



NLC-RISC & NLC MUTUAL CYBER ROADMAP

This resource was created for use by NLC-RISC and NLC Mutual members.
Any broader use or distribution requires permission from NLC-RISC &
Mutual at **nlcriscinfo@nlc.org**.



Municipalities and other local governments are facing cyber threats like never before. While the issue has existed for years, new cyber occurrences are appearing almost daily and many of your municipal members have likely already fallen victim to successful attacks. Simply put, the local government space is an attractive target for bad actors to act - and many have already. Members that haven't faced a breach likely will in the near future. Advanced ransomware plots, slow adoption of Multi-Factor Authentication and other proactive measures, and even nation-state cyber attacks are creating an environment that makes your members more susceptible than ever. This is all compounded with a hardening cyber insurance market which is applying much scrutiny to the coverages they underwrite. It is imperative for cities to take proactive measures to mitigate their risks in the cyber realm.

Ryan Draughn | Director of Information Technology,
NLC Mutual Insurance Company

STEP 1

ENCOURAGE CITY MEMBERS TO JOIN MS-ISAC



The **Multi-State Information Sharing and Analysis Center (MS-ISAC)**, housed within the Center for Internet Security (CIS), is the center point for cyber loss prevention, protection, response, and recovery for U.S. State, Local, Territorial, and Tribal (SLTT) governments.

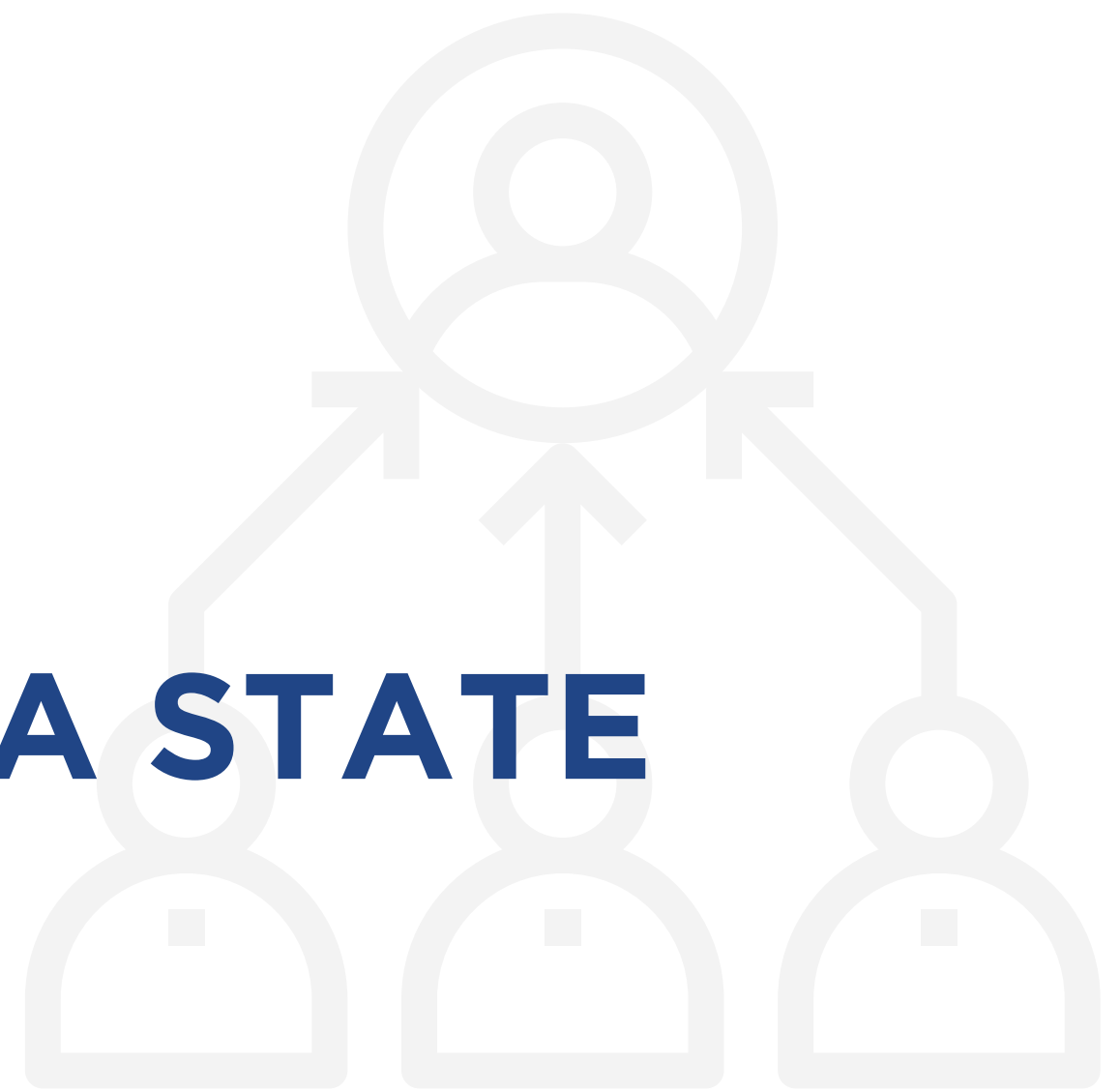
Membership in MS-ISAC is free to all SLTT governments and offers a wide variety of services, which could prevent cyber losses or expedite the recovery process if an incident occurs.

Becoming a member of MS-ISAC is an important step for your insured members to complete for a variety of reasons:

- **Proactive protection:** While there is no guarantee that a cyber incident will not happen to your member, you can show your reinsurer that the member was taking proactive steps to protect themselves from an attack.
- **Incident response:** MS-ISAC's Cyber Incident Response Team provides members with malware analysis, computer and network forensics, and malicious code analysis/mitigation at no cost, saving them money by avoiding third-party services.
- **Intergovernmental collaboration:** MS-ISAC members receive the most up-to-date information on emerging threats from a variety of sources. MS-ISAC collaborates with the FBI, U.S. Secret Service, and U.S. Dept. of Homeland Security to generate reports and disseminate information to its membership.

STEP 2

CONNECT WITH CISA STATE REPRESENTATIVE



The mission of the **Cybersecurity & Infrastructure Security Agency (CISA)** is to lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure.

CISA offers a variety of services to support SLTT governments with cyber protection and resilience, all at no cost to their members. CISA offers support for preparation, response, and recovery efforts for critical infrastructure. They conduct infrastructure assessments and analysis to influence emergency management decision-making. And they promote information sharing between public and private sector partners to expand awareness of cyber risks and incidents. In addition to these services, CISA also has dedicated staff members who communicate with members to problem solve cybersecurity issues and share information on a timely basis.

There are 10 CISA regional offices in the United States, located within the 10 FEMA regions. Connecting with your region's CISA state representative opens the door to accessing all of the resources CISA has to offer your city members. Additionally, there are CISA representatives located in each individual state that can help your members access resources, complete assessments, and answer questions.

- Determine your CISA region [here](#).
- Contact your **regional representative** according to what region your state lands in.

STEP 3

REQUIRE MEMBERS TO COMPLETE NCSR ASSESSMENT

The **Nationwide Cybersecurity Review (NCSR)** is a free assessment designed to gauge the strength of SLLT cybersecurity programs. It is sponsored by the Department of Homeland Security and MS-ISAC. The NCSR measures cyber preparedness, while also providing feedback and metrics to the governments who complete it.

Completing the NCSR is an important step for local governments to take to measure their cyber hygiene. While completing the NCSR is free, it does take a considerable amount of time to complete and generally requires someone with knowledge of cyber terms to complete. Members of MS-ISAC can request assistance with completing the assessment through their MS-ISAC or CISA state representative.

Completing the NCSR assessment provides the following benefits, according to the **Center for Internet Security**:

- Receive metrics to identify gaps and develop a benchmark to gauge progress, as well as anonymously compare results against peers
- Obtain resources & services that can fulfill the desired steps towards improvement
- For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool
- Fulfill the NCSR assessment requirement for the **Homeland Security Grant Program (HSGP)**.
- Results enable Federal partners to better understand the status quo and engage in more strategic, cyber-specific planning and preparedness to help manage national risk and improve SLTT core capabilities

STEP 4

DETERMINE APPLICABLE CISA SERVICES



As discussed in step 2, there are myriad benefits to membership in CISA. A sample of their **free services** are outlined here:

- **Vulnerability scanning** evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Remote Penetration Testing (RPT)** simulates the techniques of real-world adversaries to identify and validate exploitable pathways.
- **Cyber Resilience Review (CRR)** is an assessment intended to evaluate an organization's operational resilience and cyber risk. Provides a no-cost method to assess cyber postures and measure against the NIST cyber framework.
- **Cyber Infrastructure Survey (CIS)** is not as comprehensive as CRR, but helps identify strengths and weaknesses to start addressing them.
- **Phishing campaign assessments** evaluate susceptibility of personnel to phishing attacks and gauge phishing awareness. Assessment results can be used to provide guidance for action (i.e. adopting a training method if phishing tests are failed) OR to justify the success of current training programs.
- **Web application scanning** assesses the health of publicly accessible web applications by checking for known vulnerabilities and weak configurations.

STEP 5

ENCOURAGE MEMBERS TO OBTAIN .GOV EMAIL ADDRESSES

Eric Goldstein, Executive Assistant Director for CISA's Cybersecurity Division, describes the significance of .gov email addresses:

Using .gov and increasing trust that government communications are authentic will **improve our collective cybersecurity**. People see a .gov website or email address and know they are interacting with an official, U.S.-based government organization. Using .gov also provides security benefits, like two-factor authentication on the .gov registrar and notifications of DNS changes to administrators, over other TLDs [top-level domains]. We'll endeavor to make the TLD more secure for the American public and harder for malicious actors to impersonate.

The Cybersecurity and Infrastructure Security Agency (CISA) highlights the importance of local governments obtaining .gov email addresses to ensure the public knows they are communicating with legitimate representatives of cities, states, towns, and tribal governments. Additionally, all .gov email addresses are hosted on a secure, government platform which helps mitigate risks associated with email phishing campaigns.

For more information on obtaining a .gov email address, please refer your members [here](#). Please note there is a small fee associated with obtaining a .gov email domain, however CISA is working in accordance to the DOTGOV Act of 2020 to eliminate this fee.

STEP 6

IMPLEMENT THIRD-PARTY SERVICES AS NECESSARY

NLC-RISC and NLC Mutual offer recommendations of the following partners for your third-party cybersecurity needs. These are trusted professionals for cybersecurity training, risk mitigation, and IT services. However, these service providers are not endorsed by NLC-RISC or NLC Mutual.

NetDiligence eRisk Hub

- NLC-RISC has a partnership with preferred pricing for members
- Pools can white-label the eRiskHub and offer to city members for an additional cost
- NLC-RISC pools and pool staff can access the eRiskHub at no cost (**contact NLC-RISC** for more information about logging in)

VC3 Managed IT Services

- Services include IT management, compliance assessments, cloud hosting/security

KnowBe4

- Services including phishing tests and follow-up cybersecurity training
- NOTE: Preferred vendor for NLC, NLC-RISC, and NLC Mutual

Concierge Cyber

- Services include access to an incident response team, on-call virtual Chief Security Officer, information security policy templates

Resolute Guard

- Services include regulatory compliance, application and network security, incident response, employee training

BASIC CYBER HYGIENE



Training & Education

- Educate staff of threats!
- Enforce strong passwords
- Email phishing exercises
- Pay attention to ransomware events

Vulnerability Management

- Back up systems and data
 - Ensure what you need is backed up
 - Verify that it truly is backed up
 - Test that you can actually recover from backup
- Ensure systems are patched and updated

Network Account Management

- Create and institute remote access policies
- Enable Multi-Factor Authentication
- Offboarding of former employees/contractors

Establish Incident Response Plan

- Define staff roles and responsibilities
- Establish proper contract provisions with IT providers
- Communicate where data is located to stakeholders

Wire Authorization Policies

- Verbal confirmation before wiring funds
- Policy to NOT wire funds via email request.
- Policy of having multiple people authorize:
 - Wire transfers
 - Bank Routing/Account changes