NEW YORK STATE | Homeland Security and Emergency Services

TOP 10 THINGS CYBER THREAT ACTORS HOPE ALL GOVERNMENTS DO

SAFEGUARDING NYS'S STATE, LOCAL, TRIBAL, & TERRITORIAL (SLTT) SYSTEMS, SERVICES, AND INFRASTRUCTURE

AUGUST 1, 2025

Introductions

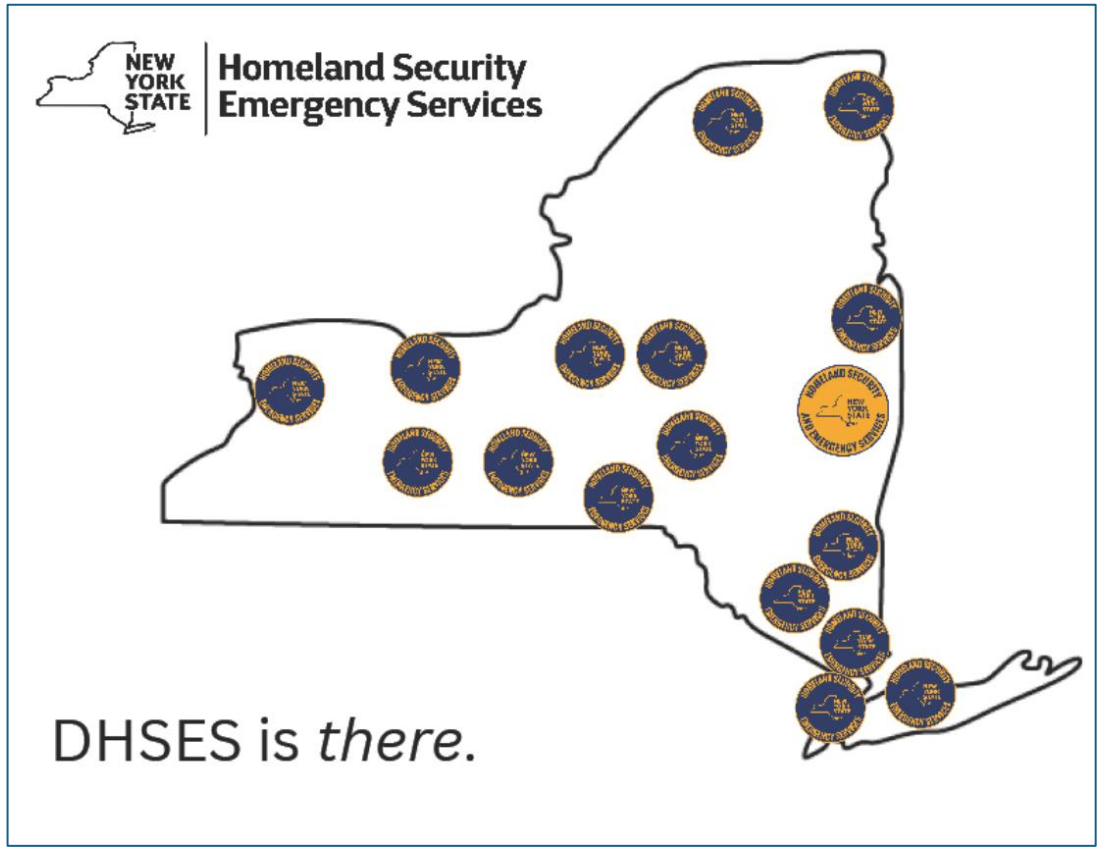
Meghan Cook

- Director, Cyber Incident Response Team
- Assistant Director, Office of Counter Terrorism, NYS DHSES

Lance Porter

- Incident Response Manager, Cyber Incident Response Team

NEW YORK STATE | Homeland Security and Emergency Services



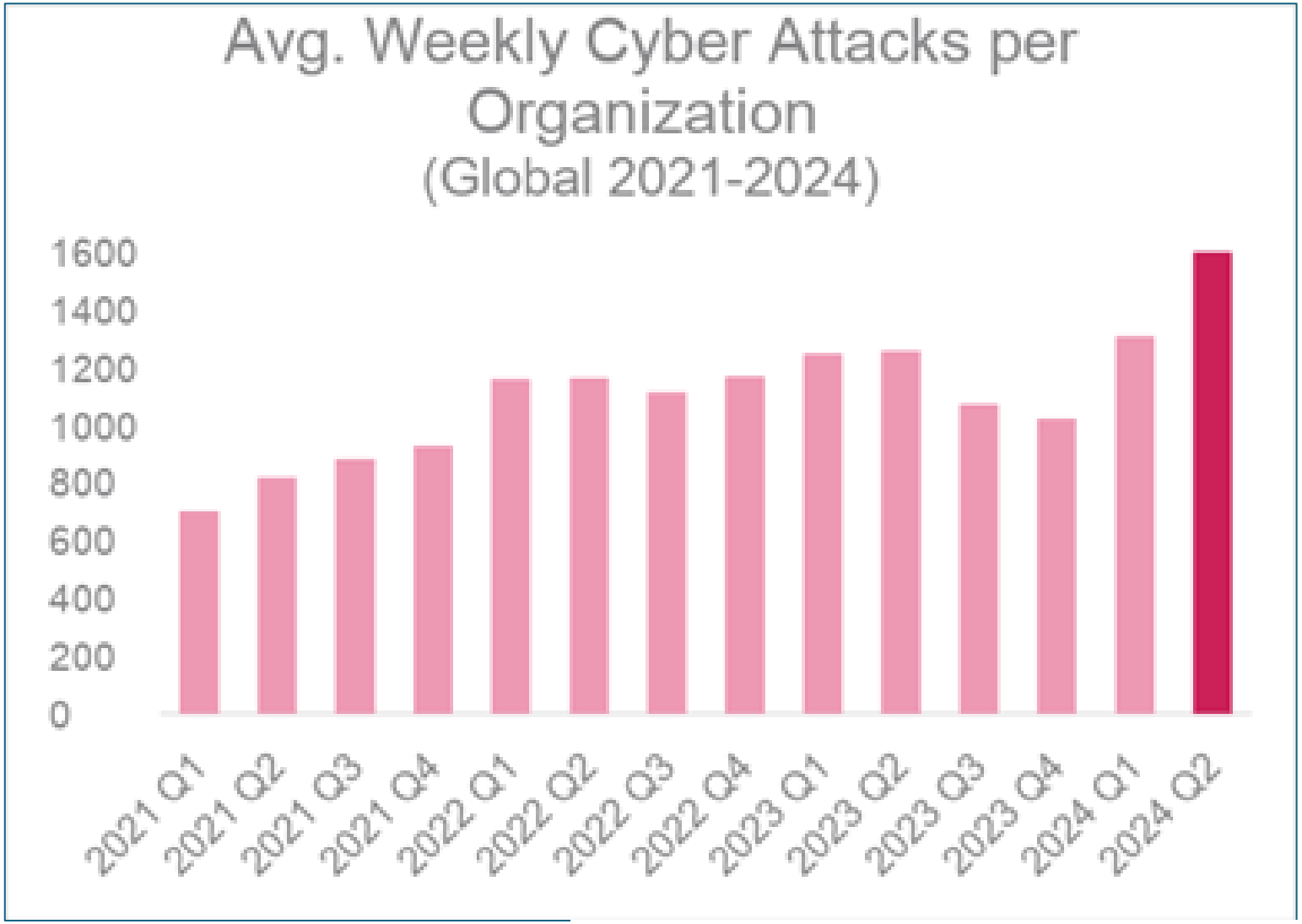
CYBERATTACKS ON THE RISE

According to the 2022-2023 CIS NCSR attacks on SLTT

- Remote Access Trojans increased by 148%
- Ransomware increased by 51%
- Malicious Command-Shell activity increased by 37%

CYBERATTACKS ON THE RISE

30% year over year increase in cyber attacks globally between 2021-2024



Check Point Security Research

ATTACK TRENDS

- ↑ Identity Attacks and Social Engineering
- ↑ Initial access broker usage
- ↑ Exploitation of vulnerabilities for initial access
- ↓ Use of traditional malware for initial access

Vishing attacks skyrocketed **442%** between the first and second half of 2024

Access broker advertisements increased **50%** year-over-year

CrowdStrike 2025 Global Threat Report

REPORTED INCIDENT STATS (VIA OCT CIRT HOTLINE)

Incident - Events Per Year	
All	432
2025	47
2024	71
2023	75
2022	57
2021	58
2020	50
2019	59
2018	15

Incident - Sectors 2025	
Education	10
General Public	4
Government	32
Public Safety	1

Top 4 Types of Incidents (2024)

Incident Type	Definition
Phishing	Seemingly legitimate emails intended to trick users into clicking links or downloading files to steal data or deploy malware.
Account Compromise	Unauthorized individuals gain access to credentials for legitimate accounts.
Other Malware (Not Ransomware)	Incidents containing malware designed for purposes other then deploying ransomware (keyloggers, spyware, trojans, etc.).
Ransomware	Malware that encrypts data across a network, halting business operations. Threat actors will demand a ransom be paid to unencrypt/delete data.

Office of the Governor, Kathy Hochul
Colin Ahern -Chief Cyber Officer
Alyssa Zeutzius Deputy Chief Cyber Officer for Policy AND Michaela Lee – Deputy Chief Cyber Officer for Operations

NYS Information Technology Services (NYS ITS)
(Chris Desain, Mike Agiovlasitis, Corey Hovak, Dave Bell)

Cyber Command (CyComm)

NY Secure Operations Center (NYSOC)

Responsibility/Authority for State-Local Network Connection

Selection and contracts for statewide shared services

Policies and Standards

Secure Ops Center Functions

NYS Division of Homeland Security and Emergency Services (NYS DHSES)
Cyber Incident Response Team (CIRT)
(Ben Voce Gardner, Meghan Cook, Tim Hartman, Lance Porter)

Incident Response- OCT CIRT

Cyber Preparedness Services

Statewide Shared Services

State Info Sharing

NYS Police
NYS Intelligence Center (NYSIC)
Cyber Analysis Unit
(Nick Barrett)

Intelligence Gathering & Distribution

Digital Forensics

Liaison to Federal Law Enforcement

Federal Bureau of Investigations (FBI)

FUNDING
NYS Division of Budget

POSITIONS
NYS Civil Service

CONTRACTS /PROCURE
NYS Office of General Services

Cyber Audits — NYS Office State Comptroller

Responsibility/Authority for State-Local Network Connection — NYS Office of Court Administration

Cyber Regulation
Responsibility/Authority for State-Local Network Connection — NYS Department of Health

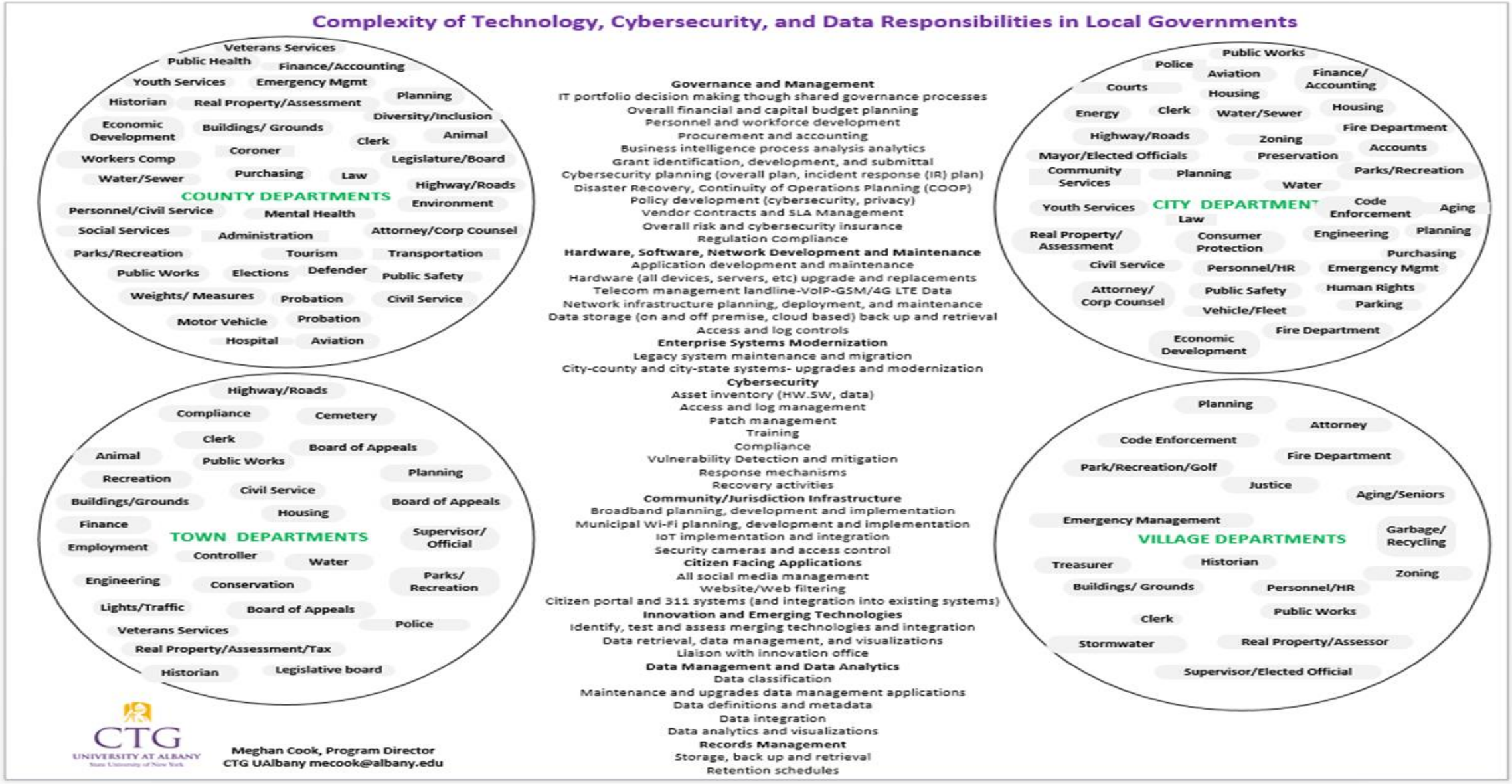
Funding
Cyber Regulation
Statewide Shared Services
Responsibility/Authority for State-Local Network Connection — NYS Board of Elections

NYS Local Governments
Counties, Cities, Towns, Villages

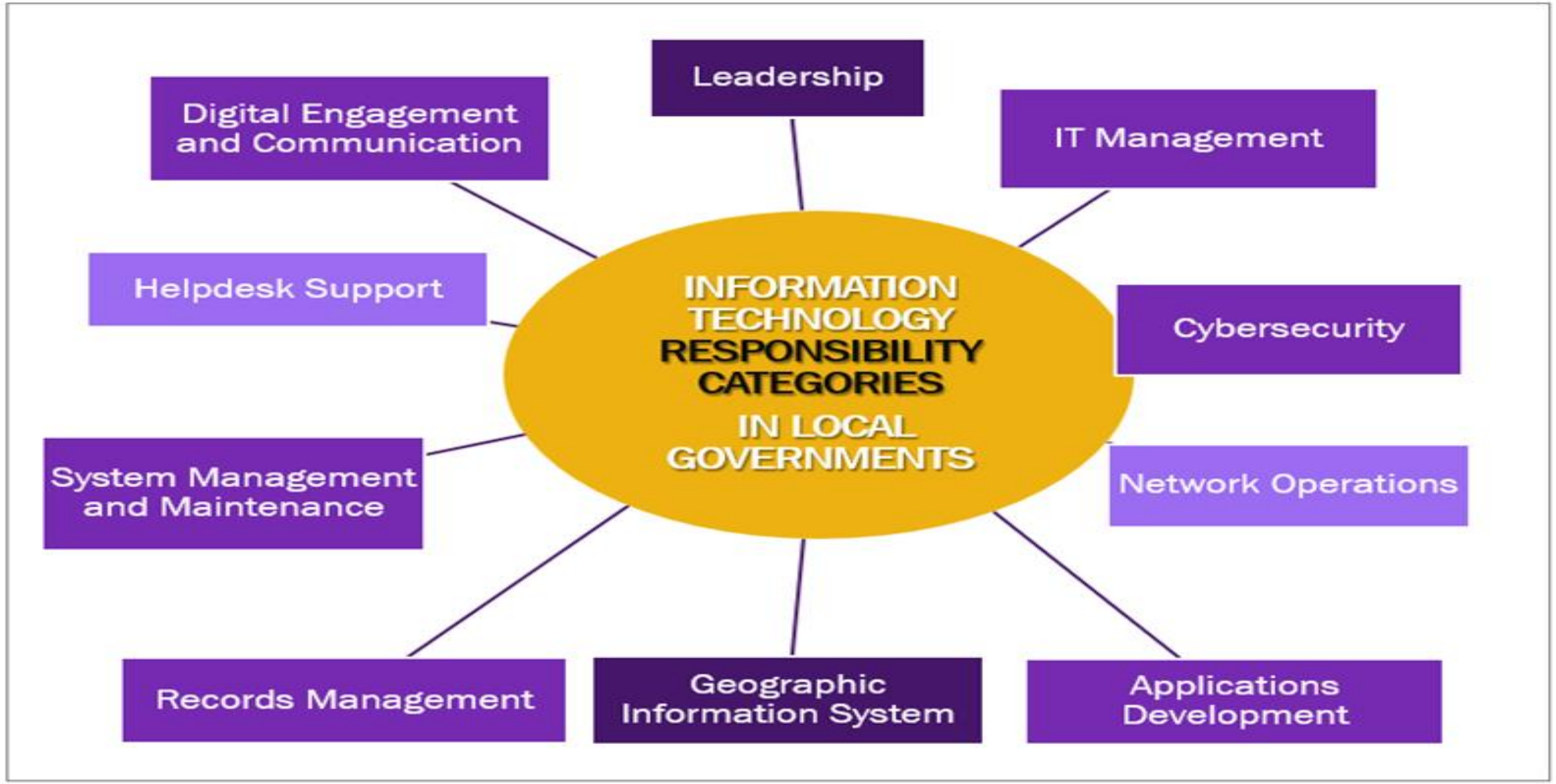
REALITIES of Local Government IT

(that make protecting governments even more challenging!)

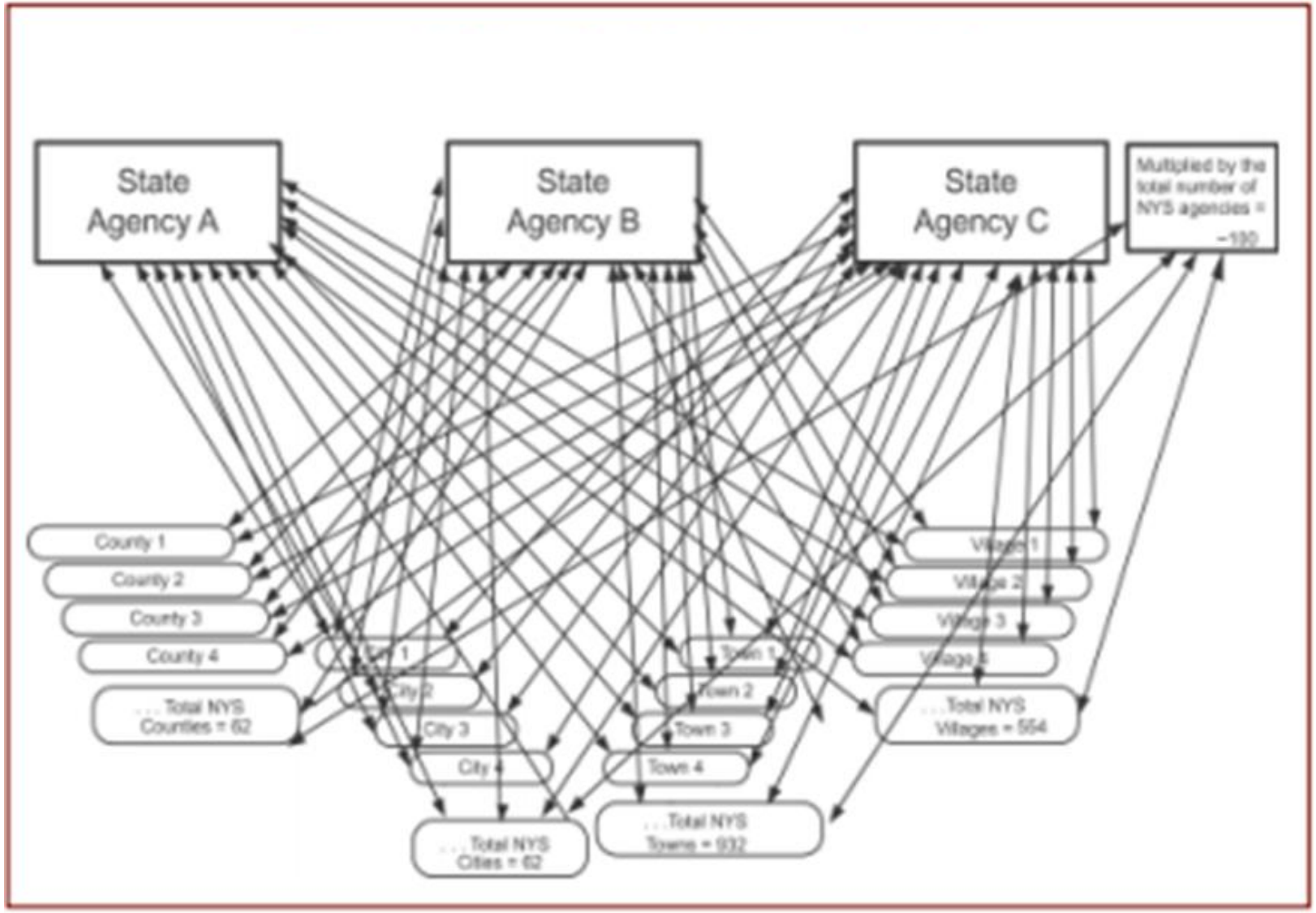
Numerous IT & Cyber Roles In Every Local Government



Limited Resources in Local Government IT Departments



New York State and Local Government is ALL Interconnected



Expanding and Changing Local Government Environments

Meeting workforce needs, responding to state agency regulations and state mandated infrastructure changes has had an impact on the local government IT environment:

- Remote workforce
- Network Segmentation
- Virtualization

CIOs and IT Directors Manage Between Two Worlds Everyday

TOP TEN MISTAKES CYBER THREAT ACTORS ARE HOPING YOU MAKE!

A Presentation for Local Government Leaders

Top Ten? Says Who?

Over 50 cybersecurity professionals who respond to and work to prevent cyber incidents in local governments were asked two questions:

- “What are cyber threat actors hoping local governments do/not do?
- “What were the biggest reasons cyber threat actors were able to cause harm in NYS local governments? (from real incidents)

1. Don’t Enforce Strong PASSWORDS Policy

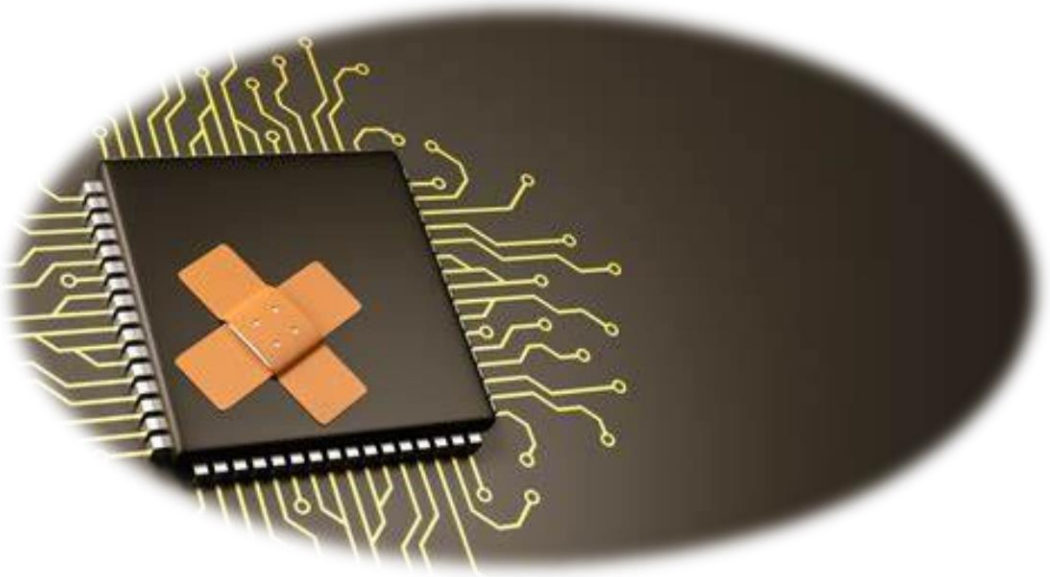
- Weak passwords are easily guessed and cracked.
- Default passwords are left on devices (i.e security cameras)
- Password cracking is sophisticated, and only strong passwords hold up.
- Passwords are a solid line of defense that threat actors want to you overlook and underestimate.

1. PREACH PASSWORDS AS PROTECTION

- Ask to see your organization's password policy and make sure you exceed NIST's policy of 8 characters.
- Strong Password Policy is around 10-12 characters – a combination of uppercase and lowercase letters, symbols, and numbers. Think PHRASES.
- Learn about how default passwords are set/not set in devices in your government
- Password management – don't store in excel sheet on the network!

2. Procrastinate PATCHING

- Identifying, acquiring, testing, and installing application updates – continuously!
- When you don’t update, you create a vulnerability
- Its not really fun or interesting but its routine and absolutely necessary.
- It can drop off the bottom of the to-do list when there is so much work to do



2. MAKE THE MUNDANE THE MOST IMPORTANT

- Ask to see the scan of everything on your network and a listing of applications (organization specific and state/local). Know what you have.
- Ask your IT leader what they need make patching a priority then provide it (this could be vendor support, ability to push out timelines on other projects, additional staff)
- Revisit this topic in meetings. As a leader you manage risk every day – this is one of them.

3. Allow SHADOW IT in Your Organization

- An individual or department is allowed to purchase, bring in, acquire an application, system, device, *and it then connects/is part of the network.*
- This occurs without IT leadership understanding Risk (vulnerabilities and needed clauses in contract)
- Threat actors don't care how it got there –or what money was used to buy it - they only care that it is exploitable

3. DON'T LET PEOPLE OR DEPARTMENTS TO GO ROGUE

- Centralized procurement process where any potential purchase (no matter what funding is used) goes through a cybersecurity review by IT professionals
- Provide funding for continuous scanning of the attack surface – typical yield is 30% more than IT leaders knew.
- Ask your IT team what departments/individuals are the biggest Shadow IT problems (believe me, they know) then address it. This group is now your weakest link.

4. Not Having MFA on Remote Access Solutions

- Multi-Factor Authentication (MFA) is the combination of two or more independent credentials.

- MFA is non-negotiable in 2025. It is the most basic layer of protection against attacks.
- Is a required security standard for HIPAA, GDPR, and PCI-DSS. It is required for cyber insurance (or you pay a higher premium).
- It is one of the easiest ways for a threat actor to gain access – leaving the front door wide open!

4. NO EXCUSES – YOU MUST HAVE MFA

- MFA should be implemented on ALL remote access solutions.
- Don’t allow this investment to be politicized or cut from the investment portfolio (yes, it happens all the time)
- Ask departments which types of remote access solutions they utilize

5. Have a FLAT NETWORK (not segmented)

A FLAT NETWORK

- Everyone can access everything.
- Provide little resistance once the network perimeter is breached and allows for access to the entire network.
- A breach in just one workstation can escalate into a full-blown network cyberattack!

A SEGEMENTED NETWORK

- Divides networks into smaller, isolated segments that limits communication between different parts of the network.
- Each segment acts as its own network and allows security teams to have increased control over the traffic to/from systems.

5 TAKE ACTION TO PARTITION OFF PARTS OF YOUR NETWORK

- When you talk to your IT leader ask them what systems, servers, or set of systems and servers would they most like to isolate if they could?
- Ask them which one should be isolated first? Ask them what is stopping them?
- Get buy in and find the funding to segment the most critical systems, servers and data.

6. Don't understand that all vendors present increased risk

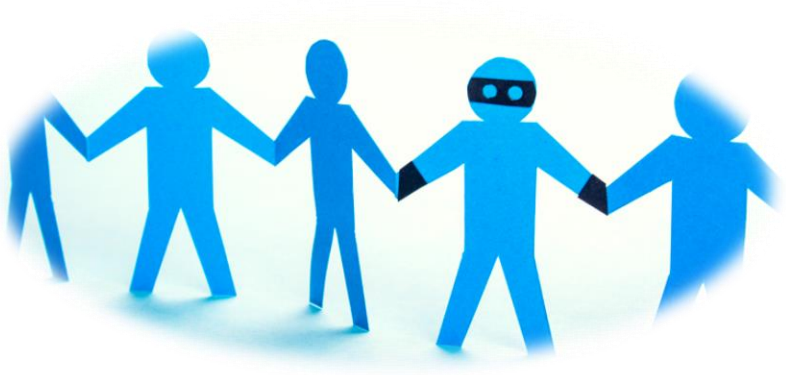
- Even the smallest government (most likely) has over 100 third party vendors that provide services or work with you – do you know all of yours?
- What type of vendors? Software, hardware, services, etc
- A breach in their company will affect you, it just depends on how severe
- If there was a data breach, then there may be regulatory reporting and penalties. Not just for them, but for you!

6. KNOW YOUR VENDORS AND BOLSTER LEGAL SKILLS

- **Assemble a list of vendors/services that the entire government has in place**. Have a contact information for each one and print it out (keep it safe). Spoiler Alert it is not all in one place and this is not a small job to assemble.
- **Allow your counsel to attend necessary education so they know what they need to have in agreements and contract**. (artificial intelligence (its embedded in most every application now), cloud (public and private), data breaches, company use of your data)
- **Conduct regular assessments**, audits, and continuous monitoring to verify that vendors are continuing their protections.

7. Allow many people to have ADMINISTRATIVE Privileges

- Administrative privileges means that that the person has full access to make all changes to every system where they are an “admin”
- Many people “demand” that they have admin privileges because it goes along with their role/job title.
- Admin privileges has (in the past) been synonymous with authority
- Threat actors want to compromise an account with admin privileges “they get the keys to the kingdom”



7. LESS IS BETTER

- Take the approach that people need LESS access rather than more
- Every person who gets admin privileges becomes a target. Ask for a list of who has it now.
- Let the IT leader make the decision on who gets admin privileges. Then allow them to require more cyber/phishing training of that person.

8. Have a Non-existent or Terrible Back Up Strategy

- Worst kind of back up is *none at all.*
- Terrible strategy looks like:
  - ✓Accessible from the credentials (username password) that is used to get other applications (it is called domain)
  - ✓Not automated (manual)
  - ✓Infrequent
  - ✓Only local
  - ✓None off site
  - ✓None offline
  - ✓Not tested
- Threat actors go right for back ups so they can delete/encrypt them – This means you have no choice but to pay the ransom or rebuild from scratch

8. FUND A BACK UP STRATEGY THAT'S DONE RIGHT

The Prep Work

- Identify what data you HAVE responsibility and what is most IMPORTANT?
- Categorize that data on SENSITIVITY, VALUE, and CRITICALITY.

Back up Strategy (3-2-1):

- 3 Copies: This means creating three distinct copies of your data.
- 2 Different Storage Types: Store these copies on different mediums, like a hard drive and the cloud.
- 1 Copy Offsite: Keep one copy in a location separate from the primary location to protect against physical disasters or regional issues

9. Not knowing your technical footprint and skipping the basics

- Sometimes its easier to just ask others (the specialists) if things are done without knowing what it means.
- Leaders MUST spend time know what it looks like and what it means.

- **Questions:**
  - What does technical perimeter look like for your government?
  - Have you ever looked at your vulnerability scan?
  - What are the basic technical components that must be in place?

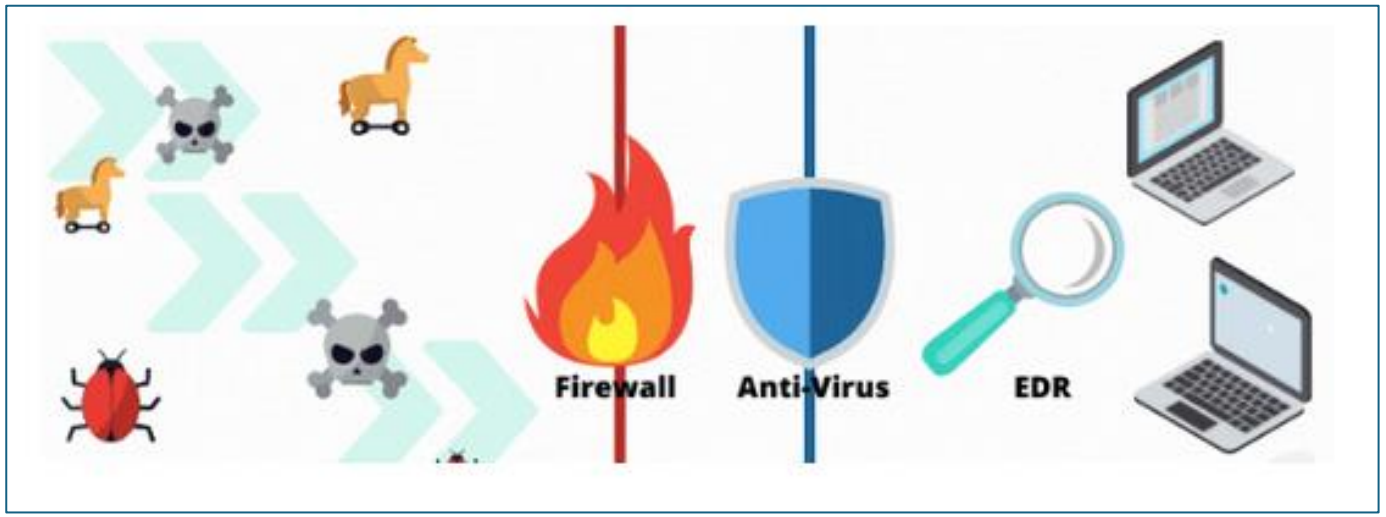
9. KNOW HOW MANY WINDOWS AND DOORS ARE NEEDED

Learn what is on your network. Inventory all hardware and software assets so you know what is in-play and at-risk from attack. Establish a monitoring strategy to identify unusual activity that could indicate an attack.

Leverage automatic updates for all operating systems and third-party software. An easy step is to establish and maintain network security/patching procedures to prevent attacks by configuring functions and programs necessary for security. Enable automatic updates whenever possible and be sure to obtain, test, and deploy the latest versions of operating systems and applications.

Implement secure configurations for all hardware and software assets so that your physical and virtual assets are protected. Create and maintain policies that identify and prioritize secure configurations. Review and implement secure configuration guidance from your vendors and other sources. Conduct frequent vulnerability scans to identify and resolve weak or unprotected entry points.

Learn the difference between a firewall, antivirus, and endpoint detection (p.s – you need all three)



10. Let every department off the hook in protecting the organization (except IT of course)

- Cybercriminals don't just target IT teams; they target people across the entire organization—because employees are often the easiest way in.
- Everyone in an organization, from HR to Finance, has a role to play in protecting the company from cyber threats.
- If leaders think that its just an IT role then others will think that too. Only leaders can shift the culture!

10. EVERYONE JUST WANTS TO KNOW WHERE THEY FIT IN

Leadership:

- Executive (governance, investment approval, and decision making)
- Counsel (contracts, T&C, Follow Up)
- Procurement (centralized review)
- Human Resource (positions, hiring)

Individual Departments:

- Cyber readiness
- Tech change readiness
- Awareness and training

NYS DHSES
CIRT SERVICES

CIRT Mission Objectives

Multi-Unit Collaboration Approach

- OCT Critical Infrastructure Unit
- Partnership with New York Division of Military and Naval Affairs

Identify / Prevent / Protect

- Training, exercises, workshops
- Proactive outreach

Respond / Recover / Mitigate

- Incident response and digital forensics
- Remediation assistance and guidance

Incident Response, Forensics and Analysis

- Incident Response and Recovery Guidance
- Digital Forensics
- Log, Malware and Root Cause analysis
  - ✓It is critical to identify how a cyber intrusion happened to prevent re-occurrence
- Resource Coordination
  - ✓ITS, DMNA, Law Enforcement, and Federal Agency coordination

Proactive and Reactive Services

- Cyber Incident Response and Digital Forensics
- Cybersecurity Risk Assessments (Rapid and Full)
- Phishing Exercises
- Tabletop Exercises
- Capability Workshops
- Penetration Testing
- Cybersecurity Grant Program

- **All DHSES CIRT services are provided at no cost to non-executive agencies, local governments and public authorities.**

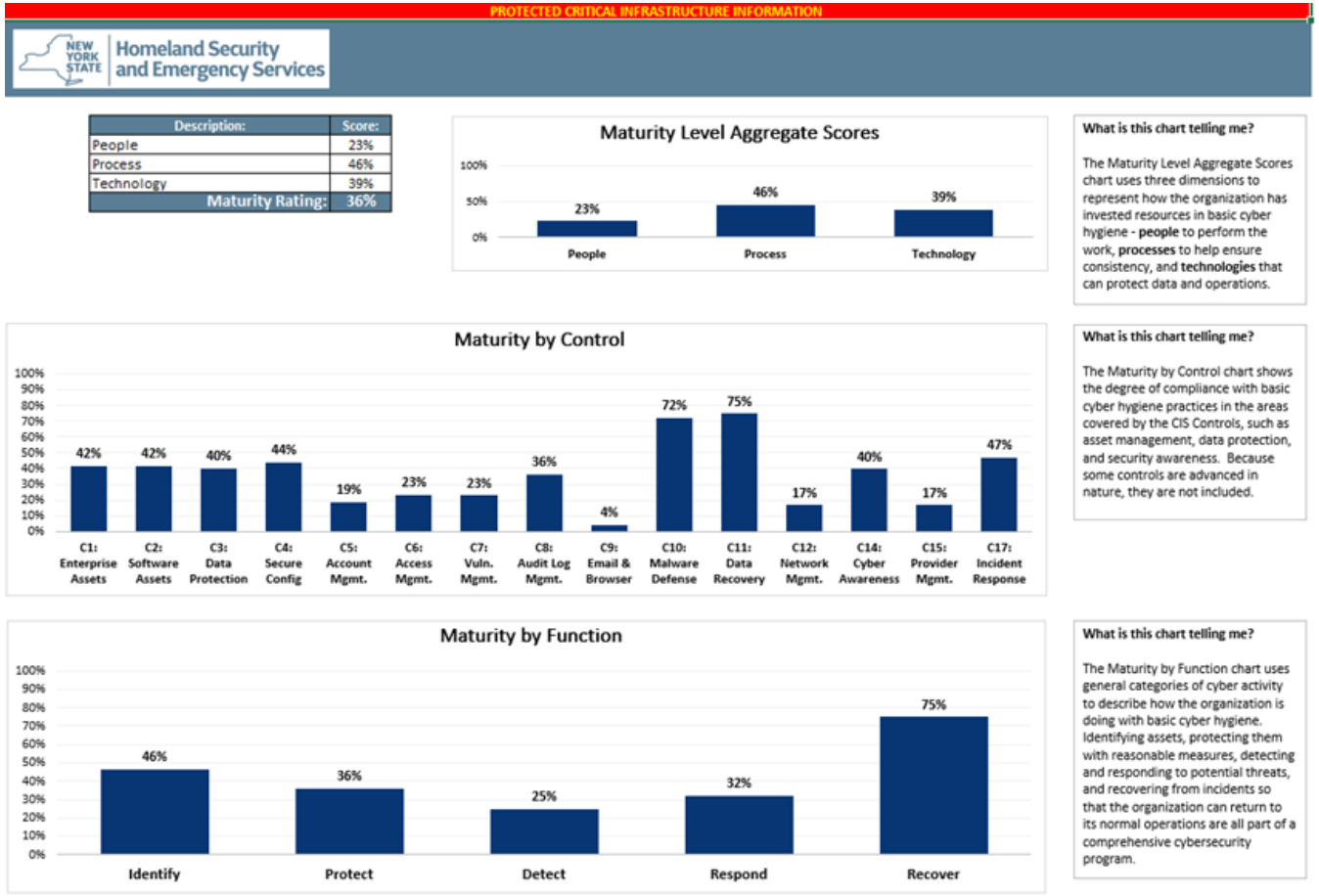
Cybersecurity Risk Assessment (Full)

- **Components:**
- Edge Assessment Service
- Internal Vulnerability Scanning
- Security Program Posture Assessment

- **Output:**
- Out-brief and comprehensive written report
- Identify weaknesses and suggest short, medium, and long term remediations
- Leverages the CIS (Center for Internet Security) Controls
- Reports are PCII (Protected Critical Infrastructure Information) protected

Cyber Risk Assessments (Rapid)

- Evaluation of customers' basic cyber hygiene as defined by the CIS Controls.
- Facilitated discussions explore the people, processes, and technology devoted to cybersecurity.
- Designed for customers with fewer cybersecurity resources.



Phishing and Training Exercises

- Simulated phishing attacks helps assess end user training
- Training modules issued to workforce Tracks completion progress
- Reports and metrics provided to customer

Goals:

- Help local governments train and educate their users
- Prevent compromises and infections

Penetration Testing

- Security testing in which evaluators mimic real-world attacks on real systems and data, using the same tools and techniques used by actual attackers.

- Exploit a combination of vulnerabilities / misconfigurations to gain more access than could be achieved through a single vulnerability.

Cyber Tabletop Exercises

- Mock cyber incident walkthrough
- Involves key stakeholders from the organization
  - ✓ Not just IT staff
- Helps evaluate IR plans and preparations
  - ✓ In addition to identifying any gaps
- Custom scenarios based on real world incidents

Capability Workshops for Local Government Leaders

Bring together government leaders in a day long workshop to:

Conduct a self assessment of their organizational capabilities in:

- ✓ General Technology Readiness
- ✓ General Cybersecurity Readiness
- ✓ Cybersecurity Roles and Responsibilities
- ✓ Cyber Culture and Communication
- ✓ Data Management and Classification
- ✓ Cyber and Data Policies
- ✓ Cyber Awareness Training
- ✓ Cyber Governance and Decision-making
- ✓ Cyber and Legal Risk Management
- ✓ Cybersecurity and Procurement
- ✓ Cyber Incident Response

STATEWIDE CYBER SHARED SERVICES AND GRANT PROGRAMS

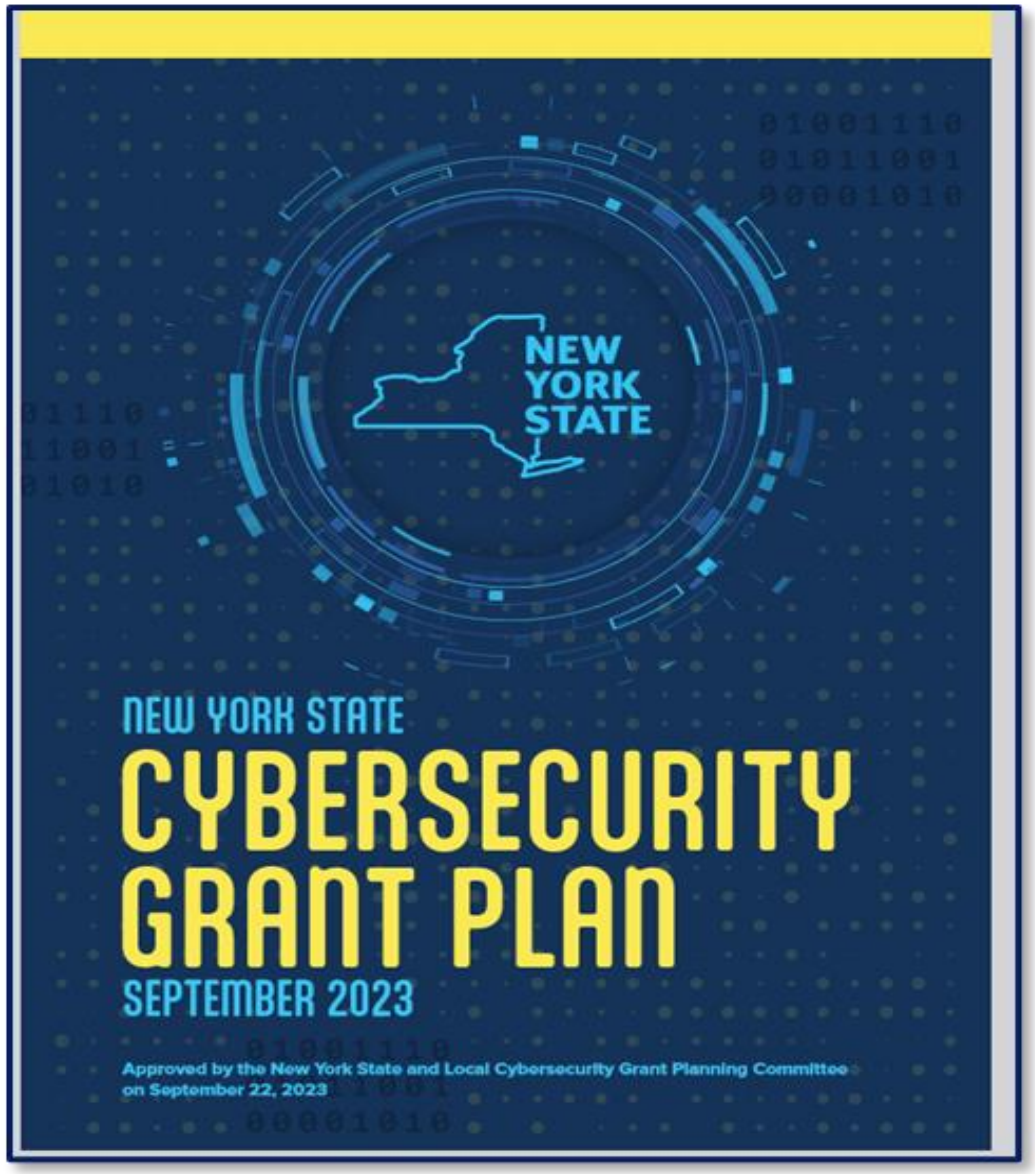
Three Current Statewide Cyber Shared Service Offerings

1. **Endpoint Detection & Response (EDR) Phase I**
   - CrowdStrike Falcon Complete in NYS Counties and 5 largest cities (Rochester, Buffalo, Syracuse, Albany, Yonkers)
2. **Endpoint Detection & Response (EDR) Phase II**
   - CrowdStrike Falcon Complete being deployed in the two largest municipalities within each county
3. **Attack Surface Management (ASM)**
   - Palo Alto Cortex Xpanse in 5 largest cities (Rochester, Buffalo, Syracuse, Albany, Yonkers) and all counties
4. **Security Information and Event Management (SIEM)**
   - NYSOC – Rochester, Buffalo, Syracuse, Albany, Yonkers, and all counties

IIJA – State –Local Cyber Grant Program (SLCGP)

Shared Service Offering for Year One:

- ✓ **Multi Factor Authentication**



DHSES Cyber Grant Program

- This is a competitive grant that supports enhancement and sustainment of cyber security capabilities for local governments by ensuring their information systems are protected from cyber incidents.
- DHSES CIRT members serve as subject matter experts on the application review panel


NEW YORK STATE
Homeland Security and Emergency Services
Cyber Incident Response Support
For New York State Local Governments
1-844-OCT-CIRT | 1-844-628-2478
Risk Assessments | Cyber Capability Workshops
Phishing Exercises | Tabletop Exercises
CIRT@DHSES.NY.GOV
www.dhses.ny.gov/cyber-incident-response-team
HOMELAND SECURITY
NEW YORK STATE
EMERGENCY SERVICES

To report a cyber incident, please call:
1 (844) OCT-CIRT | 1 (844) 628-2478

To request cyber support, please email:
CIRT@dhses.ny.gov

For more information, please visit:
https://www.dhses.ny.gov/oct/cirt

NEW YORK STATE | Homeland Security and Emergency Services

TOP 10 THINGS CYBER THREAT ACTORS HOPE ALL GOVERNMENTS DO

SAFEGUARDING NYS'S STATE, LOCAL, TRIBAL, & TERRITORIAL (SLTT) SYSTEMS, SERVICES, AND INFRASTRUCTURE

AUGUST 1, 2025