NYSAC
NEW YORK STATE
ASSOCIATION OF COUNTIES

NYCOM
New York State Conference of Mayors & Municipal Officials

AOT

NYMIR

Cybersecurity Tabletop Exercises for Local Governments

JANUARY 2023

MICHAEL ZURLO
NYSAC President

STEPHEN J. ACQUARIO
Executive Director

PAUL LUTWAK
NYSAC IT Task Force Chair

HON. FRANCIS X. MURRAY
NYCOM President

PETER BAYNES
NYCOM Executive Director

KEVIN CRAWFORD
NYMIR Executive Director

HON. DENNIS POWERS
AOT President

GERRY GEIST
AOT Executive Director

Are You Prepared for A Cyber Attack?

Every day, municipalities are at risk from increasingly sophisticated and frequent cyber attacks and continually evolving vulnerabilities. Local governments—like other organizations— must spend time and resources devising ways to reduce a range of cyber-related risks that could significantly disrupt their operations.

In today's world, almost every system that counties and municipalities use to do the work of government is connected to the Internet. Cybersecurity is the art of protecting those networks, devices, and data from unauthorized access and or criminal use. But even the best cybersecurity efforts don't always stop a breach.

One important tool for preparing your response to a cyber-attack—and testing your incidence response plan—is to conduct a table top exercise.

What is a Cybersecurity Tabletop Exercise?

A cybersecurity tabletop exercise is a discussion-based opportunity for a local government's team to practice what it would be like to respond to a breach. These exercises are designed to bring your staff members together in a non-crisis environment so that the team can examine and determine what is needed to best plan for, respond to, and recover from a cybersecurity incident in your locality. It's important to see how your team works together in a non-stressful situation, and identify ways to improve your incident response plan and overall cybersecurity playbook.

These practice sessions can take place in a classroom, boardroom, or office setting to discuss responders' roles during a cyber emergency and their responses to a particular incident. They are designed to work through a variety of potential risk or threat scenarios. For organizations that do not yet have an incident response plan, a tabletop exercise can be a great way to start the planning process.

Tabletop exercise scenarios can cover a broad array of cybersecurity events such as malware, ransomware, denial of service, or other possible organization-specific incidents. Each scenario should review pre-incident preparation, internal and external information sharing, incident response, and post-incident recovery.

N. Hanacek/NIST

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

Make sure to capture what works and what doesn't as part of the exercise, and then address those areas in future planning efforts.

It is important that municipalities consider conducting regular cybersecurity tabletop exercises as part of your team's overall cybersecurity risk management program. As has been learned in a variety of emergencies including Covid-19, government officials are not always as prepared as they may think. Identifying gaps in security, system vulnerabilities, and ways to strengthen continuity of operations plans will go a long way in helping to strengthen a government's cybersecurity posture.

Who should participate?

The plans, processes, and coordination needed to effectively manage and respond to a cyber event can be complex and involve numerous members of your local government's team as well as external groups. Participants should include all individuals who will have a role to play when responding to a cyber incident, including the chief elected official and their executive team, the IT director, chief information security officer, counsel, public safety officials, public information officer, HR, finance, and department heads. For organizations that do not have in house IT or cyber security staff, work with your IT provider to see if they can participate in a tabletop.

Tabletop exercises bring these key stakeholders together to work through a scenario for the purpose of testing preplanned actions needed in the event being practiced. The exercises should help the team work through strategies and tactics, allowing participants to assess the sufficiency and effectiveness of their planned responses, identify gaps in planning, and identify response areas that can be improved.

Where can Cybersecurity Tabletop Exercise resources be found?

Outside companies or consultants can be used to conduct tabletop exercises, or counties and local governments can use any of several free resources available from a variety of organizations to plan for and conduct their own exercises.

The New York State Cyber Incident Response Team (CIRT) at the Division of Homeland Security and Emergency Services (DHSES) can facilitate a three-hour tabletop exercise that will walk a local government or county through a mock incident and test its cyber incident response plans and preparations. These exercises are customized by CIRT staff to reflect the organization's unique structure and resources and can help drive improvements in existing plans and procedures or develop new plans and procedures. The scenarios used in these exercises are based on real world incidents that have impacted government entities in New York State. DHSES will provide a report at the end of the engagement that summarizes the exercise as well as makes recommendations for improvements in plans and process.

The National Association of Counties (NACo) has created a County Tech Xchange and teamed up with the Professional Development Academy to provide a Cyberattack Simulation. This reality-based simulation prepares county risk leaders for cyberattacks by assessing counties' current state of readiness and helps them identify potential gaps in cybersecurity response plans. This simulation helps participants evaluate their current response procedures and tools and guides them through developing a more detailed cyberattack response strategy.

The United States Cybersecurity and Infrastructure Security Agency (CISA) has introduced tabletop exercise packages that are designed to assist stakeholders in conducting their own cybersecurity attack scenario examples. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.

The Center for Internet Security (CIS) has developed tabletop exercises to help cybersecurity teams develop tactical strategies for securing their systems. These focus on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations, and communications. Some exercises can be completed in as little as 15 minutes, while others may take a few hours, depending on the risk scenario being considered. In addition, each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

Tabletop Exercise References and Resources

New York State's Cyber Incident Response Team (CIRT) in the Division of Homeland Security and Emergency Services
www.dhses.ny.gov/cybersecurity-services

National Association of Counties (NACO) Tech Xchange
NACo Cyberattack Simulation

United States Cybersecurity and Infrastructure Security Agency
www.cisa.gov/cisa-tabletop-exercise-packages

Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx

Additional Cybersecurity Resources

Cybersecurity Primer for Local Government Leaders
https://www.nysac.org/files/Cybersecurity%20Primer%20for%20LOCAL%20Government%20Leaders%20-%20September%202022%20Update.pdf

Cybersecurity Insurance Challenging for Public Entities
https://www.nysac.org/files/NYSAC%20Whitepaper%20-%20Cybersecurity%20Insurance%20Challenge(1).pdf

NYSAC
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

NYMIR
119 Washington Avenue,
Albany, NY 12210
www.nymir.org
518-465-7552

CENTER FOR TECHNOLOGY IN GOVERNMENT
UNIVERSITY AT ALBANY State University of New York
1215 Western Ave
Albany, NY 12203
www.ctg.albany.edu
(518) 442-3892