2025 EBOOK ISSUE

THE CYBER SECURITY CRISIS: A GUIDE FOR LOCAL GOVERNMENTS IN NEW YORK STATE

UNDERSTANDING THREATS, RESPONSIBILITIES, AND PROTECTIONS

By Lisa A Brown, CEO & Founder
CST Group Inc. & IT For Local Government

IT
FOR LOCAL GOVERNMENT
Powered by CST Group Inc

14923 State Route 30, Malone, NY 12953 518-483-4100 www.cstsupport.com

ABOUT THE AUTHOR

Lisa A. Brown

CEO and Founder of CST Group, Inc. | Pioneering Entrepreneur, Cybersecurity Expert, Author, Speaker and Inspirational Leader

Lisa A. Brown is a trailblazing entrepreneur, cybersecurity expert, author, speaker and inspirational leader who has transformed the landscape of technology, business, and leadership. As the founder and CEO of CST Group, Inc. (dba Computer Support & Training, dba IT For Local Government), Lisa has redefined industry standards with her unwavering commitment to excellence and innovation.

With a Bachelor's Degree in Information Technology and a Master's in Business Communications (specializing in Leadership and Influence), Lisa blends technical expertise with strategic insight. Her academic foundation has enabled her to navigate the complexities of business with confidence and foresight.

A best-selling author, Lisa co-wrote *From Exposed to Secure: The Cost of Cybersecurity and Compliance Inaction and the Best Way to Keep Your Company Safe*, which became an Amazon #1 bestseller in three categories within 24 hours of its' release in 2024. Through her writing, she offers valuable guidance on overcoming the challenges of cybersecurity and compliance, helping businesses protect their digital assets and thrive in an increasingly complex environment.

In addition to her entrepreneurial and academic achievements, Lisa recently expanded her influence into the world of media as an executive producer and co-star of the Amazon documentary *Cybercrime: Fallout*. This groundbreaking documentary explores the evolving landscape of cybercrime, its global impact, and the critical importance of cybersecurity in today's digital world. Through her leadership and on-screen presence, Lisa sheds light on the complexities of cyber threats and the urgency of proactive security measures, empowering viewers to take action and safeguard their businesses and personal information. Her role in *Cybercrime: Fallout* reflects her continued commitment to raising awareness and driving change in the fight against cybercrime.

Drawing on her early career in local government, Lisa developed a deep understanding of the challenges municipalities face in protecting their systems and data with limited resources. That insight inspired the creation of *IT For Local Government*, a division of CST Group dedicated to empowering towns, villages, and cities across New York State with enterprise-level cybersecurity and technology solutions tailored to their unique needs. Through this initiative, Lisa continues her mission to bridge the technology gap in public service, helping local governments stay secure, compliant, and resilient in an increasingly digital world.

Lisa's journey from humble beginnings to the pinnacle of success is a powerful testament to resilience, determination, and the impact of visionary leadership. Through her work, she continues to inspire others to dream big, break barriers, and make a lasting difference in the world.

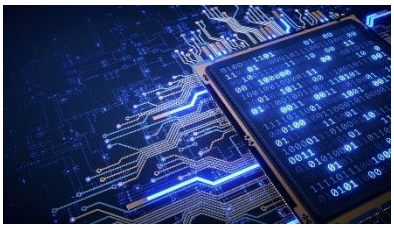
Table of Contents

Introduction

The Growing Importance of Cybersecurity

In today's increasing digital world, the security of technology systems is no longer a luxury but a necessity for local governments. Towns and villages, often with limited resources and no dedicated IT staff, face an alarming rise in cyber threats targeting their networks and data. These attacks, whether from hackers, ransomware, or data breaches, can cripple essential services, disrupt operations, and put sensitive citizen information at risk. As more government functions move online, the vulnerabilities associated with outdated systems or poorly managed technology are growing, making cybersecurity a critical issue for local leaders to address.

The consequences of a cyber-attack on local government can be devastating. Beyond the immediate financial costs, whether from ransom payments or system restoration, there are long-term reputational damages that can erode public trust. Residents expect their local officials to protect their personal data and ensure the continuity of vital services like public safety, utilities, and emergency response. Failure to prioritize cybersecurity can jeopardize these functions, leaving communities exposed to greater risk and potentially undermining the work that towns and villages do every day to serve their residents.



As the threat landscape evolves, it's imperative that local leaders take proactive steps now to address these challenges. The future success of their communities depends on a robust cybersecurity strategy that not only mitigates risks but also prepares them for the digital demands of tomorrow.

The specific challenges faced by local governments

Local governments, particularly towns and villages in New York State, face unique cybersecurity challenges that often differ from those of larger municipalities or private enterprises. One of the most significant obstacles is the lack of dedicated IT resources. Many smaller local governments do not have full-time IT staff or experts on hand, which leaves them vulnerable to evolving cyber threats. With limited budgets, these municipalities struggle to keep up with the rapid pace of technology changes, often relying on outdated or unsupported software and hardware that is prone to exploitation by cybercriminals. This lack of resources makes it difficult to implement comprehensive cybersecurity measures or respond effectively to incidents when they arise.

Another challenge local governments face is the complexity of managing diverse, often fragmented, IT systems. Local municipalities rely on a range of systems to manage everything from billing and tax collections to law enforcement records and emergency services. These systems are often created by different vendors with varying levels of security standards, making it difficult to ensure consistency and compatibility across platforms. Without a centralized strategy for cybersecurity, these disparate systems can create vulnerabilities that hackers can exploit. Furthermore, the integration of third-party vendors, who may have varying levels of security, increases the complexity and risks associated with managing sensitive data.

One of the biggest concerns for local governments is susceptibility to human error, which remains one of the most common entry points for cyberattacks. With limited training and resources, employees may not be fully aware of cybersecurity best practices or the potential threats they face, such as phishing scams or weak passwords. Given the broad spectrum of functions and employees involved in local government operations, maintaining a high level of cybersecurity awareness across all departments can be a significant challenge. In many cases, this lack of awareness leads to inadvertent vulnerabilities that cybercriminals can exploit to gain access to systems, steal data, or disrupt services, all of which can happen with a single click.

Understanding the Cyber Security Threats

Common types of cyber-attacks (e.g., phishing, ransomware, data breaches)

Local governments, like all organizations, are vulnerable to a variety of cyber-attacks, but certain types of attacks are particularly common and impactful. One of the most prevalent is **phishing**, where cybercriminals impersonate legitimate entities—such as trusted government agencies, vendors, or colleagues—to deceive employees into revealing sensitive information like usernames, passwords, or financial data. Phishing attacks often come in the form of seemingly innocent emails or text messages that contain malicious links or attachments. Once an employee clicks on the link or downloads an attachment, malware can be installed, or login credentials can be stolen, giving attackers unauthorized access to critical systems. Phishing remains one of the easiest and most effective ways for hackers to infiltrate local government networks.

Another common cyber threat is **ransomware**, a particularly dangerous type of malware that locks or encrypts the victim's data and demands payment in exchange for the decryption key. Ransomware attacks have become a serious concern for local governments, as they can disrupt essential services such as public safety, utilities, and communication systems. Cybercriminals often target small to mid-sized municipalities because their cybersecurity defenses may be less robust than those of larger organizations. A successful ransomware attack can bring operations to a halt, forcing local governments to either pay the ransom (which may not even guarantee data recovery) or attempt to restore systems from backups—often at a significant financial and operational cost.

Finally, **data breaches** are another major concern for local governments. These breaches occur when unauthorized individuals gain access to sensitive data, such as personally identifiable information (PII), financial records, or law enforcement data. In the case of local governments, these breaches can involve not only citizens' private information but also confidential municipal documents and communications. Hackers may exploit vulnerabilities in unpatched systems or weak access controls to steal this data, which can be sold on the dark web or used for identity theft and fraud. Data breaches not only compromise the privacy of citizens but can also lead to legal consequences, regulatory fines, and a loss of public trust in the government's ability to protect its residents.

Examples of recent cyber incidents in local governments

1. Suffolk County Ransomware Attack (2022)

Incident:
In September 2022, Suffolk County's government systems fell victim to a ransomware attack that severely disrupted county operations, including payment processing and emergency services.
Financial Impact:
The county incurred **over $17 million** in recovery costs, which included rebuilding IT infrastructure, enhancing cybersecurity, and restoring affected services.
Source:
ProtectNow LLC

---

2. New York State Office of Information Technology Services (ITS) Audit (2024)

Incident:
A 2024 audit of the New York State Office of Information Technology Services (ITS) revealed significant security lapses and asset management failures. Investigators found that thousands of government-owned technology devices were unaccounted for, including functional computers mistakenly marked for disposal.
Financial Impact:
The estimated loss was **$530,000**, covering missing computers and other assets.
Source:
Times Union

---

3. New York State Department of Financial Services (DFS) Data Breach (2023)

Incident:
In 2023, the New York State Department of Financial Services (DFS) suffered a data breach that exposed sensitive financial and personal information. The breach triggered regulatory scrutiny and forced DFS to enhance its cybersecurity measures significantly.
Financial Impact:
While specific cost figures were not disclosed, the breach led to substantial expenses related to compliance measures, cybersecurity enhancements, and legal fees.
Source:
Ropes & Gray

---

4. Albany Ransomware Attack (2019)

Incident:
In March 2019, the city of Albany experienced a ransomware attack that severely disrupted municipal services. Despite the attack, city officials managed to recover without paying a ransom, relying instead on backup systems and cybersecurity improvements.
Financial Impact:
Albany spent **$300,000** on system restoration, cybersecurity enhancements, and insurance coverage.
Source:
Office of the New York State Comptroller

The financial and operational consequences of these cyberattacks highlight the urgent need for stronger cybersecurity frameworks in government agencies. Investments in cybersecurity infrastructure, regular audits, and incident response planning are critical to mitigating risks and protecting sensitive public data.

The Financial and Operational Impacts of Cyber Attacks

Just based on the examples above, we know that cyberattacks can have devastating financial consequences for local governments, particularly those with limited resources. The immediate costs associated with a cyberattack can be significant, from **ransom payments** in the case of ransomware attacks to the **expenses involved in system restoration**, forensic investigations, and legal fees. For municipalities that do not have dedicated IT teams or emergency response plans in place, these costs can quickly escalate. Additionally, many local governments face financial penalties and fines for failing to comply with data protection regulations or for failing to notify residents of breaches in a timely manner. These unforeseen expenses can strain already tight budgets, diverting funds away from essential services and community development projects.

Beyond the direct financial costs, cyberattacks also result in **operational disruptions** that can cripple local government functions. Ransomware attacks, for example, can halt access to critical systems such as tax collection, utility billing, public safety records, and emergency services. This disruption can paralyze day-to-day operations, delay services to residents, and erode public trust in government institutions. Even a temporary shutdown of operations can have long-lasting effects, as municipalities may struggle to catch up on backlog tasks, reschedule essential services, and restore their public image. For smaller municipalities with limited staff, the recovery process can be drawn out, leading to months of operational inefficiencies and heightened stress for both employees and residents.

Moreover, the **long-term consequences** of a cyber-attack extend beyond immediate recovery efforts. A cyber incident can severely damage a local government's **reputation** and lead to a loss of public confidence. Residents and business owners may be less willing to trust their local government's ability to protect sensitive information, such as tax data, medical records, or law enforcement files. Furthermore, municipalities may face lawsuits or class-action claims from residents whose personal information was compromised, adding to the financial and reputational toll. In short, the effects of a cyberattack are not limited to the immediate aftermath; they can resonate for years, affecting the long-term stability and success of local governments.

Artificial Intelligence: Practical Power for Modern Local Government

How AI Tools Are Helping Municipalities Work Smarter, Not Harder

I would be remiss in this eBook if I didn't take a moment to highlight the growing role of Artificial Intelligence (AI) in local government — a technology that is no longer on the horizon, but at our doorstep.

AI is no longer just a buzzword—it's rapidly becoming a practical tool for municipalities looking to improve efficiency, responsiveness, and service delivery. From automating routine administrative tasks to enhancing public safety operations, AI is already making a quiet but powerful entrance into local government operations.

One of the most immediate applications of AI is in handling repetitive tasks that consume valuable staff time. Think of AI-powered chatbots managing resident inquiries on websites, or software that automates the processing of permits and license renewals. These solutions allow staff to focus on higher-value work and reduce waiting times for constituents.

A real-world example of this in action comes from Sullivan County, New York. With limited staffing and resources, the county deployed a generative AI chatbot using Google Cloud's Vertex AI in under three months. This tool now enables direct, two-way communication between residents and county government—enhancing engagement, improving service delivery, and increasing transparency. Sullivan County's success story proves that even smaller municipalities can effectively harness AI to better serve their communities.

AI can also support smarter decision-making through predictive analytics. For instance, AI tools can analyze data from public works systems to predict when infrastructure will need maintenance—allowing for proactive repairs rather than costly emergency fixes. Public safety departments are also beginning to use AI for everything from traffic pattern analysis to optimizing emergency response times.

But AI isn't just about automation, it's about augmentation. AI can enhance human judgment by surfacing insights from vast datasets, helping leaders make more informed decisions about budgeting, planning, and community development. It can also be used to monitor service levels in real time, identify patterns, and flag anomalies—whether in water usage, energy consumption, or citizen complaints.

Emerging Areas of Impact

- **Grant Writing and Compliance** – AI can help municipalities draft and review grant applications, identify eligible funding sources, and even generate

compliance documentation automatically—saving time and increasing access to much-needed funds.

- **Records Management** – With AI-powered document processing, towns can digitize and organize years of records, making retrieval faster and improving FOIL (Freedom of Information Law) response times.
- **Planning and Zoning** – AI can analyze land use data, building permits, and GIS layers to forecast development patterns or assess environmental impact.
- **Public Communication and Accessibility** – Generative AI can assist in creating multilingual communication, improving accessibility for residents whose first language isn't English, and ensuring ADA-compliant digital materials.

Cybersecurity and Ethical Considerations

While the opportunities are exciting, the risks cannot be ignored. AI systems depend on large volumes of data, which means data governance and cybersecurity must be top priorities. As AI becomes more embedded in government operations, municipalities must ensure they're protecting sensitive information, following clear ethical guidelines, and maintaining public trust.

New York State's Local Government Cybersecurity Grant Program and the State Office of Information Technology Services (ITS) are already emphasizing responsible AI use, data transparency, and privacy compliance. As more agencies adopt these tools, aligning AI strategy with cybersecurity policies will be essential.

Empowering People, Not Replacing Them

AI isn't here to replace human service, it's here to empower it. When thoughtfully deployed, AI has the potential to help local governments do what they do best: serve their communities, efficiently and effectively, in a rapidly changing world.

The municipalities that succeed with AI will be those that combine **innovation with intention**, leveraging technology not to reduce the human element, but to enhance it. By training staff, protecting data, and embracing digital transformation, New York's local governments can model what it means to be *smart, secure, and service-driven in the AI era.*

The Role of the New York State Comptroller

How the Comptroller's Office Supports Local Governments

The New York State Comptroller's Office plays a critical role in helping local governments improve their cybersecurity posture and manage technology risks effectively. Recognizing the unique challenges faced by municipalities with limited resources, the Comptroller's Office offers a range of resources and guidance to strengthen local governments' ability to prevent and respond to cyber threats. One of the key services provided is the Office of the State Comptroller's (OSC) Cybersecurity Services, which works directly with local governments to assess their cybersecurity risks, identify vulnerabilities, and recommend appropriate measures to mitigate those risks. Through comprehensive audits and assessments, the OSC helps municipalities pinpoint weaknesses in their systems and offers actionable strategies to enhance security, often at little to no cost to the local governments (OSC IT Governance Security Self-Assessment Form) (https://www.osc.ny.gov/taxonomy/term/263996).

In addition to cybersecurity assessments, the Comptroller's Office also provides training and education to local government officials and employees on best practices in cybersecurity. Understanding that human error is often the weak link in cyber defense, the OSC offers various training programs designed to raise awareness about common threats like phishing, malware, and social engineering attacks. These educational resources are invaluable for towns and villages that may lack dedicated IT staff and ensure that employees at all levels are equipped with the knowledge needed to protect sensitive data and systems. Local leaders can benefit from cybersecurity risk mitigation webinars that focus on practical strategies to reduce vulnerabilities (Cybersecurity Risk Mitigation Webinar Series) (https://www.osc.ny.gov/taxonomy/term/263996).

The Comptroller's Office also supports local governments by providing up-to-date guidance on state and federal cybersecurity regulations, helping municipalities navigate complex compliance requirements and avoid potential penalties for non-compliance. Additionally, the New York State Office of Information Technology Services (ITS) has developed a **Local Government Cybersecurity Toolkit**, which provides municipalities with essential information on cybersecurity best practices, risk assessments, and prevention strategies (Local Government Cybersecurity Toolkit) (https://its.ny.gov/local-government-cybersecurity-toolkit).

Furthermore, the New York State Comptroller's Office has developed a **Cybersecurity Policy Toolkit** that provides local governments with customizable templates, policies, and procedures for developing their own cybersecurity programs. This toolkit covers a wide range of topics, from disaster recovery and incident response to network security and data protection. A comprehensive cybersecurity guide is also available to assist local leaders in protecting sensitive data and municipal assets (Cybersecurity Guide for Local Leaders) (https://www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf). By offering these resources, the Comptroller's Office helps municipalities implement cost-effective, yet robust cybersecurity measures tailored to their specific needs and budget constraints.

Through its ongoing support, the Comptroller's Office enables local governments in New York State to build a strong cybersecurity foundation, empowering them to protect their communities from the ever-growing threat of cyberattacks.

Importance of compliance with Comptroller guidelines

The **New York State Comptroller's Cybersecurity Guidelines** provide an additional layer of regulatory oversight. These guidelines are designed to help local governments strengthen their cybersecurity posture by offering recommendations on governance, risk management, and best practices. The guidelines provide municipalities with essential tools to evaluate their current cybersecurity practices and develop strategies to mitigate risks related to data breaches and cyberattacks. Compliance with these guidelines is not legally mandated but is highly recommended, as it helps municipalities demonstrate they are taking the necessary steps to protect their data and systems.

Compliance with the New York State Comptroller's guidelines is essential for local governments to ensure both the security and accountability of their technology systems. The Comptroller's Office provides a set of cybersecurity frameworks and best practices designed to help municipalities reduce risk, protect sensitive data, and safeguard essential services. By adhering to these guidelines, local governments not only improve their security posture but also demonstrate to their residents, stakeholders, and auditors that they are committed to protecting public resources. Non-compliance, on the other hand, can leave local governments vulnerable to cyberattacks and expose them to potential legal and financial repercussions.

One of the primary benefits of following the Comptroller's guidelines is that they provide a **structured approach to cybersecurity** that aligns with industry standards and regulations. For local governments without dedicated IT staff, these guidelines act as a roadmap for implementing effective cybersecurity measures. The Comptroller's cybersecurity frameworks help municipalities identify and address common vulnerabilities, establish clear security policies, and implement necessary controls to ensure that systems and data are protected. Moreover, these guidelines encourage a risk-based approach, which allows local governments to prioritize their cybersecurity efforts based on the most critical areas of concern, ensuring that limited resources are allocated effectively.

Compliance with the Comptroller's guidelines also ensures that local governments are **prepared for audits and inspections**, which are increasingly common as part of the state's oversight process. Municipalities that fail to comply with these standards may face challenges in audits, leading to financial penalties, negative audit reports, or a loss of eligibility for certain state funding programs. Moreover, by demonstrating compliance, local governments can improve their relationship with the Comptroller's Office and other oversight agencies, which can lead to additional resources, support, and guidance when addressing cybersecurity challenges. Ultimately, staying in compliance not only protects the municipality from immediate threats but also builds a foundation for long-term cybersecurity resilience.

New York State Department of Finance and Cybersecurity

Role of the New York State Department of Finance in Regulating Cybersecurity

The **New York State Department of Finance (NYSDOF)** plays an important role in overseeing and regulating the financial aspects of cybersecurity for local governments, especially regarding compliance with various state and federal laws designed to protect public funds and sensitive information. While the Department of Finance is not directly responsible for setting cybersecurity standards, its regulations and oversight impact the way municipalities manage and secure their financial data and systems.

One of the key responsibilities of the NYSDOF is to ensure that local governments adhere to proper **financial management** and **accounting procedures**, which includes securing financial data from cyber threats. This includes oversight of municipal spending, accounting practices, and procurement processes to ensure that taxpayers' funds are protected from fraud, mismanagement, and cybercrime. The Department works with local governments to implement cybersecurity practices that help safeguard financial transactions, especially in areas like tax collections, budgeting, payroll, and procurement systems, where sensitive financial data is most vulnerable.

Additionally, the Department of Finance ensures that municipalities comply with **New York State's Information Security Breach and Notification Act (ISBNA)** and other regulations that require reporting of any data breaches that affect financial or personal information. In the event of a cyber incident, local governments must notify affected individuals and state agencies, including the NYSDOF, within specific timeframes. This regulatory framework emphasizes the importance of proactive cybersecurity measures and compliance to prevent financial loss or reputational damage due to breaches.

While the NYSDOF does not set specific cybersecurity guidelines, its regulatory framework influences how municipalities allocate resources to **cybersecurity risk management**, as local governments must prioritize securing financial data in alignment with these financial management rules. The department also encourages local governments to implement **best practices** related to cybersecurity in financial processes, as outlined in guidance from the **New York State Office of the Comptroller** and other cybersecurity resources. By working together with other state agencies, the NYSDOF helps ensure that local governments are prepared to defend against cyber threats and continue to manage public funds securely.

Key regulations and policies affecting local governments

New York State's Information Security Breach and Notification Act (ISBNA)
One of the most important regulations for local governments is the **Information Security Breach and Notification Act (ISBNA)**. Enacted in 2005, this law requires any governmental entity in New York State to notify individuals when their private information has been compromised due to a data breach. Local governments must comply with this law if their cybersecurity practices fail and result in an incident where personally identifiable information (PII) is exposed or accessed by unauthorized parties. Under the ISBNA, municipalities must notify affected individuals without unreasonable delay and, in certain cases, notify the New York State Attorney General and other government entities. This regulation serves as an important reminder for local governments to maintain robust cybersecurity measures to avoid breaches that could expose sensitive data and incur legal penalties.

New York State Cybersecurity Regulation (23 NYCRR 500)
For entities operating in the financial services sector, including local governments that manage financial transactions, **23 NYCRR 500** (also known as the "New York State Department of Financial Services (DFS) Cybersecurity Regulation") is a crucial standard. While primarily aimed at banks and insurance companies, local government agencies that interact with financial institutions must also be aware of this regulation. It sets out strict cybersecurity requirements for businesses, including risk assessments, data protection, and incident response plans. Local governments involved in managing financial services for their residents—such as tax collection or utility billing—must follow the key tenets of this regulation to ensure they meet the security requirements necessary for the safe handling of financial data.

New York State Freedom of Information Law (FOIL)
The **Freedom of Information Law (FOIL)** mandates that local governments make records, including electronic records, available to the public upon request. While FOIL promotes transparency, it also presents cybersecurity challenges as municipalities must ensure that sensitive data, such as confidential employee records or legal documents, is adequately protected when shared. To comply with FOIL, local governments must implement secure systems that prevent unauthorized access or disclosure of sensitive data while still enabling legitimate access to public records. This requires local governments to adopt strict controls over how data is stored, accessed, and shared, in alignment with cybersecurity best practices.

NYS Homeland Security and Emergency Services (DHSES) Cybersecurity Grant Requirements
Local governments seeking **cybersecurity grants** from the **New York State Division of Homeland Security and Emergency Services (DHSES)** must meet certain eligibility and reporting requirements. DHSES provides grants to help municipalities improve their cybersecurity posture, but in order to qualify for funding, local governments must show that they have implemented basic cybersecurity measures and meet specific **cybersecurity standards**. This includes having a **risk management strategy**, adequate **data protection** protocols, and a **cyber incident response plan**. The DHSES emphasizes the importance of **preparedness** and requires municipalities to demonstrate that they are taking steps to reduce vulnerabilities and enhance overall security before awarding grant funding.

Federal Regulations (e.g., HIPAA, FISMA)
While New York State regulations provide local governments with a strong cybersecurity framework, certain **federal regulations** also play a role in shaping local government policies. For example, the **Health Insurance Portability and Accountability Act (HIPAA)** governs the privacy and security of health information, which is particularly relevant for local governments involved in healthcare administration or public health services. Similarly, the **Federal Information Security Modernization Act (FISMA)** requires federal agencies and organizations working with them to adopt strong cybersecurity practices, and some local government agencies that partner with the federal government may need to comply with FISMA-related standards.

Resources and support provided to municipalities

Local governments in New York State have access to a variety of resources and support services to help them enhance their cybersecurity measures and protect critical data. These resources, provided by both state agencies and external organizations, are particularly valuable for municipalities without dedicated IT departments, offering guidance, technical assistance, and financial support to bolster cybersecurity defenses.

1. **New York State Office of Information Technology Services (ITS) - Cybersecurity Services**
   The **New York State Office of Information Technology Services (ITS)** offers a range of cybersecurity services to local governments, particularly through its **Cybersecurity Services Unit**. This unit provides municipalities with tools to assess their cybersecurity risks, implement necessary security measures, and stay informed about emerging threats. Local governments can access free or low-cost cybersecurity training, receive vulnerability assessments, and benefit from the state's expertise in handling common cyber threats like ransomware and phishing. ITS also offers guidance on creating effective **cyber incident response plans**, which are essential for local governments to quickly recover from a cyberattack or data breach. ITS works to ensure that municipalities stay up to date on the latest best practices and compliance requirements, making it an essential resource for towns and villages across the state.
   - **Source**: New York State Office of Information Technology Services ITS Cybersecurity
2. **New York State Comptroller’s Office - Cybersecurity Resources and Guidelines**
   The **New York State Comptroller’s Office** provides a comprehensive suite of cybersecurity resources specifically tailored to the needs of local governments. The Comptroller’s **Cybersecurity Handbook** and **Guidelines** offer practical advice on assessing and improving cybersecurity posture, including establishing governance frameworks, conducting risk assessments, and implementing security controls. Additionally, the Comptroller’s office conducts cybersecurity audits to help municipalities evaluate the effectiveness of their current measures and identify areas for improvement. These audits and resources are invaluable for local governments looking to align their cybersecurity practices with state standards and best practices.
   - **Source**: New York State Comptroller Cybersecurity Resources

3. **Cybersecurity Training and Awareness Programs**
   To help municipalities build a cybersecurity-aware workforce, several organizations and agencies offer **training programs and awareness initiatives**. For example, the **New York State Cybersecurity Awareness Program** provides free online training courses and webinars for local government employees. These training modules cover a variety of topics, including how to recognize phishing attempts, safeguard personal data, and follow secure communication practices. Additionally, local governments can participate in training programs provided by **the New York State Cybersecurity Coalition** or partner with industry experts to improve their staff's overall cybersecurity awareness. These training resources help municipalities mitigate the human factor in cybersecurity breaches by educating employees on the importance of security hygiene.

4. **Grants and Funding for Cybersecurity Improvements**
   To alleviate the financial burden of implementing robust cybersecurity measures, several grant programs are available to local governments in New York State. These include funding opportunities through the **New York State Homeland Security and Emergency Services (DHSES)**, which offers grants to support **cybersecurity preparedness and defense**. Additionally, municipalities can apply for federal funding through programs such as the **Cybersecurity and Infrastructure Security Agency (CISA) grants** to enhance their cybersecurity infrastructure. These grants are designed to help local governments with the cost of adopting new technologies, upgrading outdated systems, and improving staff training.

   - **Source**: New York State Division of Homeland Security and Emergency Services DHSES Cybersecurity Grants

5. **New York State Cyber Incident Response Team (CIRT)**
   The **New York State Cyber Incident Response Team (CIRT)** provides assistance to local governments when they experience a cybersecurity incident. CIRT offers expert guidance in managing and mitigating the effects of data breaches, ransomware attacks, and other cyber incidents. CIRT's support includes incident response planning, real-time monitoring, and coordination with law enforcement agencies when necessary. By leveraging this team's expertise, municipalities can more effectively respond to cyber threats, recover data, and ensure continuity of critical services.

   - **Source**: New York State Cyber Incident Response Team CIRT

Cyber Liability Insurance Requirements

What is Cyber Liability Insurance and Why It Is Important

Cyber liability insurance is a specialized insurance policy designed to help municipalities manage the financial risks associated with cyber incidents, such as data breaches, ransomware attacks, and other cyber threats. For local governments in New York State, where resources may be limited and cybersecurity vulnerabilities are an increasing concern, having cyber liability insurance can be a crucial safety net. This type of insurance helps cover the costs related to responding to and recovering from a cyberattack, as well as any legal fees or penalties that may arise as a result of compromised data or operational disruptions.

Municipalities are increasingly at risk of cyberattacks due to their often-outdated IT systems, lack of dedicated IT staff, and the sensitive data they handle, such as tax records, law enforcement data, and public health information. Cyber liability insurance can provide protection against the **financial impact** of a breach, including costs for **forensic investigations** to determine how the attack occurred, **notification costs** for informing affected individuals, and **credit monitoring** for those whose personal information was compromised. Additionally, in the event of a ransomware attack, cyber liability insurance can help cover the cost of ransom payments, if they are deemed necessary for restoring critical systems, although paying a ransom is discouraged and often not recommended.

In New York State, many municipalities turn to the **New York Municipal Insurance Reciprocal (NYMIR)** for their cyber liability coverage. NYMIR offers specialized cyber liability insurance policies tailored to the unique needs of local governments. These policies typically cover a wide range of risks, including **data breach management**, **business interruption losses**, and **liability claims** arising from the unauthorized release of confidential information. For local governments, having cyber liability insurance not only mitigates the financial impact of a cyberattack but also supports the municipality's broader **cybersecurity strategy**. By ensuring they have the proper coverage in place, municipalities can more confidently invest in the necessary resources to protect their data and systems while knowing they have financial protection in the event of a crisis.

How to Choose the Right Cyber Liability Insurance Policy

Choosing the right **cyber liability insurance** policy is a critical decision for local governments looking to protect themselves from the financial and operational impacts of a cyber incident. With increasing cyber threats targeting municipalities, including ransomware attacks and data breaches, having comprehensive cyber liability coverage ensures that a local government is prepared for unexpected events. Below are key considerations and steps to guide municipalities in selecting the most suitable policy.

1. **Understand the Coverage Options**

The first step in choosing the right cyber liability insurance policy is to understand the various coverage options available. Common types of coverage include:

- **Data Breach Coverage**: This covers costs associated with a data breach, such as **forensic investigations** to determine the cause and extent of the breach, **notification**

costs for informing affected individuals, and **credit monitoring services** for those whose personal information has been exposed.

- **Ransomware Coverage**: Provides protection in the event of a ransomware attack. This includes covering the ransom payment (if paid), as well as the **cost of restoring systems and data** and **business interruption costs** incurred during system downtime.
- **Network Security Liability**: This coverage protects against claims resulting from failure to secure systems, such as malware infections or denial-of-service (DoS) attacks that impact public services.
- **Regulatory Liability**: Covers costs related to fines, penalties, and legal fees if the municipality is found non-compliant with **data protection regulations** like the **New York State Information Security Breach and Notification Act (ISBNA)** or federal privacy laws.
- **Third-Party Liability**: This protects the local government from claims filed by third parties (e.g., residents, contractors) who suffer financial losses or damages due to the municipality's failure to secure personal or financial information.

2. Evaluate the Limits of Coverage

It is crucial for local governments to assess the **limits of coverage** offered by the policy. While some policies offer low coverage limits, municipalities need a policy that provides sufficient protection for their specific needs. The limits should consider:

- **The size of the municipality**: Larger municipalities or those managing more sensitive data may require higher limits to cover potential damages.
- **The value of the data**: Municipalities with significant amounts of sensitive data (e.g., tax records, healthcare information) should ensure their coverage limits are adequate to cover the cost of data recovery, notifications, and potential lawsuits.
- **Cyber risk exposure**: Municipalities with higher exposure to cyber threats (e.g., extensive use of cloud services, frequent financial transactions) may need more comprehensive coverage to safeguard against larger-scale incidents.

3. Check for Incident Response Support

In the event of a cyberattack, the local government will need immediate access to resources to mitigate the damage. Many cyber liability insurance policies offer additional services, such as:

- **24/7 incident response hotlines** to connect with cybersecurity experts who can help contain and mitigate the effects of an attack.
- **Forensic services** to investigate how the breach occurred, determine the extent of the data exposure, and help rebuild systems.
- **Public relations assistance** to help manage the fallout from the breach and protect the municipality's reputation.

Choosing a policy that includes access to these services is essential, as fast response times can help minimize the financial and reputational damage caused by a cyberattack.

4. Consider the Reputation and Experience of the Insurance Provider

Not all insurance companies specialize in cyber liability, so it is important for municipalities to choose an insurer with experience and a solid reputation in the field. The insurer should have a strong history of responding to cyber incidents and a track record of working with local governments or public-sector entities. In addition, it's beneficial to choose a provider who is familiar with **New York State's unique cybersecurity requirements**, as these regulations can influence the types of coverage and claims processes.

One commonly recommended insurer for local governments in New York State is the **New York Municipal Insurance Reciprocal (NYMIR)**, which offers tailored cyber liability policies specifically designed for municipalities. NYMIR's policies often include broader coverage options, including risk assessments, training, and incident response services, making them a good choice for municipalities with limited IT resources.

5. Understand the Exclusions

Every insurance policy will have exclusions—situations where coverage does not apply. Local governments must carefully review these exclusions to avoid unpleasant surprises after a cyber event. Common exclusions might include:

- **Acts of war** or cyberattacks from nation-states.
- **Intentional acts** of fraud or misconduct by employees.
- **Pre-existing vulnerabilities** that were known before the policy was purchased.
- **Losses due to the failure to comply with cybersecurity best practices** (e.g., failure to implement recommended updates or encryption protocols).

Being aware of exclusions ensures that municipalities understand the limits of their coverage and can take additional precautions where necessary.

6. Review Premium Costs and Deductibles

Premiums and deductibles are a critical consideration when choosing cyber liability insurance. While it may be tempting to choose a lower-cost policy, municipalities should ensure that the premium provides adequate coverage for their specific needs. A policy with a low premium but high deductible may leave the municipality with high out-of-pocket costs in the event of a claim. It's also important to factor in potential **premium increases** over time as the municipality's cyber risk profile changes or as the insurer's coverage terms evolve.

Local governments should work with their insurance brokers to find a balance between coverage and affordability and explore options for bundled coverage that might include additional services like **cybersecurity training** or **risk management assessments**.

Implementing Effective Cybersecurity Measures

Steps to Creating a Robust Cybersecurity Strategy

Developing a **robust cybersecurity strategy** is essential for local governments to protect sensitive data, maintain public trust, and ensure the continuity of critical services. A comprehensive strategy will not only help prevent cyberattacks but also enable municipalities to quickly recover in case of a security breach. Below are the key steps local governments should follow to create an effective cybersecurity strategy:

1. Conduct a Comprehensive Risk Assessment

The first step in creating a cybersecurity strategy is conducting a thorough **risk assessment**. Local governments must identify their most valuable and vulnerable assets—such as sensitive data, financial records, and critical infrastructure—and assess potential cyber threats to those assets. This assessment should involve:

- Identifying **critical systems** and data that need protection.
- Evaluating current security measures and their effectiveness.
- Understanding the municipality's **cyber risk profile**, including common threats (e.g., phishing, ransomware).
- Determining potential **vulnerabilities** in the network, software, and hardware.

By understanding the risks and vulnerabilities, local governments can prioritize their cybersecurity efforts and allocate resources effectively.

2. Develop and Implement Security Policies and Procedures

Once the risks are identified, the next step is to develop and implement **security policies and procedures** that govern how data and systems are protected. These policies should address areas such as:

- **Access control**: Define who has access to sensitive data and systems and ensure that access is restricted based on need-to-know principles.
- **Password management**: Implement strong password policies that require employees to use complex passwords and change them regularly.
- **Encryption**: Ensure that all sensitive data is encrypted, both in transit and at rest, to protect it from unauthorized access.
- **Network security**: Use firewalls, antivirus software, and intrusion detection systems to protect against external attacks.
- **Incident response**: Establish a formalized incident response plan that outlines the steps to take in the event of a cyberattack, including how to detect, contain, and recover from a breach.

These policies and procedures should be regularly reviewed and updated to stay aligned with best practices and emerging threats.

3. Implement Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is a critical security measure that requires users to provide two or more verification factors before gaining access to systems or data. For example, in addition to a password, users might be required to enter a code sent to their mobile device or use a biometric scan. By implementing MFA, municipalities can significantly reduce the risk of unauthorized access due to stolen or weak passwords. This measure is particularly important for employees accessing sensitive government systems or data remotely.

4. Regularly Update and Patch Software and Systems

Outdated software and systems are a common target for cybercriminals, as they often contain known vulnerabilities that can be exploited. Local governments must establish a system for **regularly updating** and **patching** their software, operating systems, and applications. This includes:

- Applying **security patches** and software updates as soon as they are released.
- Ensuring that **legacy systems**—which may be running outdated software—are properly maintained or replaced.
- Using automated tools to detect vulnerabilities and patch them promptly.

Regular updates help close security gaps and ensure that municipalities are protected against known threats.

5. Conduct Employee Training and Awareness Programs

Human error is one of the leading causes of cybersecurity breaches. To address this, local governments should implement comprehensive **cybersecurity training** for all employees. Training should cover:

- How to recognize and avoid **phishing** attempts and suspicious emails.
- The importance of **strong passwords** and how to create them.
- The dangers of using unsecured networks and **public Wi-Fi**.
- The procedures for reporting a suspected cyber incident or breach.

By fostering a culture of cybersecurity awareness, municipalities can significantly reduce the risk of successful cyberattacks that exploit human vulnerabilities.

6. Regularly Backup Critical Data

Data backups are essential for ensuring that local governments can quickly recover from a cyberattack, particularly **ransomware attacks** that encrypt and hold data hostage. Municipalities should:

- Regularly back up all critical data to an **off-site location** or **cloud service**.
- Test the backup systems periodically to ensure that the data can be restored quickly and accurately.
- Store backups in **encrypted formats** to protect them from unauthorized access.

Having a reliable backup system in place allows municipalities to minimize downtime and avoid paying a ransom in the event of an attack.

7. Monitor and Respond to Cyber Threats Continuously

A strong cybersecurity strategy requires **continuous monitoring** of systems, networks, and endpoints for suspicious activities. Local governments should:

- Ensure a robust managed **firewall** is in place as your first line of defense
- Use **intrusion detection systems (IDS)** and **Security Information and Event Management (SIEM)** tools to monitor for abnormal activity.
- Implement regular **penetration testing** to simulate attacks and identify vulnerabilities.
- Work with **managed security service providers (MSSPs)** or a state-level **cyber-security response team** (e.g., New York State Cyber Incident Response Team) to receive real-time threat intelligence and support during an active attack.

Ongoing monitoring enables municipalities to detect and respond to potential threats before they escalate into significant breaches.

8. Establish Clear Incident Response and Recovery Plans

A well-defined **incident response plan** (IRP) outlines how the municipality will respond to a cyberattack or data breach. This plan should include:

- **Identification and containment**: How to detect and isolate the threat to prevent further damage.
- **Communication protocols**: Clear guidelines for internal and external communication during an incident, including informing affected individuals, regulatory bodies, and the public.
- **Recovery**: Steps to restore data and systems, including from backups, and ensure business continuity.
- **Post-incident review**: An analysis of the incident to identify what went wrong, what worked, and how to improve defenses moving forward.

Having an IRP ensures that local governments can quickly and effectively manage a cyber incident, reducing the damage and speeding up recovery times.

Implementing effective cybersecurity measures is not a one-time effort, but an ongoing commitment to protecting sensitive public data, critical infrastructure, and services. By following these steps and creating a comprehensive cybersecurity strategy, local governments in New York State can strengthen their defenses, minimize risks, and respond more effectively to emerging cyber threats. Regularly reviewing and updating cybersecurity measures is essential to adapting to the ever-evolving landscape of cyber risks.

Importance of Regular Security Training for Employees

Cybersecurity is not just an IT issue—it is a **team effort** that involves everyone within a local government organization. Employees are often the first line of defense against cyber threats, and regular **security training** is essential to ensuring they are prepared to recognize and respond to potential risks. Given that human error remains one of the most common causes of data breaches and other cyber incidents, ongoing training programs are critical to building a culture of security awareness and reducing vulnerabilities within the organization.

1. Reducing the Risk of Social Engineering Attacks

Social engineering attacks, such as **phishing** and **pretexting**, are among the most common and effective cyber threats. In these attacks, cybercriminals manipulate employees into disclosing sensitive information, clicking on malicious links, or opening infected attachments. Without proper training, employees may unknowingly fall victim to these tactics, resulting in data breaches or ransomware infections. Regular security training helps employees recognize the signs of phishing emails, suspicious phone calls, and other manipulative tactics, empowering them to respond appropriately—such as by reporting the incident to IT or deleting the suspicious email.

2. Promoting Strong Cyber Hygiene Practices

Cyber hygiene refers to the routine practices that ensure systems and data are kept secure from common threats. Regular training reinforces best practices for protecting sensitive information and safeguarding systems. This includes:

- Using **strong, unique passwords** for different accounts and regularly updating them.
- Implementing **multi-factor authentication (MFA)** to add an extra layer of security.
- Understanding the importance of **software updates** and promptly installing security patches.
- Safely storing and disposing of sensitive materials (e.g., documents and devices).

By regularly reinforcing these habits, municipalities can significantly reduce the risk of security breaches caused by lapses in basic cybersecurity practices.

3. Ensuring Compliance with Security Policies and Regulations

Local governments are subject to various **security policies** and **regulations** designed to protect public data and ensure the integrity of systems. For instance, New York State mandates compliance with cybersecurity standards set forth by the **Comptroller's Office** and **the Information Security Breach and Notification Act (ISBNA)**. Regular training ensures that employees are aware of these policies and their responsibilities under the law. By educating

staff on data privacy laws, reporting requirements, and incident response protocols, municipalities can avoid costly legal consequences, including fines and penalties for non-compliance. Additionally, regular training helps foster a sense of accountability among staff, ensuring they understand the importance of adhering to security protocols.

4. Empowering Employees to Identify and Report Threats

Cybersecurity is not just the responsibility of the IT department—it requires active participation from all employees. Regular training programs teach employees how to identify potential threats, such as malware, suspicious attachments, or unverified requests for sensitive data. When employees are equipped with the knowledge to spot red flags, they become a critical part of the municipality's **cyber defense** strategy. Moreover, training empowers employees to **report incidents quickly** and accurately, ensuring that potential breaches are detected early and mitigated before they cause significant damage.

5. Fostering a Cybersecurity Culture

The most effective cybersecurity strategies involve creating a **culture of security** within an organization. Regular training reinforces the importance of cybersecurity at all levels, from front-line workers to senior leadership. When employees understand the risks and the role they play in protecting municipal data and systems, they are more likely to take ownership of security practices in their daily work. This culture shift can lead to greater vigilance, proactive behavior, and a collective effort to safeguard against cyber threats.

6. Adapting to Evolving Cyber Threats

Cyber threats are continuously evolving, with attackers constantly developing new tactics to breach systems. Regular training ensures that employees stay updated on the latest threats, vulnerabilities, and defense techniques. For example, employees may need to understand how new types of **ransomware** work, or how to recognize a **spear-phishing** attack targeting specific individuals within the organization. By keeping staff informed and prepared for the latest cyber risks, municipalities can adapt to the changing threat landscape and better protect against emerging cyberattacks.

Regular security training for employees is a crucial component of any local government's cybersecurity strategy. By equipping employees with the knowledge and tools to recognize, avoid, and report cyber threats, municipalities can create a more resilient defense against the growing number of cyberattacks. Cybersecurity awareness among all staff members helps reduce human error, ensure compliance with legal requirements, and ultimately protect the municipality from the financial and operational risks associated with cyber incidents. Ongoing training fosters a culture of cybersecurity that is essential to the long-term protection of critical data and services.

Best Practices for Data Protection and Recovery

Data protection and recovery are integral parts of a robust cybersecurity strategy. Local governments handle a wide range of sensitive data, including personal identifying information, tax records, law enforcement data, and health records. Securing this data and ensuring it can be quickly restored in the event of a cyberattack, system failure, or natural disaster is essential

for minimizing risks and maintaining public trust. Below are some best practices for safeguarding data and ensuring its recovery if necessary.

1. Implement Strong Data Encryption

Encryption is one of the most effective ways to protect sensitive data, both in transit and at rest. When data is **encrypted**, it becomes unreadable to anyone who doesn't have the decryption key. This ensures that even if cybercriminals gain access to the data, they cannot use it without the key. Local governments should ensure that:

- **Sensitive data** (e.g., personal information, financial records) is encrypted using strong encryption protocols, both during storage (at rest) and when transmitted over networks (in transit).
- **Encryption keys** are stored securely and access to them is tightly controlled.
- **End-to-end encryption** is implemented for email communications and file transfers to prevent unauthorized access.

Encryption serves as a critical safeguard in the event of a breach, making it much more difficult for attackers to exploit stolen data.

2. Regularly Backup Data

Frequent and reliable **data backups** are essential for ensuring business continuity and minimizing downtime in case of a cyberattack or disaster. Backups provide a means to restore data without paying a ransom or incurring significant recovery costs. Best practices for data backup include:

- **Perform regular backups** of critical systems and databases. Consider using a **backup schedule** that suits the municipality's needs (e.g., daily, weekly).
- Store backups in **secure, off-site locations**, such as cloud services or external hard drives, to protect against localized incidents (e.g., fires or floods).
- Use **incremental backups** to capture only changes made since the last backup, reducing storage costs and speeding up the process.
- Ensure that backups are **encrypted** to protect the data from unauthorized access.
- Regularly test the restore process to confirm that the data can be recovered quickly and accurately when needed.

Having a solid backup strategy reduces the risk of losing valuable information during a cyber incident or system failure.

3. Implement Access Control and Data Segmentation

Limiting access to sensitive data is a fundamental part of data protection. **Access control** mechanisms ensure that only authorized individuals can view or modify critical data, reducing the risk of internal breaches or unauthorized exposure. Best practices for access control include:

- **Role-based access control (RBAC)**: Employees should only have access to the data necessary for their job function. This limits exposure and reduces the potential damage caused by compromised accounts.
- **Strong authentication protocols**: Use **multi-factor authentication (MFA)** to strengthen access security and prevent unauthorized access.
- **Data segmentation**: Divide data into different security zones and apply different levels of protection depending on the sensitivity of the data. For example, highly sensitive data, such as financial records or personal health information, may require additional safeguards.
- **Least privilege principle**: Employees should be given the minimum level of access required to perform their job functions. This limits the damage that can occur if an account is compromised.

These measures ensure that access to sensitive data is tightly controlled, minimizing the risk of exposure.

4. Establish a Data Retention and Disposal Policy

Local governments should have a **data retention** policy that defines how long data will be kept, how it will be archived, and when it will be safely disposed of. Retaining unnecessary data increases the potential attack surface for hackers, as attackers may target outdated, unmonitored data for exploitation. Best practices for data retention and disposal include:

- Define clear **data retention schedules** based on legal, regulatory, and operational requirements.
- **Archive old data** in secure, easily accessible locations, while ensuring that it remains protected by encryption.
- **Safely dispose of outdated or irrelevant data** by using secure **data destruction techniques**, such as wiping hard drives or physically destroying storage devices, to prevent unauthorized access.

By implementing a data retention and disposal policy, municipalities can reduce the risk of keeping unnecessary or outdated data vulnerable to breaches.

5. Develop a Comprehensive Disaster Recovery and Business Continuity Plan

A solid **disaster recovery** (DR) and **business continuity plan** (BCP) is essential for ensuring that data can be restored and operations can resume quickly after a cyberattack, natural disaster, or system failure. A well-prepared plan includes:

- **Clear recovery objectives**: Define **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** for each critical system, identifying how quickly data needs to be restored and the maximum acceptable data loss in case of an incident.
- **Defined roles and responsibilities**: Ensure that all employees understand their role in the recovery process and know who to contact in the event of a crisis.
- **Step-by-step recovery procedures**: Create a detailed plan for recovering data and systems, including how to restore backups, re-establish access to systems, and ensure that data integrity is maintained.
- **Test the plan regularly**: Regularly **test** the disaster recovery plan to ensure that it works efficiently and that any gaps or issues are addressed before an actual event occurs.

Having a DR and BCP ensures that local governments can minimize disruption, reduce downtime, and maintain essential public services even during or after a major cyber incident.

6. Monitor and Audit Data Access

Continuous **monitoring** and **auditing** of data access is essential for identifying and mitigating unauthorized attempts to access or modify sensitive data. Best practices include:

- Implementing **real-time monitoring** systems that track who is accessing sensitive data and when.
- Regularly reviewing **audit logs** for unusual activities, such as failed login attempts or large data downloads.
- Setting up **alerts** to notify IT staff of suspicious activities that may indicate a breach.

Regular monitoring helps detect unauthorized access early, enabling municipalities to respond quickly and mitigate potential damage.

Data protection and recovery are essential components of any local government's cybersecurity strategy. By following these best practices, municipalities can safeguard sensitive data, ensure the availability of critical systems, and minimize the operational impact of cyberattacks or disasters. Data protection is not a one-time effort—it requires ongoing attention and continuous improvement to adapt to emerging threats. By taking proactive measures to protect and recover data, local governments can secure public trust, comply with regulations, and reduce the risks associated with cyber incidents.

Building a Cyber-Resilient Community

Collaboration Between Local Governments, State Agencies, and Private Sector

Building a **cyber-resilient community** requires strong collaboration between local governments, state agencies, and the private sector. Cyber threats are increasingly sophisticated and borderless, making it impossible for any single entity to address the challenges of cybersecurity on its own. By working together, municipalities, state entities, and private organizations can create a more unified defense against cyber threats, share critical information, and foster a culture of collaboration that strengthens the overall cybersecurity posture of the community.

1. Sharing Threat Intelligence and Best Practices

One of the key benefits of collaboration is the ability to share **threat intelligence**. Local governments often lack the resources or expertise to monitor cyber threats at the same scale as state agencies or private sector organizations. However, by collaborating with state cybersecurity offices and private cybersecurity firms, municipalities can gain access to real-time information on emerging threats, attack trends, and vulnerability reports.

State agencies like the **New York State Cyber Incident Response Team (CIRT)**, for example, provide local governments with critical alerts, guidelines, and best practices for preventing and responding to cyber incidents. The private sector also plays a significant role by providing threat intelligence, vulnerability assessments, and managed security services. By sharing this information, local governments can better prepare for potential cyberattacks and take proactive steps to protect public data and infrastructure.

2. Coordinating Incident Response and Recovery

Cyber incidents often require a coordinated response, and the most effective way to handle these events is through collaboration. During a major cyberattack, state agencies and private sector cybersecurity firms can offer technical expertise, legal advice, and support services to local governments. This coordination ensures a more efficient and organized response to mitigate the damage of an attack, minimize downtime, and restore systems to normal operation.

For example, in the event of a **ransomware attack**, the private sector may provide expertise in decrypting files, while state agencies help with public communications and ensuring that local governments comply with regulatory requirements for breach notifications. The private sector's expertise in cybersecurity tools, combined with the state's resources and legal frameworks, creates a comprehensive support structure for incident recovery.

Additionally, local governments should establish **cyber incident response teams** that include representation from state agencies, private cybersecurity firms, and law enforcement. These teams can develop coordinated incident response plans and conduct joint exercises to ensure seamless collaboration in the event of a real cyberattack.

3. Building Trust and Developing Cybersecurity Standards

Collaboration also helps build trust among various entities, which is crucial for addressing the cybersecurity challenges faced by local governments. Local governments, by nature, serve as custodians of a wide range of sensitive public information, and any breach of that data can erode public trust. To prevent such occurrences, it's essential that local governments work with state agencies and private-sector cybersecurity experts to develop **cybersecurity standards** and ensure their adoption across the community.

By collaborating on creating industry-standard cybersecurity practices, municipalities can ensure that their cybersecurity measures align with state and federal guidelines and meet the necessary standards of protection. For example, the **National Institute of Standards and Technology (NIST)** provides frameworks that can guide local governments in establishing robust cybersecurity programs. Private cybersecurity companies can help municipalities implement these standards, offering specialized services, tools, and training tailored to local needs.

4. Access to Funding and Resources

Cybersecurity can be expensive, especially for municipalities with limited budgets or without dedicated IT departments. Collaboration with state agencies and the private sector can provide local governments with access to **funding**, **grants**, and **shared resources** to improve their cybersecurity capabilities. For instance, New York State's **Cybersecurity Grant Program** offers municipalities financial assistance for strengthening their cybersecurity posture, including investments in secure networks, employee training, and incident response tools.

Private sector companies may also provide discounted or pro bono services to municipalities in need of cybersecurity support. By partnering with the private sector, local governments can leverage the expertise of cybersecurity firms without the significant costs of hiring full-time staff. These partnerships help local governments keep up with the latest security technologies and best practices while maximizing their limited cybersecurity budgets.

5. Raising Public Awareness and Education

A cyber-resilient community depends not only on the security of its government systems but also on the awareness and preparedness of its citizens. Collaboration between local governments, state agencies, and private companies can promote public **cybersecurity education** and **awareness campaigns**. These campaigns can inform citizens about common threats, such as phishing attacks and identity theft, and teach them how to protect their personal data online.

State and local governments can work with private cybersecurity firms to develop and distribute educational materials, hold public awareness events, and provide training for residents on how to stay safe online. By fostering a more informed public, municipalities can reduce the likelihood of successful cyberattacks targeting residents and help create a more cyber-resilient community overall.

Collaboration between local governments, state agencies, and the private sector is critical to building a **cyber-resilient community**. By sharing threat intelligence, coordinating incident response, establishing common cybersecurity standards, providing access to funding, and

promoting public education, these entities can create a stronger, more unified defense against cyber threats. Cyber resilience is a shared responsibility, and through partnerships and collaboration, local governments can improve their ability to protect sensitive data, recover from incidents, and maintain the trust of their residents.

The Role of Public Awareness and Education in Cybersecurity

Public awareness and education are essential pillars in building a **cyber-resilient community**. While local governments and organizations implement cybersecurity measures to protect systems and data, the general public plays a critical role in preventing and mitigating cyber threats. In many cases, individuals are the weakest link in the cybersecurity chain, often unknowingly exposing themselves to risks such as **phishing attacks**, **identity theft**, or **malware**. By prioritizing cybersecurity education and raising awareness, local governments can empower residents to protect themselves and contribute to the community's overall defense against cyber threats.

1. Empowering Residents to Protect Themselves Online

The majority of cyber threats, including **phishing** and **social engineering attacks**, target individuals rather than organizations. Educating the public about common cyber threats and safe online practices helps reduce the risks posed by human error. Local governments should invest in educational campaigns that inform residents about the following key topics:

- **Recognizing phishing emails**: Educating individuals on how to identify fraudulent emails and messages that ask for personal or financial information.
- **Creating strong passwords**: Encouraging the use of unique, complex passwords for each online account, along with the importance of **multi-factor authentication (MFA)**.
- **Avoiding public Wi-Fi risks**: Advising people against using unsecured networks for sensitive transactions or accessing government services online.
- **Practicing good device security**: Encouraging residents to regularly update their software and use antivirus protection to safeguard their computers and smartphones.

By providing these essential skills, local governments can help residents become more vigilant in their online activities, reducing the likelihood of falling victim to common cyber threats.

2. Promoting Digital Literacy Across the Community

In today's digital world, **digital literacy** is crucial for all age groups. A cyber-resilient community is one where residents not only understand the risks associated with cyber threats but also possess the knowledge and skills to navigate the digital landscape safely. Public education programs should focus on enhancing digital literacy, particularly for vulnerable populations such as seniors, who may be more susceptible to online scams. These programs could include:

- **Workshops** or online tutorials that teach residents how to protect their privacy, recognize online fraud, and safeguard personal information.
- **Community seminars** that explain how to safely use digital services, such as banking, healthcare, and government portals, which may be increasingly accessed online.

- Partnering with local schools, libraries, and senior centers to deliver **tailored training** based on specific needs and challenges faced by different groups.

Equipping the community with essential digital literacy skills ensures that all residents, regardless of their age or background, can participate in and benefit from the digital economy without exposing themselves to unnecessary risks.

3. Building a Culture of Cybersecurity Awareness

Building a **culture of cybersecurity awareness** requires consistent and proactive efforts from local governments. Cybersecurity should be viewed as a shared responsibility, with each member of the community playing a role in keeping the digital environment secure. This involves not only educating the public but also engaging local businesses, schools, and civic organizations in cybersecurity initiatives. Some key actions include:

- **Promoting cybersecurity as part of everyday life**: Encouraging residents to adopt safe online behaviors as part of their routine, just as they would with physical safety measures.
- **Incorporating cybersecurity education into school curriculums**: Introducing children to basic cybersecurity concepts, such as safe internet use, ethical online behavior, and privacy protection, to create a future generation that is more cyber-aware.
- **Engaging local businesses**: Supporting small and medium-sized businesses with resources and training on cybersecurity best practices, since they are often a prime target for cybercriminals but may lack the resources to defend against attacks.

By integrating cybersecurity education into everyday life and community activities, local governments can foster a culture where cybersecurity is prioritized, and the public becomes more active in safeguarding their digital interactions.

I had the pleasure of co-authoring an Amazon #1 Best Selling book title *"From Exposed To Secure: The Cost Of Cybersecurity And Compliance Inaction And The Best Way To Keep your Company Safe"* which is a great reference for building a culture of cybersecurity awareness in your business and community.

4. Leveraging Social Media and Public Campaigns

Public awareness campaigns are highly effective when leveraged through **social media**, local news outlets, and community outreach programs. Local governments can use these channels to distribute timely cybersecurity tips, updates on new threats, and guidance on how to stay safe online. Some strategies include:

- **Utilizing social media platforms** (such as Facebook, Twitter, and Instagram) to share bite-sized cybersecurity advice, alerting residents to emerging threats or new scams in real time.
- Creating **public service announcements (PSAs)** that raise awareness about the importance of strong passwords, recognizing fake websites, and securing personal devices.

- Partnering with local businesses and media outlets to distribute educational content and host cybersecurity awareness events or webinars.

These campaigns help to reach a broad audience, raise awareness about specific risks, and encourage the adoption of safer online behaviors across the community.

5. Encouraging Reporting and Community Engagement

Another essential aspect of public education is encouraging **reporting of cyber incidents**. Many residents may not know how or where to report a potential cybercrime or data breach. By educating the public on how to report suspicious activity, local governments can increase the likelihood of prompt intervention and mitigation. This includes:

- Providing clear instructions on how to report **cybercrime** to local law enforcement or **state agencies** such as the New York State Cyber Incident Response Team (CIRT).
- Offering **anonymous reporting options** to help residents feel safe coming forward with information about cyber incidents or suspicious activities.
- Creating community-driven cybersecurity networks where residents can share knowledge, resources, and advice with one another to help prevent further attacks.

Encouraging the public to be proactive in reporting incidents not only improves local cybersecurity efforts but also helps law enforcement track and respond to emerging threats.

Public awareness and education play an indispensable role in creating a **cyber-resilient community**. By equipping residents with the knowledge and skills to protect themselves online, fostering a culture of cybersecurity, and engaging the community in reporting and mitigating threats, local governments can strengthen their overall cybersecurity defenses. In a world where cyber threats continue to evolve, an informed and proactive public is one of the most effective ways to reduce risks and ensure that local governments can continue to serve their communities securely.

Success Stories and Case Studies

Below are a few **success stories and case studies** related to local governments implementing cybersecurity initiatives and successfully managing cyber threats. These examples highlight how effective cybersecurity measures and collaboration have helped mitigate risks and enhance overall resilience.

1. **City of Albany, New York – Improving Cybersecurity Posture through State-Funded Initiatives**

In recent years, the **City of Albany**, New York, faced increasing cyber threats, primarily from phishing attacks and ransomware. To combat these risks, the city took a proactive approach to improve its cybersecurity posture by partnering with the New York State **Office of Information Technology Services** (ITS) and taking advantage of state-funded initiatives aimed at strengthening local government cybersecurity.

Albany's local government adopted a comprehensive cybersecurity framework, incorporating advanced **data encryption**, **network monitoring**, and **employee training** to protect sensitive public data and municipal systems. The partnership with state agencies provided crucial

resources, including financial support to update IT infrastructure, as well as access to state-run **cybersecurity workshops** and **incident response** support.

This collaboration and investment led to a significant reduction in successful cyberattacks and ensured that Albany's municipal services, such as public health and emergency response systems, remained secure and available. Albany continues to work closely with state agencies to stay ahead of emerging threats and to ensure compliance with New York State's cybersecurity standards.

---

2. City of Rochester, New York – Ransomware Attack Response and Recovery

In 2019, the City of **Rochester, New York**, fell victim to a **ransomware attack** that compromised several municipal systems, including email and critical public-facing services. The attackers encrypted important files and demanded a ransom in exchange for the decryption keys.

Rather than paying the ransom, Rochester's leadership decided to implement a **rapid recovery strategy** with the help of the **New York State Cyber Incident Response Team (CIRT)**. Working with CIRT and private-sector cybersecurity consultants, the city successfully restored its systems from **backups** and contained the breach without further compromising sensitive data.

Rochester also used this incident as a learning opportunity, investing in comprehensive employee **cybersecurity training**, **multi-factor authentication** (MFA), and strengthening **data backup** protocols to prevent future incidents. The city then shared its lessons learned with other local governments, collaborating on **statewide seminars** to improve overall cybersecurity awareness and preparedness across New York State municipalities.

---

3. Suffolk County, New York – Enhanced Cybersecurity through Public-Private Partnerships

In 2020, **Suffolk County**, New York, recognized the increasing need to enhance its cybersecurity measures due to rising threats from cybercriminals. The county worked closely with **private cybersecurity firms** and **state agencies** to strengthen its digital defenses. One key initiative was the formation of a **Public-Private Cybersecurity Task Force**, which brought together local government officials, IT professionals, private-sector cybersecurity experts, and law enforcement to improve resilience against cyber threats.

The Task Force conducted a **comprehensive risk assessment** to identify vulnerabilities in the county's networks and deployed **network segmentation**, improved **firewalls**, and more sophisticated **intrusion detection systems**. Additionally, the county worked with local businesses and schools to promote **cyber hygiene** and best practices for protecting digital assets.

The collaboration led to increased **cyber resilience**, reducing the frequency of successful attacks and enhancing the county's ability to detect and respond to emerging threats. Suffolk

County continues to serve as a model for other local governments in New York State, demonstrating the value of public-private partnerships in tackling cybersecurity challenges.

---

4. Village of Lake Placid, New York – Successful Response to a Data Breach

The **Village of Lake Placid**, New York, faced a data breach in 2021 involving a compromised third-party vendor. The breach exposed personal data of residents and local employees, raising concerns about the security of village systems. However, the village had recently implemented a **cybersecurity incident response plan** as part of a larger effort to align with the **New York State Comptroller's cybersecurity guidelines**.

Upon detection of the breach, the village swiftly activated its **incident response team**—a collaborative effort between village officials, the state's Cybersecurity Incident Response Team (CIRT), and a contracted private-sector cybersecurity firm. The team quickly identified the nature of the breach, contained the threat, and began notifying affected parties in compliance with **New York State's Information Security Breach and Notification Act** (ISBNA).

In the aftermath, the village not only worked to strengthen its IT infrastructure but also conducted **training sessions** for employees and local business owners to educate them on the latest cybersecurity threats. As a result, Lake Placid has been able to significantly improve its overall data security and has become a leader in cybersecurity best practices for small municipalities in the region.

---

5. New York City – Comprehensive Cybersecurity Strategy for Critical Infrastructure Protection

New York City (NYC), as one of the largest and most prominent urban centers in the world, is a prime target for cybercriminals. To protect its residents and critical infrastructure, NYC has developed one of the most comprehensive and proactive cybersecurity strategies among U.S. cities. The city's **Cyber Command (NYC Cyber Command)** works closely with **state agencies**, **federal authorities**, and **private-sector partners** to defend against cyber threats.

In addition to **24/7 threat monitoring** and **real-time incident response**, NYC has implemented a series of **resilience measures** to secure the city's critical infrastructure, such as transportation systems, utilities, and healthcare facilities. The city's efforts include **cyber risk assessments** for municipal agencies and high-risk sectors, **cybersecurity training** for government employees, and **public outreach** initiatives to raise awareness among citizens.

As a result, New York City has been able to successfully thwart numerous cyberattacks, including ransomware and denial-of-service (DoS) attacks, through its robust and coordinated cybersecurity strategy. NYC continues to collaborate with state and private sector partners to stay ahead of emerging threats and maintain its status as one of the most secure cities in terms of cyber infrastructure protection.

These success stories illustrate the importance of proactive measures, collaboration, and continuous improvement in cybersecurity. Local governments across New York State have learned valuable lessons from past incidents, sharing knowledge and resources to protect their

communities. By partnering with state agencies, private sector firms, and adopting best practices, municipalities can significantly enhance their cyber resilience and mitigate the risks associated with the evolving cyber threat landscape.

Conclusion

Recap of Key Points

As local governments across New York State increasingly face the threat of cyberattacks, it has become clear that cybersecurity is not just an IT issue—it's a critical responsibility that affects all aspects of local governance and the wellbeing of communities. Here's a summary of the key points covered in this guide:

1. The Growing Importance of Cybersecurity

The need for robust cybersecurity has never been more urgent. Local governments manage vast amounts of sensitive data and oversee critical infrastructure that could be targeted by cybercriminals. Ensuring that these systems are secure is vital to maintaining public trust, protecting personal data, and ensuring the continuity of essential public services.

2. Specific Challenges Faced by Local Governments

Local governments face unique cybersecurity challenges due to limited resources, lack of dedicated IT staff, and the increasing sophistication of cyber threats. Many municipalities struggle to keep pace with evolving cyber risks, which require dedicated attention, expertise, and proactive measures to prevent attacks.

3. Common Types of Cyberattacks

Cyberattacks on local governments often include **phishing**, **ransomware**, and **data breaches**. These attacks can compromise sensitive data, disrupt critical services, and impose significant financial and operational costs. Understanding these threats is essential for local governments to develop targeted defenses.

4. How the New York State Comptroller's Office Supports Local Governments

The New York State Comptroller's Office plays a crucial role in helping local governments strengthen their cybersecurity practices by providing resources, best practices, and oversight. Compliance with the Comptroller’s guidelines helps municipalities assess their risks and improve their cyber defenses.

5. Importance of Compliance with the NYS Comptroller Guidelines

Compliance with the Comptroller’s guidelines is essential for ensuring that local governments are meeting state and federal cybersecurity standards. It helps municipalities assess vulnerabilities, safeguard sensitive data, and avoid penalties from non-compliance.

6. Financial and Operational Impacts of Cyberattacks

Cyberattacks can have devastating financial and operational impacts, including direct costs like ransomware payments and system repairs, as well as indirect costs such as reputational damage and lost productivity. Cybersecurity is a critical investment to prevent such costs.

7. Cyber Liability Insurance and Its Role in Risk Management

Cyber liability insurance is becoming an essential component of risk management for local governments. It helps mitigate the financial impact of cyber incidents, covering costs related to

data breaches, system repairs, legal fees, and more. Choosing the right policy is essential for providing comprehensive coverage.

8. Implementing Effective Cybersecurity Measures

Developing a robust cybersecurity strategy involves assessing risks, implementing preventive measures, securing networks, and regularly updating systems. Local governments should prioritize employee training, strong data protection practices, and a continuous commitment to improving their cybersecurity posture.

9. The Importance of Regular Security Training for Employees

Human error is a significant vulnerability in cybersecurity. Regular employee training on recognizing phishing attempts, handling sensitive data securely, and following best practices is critical for mitigating the risks of social engineering and other cyber threats.

10. Best Practices for Data Protection and Recovery

Implementing best practices for data protection—such as encryption, backup strategies, and access controls—helps ensure the integrity and security of critical data. Additionally, having a clear data recovery plan in place enables local governments to quickly restore operations after a cyber incident.

11. Building a Cyber-Resilient Community

Cyber resilience requires collaboration between local governments, state agencies, the private sector, and the public. Information sharing, coordinated incident response, and ongoing education help strengthen the community's ability to prevent, detect, and recover from cyber incidents.

12. The Role of Public Awareness and Education in Cybersecurity

Public education is vital for creating a cyber-aware community. Local governments must engage with residents to raise awareness about common cyber threats and safe online practices. Promoting **digital literacy** and **cyber hygiene** across all demographics helps reduce the likelihood of successful attacks.

13. Success Stories and Case Studies

Several New York municipalities, including Albany, Rochester, Suffolk County, and Lake Placid, have successfully implemented cybersecurity improvements or responded to incidents, demonstrating the importance of collaboration, planning, and investing in cybersecurity measures. These success stories provide valuable lessons for other local governments.

14. The Role of the New York State Department of Finance

The Department of Finance plays a critical role in regulating and overseeing the financial operations of local governments, including ensuring that cybersecurity measures align with state guidelines and funding opportunities. Its guidance helps municipalities build secure, efficient financial systems.

15. Resources and Support Provided to Municipalities

New York State provides a range of resources to help municipalities improve their cybersecurity posture, from grants and training programs to technical assistance. Accessing these resources enables local governments to bolster their defenses against cyber threats while maximizing limited budgets.

In today's increasingly digital world, local governments must take proactive steps to protect their communities from cyber threats. By implementing robust cybersecurity measures, adhering to state guidelines, securing cyber liability insurance, and fostering public awareness, municipalities can reduce vulnerabilities and create a more secure environment for their residents. The collaboration between local governments, state agencies, private sector partners, and the public is key to building a resilient cyber infrastructure that can withstand evolving threats.

Call to Action for Local Governments to Prioritize Cybersecurity

As cyber threats continue to evolve at an unprecedented pace, local governments across New York State must take decisive action to protect their communities, data, and critical infrastructure. Cybersecurity is no longer a luxury or afterthought—it is an essential, ongoing investment that directly impacts the safety, security, and trust of the public you serve.

Now is the time for local government leaders to take the necessary steps to fortify your systems against potential threats. Start by:

1. **Conducting a comprehensive cybersecurity risk assessment** to identify vulnerabilities and prioritize critical areas for improvement.
2. **Implementing cybersecurity best practices** such as multi-factor authentication, regular software updates, and strong data protection measures.
3. **Investing in employee training and awareness programs** to equip staff with the skills and knowledge to recognize and respond to cyber threats.
4. **Ensuring compliance** with the New York State Comptroller's cybersecurity guidelines and other relevant regulations to reduce risk and protect taxpayer dollars.
5. **Collaborating with state agencies, private sector partners, and other municipalities** to stay informed about emerging threats and share resources, expertise, and strategies.
6. **Securing cyber liability insurance** to safeguard your municipality from the financial fallout of a cyber incident.

As leaders of your community, you have the power to influence change and build a strong, cyber-resilient future. Prioritizing cybersecurity today not only protects your systems but also builds confidence with residents, businesses, and the broader community. By acting now, you can ensure the safety of your constituents and protect the public services that are vital to their well-being.

Don't wait until it's too late—take the first step today toward a more secure future for your local government and your residents.

Should Municipal Governments Outsource Their IT Needs?

As municipalities face increasing pressure to secure their digital infrastructure, manage a growing volume of data, and meet the ever-expanding expectations of residents for efficient, modern services, the question arises: Should local governments outsource their IT needs? The landscape of technology and cybersecurity is continually evolving, and many smaller towns and villages, particularly those without dedicated internal IT staff, are finding it challenging to keep up. Outsourcing IT services to external experts may offer a practical, efficient, and cost-effective solution for managing these complexities.

Outsourcing IT allows municipalities to tap into specialized expertise and experience that would be difficult or prohibitively expensive to cultivate in-house. Third-party managed service providers (MSPs) can handle critical IT functions such as network management, cybersecurity, cloud services, and system administration, freeing up municipal staff to focus on core governance responsibilities. This external support not only enhances security and operational efficiency but also enables local governments to keep pace with rapid technological changes without the burden of ongoing investment in IT infrastructure or personnel.

Given the increasing prevalence of cyberattacks targeting public sector entities and the growing reliance on digital platforms for everyday services, the stakes are high. For many municipalities, outsourcing IT can offer significant benefits, from cost savings to improved service delivery, ensuring that local governments stay secure, effective, and agile in an increasingly digital world.

Benefits of Outsourcing IT for Municipal Governments

1. **Cost Savings**
   One of the most immediate benefits of outsourcing IT is cost savings. Building an internal IT team requires significant investment in salaries, benefits, training, and technology. Outsourcing allows local governments to pay for services as needed, eliminating the costs associated with hiring, onboarding, and retaining full-time IT staff. This pay-as-you-go model can be especially beneficial for small municipalities with limited budgets.

2. **Access to Specialized Expertise**
   IT service providers bring a high level of technical expertise that is often beyond the scope of municipal in-house teams, especially in smaller towns and villages without dedicated IT departments. These experts are well-versed in the latest technologies, cybersecurity measures, and best practices, ensuring that your municipality benefits from up-to-date solutions and proactive security management.

3. **Enhanced Cybersecurity**
   Cybersecurity is a growing concern for local governments, which are frequent targets of cyberattacks. Outsourcing IT allows municipalities to work with service providers who specialize in cybersecurity, implementing robust defense measures, monitoring systems for vulnerabilities, and quickly responding to threats. Managed IT providers also ensure compliance with industry standards and government regulations related to data protection.

4. **Scalability and Flexibility**
   As municipal needs evolve, outsourced IT services can scale to meet new demands. Whether it’s supporting a new project, handling an increase in digital services, or managing data during an emergency, outsourcing allows local governments to quickly and cost-effectively adapt to changing needs without the risk of overburdening in-house staff or infrastructure.

5. **Improved Service Delivery**
   Outsourcing IT services ensures that local government operations are running smoothly and efficiently. Service providers can manage routine IT tasks—such as software updates, backups, and network monitoring—so municipal employees can focus on

delivering essential services to the community. This improved operational efficiency helps to reduce downtime, enhance productivity, and ultimately improve public service delivery.

6. **Disaster Recovery and Business Continuity**
   Effective disaster recovery and business continuity plans are essential for minimizing the impact of unexpected events, such as system failures, natural disasters, or cyberattacks. Outsourcing IT services allows municipalities to implement comprehensive disaster recovery strategies with backup systems and off-site data storage, ensuring that critical government services can continue without interruption in the event of an emergency.

7. **Regulatory Compliance**
   Municipalities must adhere to a wide range of legal and regulatory requirements related to data privacy, security, and accessibility. Outsourcing IT ensures that these requirements are met, as service providers are well-versed in compliance regulations such as those set by the New York State Comptroller's Office and other relevant authorities. A managed IT provider will help your municipality stay compliant and avoid penalties.

8. **Proactive Maintenance and Support**
   Outsourcing IT allows for proactive maintenance, meaning that service providers monitor systems 24/7 to identify and resolve issues before they become serious problems. This proactive approach minimizes downtime, improves system reliability, and ensures that your IT infrastructure is always running at optimal capacity.

Outsourcing IT services offers significant advantages for municipal governments, from cost savings and access to specialized expertise to enhanced cybersecurity and disaster recovery capabilities. For smaller towns and villages, outsourcing is not just a cost-effective solution—it's a strategic move that allows local governments to focus on their core mission: serving their communities. By leveraging the skills and knowledge of experienced IT professionals, municipalities can stay secure, efficient, and agile in the face of growing technological demands and cybersecurity threats.

About CST Group Inc.

Founded in 2000 by visionary entrepreneur **Lisa A. Brown**, CST Group Inc. is a proactive technology management firm dedicated to securing, protecting, and managing the IT infrastructures of municipalities and compliance-driven industries. With over three decades of experience, the company specializes in delivering comprehensive IT solutions tailored to the unique needs of its clients.

Suite of Services Includes

- **Managed IT Services:** Ensuring peak operation of IT networks with 24/7 monitoring and support.
- **Computer Networking:** Designing and implementing secure, efficient network infrastructures.
- **Data Backup and Recovery:** Implementing robust backup solutions to safeguard critical data.
- **Vendor Management:** Serving as a liaison between clients and their technology vendors to streamline operations.
- **VoIP Services:** Providing advanced communication solutions to enhance connectivity.
- **Risk Assessments:** Identifying vulnerabilities across networks, systems, and operations to strengthen cybersecurity posture and ensure compliance with state and federal regulations.

At CST Group, we understand the stringent compliance requirements faced by government agencies. Our in-house staff specialize in ensuring adherence to **New York State and federal regulations**, including **DFS Cybersecurity Regulations** and **Cyber Liability Insurance compliance** to name a few.

Our commitment to excellence is reflected in our client relationships. As Andrea Stewart, Supervisor of the Town of Malone, attests:

> “Knowing that our technology and staff are protected, and the security of our entire organization is monitored allows me to focus on what is important to the Town of Malone. Whether for backup, quick response, or their efficient handling of all our issues, CST is at the height of any scale provided.”

Under the leadership of Lisa Brown, along with her husband, **Shawn Brown**, CST Group has earned recognition as a **woman-owned and veteran-owned enterprise**, fostering a sustainable workplace and holding a **World-Class Customer Experience Certification**.

With offices in **Northern New York and Southwest Florida**, CST Group Inc. serves clients along the East Coast, providing tailored IT solutions to government entities and businesses in diverse industries. Our expansion allows us to bring our expertise, proactive security measures, and top-tier customer support to organizations facing the evolving challenges of modern technology.

IT For Local Government: A CST Group Initiative

As part of its continued mission to protect and empower public institutions, CST Group Inc. operates under the **DBA "IT For Local Government"** — a dedicated division focused exclusively on the cybersecurity, compliance, and technology needs of towns, villages, and cities across New York State.

IT For Local Government was created to help municipalities bridge the gap between limited resources and enterprise-level security demands. The division provides local governments with access to the same caliber of technology protection and strategic guidance used by major corporations — scaled for the realities of public service.

Its mission is simple yet vital:

To keep New York State's local governments secure, resilient, and prepared for the digital future.

Through IT For Local Government, CST Group partners with public leaders to assess vulnerabilities, modernize systems, and strengthen digital defenses — ensuring that every municipality, regardless of size, has the tools to protect its data, maintain public trust, and serve its citizens with confidence.

At **CST Group Inc.**, we are dedicated to empowering government entities with reliable, compliant, and forward-thinking IT solutions, ensuring that technology serves as a robust foundation for **public service excellence** and **community security**.

Contact Information:

CST Group Inc.
Computer Support & Training
dba IT For Local Government
14923 State Route 30
Malone, NY 12953
877-954-4100
518-483-4100

CST Group Inc.

IT
FOR LOCAL GOVERNMENT
Powered by CST Group Inc.

A Personal Note from Lisa A. Brown, CEO of CST Group Inc.

Dear Reader,

Thank you for taking the time to read this e-book. In today's world, technology is the backbone of every organization—especially in government and highly regulated industries. Cyber threats are evolving daily, and the responsibility to protect critical systems and sensitive data has never been greater. I appreciate your commitment to learning more about securing your technology and strengthening your organization's defenses.

At CST Group Inc., we understand that cybersecurity and IT management are not just technical challenges, they are essential to the success and continuity of your mission. That's why we are here—to be your **trusted partner** in navigating these challenges, providing solutions that keep you secure, compliant, and ahead of the curve.

If anything in this e-book resonated with you, if you have questions, or if you're wondering how your organization can be better protected, I invite you to reach out. Let's have a conversation about your unique needs and how CST Group can help you implement proactive, effective solutions tailored to your operations.

But don't just take my word for it—see what our clients have to say. We are honored to have built strong, lasting partnerships with businesses and government entities that trust us to protect their technology and data. I encourage you to visit our **Testimonials Page** and hear directly from those who have experienced the CST Group difference. Their success stories speak volumes about our commitment, expertise, and unwavering support.

More importantly, let's take action. Your organization deserves more than just knowledge, it deserves a strategy, execution, and a partner who is as invested in your success as you are. My team and I are ready to help you secure, protect, and optimize your technology so you can focus on what matters most—serving your community and growing your impact.

I look forward to hearing from you. Let's build something great together.

Lisa A. Brown
CEO & Founder
CST Group Inc.
📞 [518-483-4100]
📧 [lbrown@cstsupport.com]
🌐 www.cstsupport.com

Appendices

Glossary of cybersecurity terms

1. Cybersecurity
The practice of protecting computer systems, networks, and data from cyberattacks, unauthorized access, and damage. It involves implementing tools, processes, and policies to safeguard digital infrastructure.

2. Phishing
A type of cyberattack where attackers impersonate legitimate organizations or individuals to trick people into providing sensitive information such as usernames, passwords, or financial details.

3. Ransomware
A form of malware (malicious software) that locks or encrypts a victim's data, demanding payment (ransom) for its release. It can disrupt local government operations and lead to significant financial losses.

4. Malware
Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Common forms of malware include viruses, worms, and ransomware.

5. Data Breach
An incident in which sensitive, confidential, or protected data is accessed, disclosed, or used without authorization. Data breaches can involve personal information, financial records, and government data.

6. Multi-Factor Authentication (MFA)
A security process that requires users to provide two or more verification factors to access an account or system. This typically includes something the user knows (password), something the user has (a phone), or something the user is (fingerprint or face recognition).

7. Encryption
The process of converting data into a code to prevent unauthorized access. Encrypted data can only be accessed or decrypted by authorized individuals with the correct key or password.

8. Incident Response Plan
A set of procedures and guidelines that a local government or organization follows to identify, manage, and recover from cybersecurity incidents, such as data breaches or ransomware attacks.

9. Cyber Liability Insurance
An insurance policy that helps protect local governments and organizations from the financial losses associated with cyber incidents, such as data breaches, business interruption, and legal fees related to cybersecurity events.

10. Risk Assessment
The process of identifying, evaluating, and prioritizing potential cybersecurity threats and vulnerabilities within an organization. It helps determine where resources and efforts should be focused to reduce risk.

11. Network Monitoring
The continuous observation and analysis of a computer network to detect unauthorized activities, performance issues, or potential security threats.

12. Data Backup
The process of copying and storing data in a secure location to ensure that it can be restored in the event of a cyberattack, data loss, or hardware failure. Effective backups are critical for recovery after incidents like ransomware attacks.

13. Firewall
A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).

14. Social Engineering
A tactic used by cybercriminals to manipulate individuals into divulging confidential information. It often involves psychological manipulation, such as pretending to be a trustworthy entity to gain access to sensitive data.

15. Cyber Incident
Any event or occurrence that poses a threat to the security or integrity of computer systems, networks, or data. This includes incidents such as unauthorized access, data breaches, or cyberattacks.

16. Vulnerability
A weakness or flaw in a system, network, or software that can be exploited by cybercriminals to gain unauthorized access or cause damage.

17. State and Local Cybersecurity (SLC) Programs
Programs and resources provided by government agencies and private partners to help local governments enhance their cybersecurity efforts. These programs often include grants, training, and incident response support.

18. Cyber-Resilience
The ability of a system or organization to continue operating effectively in the face of cyberattacks or disruptions, and to recover quickly after an incident. It involves preparation, prevention, detection, and response strategies.

19. Backdoor
A hidden or secret method of bypassing normal authentication or encryption in a system, typically used by cybercriminals to gain unauthorized access to systems or networks.

20. Vulnerability Assessment
The process of identifying and evaluating potential weaknesses in a system, software, or network that could be exploited by attackers. It is often conducted as part of a broader cybersecurity risk management strategy.

21. Cyber Hygiene
Best practices and habits that users and organizations adopt to maintain the security of their digital environment. This includes regular software updates, strong passwords, and avoiding risky online behaviors.

22. Compliance
Adhering to regulatory standards and guidelines set by governmental or industry organizations to ensure that systems, practices, and operations meet cybersecurity requirements. For local governments, compliance with the **NYS Comptroller's Guidelines** is an example of mandatory cybersecurity measures.

23. Incident Report
A formal record or notification of a cybersecurity incident, detailing the nature of the attack, its impact, and actions taken to mitigate the threat. Incident reports help with post-attack analysis and prevention.

24. Threat Intelligence
Information about potential or active cyber threats, including tactics, techniques, and procedures (TTPs) used by cybercriminals. Threat intelligence helps organizations stay informed and proactive in defending against attacks.

25. Cybersecurity Framework
A structured set of guidelines or practices designed to help organizations identify and manage cybersecurity risks. Examples include the **NIST Cybersecurity Framework**, which outlines key functions like identifying risks, protecting systems, and responding to incidents.

List of resources and further reading

1. **New York State Comptroller's Office – Cybersecurity Guidance**
    - The Comptroller's Office provides valuable resources, audits, and guidelines for local governments in New York State to improve their cybersecurity practices and comply with state regulations.
    - **Link**: New York State Comptroller - Cybersecurity
2. **New York State Cybersecurity Incident Response Team (CIRT)**
    - This state-run initiative helps local governments and organizations in New York State respond to and recover from cybersecurity incidents. They offer resources, tools, and incident response support.
    - **Link**: NYS CIRT
3. **Cybersecurity and Infrastructure Security Agency (CISA)**
    - CISA provides a wealth of information, guidelines, and resources to help local governments and organizations strengthen their cybersecurity posture, including frameworks, best practices, and alerts.
    - **Link**: CISA
4. **Federal Trade Commission – Cybersecurity for Small Businesses**

- While tailored to small businesses, the resources provided by the FTC are also helpful for municipalities looking to improve their cybersecurity awareness and practices. Topics include securing devices, protecting data, and preventing fraud.
- **Link**: FTC Cybersecurity Resources

5. **National Institute of Standards and Technology (NIST) – Cybersecurity Framework**
   - NIST offers a comprehensive cybersecurity framework that helps organizations, including local governments, manage cybersecurity risks. The framework outlines key activities in identifying, protecting, detecting, responding to, and recovering from cyber threats.
   - **Link**: NIST Cybersecurity Framework
6. **National Cybersecurity Alliance (NCSA)**
   - The NCSA offers a range of resources for local governments, businesses, and individuals to improve their cybersecurity awareness and actions. They also provide cybersecurity training materials.
   - **Link**: National Cybersecurity Alliance
7. **New York State Department of Financial Services (NYDFS) Cybersecurity Regulation**
   - The NYDFS provides regulations and guidelines for financial services organizations, but many of the principles and standards can be adapted by local governments to enhance their overall cybersecurity measures.
   - **Link**: NYDFS Cybersecurity Resource Center

Additional Reading

1. **"Cybersecurity for Local Governments: A Guide for Building Resilience" – International City/County Management Association (ICMA)**
   - This guide offers a roadmap for local governments to establish a comprehensive cybersecurity strategy, including governance, risk management, and incident response.
   - **Link**: ICMA Cybersecurity Guide

2. **"The Cybersecurity Survival Guide for Small Local Governments" – National Association of Counties (NACo)**
    - A resource designed to help small and rural local governments navigate cybersecurity risks, featuring practical advice on everything from IT infrastructure to staff training.
    - **Link**: NACo Cybersecurity Guide
3. **"Securing Local Government: Protecting Digital Assets in the Public Sector" – National League of Cities (NLC)**
    - This report offers insights into how municipalities can secure their digital infrastructure, manage risks, and enhance cybersecurity for critical public services.
    - **Link**: NLC Cybersecurity Resources
4. **"Managing Cybersecurity Risks for Government Organizations" – Center for Internet Security (CIS)**
    - CIS provides resources and tools specifically focused on government organizations, including best practices for securing networks, conducting risk assessments, and responding to incidents.
    - **Link**: CIS Government Resources
5. **"Cybersecurity for Municipalities: Protecting Critical Infrastructure" – U.S. Department of Homeland Security**
    - This guide focuses on the cybersecurity challenges facing local governments, particularly related to critical infrastructure like water supply, transportation, and energy systems.
    - **Link**: DHS Cybersecurity for Municipalities
6. **"Cybersecurity Essentials for Local Government" – Government Technology**
    - Government Technology's cybersecurity section provides articles, case studies, and insights on how local governments can stay ahead of cyber threats with effective policies, tools, and employee education.
    - **Link**: Government Technology Cybersecurity
7. **"Understanding Cyber Threats: A Guide for Public Sector Leaders" – National Governors Association (NGA)**
    - This publication provides public sector leaders with an understanding of the evolving cyber threat landscape and outlines strategies to build resilience in the public sector.
    - **Link**: NGA Cybersecurity Resources

8. **“From Exposed To Secure: The Cost of Cybersecurity and Compliance Inaction and the Best Way to Keep your Company Safe” - #1 Amazon Best Seller**

    - Co-authored by Lisa Brown, this #1 Amazon Best Selling Book highlights the results of taking no action on implementing cybersecurity protocols

    - **Link**: From Exposed to Secure on Amazon

Cybersecurity Training Resources

1. **Federal Virtual Training Environment (FedVTE)**

    - A free, online cybersecurity training platform offered by the U.S. Department of Homeland Security. It provides training on a variety of cybersecurity topics, ideal for local government employees.

    - **Link**: FedVTE

2. **Cybersecurity & Infrastructure Security Agency (CISA) Training**

    - CISA offers training programs specifically designed for government organizations, with modules covering everything from basic security awareness to advanced incident response.

    - **Link**: CISA Cybersecurity Training

3. **SANS Institute**

    - A leading provider of cybersecurity training, SANS offers specialized courses, certifications, and materials for government employees at all levels.

    - **Link**: SANS Cybersecurity Training