic Cybersecurity

In today's digital landscape, effective cybersecurity in local government requires more than technical defenses—it demands a comprehensive governance approach that recognizes the distinct roles of operational and strategic cybersecurity. Understanding this distinction is critical for elected and appointed officials seeking to protect essential services, steward public resources, and maintain public trust.

Two Dimensions of Cybersecurity: Operational and Strategic

Cybersecurity operates across two interrelated but distinct levels:

- Operational Cybersecurity focuses on day-to-day technical defense—protecting networks, systems, applications, and data from immediate threats. It is tactical, reactive, and critical for ensuring continuity of services.
- Strategic Cybersecurity takes a broader, enterprise-wide view, aligning cyber risk management with governance, legal, financial, and reputational priorities. This perspective ensures that cybersecurity decisions support organizational goals, compliance obligations, and public trust.

Both dimensions are essential. However, to be effective, they must be governed distinctly but integrated deliberately. When operational and strategic functions work in harmony, they reinforce resilience: technical safeguards protect against immediate threats, while leadership, policy, and risk oversight ensure the organization can withstand complex, systemic cyber challenges.

> Operational cybersecurity keeps the lights on; strategic cybersecurity ensures the organization can continue delivering its mission—even under duress.

Operational Cybersecurity: Technical Execution and Defense

Operational cybersecurity is typically housed within the IT department and encompasses the technical activities that maintain the security and availability of municipal systems and digital services. Key operational responsibilities include:

- **Infrastructure Security**: Protects networks, servers, endpoints, and cloud systems against unauthorized access, ransomware, and service disruptions.
- **Data Protection**: Implements encryption, access controls, monitoring, and backup solutions to safeguard sensitive information, from resident data to internal financial records.
- **Identity and Access Management (IAM)**: Ensures that users—employees, contractors, or vendors—have appropriate access privileges, reducing the risk of accidental or malicious data exposure.
- **Patch and Change Management**: Maintains software, firmware, and applications at current versions to close known vulnerabilities and reduce attack surfaces.
- **Incident Response**: Establishes processes for detecting, containing, and recovering from cyber incidents, minimizing operational disruption and reputational damage.

While operational cybersecurity is essential for technical continuity, it alone cannot address enterprise-level concerns. Systems may be secure from immediate threats yet still fall short of regulatory compliance, contractual obligations, or third-party risk management.

Strategic Cybersecurity: Governance and Risk Oversight

Strategic cybersecurity sits outside the traditional IT function and integrates with governance, policy, enterprise risk management, and leadership oversight. It ensures that cybersecurity is aligned with organizational priorities and protects the mission, public trust, and legal obligations.

Key focus areas include:

- **Governance and Compliance**: Ensures adherence to laws, regulations, and standards (e.g., HIPAA, GDPR, CJIS), reducing legal exposure and potential financial penalties.
- **Program Strategy and Policy**: Guides the development of cybersecurity policies, sets long-term objectives, and allocates resources based on risk, organizational priorities, and community expectations.
- **Third-Party and Supply Chain Risk**: Evaluates vendor and contractor relationships to mitigate risks inherited from external partners, which are increasingly targeted in modern attacks.
- **Security Culture and Insider Threats**: Promotes awareness, training, and accountability across all staff to reduce human error and prevent internal misuse.
- **Critical Infrastructure and Operational Technology (OT) Security**: Protects essential services—such as utilities, transportation, water treatment, and emergency response systems—from attacks that could endanger public safety.
- **Election Security and Data Privacy**: Safeguards voter information and election systems, especially in counties with election oversight responsibilities.
- **Cyber Risk Oversight**: Provides leaders with actionable insights through risk assessments, performance metrics, board-level reporting, and scenario planning.

Strategic cybersecurity ensures that digital resilience is a governance responsibility, not just an IT function. It connects technical controls to organizational decision-making, ensuring that cybersecurity decisions protect the mission, maintain service continuity, and uphold public trust.

Why Distinction Matters: Aligning Roles and Responsibilities

Confusing or conflating operational and strategic cybersecurity can leave critical risks unaddressed, expose public services, and undermine trust. Clear role distinctions are essential for effective cybersecurity governance:

- **Operational Cybersecurity** should remain focused on technical defense and IT system health, including day-to-day monitoring, patching, incident response, and infrastructure protection. Its primary goal is to keep services running and systems secure.
- **Strategic Cybersecurity** should report to executive leadership or governance bodies (mayors, city managers, boards, or councils), offering an independent, enterprise-wide perspective on cyber risk. This ensures that leadership receives unfiltered insights into

vulnerabilities, regulatory compliance gaps, and potential financial or reputational impacts.

Maintaining this separation achieves multiple benefits:

1. **Risk-Informed Decision-Making**: Cybersecurity decisions are guided by organizational risk, rather than just technical feasibility, convenience, or short-term budget considerations.
2. **Cross-Departmental Alignment**: Strategic oversight enables cybersecurity to be embedded in planning, procurement, budgeting, legal review, and community engagement, ensuring that every decision considers potential cyber implications.
3. **Enhanced Accountability**: Independent reporting structures allow leadership to set risk tolerance, evaluate mitigation efforts, and hold responsible parties accountable, rather than leaving decisions solely in the hands of technical staff.

Example: When deploying a new online permitting system, IT may focus on uptime and functionality, while strategic cybersecurity evaluates sensitive data flows, vendor risks, and compliance obligations. Both perspectives are essential—but must remain distinct to be effective.

Elevating Strategic Cybersecurity to the Leadership Level

Cybersecurity cannot be managed as a purely technical function—it is a core governance and leadership responsibility. Just as finance, legal, and public safety have formal oversight at the executive level, cybersecurity must also be elevated to board- or council-level visibility.

Key actions for leadership include:

- **Incorporating Cyber Risk into Leadership Agendas**: Ensure cybersecurity is a recurring topic in executive meetings, strategic planning sessions, and council or board briefings.
- **Regular Briefings on Organizational Posture**: Leaders should receive ongoing updates on risks, incidents, mitigation efforts, and emerging threats—enabling proactive rather than reactive decision-making.
- **Policy Alignment with Service Delivery and Fiduciary Responsibility**: Cybersecurity policies should support the organization's mission, protect critical public assets, and align with legal, operational, and financial responsibilities.
- **Board and Executive Engagement with the CISO**: The Chief Information Security Officer (CISO) should have direct access to decision-makers, ensuring that executives receive accurate, unfiltered information on risk and mitigation strategies.

Elevating strategic cybersecurity reinforces public trust, enhances operational reliability, and fulfills leaders' fiduciary duty to protect digital infrastructure and citizen data. Treating cybersecurity as a governance-level responsibility ensures that technical safeguards are complemented by policy, strategy, and accountability—making the organization resilient not only to immediate threats but also to emerging and systemic risks.

For practical guidance on integrating strategic cybersecurity into governance, see the NIST Cybersecurity Framework.

Section 3 - Addressing Cyber Risk with Enterprise Risk Management

Section 3 - Addressing Cyber Risk with Enterprise Risk Management

Managing cybersecurity risks in today's complex environment requires a holistic enterprise risk management (ERM) strategy—one that extends well beyond traditional IT functions. For local governments, cyber risks touch all aspects of operations, governance, third-party relationships, and public trust. An effective ERM approach integrates cybersecurity with broader organizational risk management to protect critical services and the community.

What is "Good Cybersecurity?"

Good cybersecurity is a comprehensive, proactive strategy designed to safeguard an organization's digital infrastructure, sensitive data, and networks from a wide range of threats. It's not just about stopping attacks—it's about anticipating risks, building resilience, and maintaining trust. Strong cybersecurity protects the confidentiality, integrity, and availability of critical systems and information, making it essential to public trust, operational continuity, and responsible governance.

Barriers to Good Cybersecurity

Although funding, staffing, leadership, and awareness are often treated as separate issues, they are deeply interconnected. Improvement in one area often enables progress in others. Until local governments address these systemic barriers, they remain vulnerable to evolving cyber threats [6], [7]. Each barrier presents unique challenges that require targeted governance, policy, and operational attention.

Insufficient Funding

Limited budgets are consistently cited as the top barrier to municipal cybersecurity. In a recent national summary report, 70% of local officials identified funding constraints as their primary challenge [8].

- Cybersecurity is often perceived as optional or "technical overhead," rather than a core public infrastructure investment like roads, emergency services, or water systems.
- Insufficient funding affects multiple layers of protection, including staffing, tools, incident response capabilities, training programs, and insurance coverage.
- Without adequate investment, municipalities risk delayed detection of threats, insufficient response capacity, and prolonged recovery after an incident.

Key takeaway: Leaders must treat cybersecurity as infrastructure—allocating funding proactively and viewing it as a long-term enterprise risk investment.

Workforce Shortages and Skills Gaps

A critical barrier is the shortage of qualified cybersecurity professionals. While the global cybersecurity workforce gap numbers in the millions, local governments are particularly affected—they cannot compete with private-sector salaries or recruitment incentives.

- Surveys indicate that over half of municipal leaders cite inability to pay competitive wages and limited staff as major hurdles [9].
- A critical barrier is the shortage of qualified cybersecurity professionals. While the global cybersecurity workforce gap numbers in the millions, local governments are particularly affected—they cannot compete with private-sector salaries or recruitment incentives.

- Surveys indicate that over half of municipal leaders cite inability to pay competitive wages and limited staff as major hurdles

Key takeaway: Municipalities must invest in local talent pipelines, upskilling current staff, and fostering cross-departmental cybersecurity knowledge to maintain operational resilience.

Leadership Engagement and Misunderstandings

Cybersecurity is a strategic governance issue, not merely an IT operational concern. Yet many local leaders mistakenly assume that technical staff alone can manage risk. This mindset creates organizational blind spots and leaves agencies exposed to preventable incidents.

- A county ransomware attack illustrates the consequences: halted services, lost trust, and millions in recovery costs [10].
- Without leadership involvement, risk assessments, policy alignment, and resource prioritization often fail, leaving critical systems vulnerable [11].

Key takeaway: Leaders must embed cybersecurity into governance, receive regular briefings, engage across departments, and maintain accountability at the executive and board levels.

Expanding Attack Surfaces

Modern work environments and cloud-based service adoption have dramatically increased exposure points. The traditional network perimeter is effectively gone.

- Remote work, personal devices, and third-party integrations create multiple potential attack vectors.
- Each endpoint—laptop, mobile device, or cloud service—represents a potential vulnerability if not properly managed.
- Ransomware, phishing, and other attacks exploit these expanded surfaces, affecting continuity, data integrity, and public trust.

Key takeaway: Municipalities must update policies, monitoring, and access controls to account for a distributed and dynamic threat landscape.

Disruptive Technology

Emerging technologies introduce both opportunities and complex cybersecurity challenges. Artificial intelligence (AI), machine learning, blockchain, IoT, and other innovations can enhance public services but also create new attack vectors.

- Risks tied to disruptive technologies can become entrenched if not addressed proactively. For example, unmonitored AI applications could automate decisions that compromise data integrity or introduce bias.
- Disruptive technologies may outpace existing policies, regulatory frameworks, or workforce capabilities, leaving gaps in governance and security.
- Without anticipatory planning, local governments can inherit systemic vulnerabilities that are costly and difficult to mitigate once widely deployed.

Key takeaway: Cyber governance must anticipate technological change by assessing potential risks, integrating them into procurement and policy decisions, and ensuring that staff, systems, and leadership are prepared for new threats.

Key Cyber Risk Areas in Local Government

Third-Party Risk Management

Local governments increasingly rely on vendors, contractors, cloud providers, and other external partners. While these relationships enable efficiency and innovation, they also introduce significant cyber risks beyond IT's direct control. Examples include supply chain vulnerabilities—like the SolarWinds attack—and privacy concerns related to emerging technologies. Managing these risks requires cross-departmental collaboration among legal, finance, procurement, and IT teams to ensure contracts, insurance, and audits adequately protect the organization. For more in-depth guidance, explore resources on managing third-party cyber risks.

Insider Threats

Threats from within the organization—whether intentional or accidental—pose unique challenges. Insider risks arise when employees, contractors, or trusted partners misuse access to systems or data. Addressing these threats demands not only technical controls like identity management but also employee training, background screening, and a strong security culture. Recent incidents in election security illustrate how insider vulnerabilities can impact highly sensitive processes.

Ethical Use of Artificial Intelligence (AI)

AI technologies offer promising benefits but raise ethical and security concerns, especially when weaponized for disinformation, surveillance, or election interference. Local governments must develop governance frameworks that ensure AI use aligns with ethical standards and safeguards public interests. Awareness of AI-driven threats, such as deep fakes, is essential for protecting democratic processes and community trust.

Privacy and Data Protection

Protecting residents' personal data is both a cybersecurity and a public trust imperative. Compliance with regulations like GDPR, HIPAA, and others must be integrated into risk management strategies. Beyond legal compliance, ethical stewardship of data is essential to prevent misuse and avoid breaches that could harm individuals or expose the government to legal and reputational risks.

Disinformation

Deliberate misinformation campaigns undermine public confidence, distort democratic processes, and can incite unrest. Technologies like AI-powered deep fakes amplify these threats by generating convincing false content, sometimes impersonating officials or altering public perception. Local governments must be aware of this evolving risk and coordinate responses across communication, cybersecurity, and public affairs teams. For more information on disinformation and response efforts, consult additional resources.

Critical Infrastructure Protection

Utilities, transportation, emergency services, and other critical systems underpin community well-being. Cyberattacks targeting these assets can disrupt services with serious safety and economic consequences. High-profile attacks such as NotPetya illustrate the potential scale of impact. Local governments must prioritize cybersecurity strategies that protect critical infrastructure in collaboration with regional and federal partners. Explore resources for critical infrastructure best practices, risk assessments, and protection.

Operational Technology (OT) Security

The convergence of OT systems—controlling water treatment, power plants, transit systems—with IT networks introduces new vulnerabilities. Many OT environments run legacy software with limited security controls, making them attractive targets for attackers. As OT and IT integrate, coordinated cybersecurity governance is essential to prevent attacks that could threaten public safety or cause environmental harm.

Convergence of Physical and Cybersecurity

Digital transformation blurs lines between physical and cyber risks. IoT devices, smart infrastructure, and interconnected control systems require coordination between physical security and cybersecurity teams. Joint governance helps reduce redundancies and ensures comprehensive protection of government assets. CISA's guidance on integrated risk management illustrates the best practices in this area.

Compliance and Regulatory Requirements

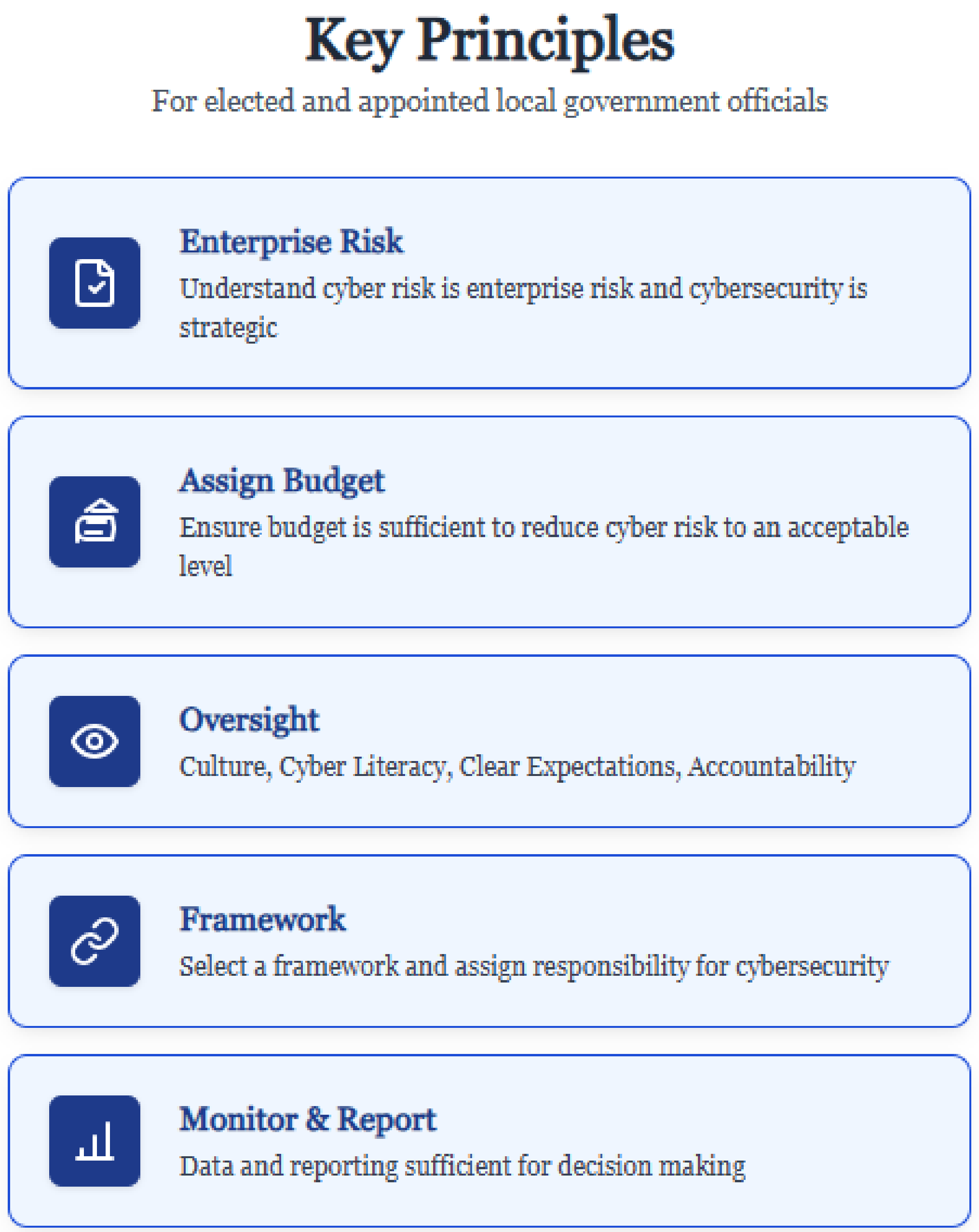
Local governments face a complex regulatory landscape—from CJIS and HIPAA to PCI and emerging cybersecurity disclosure mandates. Compliance efforts protect sensitive data, maintain public confidence, and reduce legal exposure. Effective compliance requires dedicated resources, ongoing monitoring, and often third-party validation to avoid costly penalties and reputational damage.

Section 4 - Cybersecurity Governance Principles for Local Officials

Section 4 –Cybersecurity Governance Principles for Local Officials

Cybersecurity is no longer just an IT issue—it's a leadership responsibility. As cyber threats grow more sophisticated, elected and appointed officials must take an active role in protecting public systems and data.

This section outlines five core principles—**Enterprise Risk, Budget Allocation, Oversight, Framework, and Monitor & Report**—that help guide effective cybersecurity governance. By embracing these, officials can strengthen resilience, safeguard public trust, and lead with confidence in an increasingly digital world.



Key Principles

For elected and appointed local government officials

Enterprise Risk
Understand cyber risk is enterprise risk and cybersecurity is strategic

Assign Budget
Ensure budget is sufficient to reduce cyber risk to an acceptable level

Oversight
Culture, Cyber Literacy, Clear Expectations, Accountability

Framework
Select a framework and assign responsibility for cybersecurity

Monitor & Report
Data and reporting sufficient for decision making

Principle 1- Enterprise Risk

> *"Enterprise risk is owned by the CEO and the board, not the CISOs or CSOs."*
>
> *— Jen Easterly, CISA Director*
>
> This highlights that cybersecurity is a top-level strategic concern, not just an IT issue.

Enterprise risk is defined as the effect of uncertainty on an organization's mission and objectives. For local governments and special districts, this includes a wide spectrum of threats—natural disasters, economic downturns, aging infrastructure, and public health crises. Increasingly, cybersecurity risks have emerged as a top-tier concern, with the potential to disrupt essential services, compromise sensitive data, and erode public trust.

While risks like wildfires or hurricanes often dominate headlines, cyber threats are more pervasive and may have more immediate consequences. A successful cyberattack can paralyze 911 systems, shut down water utilities, or expose confidential citizen data—making cybersecurity a matter of both operational continuity and public welfare.

Cyber threats are no longer isolated technical issues. They are strategic risks that impact every facet of municipal operations, including:

- Finance and budgeting
- Legal compliance and liability
- Emergency response and public safety
- Public health and infrastructure

To address this, many governments are adopting Enterprise Risk Management (ERM) frameworks. Within these frameworks, cyber risk must be treated as a core component, not a siloed IT issue. Learn more about ERM frameworks and integrating cyber risk from NIST.

Local government leaders, both elected and appointed, need access to unfiltered, actionable cyber risk information to make informed decisions. While transparency is paramount for finances and many government activities, cybersecurity and IT operations require a strategic degree of discretion.

This means that while financial implications are openly incorporated into staff reports and policy discussions, the full, granular details of cyber vulnerabilities, specific defense strategies, or ongoing threat intelligence should not be fully transparent to the broader public or even to all board members.[1]

Key leadership actions include:

- Understanding cyber risks as a top priority
- Grasping the potential impacts across departments
- Recognizing the need to mitigate threats proactively
- Ensuring decision-makers are equipped with timely, relevant information

[1] Why this distinction? Revealing sensitive cybersecurity information could inadvertently provide a roadmap for potential attackers, jeopardizing the very systems and data you aim to protect. A balance must be struck: leaders need enough detail to understand the risks and allocate resources effectively, but this information should be handled with a level of confidentiality to maintain security and avoid creating unnecessary panic or opportunities for exploitation.

The 2020 ICMA Cybersecurity Survey revealed a concerning gap: many local officials are unaware of the magnitude of cyber risks [5]. This lack of awareness can delay action and increase exposure.

Cyberattacks can erode confidence in government and undermine perceptions of effective governance [12].

Municipalities face similar cyber risks as private sector businesses, but with added public accountability. A breach can disrupt:

- Public health systems
- Emergency communications
- Utility services
- Citizen engagement platforms

With agencies like the TSA and EPA introducing cybersecurity mandates for critical infrastructure, non-compliance now carries regulatory and reputational risks. According to PwC's 2022 Pulse Survey, U.S. executives rank cyberattacks as the #1 business risk—a sentiment that should resonate equally in the public sector [13].

By recognizing cyber risk as a top-tier enterprise risk, local leaders can take decisive steps to protect their communities, uphold public trust, and ensure the continuity of essential services.

Cyber Risk Oversight for Leadership

Effective oversight is essential to ensuring that a local government's cybersecurity program is strategic, accountable, and aligned with organizational goals. As cyber threats grow more complex and regulations more demanding, leadership must take an active role in governing cybersecurity as a core enterprise risk.

Cyber risk oversight involves:

Key Questions for Enterprise Risk Management

To ensure a comprehensive and proactive approach to enterprise risk—including cybersecurity—elected officials and senior decision-makers should regularly ask the following questions:

1. What are the top risks—both cyber and non-cyber—that could disrupt our mission, services, or community trust? Are we regularly reviewing and updating our risk register to reflect evolving threats?
2. How are senior leaders, department heads, and governing bodies engaged in identifying, prioritizing, and addressing enterprise-wide risks? Is risk management integrated into strategic planning and decision-making?
3. How are cybersecurity risks incorporated into our broader enterprise risk management framework? Are cyber risks treated with the same urgency and oversight as financial, operational, and legal risks? Are cyber risks treated with the same urgency and oversight as financial, operational, and legal risks?
4. Do we have a well-documented and regularly tested incident response plan?
   How confident are we in our ability to respond effectively to a cyber incident or other crisis?
5. What systems or processes are in place to monitor emerging threats and adjust our risk posture accordingly? Are we leveraging internal audits, external intelligence, and peer networks to stay informed?
6. Are we dedicating adequate financial, technological, and human resources to mitigate and manage cybersecurity risks? How do our investments in cybersecurity compare to the value of the assets we are trying to protect?
7. How are we assessing and managing risks introduced by third parties, such as vendors, contractors, service providers, and intermunicipal partners? Do we require security standards or due diligence as part of procurement and contracting processes?
8. Is cybersecurity viewed as a shared responsibility across all departments and levels of leadership? Do employees and leaders understand their roles in maintaining our cybersecurity posture?

- Ensuring the cybersecurity program is effective and compliant
- Maintaining visibility into risk exposure and mitigation efforts
- Championing a culture of security across departments
- Allocating resources and talent to support cyber resilience

Given the cybersecurity talent shortage and increasing technical complexity, leaders must also consider how to leverage internal expertise and external support to maintain strong oversight.

Ultimately, cybersecurity governance is a leadership responsibility. It requires ongoing engagement, informed decision-making, and a commitment to protecting public assets and services.

For a detailed analysis of oversight challenges and recommendations, see oversight in action.

Integrating Cyber Risk into the Enterprise Risk Management Framework

Effectively managing cyber risk begins with integrating it into the broader Enterprise Risk Management (ERM) framework. This ensures that cybersecurity is not treated as a siloed technical issue, but as a strategic concern that is assessed, prioritized, and addressed alongside other critical risks.

Risk Identification and Assessment

The first step is to identify and assess cyber risks in the context of the organization's most critical assets—its "crown jewels." These may include sensitive data systems, operational infrastructure, communication networks, and public-facing services. A comprehensive risk assessment should account for both internal threats (e.g., insider misuse, policy lapses) and external threats (e.g., ransomware, nation-state actors, hacktivists).

This process involves:

- Conducting vulnerability assessments across people, processes, and technologies.
- Mapping critical assets and evaluating their exposure to cyber threats.
- Prioritizing risks based on potential impact and likelihood.

For a structured approach to identifying and protecting high-value assets, see protecting the crown jewels: how to secure mission-critical assets.

Policy and Governance Alignment

Once risks are identified, local governments must ensure that cybersecurity policies and procedures are current, comprehensive, and enforceable. This includes:

- Reviewing access control, data protection, and incident response policies.
- Ensuring alignment with legal and regulatory requirements.
- Updating business continuity and disaster recovery plans.

Third-Party Risk Management

Cyber risk doesn't stop at the organizational boundary. Vendors, contractors, and partners can introduce vulnerabilities that compromise government systems. As part of ERM, local governments should:

- Assess third-party cybersecurity practices.
- Include security requirements in contracts and procurement processes.
- Monitor compliance and performance over time.

By embedding cyber risk into the ERM framework, local leaders can ensure that cybersecurity is treated with the strategic importance it demands—not just as a technical safeguard, but as a pillar of operational resilience and public trust.Risk Mitigation and Cybersecurity Governance

Once cyber risks are identified, local governments must develop risk mitigation strategies to reduce or eliminate potential threats. These strategies should be both preventative and responsive, ensuring that systems are protected and that incidents are swiftly managed when they occur.

Preventative Measures

Mitigation begins with implementing technical safeguards such as:

- Firewalls and intrusion prevention systems
- Encryption for sensitive data
- Secure access controls and multi-factor authentication

These measures help reduce the attack surface and prevent unauthorized access. For guidance on implementing foundational cybersecurity controls, local leaders can refer to the MS-ISAC Local Government Cybersecurity Guide.

Cybersecurity Governance Structures

To ensure these strategies are effective and sustainable, local governments should adopt cybersecurity governance frameworks. Governance provides the structure and authority needed for decision-making, resource allocation, and accountability.

Key governance actions include:

- Establishing a cybersecurity oversight committee with representatives from IT, legal, finance, and operations.
- Defining clear roles and responsibilities for cyber risk management.
- Aligning cybersecurity goals with the organization's mission and risk appetite.

Incident Response Planning

Governance must also include incident response planning. A well-developed and regularly tested response plan ensures that when a cyber incident occurs, the organization can act quickly and effectively.

An incident response plan should cover:

- Containment of the threat
- Eradication of malicious actors or code
- Recovery of systems and data
- Post-incident analysis to improve future resilience

Templates and best practices for incident response planning are available in the NIST Cybersecurity Framework Policy Guide.

Leadership Responsibility and Culture of Cybersecurity

As emphasized throughout this guide, cyber risk is enterprise risk—and must be treated as such. For local governments, this means that elected officials, senior executives, and department heads must recognize cybersecurity as a strategic concern that directly affects their ability to deliver public services, protect taxpayer resources, and maintain public trust.

Cybersecurity Is a Leadership Issue

Cybersecurity is not just a technical challenge—it is a governance and leadership responsibility. Leaders must ensure that cybersecurity is embedded into organizational priorities, decision-making processes, and resource allocation. This includes:

- Setting the tone from the top
- Championing cybersecurity initiatives
- Holding departments accountable for cyber hygiene

For a foundational overview tailored to local government leaders, see the MS-ISAC Local Government Cybersecurity Guide.

Building a Culture of Cybersecurity

Creating a culture of cybersecurity means fostering values, attitudes, and behaviors that prioritize security across all levels of the organization. This culture should:

- Encourage proactive risk management
- Promote continuous learning and awareness
- Integrate cybersecurity into daily operations and strategic planning

The Organizational Cybersecurity Culture Model developed by MIT Sloan outlines practical mechanisms for leaders to build and sustain a strong cybersecurity culture.

Governance and Resource Commitment

Effective cybersecurity governance requires:

- A clear structure for oversight and accountability
- Regular review of policies and procedures
- Adequate funding for cybersecurity tools, training, and staffing

Leaders should also participate in assessments like the Nationwide Cybersecurity Review (NCSR)[2], which helps local governments benchmark their cybersecurity maturity and identify areas for improvement.

Continuous Monitoring and Improvement

Cybersecurity is not a one-time initiative—it is a continuous, evolving responsibility. As threats grow more sophisticated and dynamic, local governments must adopt a proactive approach to monitoring and improving their cybersecurity posture.

Real-Time Threat Detection

Continuous monitoring involves the ongoing assessment of systems, networks, and controls to detect vulnerabilities and threats in real time. Key practices include:

- Vulnerability scanning to identify exploitable weaknesses
- Penetration testing to simulate attacks and evaluate defenses

[2] Learn more about the Nationwide Cybersecurity Review (NCSR), an anonymous annual self-assessment designed to help state, local, tribal, and territorial (SLTT) governments measure and improve their cybersecurity programs based on the NIST Cybersecurity Framework.

- Security control evaluations to ensure safeguards remain effective

For practical guidance on implementing continuous monitoring, refer to the NIST SP 800-137 Information Security Continuous Monitoring (ISCM) Framework.

Adaptive Risk Management

Cyber threats evolve rapidly. To stay ahead, local governments must implement processes for continuous improvement, including:

- Regular updates to cybersecurity policies and procedures
- Integration of lessons learned from incidents and audits
- Ongoing training and awareness for staff and leadership

The CIS Cybersecurity Best Practices offer actionable steps for maintaining and improving cybersecurity defenses over time.

Maintaining a Risk Register

A risk register is a living document that tracks identified risks, their potential impacts, and the status of mitigation efforts. It serves as a central tool for:

- Communicating risk status to senior leadership
- Prioritizing resource allocation
- Documenting progress and accountability

The GAO Cybersecurity Program Audit Guide outlines best practices for maintaining a risk register and conducting regular audits to ensure transparency and effectiveness.

Principle 2 - Assign Budget

Key Questions for Assigning Budget to Cybersecurity

To ensure public funds are strategically allocated and cybersecurity risks are properly managed, decision-makers should ask:

1. What is the potential financial impact of a cyber incident on our operations, services, and reputation? Have we assessed the cost of downtime, data loss, legal liability, and recovery?

2. How much of our total budget is spent on technology, and what percentage of that is dedicated to cybersecurity (prevention, detection, and response)? Are we aligning our spending with the criticality of our systems and data?

3. Does our procurement process require it and cybersecurity staff to be involved in the evaluation and selection of new hardware, software, and services? Are purchases reviewed for security and operational risks before contracts are signed?

4. Are we conducting cybersecurity risk assessments for all new technologies, systems, or major upgrades before implementation? How are we weighing cybersecurity risks alongside functionality and cost?

5. Do our procurement policies require cybersecurity clauses in contracts with third-party vendors, including breach notification, incident response coordination, and data handling requirements? Are we minimizing our exposure to supply chain and vendor-related threats?

6. How often do we benchmark our it and cybersecurity spending against peer municipalities or relevant industry standards? Are we investing enough to meet basic expectations for resilience, compliance, and risk mitigation?

Cybersecurity is not merely a technical expense—it is a strategic investment in the continuity, safety, and trustworthiness of local government services. Cyberattacks can disrupt essential services, compromise sensitive citizen data, and result in financial losses that far exceed the cost of proactive investment. To manage cyber risk effectively, budgeting must be centralized, intentional, and risk-informed, ensuring that cybersecurity is prioritized across the entire organization.

Why Centralized Budgeting Matters

When technology spending is decentralized or ad hoc, often referred to as "shadow IT," it can lead to:

- Unsecured systems lacking standardized controls
- Inconsistent cybersecurity policies across departments
- Duplication of efforts and wasted resources
- Increased vulnerability to attacks due to fragmented oversight

A centralized IT and cybersecurity budget addresses these issues by:

- Improving visibility and accountability over all technology investments
- Reducing inefficiencies and redundancy in procurement and operations
- Aligning spending with organizational risk priorities, ensuring that high-risk areas receive appropriate attention and funding
- Facilitating coordinated planning across departments, integrating cybersecurity into strategic initiatives, service delivery, and long-term digital transformation

Centralized budgeting also empowers executive leadership and governing boards to see the full scope of cyber risk, make informed decisions, and set clear risk tolerance for the organization.

What Cybersecurity Funding Should Cover

A comprehensive cybersecurity budget should account for both capital and operational needs, including:

- **Initial Capital Investments**
    - Secure infrastructure (network segmentation, firewalls, cloud security)
    - Endpoint protection tools and multi-factor authentication (MFA) systems
    - Backup and disaster recovery solutions
- **Ongoing Operational Costs**
    - Security monitoring, vulnerability scanning, and threat intelligence services
    - Software subscriptions, patch management, and license renewals
    - Incident response planning and exercises
- **Human Resources**
    - Salaries and benefits for internal cybersecurity staff
    - External expertise (consultants, managed security services, penetration testing)
    - Training and upskilling programs to maintain a knowledgeable, vigilant workforce

By explicitly funding these areas, local governments can proactively manage risk, rather than relying on reactive spending after an incident occurs.

Industry Benchmarks for Budgeting

While there is no one-size-fits-all approach, several respected organizations provide benchmarks to guide budgeting decisions:

- NASCIO: 0–3% of the IT budget
- GFOA: ~2% of the IT budget
- ICMA: 0–10%, depending on risk profile and service complexity

These benchmarks are intended to help local leaders calibrate investments relative to the size, complexity, and risk exposure of their municipality, rather than as rigid mandates. Leaders should also adjust allocations dynamically as threat landscapes, technologies, and service priorities evolve.

Balancing Risk with Limited Funds

Local governments operate under tight financial constraints, yet the risks posed by cyber threats continue to escalate. To manage this tension, leaders must adopt a risk-based approach to cybersecurity budgeting—one that aligns spending with the potential impact and likelihood of threats.

Why Risk-Based Budgeting Matters

Cybersecurity investments should be strategic, not reactive. By prioritizing risks, governments can:

- Focus resources on the most critical vulnerabilities
- Avoid overspending on low-impact threats
- Ensure that cybersecurity supports broader public service goals

Understanding the full financial exposure to cyber risk—including direct costs (e.g., legal fees), indirect costs (e.g., reputational damage), and insurance implications—is essential for informed decision-making.

Learn more about effective risk-based budgeting strategies for local governments.

The True Value of Cybersecurity Investment

Cybersecurity is often seen as a cost, not a return. But the financial fallout from a cyberattack – service disruptions, investigations, recovery, fines, and reputational damage – can vastly outweigh proactive security spending.

Think of cybersecurity as risk avoidance. Preventing just one incident can save millions and preserve public trust. A single breach can lead to:

- Service disruptions
- Emergency response costs
- Increased insurance premiums
- Lower credit ratings

It's crucial to understand that a bigger cybersecurity budget doesn't automatically mean better protection. Effectiveness hinges on how resources are used, not just the amount spent.

Key factors for cybersecurity success include:

- Strong governance and executive oversight
- Clear staff roles and accountability
- Ongoing training and awareness
- Risk-informed decision-making
- Operational resilience and recovery capabilities

Organizations that invest wisely, focusing on outcomes rather than just expenses, are far better prepared to prevent attacks and recover quickly when incidents happen.

Strategic Approval of Cyber Investments

Cybersecurity expenditures—whether for infrastructure, software, or third-party services—must be justified, transparent, and aligned with public accountability. Leaders should:

- Require formal business cases for major IT projects
- Tie spending to specific service outcomes
- Ensure procurement follows established policies

For more in-depth guidance on budgeting, financial planning, and robust procurement policies specific to local government IT and cybersecurity investments, explore strategies for getting cyber investments approved.

Capital vs. Operational Budgets and Cost Comparisons

Understanding the difference between capital and operational spending is essential when evaluating cybersecurity investments. One-time infrastructure upgrades and hardware purchases often fall under capital budgets, while recurring expenses—such as software licensing, monitoring tools, and security services—are typically part of the operational budget.

This distinction can complicate internal budget planning and external cost comparisons, especially across organizations with differing accounting practices. Relying solely on benchmarks or percentage-of-IT-spend metrics can be misleading. Instead, cybersecurity funding should be aligned with the organization's overall risk tolerance, digital footprint, and strategic priorities.

Find out more about structuring cyber budgets for guidance on aligning funding with enterprise risk.

Staffing and Outsourcing

Human capital remains one of the most critical components of any cybersecurity strategy. Many local governments operate with lean IT teams, and cybersecurity roles may be under-resourced or entirely absent. This creates gaps in monitoring, response, and overall preparedness.

For organizations with limited internal capacity, external partnerships can play a supporting role—but cannot fully replace the need for internal knowledge and readiness. Cybersecurity is not a one-time task, and success depends on maintaining institutional awareness, internal coordination, and leadership engagement.

Staffing decisions must also account for the evolving threat landscape. Ongoing professional development, role clarity, and accountability are essential for sustaining a workforce capable of responding to today's risks and tomorrow's challenges.

Explore staffing models and outsourcing options to evaluate what works best for your agency's size and capacity.

Strategic Cybersecurity and Technology Needs

Cybersecurity and technology infrastructure should be treated as strategic assets—not just operational necessities. As government services become increasingly digital, the resilience of IT systems directly affects public trust, service continuity, and regulatory compliance.

Investments in technology must be forward-looking and risk-informed. This includes ensuring core systems are maintained, patched, and adequately protected against emerging threats. Treating IT and cybersecurity as shared priorities across leadership ensures that decisions about infrastructure, staffing, and policy are made with security in mind from the outset.

Access to funding—whether from internal budgets or external grants—can be a critical enabler. Competitive grant programs may offer opportunities for high-impact projects, particularly in areas related to critical infrastructure or regional coordination.

Insurance and Risk Pooling

Cyber insurance is increasingly a component of municipal risk management strategies. However, the cost and availability of coverage can fluctuate significantly based on an organization's size, security posture, and claims history.

Participating in a risk pool or consortium can offer municipalities better negotiating power, more predictable premiums, and shared access to expertise. In addition to financial benefits, such collaborations can foster stronger regional resilience by encouraging common security standards and coordinated response planning.

Read our overview of municipal cyber insurance for a breakdown of trends, benefits, and emerging challenges.

Explore options for risk pooling and shared services to support sustainable cyber risk management.

Principle 3 - Oversight

Cybersecurity oversight is a legal, ethical, financial, and strategic responsibility for senior leadership in local government. As cyber threats grow in complexity and impact, elected and appointed officials must ensure that systems are in place to monitor risks, assess vulnerabilities, allocate resources, and inform decision-making. Oversight cannot be delegated solely to IT staff—it requires direct engagement at the governance level.

Why Oversight Matters

Oversight is not just about compliance—it is about resilience, accountability, fiduciary responsibility, and public trust. Local officials are stewards of public resources, and cyber incidents can cost anywhere from minimal sums to millions of dollars. Because the financial, operational, and reputational consequences are so significant, cyber risk must be overseen with the same seriousness as financial and legal risk.

Leaders must:

- Stay informed about cyber risks, emerging threats, and their financial implications.
- Ensure safeguards are in place, resourced appropriately, and functioning as intended.
- Promote transparency and responsible disclosure to maintain public trust.
- Treat cyber risk explicitly as an enterprise risk, not just a technical issue.

Recent legal and regulatory decisions have reinforced that executives and governing bodies must take reasonable steps to oversee cybersecurity, making it a core governance issue.

The Role of Internal Audit

Internal audit teams provide **independent assurance** that cybersecurity measures are effective. Their evaluations help leadership understand:

- System vulnerabilities.
- Control effectiveness.

Key Questions for Cybersecurity Oversight:

Elected officials and senior decision-makers play a critical role in ensuring that cybersecurity is treated as a governance priority—not just a technical issue. the following questions can help guide oversight conversations to ensure the municipality is proactively managing cyber risk.

1. What sensitive data do we collect, store, and share—and what protections are in place to keep it secure? (think: financial records, personal information, infrastructure systems.)
2. What are the most significant cyber risks facing our municipality? How are we preparing to prevent, detect, and respond to them?
3. Do we have clear, up-to-date policies and procedures for cybersecurity? How do we know they are being followed?
4. Who is responsible for cybersecurity across departments? How are staff and contractors trained, monitored, and held accountable?
5. What is our incident response plan? Do we know what to do if we are hacked or experience a ransomware attack?
6. Are we budgeting enough for cybersecurity? How do we ensure those dollars are being spent strategically and effectively?
7. What cybersecurity regulations or legal requirements apply to us? How do we ensure compliance?
8. Who oversees cybersecurity at the leadership level? How often are we briefed on cyber risks and progress?
9. What cybersecurity best practices or frameworks are we following? How do they help guide our efforts?

- Risk exposure across departments.

Audit findings should be reported directly to senior officials or boards to ensure independence and transparency. For audit tools and assessment frameworks, see MRSC's Cybersecurity Resources for Local Governments.

Board Oversight and Accountability

Cybersecurity is no longer just a technical issue—it is a governance and fiduciary responsibility. Councils and boards must treat cyber risk with the same level of attention and urgency as financial oversight, because both have direct implications for public trust and fiscal stability.

As emphasized in the Cyber Risk Oversight 2023 report, boards and councils have a duty to ensure that management is actively building resilient systems and that cybersecurity is embedded into all organizational decisions [14].

Cyber Literacy and Strategic Alignment

Boards must develop cyber literacy to understand the implications of technology and data-related decisions. Every major initiative—whether operational, financial, or service-related—carries potential cyber risk. Cybersecurity should therefore be integrated into strategic planning, enterprise risk management, and performance evaluation. Building cyber literacy at the governance level ensures that leaders can ask the right questions and hold management accountable.

Explore practical guidance on building board-level cyber literacy and aligning cybersecurity with governance.

Executive Access and Budget Transparency

Boards should ensure that the Chief Information Security Officer (CISO), or equivalent role, has a direct and unfiltered voice at the leadership table. In smaller jurisdictions, this role may be shared or outsourced, but the function must exist.

Cybersecurity budgets should be clearly defined and transparent, covering both capital and operational expenditures. Given that cyber incidents can have multimillion-dollar consequences, funding must be risk-informed and explicitly overseen by governing bodies.

It is important to note that some municipalities may have rules governing what information can be shared with different officials. For example, council members, boards, or committees may have varying levels of access to sensitive cybersecurity data. Leaders must ensure that the right parties are privy to the right information, balancing transparency with security and legal compliance.

Briefings and Ongoing Education

Regular briefings from cybersecurity leadership help boards stay informed about current threats, vulnerabilities, and response efforts. Ongoing education ensures that board members remain up to date on emerging risks, evolving technologies, and best practices in governance.

Cross-Departmental Collaboration

Cybersecurity must be a shared responsibility across the organization. Boards should support collaboration between IT, finance, legal, risk management, and operational departments to ensure that cybersecurity is integrated into all aspects of governance, not siloed as a technical function.

Learn how to foster collaboration within and across departments.

Reporting Cybersecurity Incidents

Transparent and timely reporting of cybersecurity incidents is essential for maintaining public trust, accountability, and operational integrity. When a breach occurs, local officials must communicate clearly and responsibly—balancing openness with the protection of sensitive information and compliance with municipal rules.

Why Reporting Matters

Failure to disclose incidents appropriately can have serious consequences:

- Undermining public confidence in government operations.
- Delaying corrective action or remediation efforts.
- Increasing reputational, legal, and financial damage, sometimes reaching millions of dollars in impact.

The Marin County Grand Jury's 2023 report highlighted the consequences of delayed disclosure, including losses from wire fraud and multiple network breaches that were not publicly reported until years later [15]. These events underscore the need for predefined, well-documented incident reporting protocols that clarify who receives information, when, and in what format.

Leadership's Role

Elected and appointed officials have a fiduciary responsibility to ensure that cyber risks are communicated promptly and accurately. Key leadership responsibilities include:

- Ensuring cybersecurity incidents are reported directly to the governing body or relevant decision-makers without filtration or delay.
- Making sure public communications are accurate, appropriately scoped, and legally compliant.
- Protecting sensitive details to avoid compounding operational or reputational risk.
- Following municipal rules regarding information sharing, so that only the appropriate officials—e.g., council members, boards, or executive leadership—receive specific details.

Direct access to the Chief Information Security Officer (CISO), or CISO equivalent, is critical in this context. The CISO provides unfiltered, risk-informed information that allows officials to make timely, strategic, and legally sound decisions.

Local Governments' Role in Cyber Incident Response

Cybersecurity is a shared, enterprise-wide responsibility. Leaders—from mayors and city managers to board members—must treat cyber risk with the same urgency as public safety, financial oversight, and legal compliance. Effective incident response is not merely a technical exercise; it is a coordinated organizational effort that requires governance engagement, resource allocation, and cross-departmental collaboration.

Key responsibilities for elected and appointed officials include:

- Modeling secure behavior and ensuring staff comply with organizational policies.
- Fostering a cyber-aware culture across all departments.
- Understanding the organization's risk exposure, critical assets, and continuity plans.

- Knowing their roles in the event of a breach, including decision-making authority and communication responsibilities.
- Allocating and approving appropriate budget and resources for cybersecurity and incident response.
- Preventing shadow IT and unauthorized systems through centralized oversight.
- Ensuring that vendor contracts include cybersecurity provisions and accountability clauses.

For real-world examples and detailed guidance, visit NIST's incident response resources.

Testing and Readiness

Having an incident response plan is necessary but not sufficient. Plans must be exercised regularly to ensure readiness, identify gaps, and validate coordination across departments. Leadership must actively participate in exercises to understand response workflows, decision-making processes, and reporting protocols.

For practical guidance, local governments can reference:

- NIST Incident Response Resources for step-by-step guidance and best practices.
- CISA Cybersecurity Incident Response Playbooks for exercise design, scenario testing, and lessons learned.

By embedding incident response into governance and ensuring oversight at all levels, local governments strengthen their resilience, accountability, and public trust, while reducing the potential financial, operational, and reputational impacts of cyber incidents.

Principle 4 - Framework

A cybersecurity framework provides the strategic structure that guides how local governments manage cyber risk. It defines the principles, roles, and processes that shape how an organization identifies, protects against, detects, responds to, and recovers from cyber threats.

Frameworks are essential because they:

- Standardize cybersecurity practices across departments
- Align with regulatory requirements
- Support communication between technical teams and leadership
- Enable benchmarking and continuous improvement

The most widely adopted frameworks—such as the **NIST Cybersecurity Framework (CSF)**—are designed to be flexible, scalable, and adaptable to evolving threats. These frameworks are foundational to many public-sector cybersecurity policies and are increasingly required for compliance and funding eligibility.

For a comparison of leading cybersecurity frameworks and guidance on selecting the right one for your organization, visit the resource center.

By adopting a recognized framework, local governments can ensure that cybersecurity is integrated into governance, risk management, and operational planning—not treated as an isolated technical issue.

Benefits of Using a Cybersecurity Framework

Adopting a cybersecurity framework provides local governments with a structured, strategic approach to managing cyber risks. Frameworks like the NIST Cybersecurity Framework (CSF) help ensure that cybersecurity efforts are aligned with best practices, regulatory expectations, and organizational goals.

Why Frameworks Matter

Adopting a recognized cybersecurity framework provides a structured, repeatable approach to managing cyber risk. Frameworks help local governments translate technical security practices into organizational priorities, creating a common language across departments, boards, and external partners.

Key Questions for Cybersecurity Framework Selection:

Selecting a cybersecurity framework is a foundational decision that shapes how a local government manages risk. Elected officials and senior leaders can support this effort by asking:

1. Is the cybersecurity framework appropriate for our size, mission, and the services we provide to the public?
2. How does this framework help us align cybersecurity with our overall risk management and continuity planning?
3. Given our staffing and budget constraints, how can we use this framework in a practical way—through regional partnerships, shared services, or vendors?
4. Does the framework help us meet our legal and regulatory obligations—such as those tied to criminal justice data, healthcare, or financial systems?
5. Will this framework improve how we communicate cybersecurity risks and responsibilities across departments—and with the public, board, or council?
6. What steps are in place to review and update our approach regularly as new threats and technologies emerge?
7. How does the framework help define roles and responsibilities—so that staff, leadership, and third-party partners understand what's expected of them?

Key benefits include:

- **Integration with Enterprise Risk Management (ERM):** Frameworks embed cybersecurity into broader organizational risk strategies, ensuring that digital threats are assessed alongside financial, operational, and legal risks.
- **Improved Communication:** By standardizing terminology and processes, frameworks make it easier for IT teams, leadership, governing boards, and external stakeholders to discuss cyber risks, mitigation strategies, and progress.
- **Regulatory Compliance and Due Diligence:** Frameworks guide adherence to relevant laws, regulations, and contractual obligations, helping municipalities demonstrate "reasonable security" in the event of an incident—a critical factor for legal and insurance purposes.
- **Continuous Improvement:** Established frameworks encourage ongoing assessment, monitoring, and adaptation, enabling organizations to evolve with the threat landscape rather than react only after incidents occur.

Examples of widely used frameworks include:

- **NIST Cybersecurity Framework (CSF 2.0)** – Focuses on Identify, Protect, Detect, Respond, Recover, with an added **Govern Function** emphasizing leadership responsibility and governance.
- **CIS Controls** – Provides prioritized, actionable guidance for operational security improvements.
- **ISO/IEC 27001** – Offers comprehensive standards for information security management systems.

Cybersecurity Framework Considerations for Small Local Governments:

For smaller local governments with limited resources, adopting a cybersecurity framework can feel overwhelming. These guiding questions can help tailor an approach that's right-sized, realistic, and effective:

1. Can we partner with neighboring towns, regional councils, or county agencies to share cybersecurity expertise and reduce costs?
2. Which parts of a cybersecurity framework—like monitoring, backups, or incident response—can we outsource to trusted vendors or managed service providers?
3. How do we make sure outside experts or vendors are aligned with our policies and reporting structures, and are accountable for protecting our systems and data?
4. Are we focusing on the most important first steps—such as password policies, backups, staff training, and multi-factor authentication—to reduce risk with minimal cost?
5. How will we review and update our cybersecurity practices regularly, even if we don't have a full-time IT or security team?

Framework Adoption for Small and Mid-Sized Governments

Smaller jurisdictions often face challenges in adopting full frameworks due to limited staff, expertise, and budget. However, the benefits—reduced risk, improved operational resilience, and alignment with cyber insurance requirements—are substantial.

Practical approaches for smaller governments include:

- **Shared Services:** Collaborate with regional councils, state agencies, or municipal networks to pool expertise and resources.
- **CISO-as-a-Service or Managed Security Services:** Outsourcing strategic cybersecurity leadership or operational functions can provide guidance and framework implementation without requiring full-time internal staff.

Scaled Implementation: Focus on high-priority functions first, such as access control, incident response, and critical infrastructure protection, then expand as capacity allows.

Explore scalable adoption strategies for smaller local governments.

Aligning Cybersecurity and Risk Management

To be effective, cybersecurity must be treated as a strategic, enterprise-level concern. Alignment with ERM ensures that cyber risk is not siloed within IT but incorporated into governance, budgeting, and service delivery decisions.

Why Alignment Matters:

- **Holistic Risk Evaluation:** Cyber risks are assessed alongside operational, financial, and legal risks, enabling leadership to prioritize mitigation based on organizational impact.
- **Leadership Visibility and Accountability:** Boards, councils, and executives receive clear, actionable insights, supporting informed decision-making and demonstrating due diligence.
- **Strategic Integration:** Cybersecurity initiatives are linked to organizational objectives, service continuity, and fiduciary responsibilities, ensuring that investments and policies reflect both risk reduction and mission alignment.

Ongoing Cybersecurity Awareness and Training

A framework or risk-aligned strategy is only effective if people understand and act on it. Cybersecurity is a shared responsibility across the organization, and leadership plays a critical role in modeling expectations.

Best practices for cultivating awareness include:

- **Regular Training for All Staff:** Cover phishing, social engineering, data handling, and incident reporting.
- **Executive and Board Briefings:** Ensure leadership understands current threats, risk mitigation progress, and resource needs.
- **Simulated Exercises and Drills:** Test incident response, continuity plans, and decision-making processes in realistic scenarios.
- **Clear Accountability:** Establish roles and responsibilities for all departments, integrating cybersecurity into performance evaluations where appropriate.

Access training strategies and awareness-building tools.

By combining a recognized framework with ERM alignment and continuous awareness-building, local governments can transform cybersecurity from a technical function into an enterprise-wide strategic asset, enhancing resilience, regulatory compliance, and public trust.

Principle 5 - Monitor & Report

Effective cybersecurity governance depends on continuous monitoring and transparent reporting. Oversight is not a one-time check; it is an ongoing process that enables leadership to understand, prioritize, and mitigate risks in alignment with organizational objectives. Boards and councils play a central role in this process, receiving regular updates that allow them to make informed, risk-based decisions.

Strategic Oversight

Cybersecurity is now a strategic concern for local governments. Boards must ensure that:

- Cyber risks are monitored continuously, with alerts and trend analysis informing leadership of emerging threats.
- Management provides regular, meaningful updates on risk posture, remediation efforts, and resource allocation.
- Organizational resources—budget, staff, and tools—are aligned with the most pressing cyber threats.

Frameworks like the NIST Cybersecurity Framework (CSF) and Capability Maturity Model Integration (CMMI) help organizations assess their cybersecurity maturity and track progress over time.

Boards must make cybersecurity decisions in the context of enterprise risk management. Perfect cybersecurity is unattainable, but informed decision-making enables:

- Prioritization of high-impact risks
- Strategic allocation of budget and personnel
- Integration of cybersecurity with operational, financial, and legal planning

By linking cyber reporting to strategic objectives, boards can balance technical input with fiduciary responsibility, ensuring that security investments support both resilience and public accountability.

Key Questions for Monitoring & Reporting on Cybersecurity:

To fulfill their oversight role, elected officials and decision makers need clear, consistent insights into cybersecurity risks and readiness. These questions can help guide meaningful dialogue with staff and ensure accountability:

1. How are we, as a board or council, regularly informed about cybersecurity risks, incidents, and progress—beyond just technical updates?
2. How is our local government using recognized tools like the NIST cybersecurity framework to assess and improve our cyber risk posture?
3. Can models like CMMI or other maturity assessments help us understand where we stand and where we need to improve?
4. Given limited time and budget, how do we decide which cybersecurity risks to address first—and which investments will deliver the most impact?
5. What cybersecurity performance indicators should we expect in reports—such as incidents detected, staff training completion, or response times?
6. Are reports to the board or council clear, focused on risk and outcomes, and designed to support informed decisions—not just technical summaries?
7. How are cybersecurity decisions aligned with our broader risk management and budget planning efforts?
8. Are we spending based on the most pressing risks?

Reporting and Communication

Cybersecurity reports should be clear, actionable, and appropriately scoped. Key principles include:

- **Clarity:** Avoid excessive technical jargon; highlight key findings and risk trends.
- **Actionability:** Reports should indicate areas needing leadership attention or decision-making.
- **Confidentiality:** Sensitive data should be shared securely and, when necessary, only in closed sessions with decision-makers.

Boards must also account for local policies and regulations that dictate what information can be shared with council members versus elected officials, ensuring that the right parties have access to the right information at the right time.

Relevant Report Metrics

Metrics are the backbone of strategic cybersecurity oversight. Reports should provide concise, meaningful insights without overwhelming non-technical decision-makers.

Metrics should enable leadership to:

- Understand the evolving threat landscape and emerging risks
- Evaluate the organization's overall risk exposure
- Monitor compliance with regulations and cybersecurity frameworks
- Assess the effectiveness of incident response and recovery efforts
- Track staff awareness and training participation across departments
- Review budget allocation and resource utilization
- Measure security performance, progress, and trend improvements over time

Designing Metrics for Impact:

Metrics should be aligned with strategic goals, supporting discussion among boards, councils, and executives. Examples include:

- Number of critical vulnerabilities identified and mitigated
- Time to detect, respond, and recover from incidents
- Progress against framework or ERM-aligned objectives
- Level of departmental compliance with security policies
- Cybersecurity budget utilization versus planned investment

When properly designed, these metrics help boards translate technical activity into actionable governance insights, enabling proactive oversight and fostering a culture of accountability and resilience.

Key Areas to Monitor

Reports should include high-level insights in the following categories:

- **Threat Landscape**: Emerging threats and potential impacts
- **Risk Assessment**: Top risks and mitigation status
- **Compliance**: Regulatory alignment and gaps

- **Incident Response**: Recent events and lessons learned
- **Awareness & Training**: Culture-building efforts and outcomes
- **Budget & Resources**: Financial commitment and constraints
- **Security Metrics**: Trends in detection, response, and vulnerability management

Boards should also be briefed on the methodology used to balance cyber risk with financial investment, ensuring that resources are directed toward the most pressing threats.

For guidance on risk-based prioritization and investment strategies, visit our resource center.

Implementing Key Performance Indicators (KPI)

Cybersecurity performance should be measured with clear, objective indicators that go beyond ad hoc updates or reactive reporting. While IT leadership often bears the burden of communicating cyber risk, boards and executives need structured, strategic insights to make informed decisions—especially during a crisis.

Key performance indicators (KPIs) help organizations:

- Track progress toward cybersecurity goals
- Evaluate the effectiveness of training, insurance coverage, and incident response
- Benchmark performance using recognized standards (e.g., NIST, COBIT, ISO 27001, CIS)
- Dashboards that consolidate and visualize these KPIs over time can support better governance and resource allocation.

For KPI templates and examples, visit the resource center.

Cybersecurity Legal Review and Updates

Cybersecurity laws and regulations are evolving rapidly. Boards and senior leaders must stay informed about new and emerging legal obligations that affect data protection, incident reporting, and organizational accountability.

Recent developments include:

- **Federal Information Security Modernization Act (FISMA)** – Now applies more stringently to state and local governments, requiring them to implement robust protections for information systems and report incidents in a timely manner.
- **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)** - Requires organizations in critical infrastructure sectors—including many local government services—to report cyber incidents within 72 hours and ransomware payments within 24 hours.
- **State and Local Government Cybersecurity Act of 2021** - Continues to provide federal support and resources to local governments through grants, cooperative agreements, and training programs.
- **State-level privacy laws**, such as California's CCPA and CPRA, which expand consumer data rights and organizational responsibilities.

For summaries of relevant laws and compliance checklists, visit the resource center or contact your respective legal counsel.

Conclusion

Cybersecurity is no longer a peripheral concern—it is a core leadership responsibility. As local governments increasingly depend on digital infrastructure to deliver essential services, the risks posed by cyber threats have become both strategic and existential. These risks, if left unaddressed, can disrupt operations, compromise sensitive data, erode public trust, and inflict lasting financial damage.

Local government officials must recognize that cyber risk is enterprise risk. It affects every department, every service, and every resident. Just as leaders prepare for natural disasters or public health emergencies, they must now prepare for cyber incidents with the same level of urgency and foresight.

The reality is stark: cybersecurity failures are no longer just technical failures—they are governance failures. Inaction or disengagement at the leadership level is no longer defensible. The consequences of a breach can extend beyond operational disruption to legal liability, reputational harm, and even electoral accountability.

Yet the path forward is clear. By:

- Embracing cybersecurity as a strategic priority,
- Embedding it into governance and risk management,
- Allocating resources based on risk, and
- Fostering a culture of awareness and resilience,

local leaders can transform cybersecurity from a point of vulnerability into a pillar of public trust and operational strength.

This guide has outlined the “what” and “why” of cybersecurity for local government officials. The “how” is available through the companion resources—but the first and most important step is leadership engagement.

References

[1] News Staff, “What is the average downtime for a ransomware attack on a government entity?,” GovTech. Accessed: Sep. 20, 2025. [Online]. Available: https://www.govtech.com/question-of-the-day/what-is-the-average-downtime-for-a-ransomware-attack-on-a-government-entity

[2] P. Mahendru, “The State of Ransomware in State and Local Government 2024,” Sophos News. Accessed: Apr. 29, 2025. [Online]. Available: https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/

[3] S. Fox-Sowell, “Cyberattacks on state and local governments rose in 2023, says CIS report,” StateScoop. Accessed: Sep. 20, 2025. [Online]. Available: https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024/

[4] P. Harmon, “Cybersecurity challenges faced by local governments in 2025 | Smart Cities Dive,” Smart Cities Dive. Accessed: Sep. 20, 2025. [Online]. Available: https://www.smartcitiesdive.com/news/archive-acc-cybersecurity-challenges-faced-by-local-governments-in-2025/754778/

[5] D. Norris, “A Look at Local Government Cybersecurity in 2020,” *ICMA*, Jul. 2021. Accessed: Dec. 05, 2022. [Online]. Available: https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020

[6] D. Warn, “Why Cyber Resilience Must Be A Local Priority,” Forbes. Accessed: Sep. 20, 2025. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2025/07/23/why-cyber-resilience-must-be-a-local-priority/

[7] S. Brandofino, “Unseen Threats: Addressing Cybersecurity In All Local Governments | GovPilot,” GovPilot. Accessed: Sep. 20, 2025. [Online]. Available: https://www.govpilot.com/blog/unseen-threats-addressing-cybersecurity-in-all-local-governments-govpilot

[8] Center for Internet Security, “Nationwide Cybersecurity Review: 2023 Summary Report,” 2023. Accessed: Jan. 21, 2025. [Online]. Available: https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report

[9] SmartCitiesWorld, “Funding a barrier to local government cyber-security,” Smart Cities World. Accessed: Sep. 20, 2025. [Online]. Available: https://www.smartcitiesworld.net/news/funding-a-barrier-to-local-government-cyber-security-1640

[10] Suffolk County Legislature, “Report On The 2021-2022 Cyber-Attack On Suffolk County,” Sep. 2024.

[11] ICMA, “Expert Interview: Cybersecurity Awareness Training for Local Government Employees,” ICMA Blog. Accessed: Sep. 20, 2025. [Online]. Available: https://icma.org/blog-posts/expert-interview-cybersecurity-awareness-training-local-government-employees

[12] R. Shandler and M. A. Gomez, “The hidden threat of cyber-attacks – undermining public confidence in government,” *Journal of Information Technology & Politics*, vol. 20, no. 4, pp. 359–374, Oct. 2023, doi: 10.1080/19331681.2022.2112796.

[13] PricewaterhouseCoopers, “PwC Pulse Survey: Managing business risks 2022,” PwC. Accessed: Sep. 20, 2025. [Online]. Available: https://www.pwc.com/us/en/library/pulse-survey/managing-business-risks.html

[14] L. Clinton, “Director’s Handbook on Cyber-Risk Oversight,” NACD, 2023.

[15] M. Pera and The Marin Independent Journal, “Marin Grand Jury Report: Cybersecurity Improved, Not Perfect,” GovTech. Accessed: Sep. 20, 2025. [Online]. Available: https://www.govtech.com/security/Marin-Grand-Jury-Report-Cybersecurity-Improved-Not-Perfect.html