NATIONAL ASSOCIATION of COUNTIES NACo

COUNTY TECH XCHANGE

NACo CYBER SECURITY PRIORITIES AND BEST PRACTICES

Fighting cyber-attacks in local government in 2025 involves addressing several key challenges and leveraging advanced technologies to enhance cybersecurity defenses. Local governments hold sensitive data, making them attractive targets for cybercriminals. However, they often face budget constraints and a shortage of skilled IT professionals. In addition, many local governments rely on outdated systems that are vulnerable to cyber threats through phishing attacks and social engineering tactics intended to exploit human vulnerabilities. The National Association of Counties through the NACo County Technology Advisory Council, the IT Standing Committee, and the Telecommunications and Technology Policy Steering Committee:

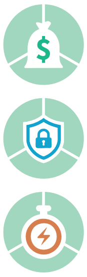
- Funding assistance in any form deemed necessary to provide the information technology resources required to adequately provide security at all levels.
- Funding assistance for basic security awareness training of employees and advanced security training for information technology professionals within local government including assistance in the completion of advanced certification and degree programs
- Cooperative efforts in information sharing among all federal, state, and local governments in addition to private sector organizations regarding breaches, potential threats, threat levels, and any techniques that would assist in the prevention or mitigation of cyber-related threats
- Collaborative efforts in the form of committees or task forces that are inclusive of local government membership with federal agencies such as the Department of Homeland Security and subprograms such as NSC, US-CERT, and ICS-CERT
- Creation of programs and initiatives that designate local government Cybersecurity liaisons and/or representatives that serve in conjunction with federal agencies such as the Department of Homeland Security

Through collaboration with the NACo Tech Xchange, insights from national resources, and discussions with county IT leaders nationwide, a stark reality emerges: the need for adequate funding and adequate resources is crucial for counties, particularly small to mid-sized counties. These smaller counties often face unique hurdles. Limited budgets, smaller IT teams, and a lack of specialized expertise put them at a significant disadvantage when defending against the ever-evolving onslaught of cyberattacks. Recognizing these vulnerabilities and implementing best practices is the first step toward improvement for all counties.

About the NIST Icons

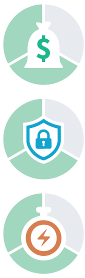
The icons are adopted from the National Institute for Standards in Technology (NIST), Center for Internet Security (CIS), and Cybersecurity and Infrastructure Security Analysis (CISA) cybersecurity prioritization best practices. They represent the percentage of cost, impact on cyber defenses and workload effort needed to implement the priority. The more complete the outer circle of the icon is, the higher the percentage of cost, impact or workload, keeping in mind that current county circumstances may influence the icon status.

Cost
Cyber Defense Impact
Effort



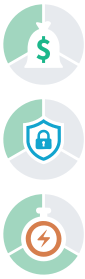
MFA (Multi-Factor Authentication)

Multi-factor authentication significantly decreases the amount of successful cyber-attacks on organizations. The technology platform that a county has implemented for end user authentication, will determine the cost, as well as time and resources needed to implement MFA. Also, it is important to not forget end user education. Cost will be a factor since MFA solutions can run into hundreds of thousands of dollars, depending on the size of the county.



DMARC (Domain-Based Message Authentication, Reporting and Conformance)

DMARC is an email authentication protocol. Currently there is a low percentage of local governments implementing this security feature. The main cost associated with DMARC is hiring the resource to manage implementation of the feature on a county's existing infrastructure or training current IT staff to implement and manage.



DotGov (.Gov)

The main benefit of local governments switching their domain (website, email extension) to .Gov over a .us, .com or .org is that it increases security. In addition to concerns around name recognition, there are financial challenges, especially with rebranding. February 2024 Dotgov data shows that to date, only 42% of counties have implemented the Dotgov domain. Counties can start the process at https://get.gov/.

Policies

It is imperative to have a stand-alone cybersecurity policy that at a minimum covers roles and responsibilities. Security incident policy, forms and procedures can also fall under this stand-alone policy. While many counties have the resources to create such a policy, smaller counties may need paid outside assistance. NACo provides access to a program called "CIO Reservists" to assist.*

Scan to learn more about policies.

Monitoring Tools

County infrastructure includes a massive amount of machine data (digital information that is automatically created by the activities and operations of networked devices) across an organization. This data can be used to proactively identify exploits before they are fully deployed, identify data patterns, provide metrics, and diagnose problems. Consider an aggregator tool like Splunk or the CIS/MS-ISAC Albert Sensor is a horizontal technology used for application management, security and compliance, as well as business and web analytics. There is a high cost to implement these tools from both a financial and resource perspective.

Certified Third Party Providers

Counties should consider cloud-based technologies to improve scalability, cost efficiency, disaster recovery, and service delivery. However, the adoption of cloud solutions requires a proactive approach to cybersecurity including a shared responsibility to who has access, continuous monitoring, compliance with regulatory requirements, and regular vendor due diligence. Counties must also ensure visibility into their cloud environments and maintain control over sensitive data to mitigate risks associated with cloud adoption. Knowing that county third party providers are following and implementing best practices is critical. The liability, regardless of where your data or technology tools reside, is still a county responsibility. To assist in this responsibility are national resources such as GovRamp. Additionally, there are solutions that provide "risk ratings" for all types of entities including other vendors, local government, and any organization with a web presence. A selection guide is available through Gartner.*

Scan to learn more about Certified Third Party Providers.

Regional Expertise- Resources

It is often difficult for some counties find local security resources to help implement needed security best practices let alone pay the high cost for such resources. While more counties are investing in a Chief Information Security Officer, the security responsibility may still fall to the CIO, IT Director, or the Network Administrator. Hiring a full-time security resource can cost counties upward of $100,000, and forces many to look for part-time support. Accessing regional expertise (sometimes referred to as cyber navigators for hire) or the NACo CIO Reservist program, can help bridge that gap. However, justifying the cost or finding the budget to address this need is difficult, especially if IT Assessment supporting documentation is not available (see next priority).

IT Assessments

It is often said: "you don't know what you don't know," and this is especially true when it comes to knowing all the security vulnerabilities within the county infrastructure. IT Assessments, such as penetration testing, vulnerability and risk assessments identify gaps that may have existed for years or just cropped up overnight with the implementation of new devices and applications. Security IT Assessments can cost from $15,000 to six figures, depending on the size of the county.

End User Education

More counties are seeing the benefits in implementing a COTS (commercial off-the-shelf) solution for phishing tests and follow-up end user education. Both of those efforts involve time, as well as funding to address. An average size county of two hundred employees would cost $5,000 or more depending on the modules included. Further, counties should be participating in cyber simulations and tabletops on a regular basis. Depending on the provider, this cost can range from $900 per person or $5000 per event.

End User Exercises

Counties should take a further step beyond phishing tests and incorporate regular table-top exercises with departments and relevant stakeholders. End user cybersecurity exercises help staff recognize and respond to threats such as phishing, social engineering, and malware. These table-top exercises often include simulated attacks, interactive training modules, and scenario-based quizzes to reinforce security awareness. National and regional entities such as NACo, CISA and the National Guard can augment county efforts at little to no cost.

Scan to learn more about End User Exercises.

End User Protection

With the prospect of many county employees continuing to work remotely in some fashion, there is the need for increased end user device and access protection. This includes implementing the next generation of anti-virus, implementing automatic remote patching and other tools and software that will secure these endpoints devices. All of which involve increased expenses, both initially and on-going.

MS-ISAC membership

The Multi-State Information Sharing and Analysis Center provides valuable security resources for counties. Initial membership is available at low or no cost, with add-on services available for an additional fee. Those that are not a member miss security benefits such as vital alerts and notifications of exploits, patches and breaches. Currently, challenges include federal support for this organization and the time and resources to create marketing campaigns that will reach all counties.

NATIONAL ASSOCIATION *of* COUNTIES NACo® | COUNTY TECH XCHANGE

660 North Capitol Street, N.W.
Suite 400 ▪ Washington, D.C. 20001
202.393.6226 ▪ www.NACo.org

FB.COM/NACoDC f
TWITTER.COM/NACoTWEETS 𝕏
YOUTUBE.COM/NACoVIDEO You Tube
WWW.NACo.ORG/LINKEDIN in