NACo CYBER SECURITY PRIORITIES AND BEST PRACTICES

NATIONAL ASSOCIATION of COUNTIES NACo | COUNTY TECH XCHANGE

Fighting cyberattacks in local government has become even more difficult in recent months due to attacks such as the SolarWinds breach and Microsoft Exchange (email) exploit, as well as the current pandemic environment and resulting increases in cloud adoption and remote work. These recent events coupled with the rise in ransomware, IoT devices and user credential harvesting, are raising the security bar for what counties need to implement and what they should be doing with end users as it pertains to cyber security. The National Association of Counties through the NACo Telecommunications and Technology Policy Steering Committee established the following priorities:

- Funding assistance in any form deemed necessary to provide for 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 advance 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 NCC, 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

Further, in working with the NACo Tech Xchange, as well as national resources and other county IT leadership, it has become apparent how important funding and related resources are needed by counties. This is especially evident in the small to mid-size counties, who face the greatest challenges with implementing and maintaining cyber best practices. Specifically, the following are best practices that are the most important for county cyber needs that exist today to address the increasing onslaught of Cyber Attacks.

Cost **Cyber Defense Impact** **Workload Effort**

The icons 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, but also is dependent on current county circumstances.

MFA (Multi-Factor Authentication)

It is a proven fact that multi-factor authentication significantly decreases the amount of successful cyber-attacks on a county. Depending on the main technology platform that a county has implemented for end user authentication, will determine the cost, as well as time and resources needed. And let us not forget the education with end users. MFA solutions alone 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. The percentage of local government implementing this security feature is on the low side. The main cost associated with DMARC is hiring the resource to handle implementation of the feature on a county's existing infrastructure or training current IT staff to do so.

DotGov (.Gov)

The Dotgov (.Gov) domain administration has been moved from the GSA to CISA. The main benefit of local governments switching their domain (website, email extension) to .gov over a .us, .com or .org is that it raises the security. In addition to concerns around name recognition, there are financial challenges, especially with rebranding. March 2021 Dotgov data shows that only 30% of counties have implemented the Dotgov domain.

Monitoring tools

County infrastructure includes a massive amount of machine data accessible across an organization. This data can be used to proactively identify exploits before they are fully deployed, identify data patterns, provide metrics, diagnose problems, and provide intelligence for business operations. 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. To implement those tools, however, involves financial and skillset resources, currently not available in many counties.

Certified Third Party Providers

Given the rise in cloud products and services, as well as the shift to more remote workers, knowing that county third party providers are following and implementing best practices is critical. The liability, no matter where your data or technology tools reside, is still on the county. At the federal level, there is FedRamp. And now for state government there is StateRamp. This may help, but it is not mandatory and will prove difficult for counties to find local vendors that meet the state requirements. Having a central entity (similar to FedRamp and StateRamp) to address the local certification issue will involve significant funding and mandatory support from all levels of government.

Regional Expertise-Resources

For smaller counties, it is especially difficult if not impossible to find local security resources to help implement needed security best practices. Further complicating this is the cost for such resources. The percentage of counties with a Chief Information Security Officer is relatively low, as more often than not, the security responsibility falls to the CIO, IT Director or the Network Administrator. Hiring a full-time security resource can cost a county easily $100,000, which then causes a county to look for part-time support. Hiring Regional Expertise (sometimes referred to as cyber navigators for hire), 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

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

End User Education

More counties are seeing the benefits in implementing a COTS solution for phishing tests and then follow-up end user education. Both of those efforts involve time, but more importantly funding to address. An average size county of 200 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, neither of which is affordable even for mid-size counties.

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 initial and on-going.

MS-ISAC membership

The Multi-State Information Sharing and Analysis Center provides valuable security resources for counties. Initial membership is no-cost, with additional services available for cost. Given the significant no-cost benefits, every county should be a member. To date, less than one third of counties are members. This means that counties are missing out on security benefits such as vital alerts and notifications of exploits, patches and breaches. The challenge is that it takes time and resources to create marketing campaigns that will reach all counties. Conversations with a county explaining the benefits and getting a county signed up takes resources as well.

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 to create.

These eleven represent the county cybersecurity needs for 2021. More information can be provided by contacting NACo staff at **rreynolds@naco.org**.