NYSAC
NEW YORK STATE
ASSOCIATION OF COUNTIES

NYCOM
New York State Conference
of Mayors & Municipal Officials

AOT

CENTER FOR TECHNOLOGY IN GOVERNMENT
UNIVERSITY AT ALBANY State University of New York

Cybersecurity Primer for Local Government Leaders

FEBRUARY 2022

HON. MARTHA SAUERBREY
NYSAC President

HON. FRANCIS X. MURRAY
NYCOM President

HON. EDMOND THEOBALD
AOT President

STEPHEN J. ACQUARIO
NYSAC Executive Director

PETER BAYNES
NYCOM Executive Director

GERRY GEIST
AOT Executive Director

Acknowledgments

The New York State Association of Counties (NYSAC), The New York Conference of Mayors (NYCOM), the Association of Towns of the State of New York (AOT), and the Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany) would like to recognize the following individuals for their support in creating this Primer.

AUTHORS:

Meghan Cook, Program Director, Center for Technology in Government, University at Albany, State University of New York (CTG UAlbany) and Advisor, NYS Local Government Information Technology Directors Association (NYSLGITDA)

Mark LaVigne, Deputy Director, New York State Association of Counties (NYSAC)

Alondra Berroa, Program Associate, Center for Technology in Government, University at Albany, State University of New York (CTG UAlbany)

Sincere thanks to the eight state and local government leaders who served as the Advisory Team. Their practical insights and deep experiences were critical in the design and development of this document.

- **Peter Bloniarz**, Executive Director and Senior Policy Advisor for NYS Cybersecurity Advisory Board
- **Robert Corpora**, County Administrator, Cortland County, NY
- **Loren Cottrell**, Deputy Director of Information Technology, Tompkins County, NY
- **Ruth Doyle**, County Administrator, St. Lawrence County, NY
- **Glenn Marchi**, Commissioner of the Office of Central & Information Services, Dutchess County, NY
- **Karen Pratt**, Chief Information Security Officer, Washington County, NY
- **Karen Sorady**, (retired) NYS Chief Information Security Officer, and **Michael Agiovlasitis**, Director of Governance, Risk and Compliance, NYS Office of Information Technology Services
- **Benjamin Voce-Gardner**, Director Office of Counter Terrorism, and **Christopher DeSain**, Director Cyber incident Response Team, NYS Division of Homeland Security and Emergency Services

The following organizations show support for the Cybersecurity Primer for Local Leaders.

THE COLLEGE OF EMERGENCY PREPAREDNESS,
HOMELAND SECURITY AND CYBERSECURITY
UNIVERSITY AT ALBANY
State University of New York

Executive Summary

The cybersecurity threats to our governments cannot be understated.

These are not theoretical threats. Breaches are happening right here in New York. Hackers are trying to access your systems right now, as you are reading this Primer. They are sending emails to county employees, they are looking for vulnerabilities in your website, and they are looking for ways into your databases. They want to disrupt your work, destroy your systems, exploit your data, and hold it ransom for payment.

Almost everything that local governments do today rely on some type of information technology system including but not limited to email, public health programs and services, social service case management, elections, highway and road and road maintenance, public safety, snow removal, mental health care, financial management, court and judicial operations, and many other functions. Hardware, software and connection to the local government network is an integral part of just about every government operation and service.

And even if these systems are not connected directly to the Internet, once a bad actor infiltrates any of these systems, they may be able to move throughout the interconnected network infrastructure and reach desktops and laptops that we all use to conduct our business each and every day.

This Primer is designed as a tool to help you build your own understanding and capabilities so that you can work with your IT and security leaders to manage your county's cyber risks. It provides a snapshot of select cybersecurity considerations for protecting public assets. It answers questions that county leaders said were most pressing to them. It presents, in simple business terms, the most common cyber threats and current practices for addressing them.

In short, this Primer is designed to help local leaders know what it needs to identify, protect, detect, respond to, and recover from security breaches, and presents a set of actions you can start taking today to increase your ability to manage cyber risks.

After two years of being on the front lines of the COVID -19 pandemic, the last thing NYS local governments need is to face a cybersecurity breach that brings down computer networks. But it could happen. Being ready for that day starts with a well prepared local government.

This Primer is our effort to help with those preparations as you continue to protect and serve the citizens of NYS.

Stephen J. Acquario, Esq.
NYSAC Executive Director

Peter Baynes
NYCOM Executive Director

Gerry Geist
AOT Executive Director

What is the Primer and Who is the Audience?

This Primer provides a snapshot of cybersecurity considerations for local government leaders who are responsible for protecting their county's assets. It presents, in layman's terms, insights from New York state and local government leaders as well as gathers information from leading cybersecurity agencies and organizations such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), the Cybersecurity Infrastructure and Security Agency (CISA), the NYS Office of Information Technology Services (NYSITS), and the NYS Division of Homeland Security and Emergency Services (NYSDHSES).

The purpose of the Primer is not to be exhaustive but to help build general awareness and understanding of cyber risk management and encourage local leaders to continue to take action in their county's cyber preparedness.

The Primer is organized into three sections.

1. Why Cybersecurity Should be a Priority for Local Leaders
2. Common Cybersecurity Questions and Answers
3. Top Three Cybersecurity Preparedness Actions for Local Leaders

APPENDICES

Appendix A: Select Cybersecurity Terms and Definitions

Appendix B: Cybersecurity Resources by Agencies & Entities

Appendix C: References

TABLE OF CONTENTS

1. Why Cybersecurity Should Be A Priority For Local Leaders

Cybersecurity Breaches Happen Right Here in New York

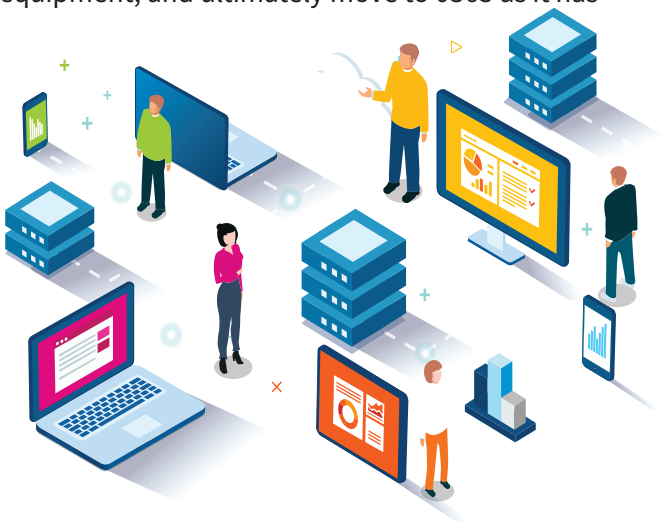
> Cybersecurity is the "art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."
>
> *Cybersecurity Infrastructure and Security Agency (CISA)*

On Saturday, October 18, 2020, Chenango County public health officials came into the office to carry out critical COVID related duties, only to find they had no access to the files on their computers. It was the height of the pandemic and days before early voting would begin for the presidential election, and unknown to them at the time, their county's data was being held for ransom.

Ransomware is a serious threat to all governments and while almost all have precautions in place, it is still a shock when it occurs. For Chenango County this meant a very tense couple of hours of phone calls back and forth from the County IT leaders to NYS Cyber Incident Response Team (CIRT) at NYS Division of Homeland Security and Emergency Services (NYSDHSES), the NYS Board of Elections (NYSBOE), the State Police, and the Federal Bureau of Investigation (FBI). On-site sign-in logs were exchanged and hard drives were picked up by teams of forensic professionals to investigate the source of the breach.

In a short period of time, pressure mounted to get the data restored and the county up and running. The County IT team was triaging with what they could address right away and working to secure boots-on-the-ground assistance from NYS Office of Information Technology Services (NYSITS) and NYSBOE to be on site to help rebuild critical county infrastructure. Even with this assistance, the IT department worked for three months of around the clock work to get back to "normal."

In the end, state and local officials restored their data from backups and did not pay the ransom but they had to rebuild the entire network, secure a large amount of new equipment, and ultimately move to 0365 as it has cybersecurity and resiliency protections built in. The cost for remediation topped $200K and while this amount is lower than many other remediation and recovery efforts, this might be attributed to the fact that the county contracted with a state agency for remediation and recovery assistance and not a private company, which would have cost significantly more. Response and remediation took a financial and organizational toll on the county, and now they are actively revisiting their disaster recovery and Incident Response Plans.



What's at stake with a cyber event?

Chenango County is not alone. Government agencies are one of the most vulnerable industries to cyber attacks. While many of these stories go unreported, cyber incidents take place frequently in NYS local government. The remediation costs – financially, organizationally, and politically – cannot be understated.

When a cyber incident occurs in local governments, elected leaders are immediately thrust into responding to and remediating the breach. They must be able to work across functions and levels of government and in a topic area that is largely outside their expertise.

It is fast paced, and while they typically have a team of colleagues by their side, leaders who understand cybersecurity and their local government's risks are better poised to respond. Even more so, leaders with a strong working relationship with their Chief Information Officer (CIO) and Chief Information Security Officer (CISO) and have practiced their Incident Response Plan are best positioned to gain control of the situation.

This doesn't mean that an incident will be without financial and organizational pain. It just means that the local leader who invests time and energy in building their own cybersecurity understanding and capabilities will be able to help their local government weather the incident quicker and get back to carrying out the critical functions of governing and serving citizens.

Local Government Cyber Events Reported to NYS Intelligence Center

2020-2021*

- 46 County Governments
- 22 Municipal Governments
- 11 School Districts
- 6 Emergency Services Organizations

*These are reported events, the actual number of events is higher than reported.

General Breaches and Ransomware Facts

- About 1 in 6,000 emails contain suspicious URLs, including ransomware. (Fortinet, 2020)
- 71 percent of those impacted by ransomware have been infected. Half of the successful ransomware attacks infect at least 20 computers in the organization. (Acronis, 2020)
- The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)
- The average downtime an organization experiences after a ransomware attack is 21 days. (Coveware, 2021)
- 42 percent of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages caused by the ransomware attack. (Cybereason, 2021)

Understanding and Mitigating Cyber Risk

Risk, in general, is the "possibility of loss or injury," as stated by Merriam Webster. In the cyber realm, risk is "the risk of depending on a system or system elements which exist in or intermittently have a presence in cyberspace" as defined by the National Institute of Standards and Technology (NIST).

Cyber risk is not all that different than the many other risks that local leaders assess and manage every day. Risk permeates most aspects of county operations, with federal, state, and local laws and regulations requiring regular compliance.

The cybersecurity framework developed by the National Institute of Standards and Technology (NIST) is a straightforward way for local leaders to better understand their role in and managing cyber risk within their counties.

While there are numerous tasks associated with carrying out the work within the framework, the overall responsibility of local government leaders is to ensure that all five areas are addressed. The way to assess if this is happening is to conduct a cyber risk assessment. Essentially, a cyber risk assessment provides a cyber report card. While this assessment is highly technical and requires specialized expertise to conduct over a period of time, the results can be used to make both short and long term investment decisions.

N. Hanacek/NIST

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

In 2022, it will be even more important for local leaders to understand cybersecurity and their own cyber profile. This Primer is a launching point for helping make that happen.

The cybersecurity framework developed by National Institute of Standards and Technology (NIST) is a straightforward way for local government leaders to better understand their role in managing cyber risk within their local government. This table presents the NIST framework in both business and technical terms.

Understanding Cyber Risk Management: The NIST Framework in Layman's Terms

NIST Framework Category	Business Description	Technical Description
Identify	Determining what your locality has, what is most important, and what are the biggest threats to what you have.	Identify assets (i.e. hardware, software, and network infrastructure), policies, vulnerabilities, threats, legal and regulatory requirements.
Protect	All the technology, people, and processes that protect your assets.	Safeguards (technology, policies, and training) that are put in place to limit or contain a potential cyber event.
Detect	Ways to know if someone has accessed the locality's assets.	Activities designed to monitor, identify, and alert of a potential cybersecurity event.
Respond	Making sure all leaders, technical staff, and employees know what to do if someone accesses the government's assets, then they do it.	A plan and set of activities to take action on a detected cyber event to contain and mitigate the potential impact.
Recover	Activities to get the government's assets back, protected, and then get back to normal operations.	Activities to restore all functions, capabilities, and services impacted by the cybersecurity event.

2. Common Cybersecurity Questions and Answers

What does cybersecurity mean?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity goes beyond information technology and is the responsibility of every member of your workforce.

What is a Chief Information Security Officer (CISO) and what do they do?

A chief information security officer (CISO) is the executive responsible for an organization's information and data security. CISO responsibilities include (but are not limited to) ensuring oversight of end-to-end security operations, training, and compliance. In addition to an executive there may be staff who carry out the day-to-day cybersecurity work. While this is an ideal scenario, many governments do not have the resources to have a dedicated CISO and staff. In these cases, CISO responsibilities are designated to an IT Director or CIO, and they assign cybersecurity duties to their IT professionals. For local governments that do not have any IT or security staff, cybersecurity oversight and implementation must be procured by a vendor who can provide those services.

What is cybersecurity governance and why is it important?

Governance is "an executive level function that defines government-wide priorities, processes, metrics, tolerance, and implementation methods for making decisions and establishing effective programs to managing cybersecurity risk" as described by the Center for Internet Security (CIS) and the Center for Technology in Government (CTG UAlbany) in their *Managing Cyber Threats Through Effective Governance: A Call to Action* report. It might also be called cyber risk management where all programs, plans, policies, and investment decisions fall under a government's cybersecurity portfolio.

What does it mean to detect a potential cyber attack?

Detection is the practice of monitoring and tracking to identify any malicious activity that could compromise the local government. A local government puts mechanisms in place to determine who has accessed any of their assets. Detection can be carried out through technical, analytical, and procedural measures. Common technical measures include implementation of intrusion detection system (IDS) that monitor a network for malicious activity or policy violations; analytical measures include anomaly detection; and procedural measures include adherences to use policies.

What is a cyber attack and what are the common examples of cyber attacks?

A cyber attack as defined by NIST is the "targeting of an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." The common examples include:

Malware
All types of malicious software, from worms and viruses to spyware and ransomware that is installed on a local government's network without their knowledge.

Phishing
A digital form of social engineering that uses authentic-looking emails to request information from users or directs them to a fake website where malware or ransomware is launched.

Ransomware
Malicious software designed to block access to and hold a IT system and its data files hostage until a sum of money is paid.

Social Engineering
Social engineering leverages individuals' traits such as a desire to be helpful or productive to get them to inappropriately divulge information or provide access to facilities.

Distributed Denial of Service
This attack makes a service such as a website or form unusable by "flooding" it with malicious traffic or data from multiple sources.

Spoofing
Sending an email disguised to look like it is coming from someplace besides its actual origin for purposes of launching malware or ransomware.

Advanced Persistent Threat
Access to a local government's network by multiple vectors (e.g., cyber vulnerabilities, physical, and social engineering) to generate opportunities and remain undetected for an extended period of time in order to launch malware or ransomware.

What are the laws and regulations that govern cybersecurity in NYS?

Cybersecurity laws and regulations that local leaders should be aware of include:

- **The NYS Stop Hacks and Improve Electronic Data Security (SHIELD) Act of 2019** amends New York's 2005 Information Security Breach and Notification Act. https://ag.ny.gov/internet/data-breach.
- **State Technology Law, Article 2 – Internet Security & Privacy Act.** https://www.nysenate.gov/legislation/laws/STT/A2. The most relevant sections for cybersecurity are Section 204 which describes the collection and disclosure of personal information and Section 208 which describes the information security breach and notification.
- **General Business Law Article 39-F** - https://www.nysenate.gov/legislation/laws/GBS/A39-F. The most relevant section is Section 899-AA – Notification; person without valid authorization has acquired private information (breach) and Section 899-BB – Data security protections.
- **NYS Board of Elections Cyber Regulation** for all County Boards of Elections. Part 6220 https://www.elections.ny.gov/NYSBOE/download/law/Part6220_ElectionsCyberReg.pdf.

Certain local government programs and services may require compliance with other mandates such as:

- **The Health Insurance Portability and Accountability Act** HIPPA for healthcare https://omh.ny.gov/omhweb/hipaa/phi_protection.html.
- **The Federal Bureau of Investigation Criminal Justice Information Services** FBI CJIS for law enforcement https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.
- **The PCI Security Standards Council Data Security Standard** PCI DSS for credit card processing https://www.pcisecuritystandards.org/.

There are other laws and mandates that are helpful, even if not directly related to local governments:

- **Federal Executive Order 14028** in May of 2021 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

  This EO sets forth a new list of foundational steps that must be followed at the federal level, and are just as valuable at the local level.

- **K-12 Cybersecurity Act of 2021** https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info. This act starts the development of federal recommendations and tools to assess the security of school districts, and may lead to future requirements.

- **The Cybersecurity Information Sharing Act of 2015** Procedures and Guidance provides guidelines to help non-federal entities share cyber threat indicators with the Federal Government https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance .

- A local law (Nassau County) that is only applicable within that county but something that all local governments might consider. https://www.nassaucountyny.gov/DocumentCenter/View/26390/Local-Law-15-2019.

What are some select current practices in protecting against a cyber attack?

Cybersecurity experts believe the following best practices can get a government well on its way to protecting against a cyber attack.

- **Multi-Factor Authentication (MFA).** MFA is an additional layer of protection on top of your existing username and password. With MFA, you will need a second factor, such as your smartphone, to successfully log in.
- **End Point Security and Host Based Firewalls.** Install anti-malware software and ensure its signatures are regularly updated. Anti-malware software is a key protective measure to detect, quarantine, and remove various types of malware.
- **Regularly Update Software.** Regularly performing software updates is one of the most effective steps one can take to improve their overall cybersecurity posture. Software updates can be for operating systems, firmware, patches, and security fixes.
- **Regular and Robust Back Up Program.** Regularly back up your data, either on removable media or within a cloud-based service. This includes ensuring your data is encrypted when backed up. Backing up data is critical in the event your data is corrupt, lost, stolen, or is no longer recoverable.

- **Limit Administrative Accounts.** Administrative accounts are privileged accounts which can perform many actions a non-privileged user account cannot. Examples of these privileged actions include installing software, disabling anti-malware software, adding and removing user accounts, and stopping/starting services.
- **Lock Devices.** Whenever you step away from your device, lock the device so that a password is needed to regain access. This prevents others from accessing your information without the need for a password.
- **Zero-Trust Security.** An IT security model that requires strict identity verification for every person and device trying to access resources on the network (regardless if they are inside or outside the local government). There is no trust for any user until they verify each time they try their identification.
- **Strong Password Policy.** Password policies are only as good as they are enforced. Typically, passwords must be 8-32 characters long as there is MFA installed. If there is no MFA, then they might be 14-32 characters long. Passwords must never be reused and changed by NIST standards.
- **Phishing Training.** Phishing is one of the most common and simplest ways attackers attempt to compromise your devices and steal sensitive information. The best way for local government employees to thwart phishing attempts include not clicking on suspicious or unknown links or opening attachments in emails. Employees can hover over suspicious links in their emails to see if they are for the correct site and check to see if the email is poorly worded and has misspelled words.
- **Least Privilege Access.** Restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

What is a cyber risk assessment and why should a local government conduct one?

A cyber risk assessment "identifies organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, incorporates the threats and vulnerability analyses, and considers mitigations" as described by NIST.

In short, the outcome of a cyber risk assessment is how the local government would weather a cyber attack and provide existing gaps in identification, protection, detection, response, and recovery for a robust understanding of the locality's overall cybersecurity maturity.

A cyber risk assessment is a highly technical process that must be carried out by cybersecurity experts. More specifically, those with cybersecurity as their core capability. The Center for Internet Security's (CIS) 18 Critical Controls https://www.cisecurity.org/controls/cis-controls-list/ is typically used as the basis of most assessments. It is different than a cyber audit or cyber review, which only verifies if controls are in place.

A cyber risk assessment determines the effectiveness of the controls and gives the locality a government-wide cyber maturity assessment. An assessment is typically carried out in the following phases:

Scope of Risk. What is in the scope of this assessment in terms of operations, locations, critical systems?

Risk Identification. Identifies all the assets critical to your organization, and the threats to each asset.

Risk Analysis. What is the likelihood of the risk identified and its potential impact?

Risk Evaluation. Uses a risk matrix. Then prioritizes which risk should be mitigated first.

Documentation. Documents all risk scenarios. Should be reviewed and updated regularly.

A comprehensive cyber risk assessment provides the local government with a roadmap for where to invest to improve their cyber maturity.

What is an Incident Response Plan and why is it so important for a local government to have one?

An Incident Response Plan documents the "instructions or procedures to detect, respond to and limit consequences of a malicious cyber attack," according to NIST. The incendent response plan sets forth the activities, roles and responsibilities, and chain of command for everyone in the local government. It is the plan the local government will use to respond and work towards recovery in a more timely and organized way to mitigate the impact on your data, systems, and any potential reputational and financial loss. Putting together and testing a response plan is not for one person or department. It must be informed, developed, and practiced by the government's leadership team. The Center for Internet Security's (CIS) Policy Template Guide is a great resource for how to develop your plan.

Developing and practicing an Incident Response Plan should be a priority for your local government. If a data breach or security incident occurs in your government and is not managed, the risks can escalate exponentially, causing significant losses that may be irreparable. Recovering from an incident can take months or years to repair. If there is not a documented plan on the steps your government should take for recovery efforts, every second following a breach can create long-lasting consequential damages. A robust Incident Response Plan should empower critical employees within your local government to leap into action and mitigate the damages as quickly as possible.

What are the necessary elements of a local government's cybersecurity program?

A local government's cybersecurity program consists of a set of plans (actions) and associated policies (standards). Together, it sets forth the government's roadmap in managing cyber risk.

Cybersecurity Plan and Government-wide Actions

- Introduction and overview of cybersecurity include definitions and common terms
- IT and security staff, roles and responsibilities
- Protection of hardware, software, and network infrastructure
- An Asset Inventory
- Access Controls
- Compliance and control mechanisms
- Data classification
- Procurement guidelines
- Training requirements
- Workforce development
- Insurance Information
- Evaluation and metrics
- Membership in the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

Disaster Recovery (DR) and Continuity of Operations Plan (COOP)

- Introductions, purpose, situations, assessment and general chain of command
- Preparedness (similar to IR Plan includes team, roles, responsibilities, risk assessment, mission critical functions, facilities, business impact, mitigation measures, continuity of communications, essential staff, lines succession, and logistical support)
- Response – alerts, notifications, response by department, critical recovery tasks, priority of critical applications, team and leaders' roles and responsibilities, facilities
- Recovery and Reconstitution –personnel, facilities, critical applications

Cybersecurity Policies

- Acceptable Use Policy (AUP)
- Access Control Policy (ACP)
- Patch Management Policy
- Information Security Policy
- Remote Access Policy
- Email/Communication Policy
- Data Classification Policy

Cyber Incident Response (IR) Plan

- Introduction and overview of IR include definitions and common terms
- IR Team, Roles and Responsibilities, and Chain of Command
- Federal and State Required Notifications and Reporting
- Technology and Cybersecurity Specific Actions
- Communication Messaging (internal and external) Specific Actions
- Legal and Risk Specific Actions
- Document Management (Reports, checklists, contact lists)

There are many resources available for the development of the plans and policies. The following present a select few:

- **Center for Internet Security's NIST Cybersecurity Framework Policy Template Guide** https://www.cisecurity.org/wp-content/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v21.11.Online.pdf.
- **Office of Information Technology Services (NYSITS) Policy Index** https://its.ny.gov/tables/technologypolicyindex .
- **NYS Division of Homeland Security and Emergency Services CIRT resources** https://www.dhses.ny.gov/oct/cirt/.
- **US Ready.Gov Business Continuity Plan** https://www.ready.gov/business-continuity-plan .

What do local leaders need to consider in all technology procurements?

Cybersecurity implications are embedded in every technology purchase made in every department within every local government. Any department considering a technology purchase (regardless if it is part of a grant or the local government's IT budget) should answer a set of questions to reveal potential vulnerabilities that will need cybersecurity protections. The following table presents select questions and the reasons the answers matter, so that local leaders can understand how cybersecurity must be considered with every technology procurement.

Questions to Answer Before Technology Procurements

Question	Why The Answer Matters
What is the nature of the technology and how will it be used to carry out local government operations?	There are numerous security considerations, these are just a select few: ■ Hardware and software are vulnerable if not configured properly and patched as necessary. A patching schedule must be integrated into the IT budget and schedule, it may require additional resources within the department. ■ Any connection to the local government's network presents a vulnerability and must be configured securely and monitored. This work must be integrated into the IT budget and schedule, it may require additional resources within the department. ■ Decisions associated with where the data is stored and backed up have numerous implications on cybersecurity needs (on premise, off premise and cloud based).
Is the data collected, stored, used, and shared protected by a specific law or regulation?	The classification of data collected, stored and used in a software application will prescribe the cybersecurity implications. Data that is under protection will require technical and policy controls for the local government and all related vendors.
Is there a vendor that will collect, store, or process the local government's data (in full or part)?	The local government is responsible for making sure its vendors are securing the government's data, providing secure access to the data, and setting forth a plan for how the local government will get the data if there is separation from the vendor or if the vendor is sold. All language must be specified in the terms and conditions of the contract.
Does the vendor provide software or hardware for the local government's use?	Responsibility for cybersecurity will always be shared between the vendor and the local government and the answer to this question will help determine who plays what role in that partnership. If there is on premise hardware and software, the local government may play primary role in securing the assets and the vendor a supporting role. If it resides off premise (on another premise or cloud based), the vendor may play primary role in securing all assets. Although if this is the case, the local government has the responsibility to ensure the terms and conditions in the agreement are documented and adequate for protecting all county assets. Essentially, the local government is still responsible for the security of its assets by ensuring that the vendor has adequate protection in place and it is all specified in the agreement.
Is there a vendor providing a service that connects to our technology or assets?	This will require a technical configuration to ensure a secure connection. This work will require both your government and the vendor to work closely for set up, monitoring and testing.
Does the vendor process credit/debit cards on our behalf?	All credit card payments must follow federal standards and ultimately it is the local government's responsibility to ensure that the vendor is following standards and has security protocols in place to protect the data.

Do local governments need specific language in their contracts and agreements to protect their assets?

The short answer is YES! With emerging technologies and "as a service" offerings on the rise, the necessary documents such as requests for proposals, contracts and agreements, can be a challenging task for any local government. In the past, these binding documents might have only been prepared by local government counsel, but now all development and review must include IT and cybersecurity leaders to ensure that all procurements and services protect the government's assets. State and federal resources are available to assist local governments, including the following from NYS Office of General Services and the United States General Services Administration:

- **New York State's Office of General Services (OGS) Bid Document Files Information Technology Umbrella Contract** https://ogs.ny.gov/procurement/biddocument/22802BID03 Manufacturer Based (Statewide) is a contract that can be leveraged by counties. While the entire document could be leveraged, the following sections might offer useful language:
  - ◊ Section 6 covers SSDLC and other security specifications, and details requirements that might be put into an RFP.
  - ◊ Section 9 has more cloud specific terms and conditions clauses that might be used in county agreements.
  - ◊ Appendix D https://ogs.ny.gov/procurement/bid-22802-3-appendix-d has some specific compliance language also that might apply.
- **United States General Services Administration (GSA)** set of sample statements of work provide numerous links for language in a range of emerging technologies and "as a service" contracts. https://www.gsa.gov/technology/technology-products-services/it-acquisition-help/sample-technology-statements-of-work

What are the considerations for cyber insurance?

Cybersecurity and ransomware insurance can help protect your local government against losses resulting from a cyber attack. Like the government's other insurance, cyber coverage is designed to manage the overall risk of loss to the locality. The cybersecurity insurance market is volatile and there are a range of levels and categories of coverage as well as technical and policy requirements.

First, explore your existing policies to see if your business continuity, liability, and property damage coverages may include the costs associated with a data breach or cyber incident.

In order to qualify for cyber insurance, most insurers now require organizations to attest to a series of cybersecurity controls, including (but not limited to) multi factor authentication (MFA), segregation of end-of-life software from the network, a backup separate from network, tested backup restoration, a designated CISO, stated processes for software updates and patches, and a tested Incident Response Plan.

Local leaders should consult with their insurance broker, CIO, CISO, IT service provider, and counsel to identify their coverage needs, then potentially reach out to statewide and national organizations that have done the most up to date research on insurance coverage and premiums. As a start, some of the questions a leader might consider are listed below.

- Does the insurer provide cybersecurity risk management training?
- Is your local government looking for first-party coverage, third-party coverage, or both?
- Does the coverage include data breaches (theft of personal information), cyber attacks on your data held by vendors and other third parties, and general cyber attacks (breaches of your network)? What are the levels of coverage for each?
- Does the coverage defend you in a lawsuit or regulatory investigation (such as a HIPAA violation) and for how much? Look for "duty to defend" wording.
  - ◊ Are defense costs inside or outside coverage limits?
- Does your local government need multiple cyber coverage plans?
- Does your local government comply with Security Breach Notification Laws?
- What are the cybersecurity control requirements for insurance (MFA)?
- What incidents are covered and what is excluded by your policy?
  - ◊ Forensic expenses?
  - ◊ Notification expenses?
  - ◊ Regulatory fines and penalties?
  - ◊ Credit monitoring and ID theft repair?
  - ◊ Public relations expenses for reputation risk?
  - ◊ Business interruption/denial of service?

What are the cybersecurity responsibilities of local government officials and employees?

Every employee in local government has a role in cybersecurity and should consider themselves part of the cyber team. The following table presents responsibilities for employees by position so that they can better understand their role in preventing and responding to cyber attacks.

Position	Cybersecurity Related Responsibilities
Chief Information Security Officer (CISO) and Chief Information Officer (CIO)	■ Responsible for the county's information and data security, including (but not limited to) ensuring oversight of end-to-end security operations, training, and compliance.
Executive, Mayoral, Supervisor, Administration, and Legislative	■ Ensure that cybersecurity governance is in place for all investment and decision making based on the risk profile for the entire local government. ■ Require compliance in adhering to IT procurement policies and procedures. ■ Encourage and reward compliance in cybersecurity training and use policies. ■ Champion initiatives to develop and test disaster recovery and continuity of operations plans. ■ Lead the development of and practice an Incident Response Plan. ■ Model a culture of learning by actively discussing general cyber preparedness in both formal and informal settings. ■ Make certain that cyber protections are specified in all binding docuemtns for procured products and services. ■ Engage in regular executive level discussions with IT and cyber leaders on your local government's cyber risk profile. ■ Become a member and leverage the resources available through the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)
Department Heads	■ Ensure all employees within their departments have completed training. Any department not completing training may become one of the local government's weakest links. ■ Assess cybersecurity for all IT procurements (products and services) by answering the pre-procurement questions and reviewing answers with IT and cybersecurity leaders. ■ Work with leadership to develop and champion disaster recovery and continuity of operations plans. ■ Participate in the development and testing of Incident Response Plans. ■ Model a culture of learning by actively discussing general cyber preparedness in both formal and informal settings.
Counsel and Comptroller or Chief Financial Officer	■ Review and discuss all language of binding documents for existing and new procurements with IT and cybersecurity leaders. ■ Leverage state and federal templates and expertise when reviewing or developing binding documents for IT procurements. ■ Lead cybersecurity discussions with executive, mayoral, supervisor, administration, legislative, IT, and cybersecurity leaders to assess the options for your local government.
All Employees	■ Adopt new technologies and use policies set forth by IT and security leaders. ■ Complete all cybersecurity training. ■ Be skeptical of the origin of all emails. ■ Report all suspicious cyber activity. ■ Lock devices when not in use. ■ Ask questions of IT and security leaders to better understand your role in protecting the county.

What are the common outcomes of a cyber attack?

When a cyber attack takes place, there are typically four types of outcomes an attacker is looking to achieve in their target.

- Data loss, sometimes called a data breach, leaves your county's data (including financial and personally identifiable) at risk to be blocked, encrypted, exposed, or used maliciously.
- Disruption sets out to impair your county's ability to carry out critical functions.
- Destruction happens when an attack aims to harm your county's IT infrastructure or data.
- Disinformation is meant to spread false information about an individual, program, service, or government.

All of these attacks cause financial, reputational, legal, and political damage that must be remediated by local leaders. Many are carried out through organized cyber-crime and are intended to generate ransom funds and/or stress to the target.

What do we do if we think there is a cyber attack in our local government?

The first thing any local government employee should do is contact their own IT or cybersecurity leader to alert them. If the local government uses an IT service provider, then the employee contacts the local leader designated as the point of contact for the IT service provider. The role of the IT and cybersecurity leaders (and providers) is to assess the severity of the attack. It is the role of the IT and cybersecurity leaders, in partnership with the local government leaders, to determine next steps which may include launching the actions set forth in the Incident Response Plan and notifying the NYS Department of Homeland Security and Emergency Service Cyber Incident Response Team (CIRT), and 24 hour hotline (1-844-OCT-CIRT) in conjunction with the New York State Intelligence Center (NYSIC).

In 2019, the New York State Local Government Information Technology Directors Association (NYSLGITDA) formally communicated to the Governor's Office that NYSDHSES CIRT, NYS's lead agency in cybersecurity, was the point of contact for NYS local governments in the event of a cyber attack. The NYSDHSES CIRT team provides guidance for the local government as they respond and recover and, most importantly, shares information with other state agencies so that other critical stakeholders are made aware.

What resources are available for local governments to fund cybersecurity efforts?

New York State and local governments are expected to receive between $20-30 million over four years from the Federal, State, and Local Cybersecurity Improvement Act, which creates a new grant program through the U.S. Department of Homeland Security to be administered by the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA). Counties and local governments will be able to apply for a share of this cybersecurity funding beginning in late 2022. This funding will flow through the state and a cybersecurity plan will be required with grant applications.

In addition there are grant programs to fund county cybersecurity efforts.

- New York State Homeland Security Program funds assistance with cybersecurity needs. Grant guidance is issued by NYS Division of Homeland Security and Emergency Services (NYSDHSES) and outlines how the funding can be used as per the requirements set forth by the U.S. Department of Homeland Security (DHS) and the U.S. Federal Emergency Management Agency (FEMA). The guidance is defined by national priorities and spending requirements and is typically announced in the March-April timeframe. All counties in New York State receive funding through this program and are able to use a portion for cybersecurity needs. https://www.dhses.ny.gov/grants/hsgp.cfm.
- The Cybersecurity Grant Program is a competitive program for eligible local governments including counties, cities, towns, and villages. It is funded through Federal, State Homeland Security Program, with an 80% local share and is administered by the NYS Division of Homeland Security and Emergency Services (NYSDHSES). At present, the funding levels are $50,000 per eligible jurisdiction which is to be devoted to support planning, exercise, training, and equipment needs as it relates to enhancing and sustaining their cybersecurity posture. Requests for applications are posted to the DHSES website as they are approved and released. https://www.dhses.ny.gov/grants/programs.cfm.
- The NYS Board of Elections (NYSBOE) Cybersecurity Remediation Grant, through the Help America Vote Act (HAVA) Elections Security Grant is a program that has been underway since 2018 and has allowed NYSBOE to:
  - Fund cyber risk assessments for each County Board of Elections (CBOE).
  - Establish and fund statewide contacts for intrusion detection system (IDS) and managed security services for County Board of Elections (CBOE).
  - Disperse approximately 9 million (reimbursement grant) to NYS counties to assist in the remediation of cyber risks identified in their assessment.

3. Top Three Cybersecurity Preparedness Actions for Local Leaders

ACTION # 1: Use the NIST Framework to Facilitate Executive Level Discussions About Your Local Government's Cyber Preparedness

Questions for Executive Level Discussion on Cyber Risk Management	
NIST Framework	**Discussion Questions**
IDENTIFY	■ Have we identified all our assets? Hardware, software, data? If so, have we prioritized? Talk through that inventory. Are there questions? Is everything accounted for? ■ If not, what do we need to do to get this complete? How long will that take? What resources are necessary to support this effort? What is the role we all play in this effort? ■ Do we all know and understand our biggest vulnerabilities? ■ What are the 1-2 actions we should and can realistically do over the next 6 months to address this part of the framework?
PROTECT	■ What are the mechanisms we already have in place? Does the CISO and IT Director think it is enough? Where are we falling short? What can we do about it? ■ Do we have multi-factor authentication (MFA) in place? ■ How much does it cost per year to continue these protections? Are we able to sustain the level of effort and resources necessary? ■ Do we have cyber insurance and are we all aware of what it covers and does not cover? ■ If there is more we can do, what will it take to carry it out? ■ What people, processes, or technology protections need attention over the next 6 months?
DETECT	■ What technical, human, and analytical mechanisms do we have in place to detect if someone has accessed our assets? ■ What is the evidence to show our strategies have worked? ■ Could we do anything more? What are the resource implications of doing more?
RESPOND	■ Do we have an Incident Response Plan? If so, does that plan cover technical, legal, communication, public information, and insurance with clear roles and responsibilities for each employee? ■ If we have a plan, have we practiced it? Have we held a tabletop exercise? How will we implement recommendations from that exercise? ■ If we do not have a plan, do we have a plan to develop a plan? What resources and information will it take to develop a plan? How long and who should be involved? ■ What are our short-term and long-term actions to meet this part of the framework?
RECOVER	■ What is our plan to restore all functionality to our government operations? Who is leading the effort? ■ Do we have a Continuity of Operations Plan? ■ Have we identified and vetted vendors who can assist if there is cyber event? ■ Have we budgeted funding (IT and security assistance, overtime, products) for when a cyber event takes place? (Cyber insurance will not cover all expenses)

This executive level discussion should include all IT and cybersecurity leaders, emergency management, counsel, executive, administration, mayoral, supervisor, and legislative as cross information sharing is essential.

If they haven't already done so, your team might conduct a self-assessment through the Nationwide Cybersecurity Review (NCSR), which is anonymous, no-cost tool designed to measure gaps and capabilities of your county's cybersecurity programs. It is based on the NIST framework, and provides actionable feedback that the group can focus on to identify next steps that should be taken. If your county has already gone through a cyber risk assessment then results from this assessment might be used as the basis for these discussions.

Local government leaders who have already engaged in these discussions have stressed that it is important for everyone to recognize that the information shared as a part of executive level discussion is highly sensitive to the protection of their government's assets. Some local governments have stated that they move into a formal "executive session" in order to protect the privacy of the information shared whereas other local governments have said they hold several discussions with smaller groups of individuals so it is not considered a meeting requiring publically shared notes. Again, these discussions are essential but must be handled with care and attention because of the context specific information shared about the local government's cyber preparedness and overall cyber risk management approach.

ACTION # 2: Develop a Draft Local Government Incident Response Plan Within 6 Months

An Incident Response Plan is the local government's roadmap for how all actions and communication will take place when there is a cyber attack. The Incident Response Plan is a document that will guide everyone within the local government, not just the IT and cybersecurity team, on what to do in the event of a cyber attack. Incident Response Plans are essential for every local government to develop and practice.

Incident Response Plans have information about the conditions necessary and the processes required for all technical and organizational actions and communication. The following are categories of information that is typically found in Incident Response Plans.

- Common terms and definitions used in incident response.
- Contact information of all stakeholders (federal, state, local, and vendor).
- Incident response team roles and responsibilities.
- Threat and impact analysis (criteria and processes).
- Federal and state notification and reporting requirements.
- Technology specific response and recovery actions and processes.
- Communication and public information actions and processes (declaration, internal, and external messaging, processes).
- Legal and risk specific response and recovery process actions and processes (insurance, liability, claims).
- Document management (index of all required documents).

There are resources available that provde templates, step by step guidance, and training so that all local governments can create their Incident Response Plans, some of those resources include:

- The Center for Internet Security's NIST Framework CIS Policy Template Guide provides a standard Incident Response Plan https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf.

- CISA Incident Response Resources including reporting requirements, templates, training and playbooks https://www.cisa.gov/cyber-incident-response.

- CISA Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

Of the local governments that have already drafted an Incident Response Plan, they say that the plan must be developed with a range of stakeholders at the table and might take six months from the first meeting to producing the draft plan. If the plan is developed by one department or person, it will not have the buy in and support from across the local government, which is necessary for it to work. Finally, Incident Response Plans can establish and strengthen cross department relationships which are the cornerstone of all response and recovery efforts.

ACTION # 3: Conduct a Cyber Event Tabletop Exercise

Any local government that has been through a cyber attack will tell you either they are happy they carried out a tabletop exercise or they wish they had practiced a cyber attack tabletop exercise. Carrying out a tabletop exercise can include a range of approaches and levels of effort but is traditionally "a discussion based exercise intended to stimulate discussion on various issues regarding a hypothetical situation. It can be used to assess plans, policies, and procedures, or to assess types of systems needed to guide the prevention of, response to, and recovery from a defined incident, such as a cyber incident" as per NYSDHSES Office of Emergency Management.

Tabletop exercises can be carried out in a couple of different ways, but typically take place with a range of stakeholders from a single local government or a range of stakeholders across a small group of local governments. Many tabletop exercises in local government are run by a trained organization and facilitator to lead all stakeholders through the process. They also provide recommendations for next steps and improvement. An initial discussion with your IT and cybersecurity leaders will help identify your critical stakeholders, resources available, and target timeframe so that you can explore options that are the right fit for your local government.

The following organizations provide resources and services for tabletop exercises and might be considered:

- **Center for Internet Security's Tabletop Exercise Guide** can help your team "develop tactical strategies for securing their systems" https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/.

- **NYS Division of Homeland Security and Emergency Services (NYSDHSES) Office of Emergency Management** (OEM) https://www.dhses.ny.gov/oem/exercise/ and Cyber Incident Response Team (CIRT) https://www.dhses.ny.gov/oct/cirt/index.cfm offers information on exercises and a pilot program to carry out cyber event table top exercises in NYS.

- **Cybersecurity and Infrastructure Security Agency (CISA) Tabletop Exercise Packages** are a "comprehensive set of resources designed to assist stakeholders in conducting their own exercises." https://www.cisa.gov/cisa-tabletop-exercises-packages.

- **National Association of Counties (NACo) Cyber Attack Simulation** "is a reality-based simulation that prepares county risk leaders for cyber attacks by assessing counties' current state of readiness and identifying gaps. This simulation will help attendees evaluate their incident response procedures and tools and guide them in developing a detailed cyber attack response strategy." https://www.naco.org/naco-cyberattack-simulation.

- **National Association of Regulatory Utility Commissioners Cybersecurity Tabletop Exercise Guide** "steps PUCs through the process of creating and executing an exercise specifically designed to examine capacities and capabilities to plan for, respond to, and recover from a cybersecurity incident involving critical energy infrastructure." https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504.

It is important to note that in addition to the guidance and boots-on-the-ground leadership provided by the agencies and nonprofit organizations listed above, there are also many vendors that can provide the same assistance.

APPENDIX A:
Select Cybersecurity Terms and Definitions

TABLE # 1: General Cybersecurity Terms

Term	Definition
Cybersecurity	Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity goes beyond information technology and is the responsibility of every workforce member.
Chief Information Security Officer (CISO)	CISOs are responsible for cybersecurity strategy and are accountable for managing and monitoring the cybersecurity program.
Cybersecurity Governance	Cybersecurity governance is the process by which decisions are made about cybersecurity risk, and ensures effective programs are established that manage that risk to a degree that is acceptable to the organizational leadership. Governance defines organization-wide priorities, processes, metrics, tolerances, and implementation methods. Cybersecurity governance: • Consists of the executive level decision-making processes and the policies and procedures for overseeing the cybersecurity program. • Provides the necessary control and influence an organization's leaders need to have over their cybersecurity programs. • Establishes clear definitions and assigns roles and responsibilities. • Defines processes, tolerances, metrics, priorities, and implementation methods. • Links the organization's cybersecurity programs into decision-making processes that enable the organization's elected leaders to understand and minimize the cybersecurity risks that their organization faces.
Cybersecurity Program	A documented set of your organization's information security policies, procedures, guidelines, and standards. It also includes a collection of effective security management practices and controls, such as risk assessment, awareness, and threat defense. • Create a current profile: An evaluation of your current security status. • Conduct a risk assessment. • Create a target profile (What additional controls from your "current profile" would you like to add? Who needs to be in the loop about the changes needed to reach the target profile?). • Determine, analyze, and prioritize gaps (What are the gaps between your current and target profile? What action is needed to fill those gaps?). • Bring key stakeholders to the table to confirm an analysis and implementation plan. • Implement your plan-of-action. Develop and track metrics to ensure you stay on track.
Cybersecurity Policies	Governance documents which prescribe and proscribe course(s) of action or behavior with respect to the acquisition, deployment, implementation or use of information technology resources.

APPENDIX A:
DEFINITIONS OF SELECT CYBERSECURITY TERMINOLOGY

Cybersecurity Insurance	The insurance policies that address first- and third-party losses as a result of a computer-based attack or malfunction of an organization's information technology systems. There are three main components of cyber insurance: coverage and exclusions, security questionnaires, and rate schedules.
Cybersecurity Training	The process and procedures that involve educating the workforce to understand cybersecurity issues, how to identify risks, and be proactive to mitigate cyber vulnerabilities. 1. Invest in or create a cybersecurity training guide. 2. Ensure that cyber training addresses relevant risk assessment findings (see "Cybersecurity Program"). 3. Provide interactive training courses. 4. Schedule regular testing. 5. Compile test results and improve through adjustments to the training program and content. 6. Implement and enforce new policies. 7. Re-train workforce members on a regular basis. 8. Be consistent with all the steps.
Cyber Attack	An attack, via cyberspace, targeting an organization's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Breach	An incident wherein information is accessed, stolen or taken from a system without the knowledge or authorization of the system's owner. Note: For legal determination of a breach, counties should consult the definition in the NYS Information Security Breach Notification Act of 2005 *(currently "unauthorized access or acquisition of computerized data which compromises the security, confidentiality or integrity of private information").*
Cyber Framework	A collection of best practices that an organization should follow to manage its cybersecurity risk.

TABLE # 2: CATEGORIES OF CYBER ATTACKS

Term	Definition
Data Loss	Also known as data breach, this can be one of the most damaging cyber attacks, depending on the importance of your data. Your organization's election information, financial data, and PII (personally identifiable information) may be at risk of being exposed or used maliciously. Note: For legal determination of a breach, counties should consult the definition in the NYS Information Security Breach Notification Act of 2005 *(currently "unauthorized access or acquisition of computerized data which compromises the security, confidentiality or integrity of private information").*
Disruptive	This type of attack is designed to disrupt or impair your organization's ability to function properly. Examples of this type of attack include ransomware and Distributed Denial of Service (DDoS). This type of attack can last days or weeks. In the case of a disruptive ransomware attack, an unprepared organization may find themselves with no choice but to pay the ransom.
Destructive	In this attack, adversaries such as malicious insiders and hacktivists deliver destructive attacks designed to harm an organization by damaging its IT infrastructure or data. A destructive attack could be as simple as deleting data or wiping all the software off a computer.
Disinformation	This attack spreads false information about a workforce member or an organization's activities and inflicts reputational, financial, and even legal damage. Malicious disinformation about an organization can spread quickly through many different social and digital channels.

APPENDIX A:
DEFINITIONS OF SELECT CYBERSECURITY TERMINOLOGY

TABLE # 3: Examples of Cyber Attacks

Term	Definition
Malware	Malware is an umbrella term for all types of malicious software, from worms and viruses to spyware and ransomware. Two common sources of malware infection for an organization are workforce members visiting compromised or malicious websites and workforce members engaging with phishing emails, clicking links or opening attachments. Once malware gets a foothold, it can be difficult and expensive to remove. Popular malware: • Remote Access Trojan: Allows the attacker "backdoor" entry into systems. • Ransomware: Encrypts data until a ransom is paid. • Spyware: Logs key strokes to gather data such as passwords. • Adware: Exposes the victim to potentially malicious ads. • Worm: Malicious program which self-replicates, spreading without user interaction. • Virus: Malicious programs which must be activated in some way.
Phishing	A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake web site that requests information.
Social Engineering	The practice of exploiting human psychology instead of technical system vulnerabilities. This type of attack is difficult to defend against because it focuses on workforce members who may be unprepared for it. Social engineering leverages individuals' traits such as a desire to be helpful or productive to get them to inappropriately divulge information or provide access to facilities. One step organizations may take to defend against social engineering is to educate their workforce on what types of information can or cannot be disclosed and to whom.
Distributed Denial of Service - DDoS	This attack makes a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources. This in turn renders legitimate organizational communications slow or impossible and may have other undesirable effects.
Spoofing	Mimicking legitimate network traffic for a malicious purpose. For example, sending an email disguised to look like it is coming from someplace besides its actual origin. In this example, the IP address may be changed, and the email address may mimic a known domain.
APT (Advanced Persistent Threat)	An adversary with sophisticated levels of expertise and significant resources that gains access using multiple attack vectors (e.g., cyber vulnerabilities, physical, and social engineering) to generate opportunities to achieve its objectives. These attacks remain undetected for an extended period of time and can prove difficult to eradicate (persistent).

Business Email Compromise	Business email compromise (BEC) is a type of email cyber-crime in which an attacker targets a business to defraud the company. The BEC attack may use a compromised email account within the organization or an external "look-alike" account that is very similar to the organization's email addressing scheme. From there, the adversary may impersonate an executive or finance team member to submit false invoices, initiate fraudulent wire transfers or steal data.

TABLE # 4: Cyber Protection Terms

Term	Definition
Encryption	A technique used to protect the confidentiality of information. The process transforms ("encrypts") readable information into unintelligible text through an algorithm and associated cryptographic key(s).
Network Security	Sets forth who can access your network and once on the network, controls access to data and functions.
Multi Factor Authentication	Using more than one of the following factors to authenticate a system: • Something you know (e.g., user-ID, password, personal identification number (PIN), or passcode). • Something you have (e.g., a one-time password authentication token, 'smart card'). • Something you are (e.g., fingerprint, retina scan).
Endpoint Security	A holistic approach to protecting your organization's end-user devices, such as laptops, desktops, and smartphones, whether on the network or by accessing it remotely. Endpoint security leverages controls such as anti-malware software, web filtering, and host-based firewalls to reduce the risk that end-user devices will be entry points for security threats.
Virtual Private Network (VPN)	Extends a private network across a public network and enables users to securely send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
Firewall and Intrusion Prevention Systems	These defensive technologies can be positioned at the "edge" of your network (i.e., on your Internet connection) and/or installed on endpoints such as end-user computers. They are designed to monitor network traffic and detect anomalies on several levels that could be indicative of an attack. When this type of traffic is detected, it is not permitted, and IT personnel may be notified of a potential attack.
Zero Trust	The security concept that organizations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything each time it tries to connect to its systems/data before granting access.

APPENDIX A:
DEFINITIONS OF SELECT CYBERSECURITY TERMINOLOGY

Data Backups	A copy of the important data on a device, a data backup provides an option for restoring a device quickly in the event of data loss (it is important to note that an archive is different than a backup). Effective backup processes include: 1. Periodically and automatically creating a copy of your important data. 2. Storing it "offline, in a separate location from the original data." 3. Testing restoration processes periodically to ensure the integrity of your backups. 4. Physically securing or encrypting backups, and tracking their location to prevent unauthorized use or access.
Content Filter/ Access Gateway	Technology that prevents user access to questionable or malicious websites and or email messages.

Definition References

Excerpts for the definitions of the above terms were gathered from the following documents and agencies:

Center for Internet Security, Managing Cyber Threats through Effective Governance
https://www.cisecurity.org/white-papers/managing-cyber-threats-through-effective-governance/

Cyber and Infrastructure Security Agency Security Tip (ST04-001)
https://us-cert.cisa.gov/ncas/tips/ST04-001

Cyber Florida at the University of South Florida, Cybersecurity for Local Government
https://flmanagers.com/wp-content/uploads/2021/01/Cybersecurity-for-Local-Government-Guide.pdf

Cybersecurity Framework, NIST
https://www.nist.gov/cyberframework

Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/cybersecurity

Cybersecurity & Infrastructure Security Agency,
https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Workforce%20Training%20Guide%207.28.21%20508c.pdf

Cybint Solutions, 25 Cybersecurity Terms
https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/

Journal of Cybersecurity, Oxford Academy
https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419

National Association of Counties, NACo Cybersecurity Priorities & Best Practices
https://www.naco.org/resources/naco-cyber-security-priorities-and-best-practices

National Institute of Standards & Technology, Computer Security Resource Center
https://csrc.nist.gov/glossary?index=E

New York State Office of Information Technology Services
https://its.ny.gov/

Norton, Data Backups
https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html

NYSBOE, Cybersecurity Requirements for Board of Elections
https://www.elections.ny.gov/NYSBOE/download/law/Part6220_ElectionsCyberReg.pdf

Tech Networks of Boston, Cybersecurity Terms You Need to Know
https://techboston.com/nonprofit-cybersecurity-cheat-sheet/

APPENDIX B:
Cyber Resources by Organization

The following tables were created to identify and categorize cyber resources by state, federal, and nonprofit organizations. The tables were developed by accessing information available on each organization's public web site. Every effort was taken to use create common categories across a range of organizations where they each describe their work differently. These tables are meant to be an approximation and not an absolute identification of resources available. It is important to check with each organization to confirm their resources and services available to local governments.

New York State Agencies						
	NYS Division of Homeland Security & Emergency Services (NYSDHSES)	NYS Office of Information Technology Systems (NYS ITS)	NYS Intelligence Center (NYSIC)	NYS Board of Elections (NYSBOE)*	Office of General Services (OGS)	Office of the New York State Comptroller (OSC)
GENERAL						
Cybersecurity Tips	✓	✓	✓	✓		✓
Best Practices (case studies)						
Procurement Template					✓	
Grant Programs/Funding	✓			✓		
Overall Cybersecurity Program Management				✓ *		
IDENTIFY						
Risk Management Strategies	✓	✓		✓		
Risk Assessments	✓					
Audits						✓
PROTECT						
Policy Templates		✓		✓		
Cyber Awareness Training	✓	✓				
Threat and Vulnerability Notifications		✓	✓			
Protective Technologies, Toolkits **	✓			✓		
DETECT						
Vulnerability Scans		✓				
Infrastructure Penetration Testing	✓					
RESPOND AND RECOVER						
Incident Response Assistance	✓					
Recovery Assistance "boots on the ground"						
Cyber Insurance						

* NYSBOE services are available to County Boards of Elections.

** The technologies and tools also assist with the Identify and Detect categories.

Federal, Non Profit, and Private Organizations								
	Cybersecurity & Infrastructure Security Agency (CISA)	National Institute of Standards and Technology (NIST)	Center for Internet Security (CIS) (MS-ISAC) (EI-SAC)	Federal Bureau of Investigation (FBI)	U.S. General Services Administration (GSA)	National Association of Counties (NACo)	New York Municipal Insurance Reciprocal (NYMIR)	Private Sector Consulting and Service Firms
GENERAL								
Cybersecurity Tips	✓	✓	✓	✓		✓	✓	✓
Best Practices (case studies)	✓	✓	✓					✓
Procurement Template			✓		✓			✓
Grant Programs/Funding						✓		
Overall Cybersecurity Program Management								✓
IDENTIFY								
Risk Management Strategies	✓	✓	✓					✓
Risk Assessments	✓		✓ ***					✓
Audits								✓
PROTECT								
Policy Templates		✓	✓					✓
Cyber Awareness Training	✓	✓	✓			✓		✓
Threat and Vulnerability Notifications	✓		✓					✓
Protective Technologies, Toolkits			✓ ***					✓
DETECT								
Vulnerability Scans	✓		✓					✓
Infrastructure Penetration Testing	✓		✓ ***			✓		✓
RESPOND AND RECOVER								
Incident Response Assistance	✓		✓	✓				✓
Recovery Assistance "boots on the ground"								✓
Cyber Insurance							✓	✓

*** Fee for Service

APPENDIX B:
CYBER RESOURCES BY ORGANIZATION

New York State Agencies

- **NYS Division of Homeland Security & Emergency Services (DHSES)**

  The Cyber Incident Response Team (CIRT) within the New York State Division of Homeland Security and Emergency Services (DHSES), to provide cybersecurity support to non-Executive agencies, local governments, and public authorities. The DHSES CIRT, which has been established within the Office of Counter Terrorism, will provide support through outreach, information sharing, and cyber incident response. 844-628-2478 CIRT@dhses.ny.gov.

- **NYS Office of Information Technology Services (ITS) The New York State Office of Information Technology**

  Services (ITS) was created in 2012 to centralize IT services and develop cutting edge technology solutions that enable state government to serve its citizens in a better, smarter and more cost effective way. ITS provides statewide IT strategic direction, directs IT policy and delivers centralized IT products and services that support the mission of the State. ITS operates data centers 24 hours a day, 365 days a year to support statewide mission-critical applications for 53 Agencies. ciso@its.gov.

- **NYS State Board of Elections (SBOE)**

  The State Board of Elections is a bipartisan agency vested with the responsibility for administration and enforcement of all laws relating to elections in New York State. The Board is also responsible for regulating disclosure and limitations of a Fair Campaign Code intended to govern campaign practices. 518-474-6220 INFO@elections.ny.gov.

- **NYS Intelligence Center (NYSIC) Cyber Analysis Unit**

  The New York State Intelligence Center is a multi-agency, all-crimes fusion center that identifies, prevents, and protects New York against emerging domestic and international terrorist and criminal threats through information collection, analysis, and dissemination of intelligence. 518-786-2191 CAU@nysic.ny.gov.

- **Office of General Services (OGS)**

  The Office of General Services provides essential support services for the operations of state government. They manage and lease real property; design and build facilities; contract for goods, services and technology; and deliver a broad scope of critical services for agencies. 518-474-3899 comments@ogs.ny.gov.

- **Office of the New York State Comptroller (OSC)**

  The Office of the New York State Comptroller serves a wide range of audiences, including New York State taxpayers, local governments, State agencies, vendors, New York State employees, New York State and Local Retirement System members and retirees, individuals entitled to unclaimed funds, policymakers and public interest groups. 518-474-4044 contactus@osc.state.ny.us.

Federal Organizations

- **General Services Administration (GSA)**

  GSA provides workplaces by constructing, managing, and preserving government buildings and by leasing and managing commercial real estate. GSA's acquisition solutions offer private sector professional services, equipment, supplies, and IT to government organizations and the military. GSA also promotes management best practices and efficient government operations through the development of government-wide policies. 347-417-4339.

- **US Cybersecurity & Infrastructure Security Agency (CISA)**

  CISA works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future. CISAs partners in this mission span the public and private sectors. Programs and services they provide are driven by their comprehensive understanding of the risk environment and the corresponding needs identified by their stakeholders. They seek to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities. (888)282-0870 https://us-cert.cisa.gov/.

- **US National Institute of Standards and Technology (NIST)**

  The National Institute of Standards and Technology is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (301)-975-8616 itl_inquiries@nist.gov

- **Federal Bureau of Investigation (FBI)**

  The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. The FBI works to protect the U.S. from terrorism, espionage, cyber attacks, and major criminal threats, and to provide its many partners with services, support, training, and leadership. Albany - 518-465-7551 albany.fbi.gov, Buffalo - 716-856-7800 buffalo.fbi.gov, New York - 212-384-1000 www.newyork.fbi.gov

Non Profit Organzations

- **The Center for Internet Security (CIS)**

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. (518) 266-3460 contact@cisecurity.org

  - **The Multi-State Information Sharing and Analysis Center (MS-ISAC)**

    The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. info@msisac.org

  - **The Elections Infrastructure and Information Sharing Analysis center (EI-SAC)**

    The EI-SAC supports the cybersecurity needs of the elections subsector. Through the EI-ISAC, election agencies will gain access to an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.

- **New York Municipal Insurance Reciprocal (NYMIR)**

  NYMIR is a full service insurer spread across the state that provides comprehensive coverages and risk management programs. It is the largest municipal property and casualty underwriter in the entire State. It is an insurance company for local governments that is run by local government officials, endorsed by the municipal associations, and responsive to the ever changing needs of today's municipalities.518-465-7552 info@nymir.org

- **National Association of Counties (NACo)**

  NACo serves nearly 40,000 county elected officials and 3.6 million county employees. They advocate county priorities in federal policymaking; promote exemplary county policies and practices; nurture leadership skills and expand knowledge networks; optimize county and taxpayer resources and cost savings; and enrich the public's understanding of county government. (518) 465-1473 membership@naco.org

Private Organizations

- **Private Sector Consulting and Service Firms**

  Private firms can also offer a variety of services to your organization. A consulting firm is a professional service firm that provides expert advice for a fee. Consulting firms may have one employee or thousands; they may consult in a broad range of domains.

APPENDIX C: References

- All Info - S.1917 - 117th Congress (2021-2022): K-12 Cybersecurity Act of 2021. (2021, October 8). https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info
- Balbix. (n.d.). What is Asset Inventory Management?. https://www.balbix.com/insights/what-is-asset-inventory-management/
- Brainard, J. (2020, April 7) The State of Email Security in 2020. Fortinet. https://www.fortinet.com/blog/business-and-technology/state-of-email-security-more-spam-malware-phishing-ransomware-ahead
- Breg, D. (2021). Responding to a Small Business Breach - the First 24 Hours. WSJ Pro Cybersecurity.
- Center for Internet Security. (n.d.). CIS Critical Security Controls. https://www.cisecurity.org/controls/
- Center for Internet Security. (n.d.). CIS Benchmarks Community. https://www.cisecurity.org/communities/benchmarks/
- Center for Internet Security. (n.d.). CIS-CAT - Test Your Security Configuration. https://learn.cisecurity.org/cis-cat-lite
- Center for Internet Security. (n.d.). Election Security Spotlight – Disaster Recovery Plan (DRP). https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp/
- Center for Internet Security. (n.d.). NIST Cybersecurity Framework Policy Template Guide. https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf
- Center for Internet Security. (n.d.). Six Tabletop Exercises to Help Prepare Your Cybersecurity Team. https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/
- Cloudflare. (n.d.). Zero Trust Security|What is a Zero Trust network?.
- Cobb, M. (n.d.). How to perform a cybersecurity risk assessment in 5 steps. TechTarget. https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step?amp=1
- Costantini, L. P. & Raffety, A. (2021, October). Cybersecurity Tabletop Exercise Guide. National Association of Regulatory Commissioners. https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504
- Contracts Counsel. (n.d.). Acceptable Use Policy. https://www.contractscounsel.com/t/us/acceptable-use-policy
- Coresecurity. (n.d.). What is IAM Security?.
- CoveWare. (2021, February 1). Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020?format=amp
- Cybereason. (n.d.). Ransomware: The True Cost to Business. https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business
- Cybersecurity and Infrastructure Security Agency. (n.d). CISA Tabletop Exercise Packages. https://www.cisa.gov/cisa-tabletop-exercises-packages
- Cybersecurity and Infrastructure Security Agency. (2021, November). Cybersecurity Incident & Vulnerability Response Playbooks. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- Cybersecurity and Infrastructure Security Agency. (n.d). Cyber Incident Response. https://www.cisa.gov/cyber-incident-response
- Cybersecurity and Infrastructure Security Agency (n.d.). Cybersecurity Information Sharing Act of 2015 Procedures and Guidance. https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance
- Cybersecurity and Infrastructure Agency. (n.d.). Cybersecurity Insurance. https://www.cisa.gov/cybersecurity-insurance
- Cybersecurity and Infrastructure Agency. (n.d.). Cybersecurity Training & Exercises. https://www.cisa.gov/cybersecurity-training-exercises
- Cybersecurity and Infrastructure Security Agency. (n.d). Stop Ransomware: Ransomware 101. https://www.cisa.gov/stopransomware/ransomware-101
- Department of Homeland Security. (2016, November). Cybersecurity Workforce Development Tool. https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf

References, continued

- Department of Homeland Security. (2009, September). Department of Homeland Security: Cybersecurity Procurement Language for Control Systems. https://www.cisa.gov/uscert/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf
- Division of Homeland Security and Emergency Services. (n.d.). Cyber Incident Response Team. https://www.dhses.ny.gov/cyber-incident-response-team
- Division of Homeland Security and Emergency Services. (n.d.). Exercises. Office of Emergency Management. https://www.dhses.ny.gov/training-exercise
- Division of Homeland Security and Emergency Services. (n.d.). Homeland Security Grant Program (HSGP). https://www.dhses.ny.gov/federal-programs
- Division of Homeland Security and Emergency Services. (n.d.). Homeland Security Preparedness Grant Programs. https://www.dhses.ny.gov/grant-programs
- Exabeam. (2019, May 30). The 8 Elements of an Information Security Policy. https://www.exabeam.com/information-security/information-security-policy/
- Federal Bureau of Investigations. (n.d.). CJIS Security Policy Resource Center. https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/fbi-cjis-security-policy-resource-center-links-of-importance
- Federal Emergency Management Agency. (n.d.). What is Continuity of Operations?. https://www.fema.gov/pdf/about/org/ncp/coop_brochure.pdf
- Federal Register. (2021, May 12). Executive Order 14028. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
- Federal Trade Commission. (n.d.). Cyber Insurance. https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance
- Gartner. (2021, September 18). Build a Defensible Cybersecurity Program in 3 Steps. https://www.gartner.com/smarterwithgartner/build-a-defensible-cybersecurity-program-in-3-steps
- IBM. (2021, July 28). IBM Report: Cost of a Data Breach Hits Record High During Pandemic. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic
- LaPierda, J. (n.d.). The Information Security Process Prevention, Detection, and Response. Global Information Assurance Certification. https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197
- MITRE. (2018, September). Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf
- Nassau County New York. (2019). A Local Law to Amend the County Government of Nassau in Relation to Cybersecurity. https://www.nassaucountyny.gov/DocumentCenter/View/26390/Local-Law-15-2019
- National Association of Counties. (2021, October 20). Is Cyber Insurance Coverage Holding Local Government Ransom?. [Zoom]
- National Association of Counties. (2021) NACo Cyberattack Simulation. [Zoom]
- National Initiative for Cybersecurity Careers and Studies. (2021, October 14). Reduce the Risk of Ransomware. https://niccs.cisa.gov/about-niccs/featured-stories/reduce-risk-ransomware
- National Institute of Standards and Technology. (n.d.). Back to basics: Multi-factor authentication (MFA). https://csrc.nist.gov/glossary/term/Multi_Factor_Authentication
- National Institute of Standards and Technology. (2012, August) Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. https://csrc.nist.gov/glossary/term/access_control
- National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. https://csrc.nist.gov/glossary/term/continuity_of_operations_plan
- National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. https://csrc.nist.gov/glossary/term/hardware
- National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. https://csrc.nist.gov/glossary/term/security_policy
- National Institute of Standards and Technology. (n.d.). Computer Security Resource Center. https://csrc.nist.gov/glossary/term/software
- National Institute of Standards and Technology. (2021, May). Computer Security Resource Center: Preparing Your Organization for Ransomware Attacks. https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf

References, continued

- National Institute of Standards and Technology. (2021, May). Data Classification Practices. https://www.nccoe.nist.gov/sites/default/files/legacy-files/data-classification-project-description-draft.pdf
- National Institute of Standards and Technology. (2021, October 26). NIST: Cybersecurity framework. NIST. https://www.nist.gov/cyberframework.
- National Institute of Standards and Technology. (2018, April 12). The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions
- National Security Institute. (n.d). The Growing Ransomware Wave. SecuritySense. https://www.nsi.org/2021/02/15/employee-cyber-security-awareness-ransomware-wave/
- New Hampshire Municipal Association. (2019). Cybersecurity Best Practices for Municipalities. https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities
- New York State Board of Elections. (n.d.). Cybersecurity Requirements for Board of Elections. https://www.elections.ny.gov/NYSBOE/download/law/Part6220_ElectionsCyberReg.pdf
- New York State Office of General Services. (n.d.). Appendix D Primary Security and Privacy Mandates. https://ogs.ny.gov/procurement/bid-22802-3-appendix-d
- New York State Office of Information Technology Services. (2018, December 7). Acceptable Use of Information Technology (IT) Resources Policy. https://its.ny.gov/document/acceptable-use-information-technology-it-resources-policy
- New York State Office of Information Technology Services. (2020, December 1). Account Management Access Control Standard. https://its.ny.gov/document/account-management-access-control
- New York State Office of Information Technology Services. (2018, September 10). Cyber Incident Response Standard. https://its.ny.gov/document/cyber-incident-response-standard
- New York State Office of Information Technology Services. (2018, December 7). Information Security Policy. https://its.ny.gov/document/information-security-policy
- New York State Office of Information Technology Services. (n.d.). ITS Policies. https://its.ny.gov/tables/technologypolicyindex
- New York State Office of Information Technology Services. (2021, May 4). Patch Management. https://its.ny.gov/document/patch-management
- New York State Office of Information Technology Services. (2020, July 16). Remote Access. https://its.ny.gov/document/remote-access
- New York State Office of Information Technology Services. (n.d.). Bid Document Files — Information Technology Umbrella Contract - Manufacturer Based (Statewide). https://ogs.ny.gov/procurement/biddocument/22802BID03
- New York State Office of Mental Health. (n.d.). HIPAA Privacy Rules for the Protection of Health and Mental Health Information. https://omh.ny.gov/omhweb/hipaa/phi_protection.html
- New York State Office of the Attorney General. (n.d.). Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"). https://ag.ny.gov/internet/data-breach
- Office of the New York State Comptroller. (2021, November 12). DiNapoli: New York Needs to Improve Cybersecurity Support to Local Governments and Public Authorities. https://www.osc.state.ny.us/press/releases/2021/11/dinapoli-new-york-needs-improve-cybersecurity-support-local-governments-and-public-authorities
- Oregon State University. (2018, January 1). Information Services Divisional Change Management. https://is.oregonstate.edu/sites/is.oregonstate.edu/files/projects/change-management-policy.pdf
- PCI Security Standards Council. (n.d.). The PCI Security Standards Council Data Security Standard. https://www.pcisecuritystandards.org/
- Ready. (n.d.). Business Continuity Plan. https://www.ready.gov/business-continuity-plan
- Security Scorecard. (2020, January 2). Best Practices for Compliance Monitoring in Cybersecurity. https://securityscorecard.com/blog/best-practices-for-compliance-monitoring-in-cybersecurity
- Slaby, J. R. (nd.). Understanding the true, hidden costs of ransomware attacks on the business. Acronis. https://www.acronis.com/en-us/articles/costs-of-ransomware-attacks/
- TechTarget. (n.d.). Access Management. https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

References, continued

- The SANS Institute. (n.d.). Security Policy Templates. https://www.sans.org/information-security-policy/
- The New York State Senate. (2019, November 1). General Business Law Article 39-F. https://www.nysenate.gov/legislation/laws/GBS/A39-F
- The New York State Senate. (2014, September 22). State Technology Law, Article 2 – Internet Security & Privacy Act. https://www.nysenate.gov/legislation/laws/STT/A2
- United States General Services Administration (n.d.). Sample Technology Statements of Work. https://www.gsa.gov/technology/technology-products-services/it-acquisition-help/sample-technology-statements-of-work
- University of Hawai'i. (n.d.). UH Information Security. https://www.hawaii.edu/infosec/
- VMWARE. (2021). What is Network Infrastructure Security?. https://www.vmware.com/topics/glossary/content/network-infrastructure-security

New York State Association of Counties

The New York State Association of Counties (NYSAC) is a nonprofit bipartisan association serving the counties of New York State including the City of New York. The mission of NYSAC is to represent, educate, advocate for and serve New York's counties and the thousands of elected and appointed county officials who serve the public. As the voice of county leaders throughout New York State, NYSAC is steadfast in communicating the needs and recommendations of our county officials to State lawmakers. Local government is at the heart of New York State, and NYSAC is proud to represent the 62 counties and their elected and appointed officials throughout New York. Learn more at https://www.nysac.org/.

Association of Towns of the State of New York

The Association of Towns of the State of New York (AOT) was established in 1933 to help towns obtain greater economy and efficiency. AOT serves town governments by providing training programs, research and information services, technical assistance, legal services, insurance programs, and a variety of publications to member towns. It represents town governments through its advocacy work in Albany, monitoring legislation and regulatory action, lobbying and presenting initiatives solely on behalf of towns. AOT gains all of its revenue from dues and activities and receives no State or federal assistance. For more information, email info@nytowns.org

New York State Conference of Mayors and Municipal Officials

The New York State Conference of Mayors and Municipal Officials (NYCOM) is the association of, and for, cities and villages in New York. Since 1910, NYCOM has united local government officials in an active statewide network focused on the singular purpose of supporting the most effective means of providing essential municipal services. Through the active participation of our membership, which represents more than 12 million New Yorkers, NYCOM is an aggressive advocate for city and village interests before the Executive, Legislative and Judicial branches of state government. Our association is a readily accessible source of practical information touching upon every area of municipal activity, and is also a leader in the on-going training and education of local officials. Learn more at https://www.nycom.org/

Center for Technology in Government, University at Albany, SUNY

The Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany), is an award-winning research institute, world-renowned for transforming public service through innovations in technology, policy, and management. Established in 1993, CTG UAlbany has led applied research and problem solving projects at all levels of government and around the world. CTG UAlbany experts work to create, and then translate to practice, new knowledge about public service transformation and serve as advisors and facilitators for local, state, federal, and international government bodies, focusing on management and policy decisions. The Institute partners with governments and other organizations to address the critical interplay among policy, management, and technology innovations. Learn more at https://www.ctg.albany.edu/.

Cybersecurity Primer for Local Government Leaders

NYSAC
NEW YORK STATE
ASSOCIATION OF COUNTIES

515 Broadway, Suite 402
Albany, NY 12207

www.nysac.org

518-465-1473

NYCOM
New York State Conference
of Mayors & Municipal Officials

119 Washington Avenue,
Albany, NY 12210

www.nycom.org

(518) 463-1185

AOT

150 State St
Albany, NY 12207

www.nytowns.org

(518) 465-7933