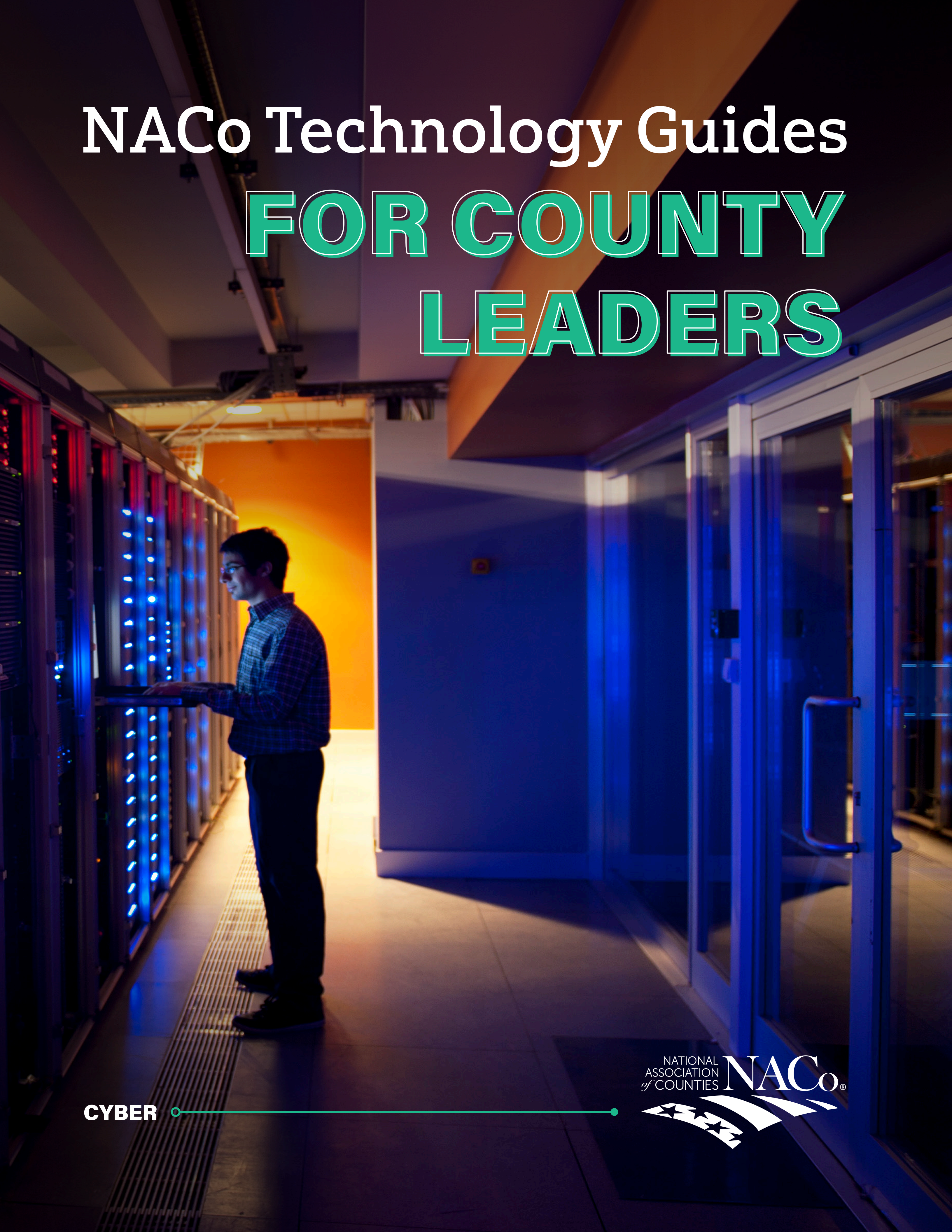
NACo Technology Guides FOR COUNTY LEADERS



CYBER

NATIONAL ASSOCIATION of COUNTIES NACo®

EXECUTIVE SUMMARY

The NACo IT Advisory Council is developing layman's guides for county elected officials, as well as other county executive leadership to help raise the awareness and understanding of the technology that is needed to support county essential functions. The guides will further provide for education in the innovative uses of technology to take the county beyond the essentials and improve the delivery of citizen services and programs.

Each guide will include an executive summary and then will focus on a series of questions to ask that will include the risk or missed opportunity if not implemented. Guides identified include:

CYBER

- *Detection*
- *Prevention*
- *Response*

GEOSPATIAL TECHNOLOGIES

- *Use Cases and Investment*
- *Strategy*
- *Policies and Data Sharing*

BUDGETING & GRANTS

- *Procurement*
- *Contracts*
- *Grants*

WORKFORCE TALENT

- *Flextime*
- *Benefits*
- *Career Growth*

TECHNOLOGY PLANNING, STRATEGY

- *Projects*
- *Priorities*
- *Innovation*

CYBER

Purpose:

It is vital that county leaders communicate with the county IT leadership or the outsourced IT support concerning the important cyber posture of the county. One may ask "why is this important?" While it is the responsibility of IT to implement many of the day to day cyber best practices and for other department leaders to provide the business requirements, it is your responsibility to understand the impacts that these cyber efforts have in relation to resources, budget, legal requirements, and ultimately the safety of the county data assets.

Elected Officials, both incoming as well as seasoned, can benefit from a layman's guide for emerging and innovative technologies that are required in local government. The theme of this guide is Cyber Security and is the first in a series that will provide an overview as well as a checklist of questions to dialogue with county IT leadership and outsourced IT support (if outsourced). As you dialogue concerning the county cyber defenses, please keep in mind that many of these conversations will cover sensitive information and should be considered confidential.

These guides have been compiled with input from the IT Advisory Council, as well as NACo Tech Xchange members. The next two pages are the executive summary of benefits and top ten questions to ask in the area of cyber. As you dialogue with your IT support, whether full-time with the county or outsourced, it is important to remember that cybersecurity is a journey requiring ongoing assessment, adjustment, and dialogue. Think of it through the lens of people, processes, technology, and data.

Top Ten Benefits that Cyber Defenses Can Bring to Your County

1 INCREASED SECURITY

By implementing cyber best practices, the county exposure to theft and destruction of county data is significantly reduced.

2 PROTECTION OF RESIDENTS

When a county provides cyber education (through the website or other means), county residents not only have greater confidence in county government, but they also have access to tools and resources that can increase the safety of their personal lives and activities.

3 LOWER CYBER INSURANCE COVERAGE

Due to the increase in cyber attacks and ransomware on local government, cyber insurance premiums have significantly increased while coverage has decreased. By increasing cyber defenses, a county can receive better coverage and less of an increase in cyber insurance premiums.

4 PROTECTION OF END USERS

It is often said that the end user is the greatest risk. By implementing sound cyber tools and best practices, this exposure becomes less of a vulnerability.

5 PROTECTION OF DATA ASSETS

County government collects a plethora of resident and client information that is stored in documents, software applications and transmitted electronically to the state and other service providers. By increasing cyber defenses, the protection of this sensitive data in turn increases the protection of county residents.

6 PROTECTION OF THE COUNTY BRAND

When a county is attacked and a breach of data occurs, media will publicize such events. This in turn can weaken the credibility and trust of government services such as election procedures, tax collection, and online payments for county residents. Sound cyber security best practices can help to mitigate this situation.

7 PROTECTION OF THE WEBSITE

The county website is a main source of online information, services and digital applications. If the website is defaced or taken down by a cyber attack, county residents cannot access those resources. Further, county websites are key during an emergency for the residents to look up information; an attack on weak cyber security puts that at risk. Addressing website security weaknesses is no longer a nice to have but rather a necessity.

8 PROTECTION OF THE NETWORK

County employees rely on their computer and access to the network resources (email, software applications, case management systems) to perform their job functions. Cyber defenses are a necessity to ensure that those functions are available 24/7.

9 PROTECTION OF ELECTION EQUIPMENT

When a county follows the Election Administration Commission, Department of Homeland Security, and vendor guidance on the physical protection of election equipment including strict chain of custody processes, county residents will have a better appreciation of election security in their county.

10 PROTECTION OF ELECTION PROCESSES

When a county invites the public to view election system testing, or other activities that the county undertakes before, during and after an election, county residents will have more confidence in election processes.

Top Ten Cyber Questions for County Leadership

1 Does the County have a Board adopted Information Security Program in place to govern cyber risk management, that includes:

- Cybersecurity policies and procedures
- Proper cyber hygiene that covers patching, routine assessments, annual security risk analysis, cyber insurance, and incident response
- Identification of cyber strengths, weaknesses, opportunities, and threats in terms of people, process, and technology
- Level of current and desired maturity of the county

2 Does the county have Multi-Factor Authentication (MFA) in place?

3 Does our county have a security incident plan in place and

- is that plan part of the overall continuity of government plan
- is the IT department aware of the security incident plan?
- is the plan prioritized based on criteria that takes into account critical services and potential impact?
- is the plan tested with county departments so that they know what to do if a cyber incident occurs, and
- does the plan include what is an acceptable computer/communication systems outage timeframe?

4 What cyber-related issues have we experienced in the past year or key high-level findings that have been uncovered through an assessment, and what is our plan for addressing them?

5 Are there security initiatives which you believe are important to take on in the next several years? And does that involve new tools and funding? How can elected leadership support you in those?

6 Does our county have an employee security awareness training program in place? Tell me more.

7 Are our backups safe from a security threat and have we conducted exercises to test reinstalling data from backup?

8 How does our county ensure the cyber safety of county employees, contractors and others that connect to the network, especially in a remote environment?

9 Is our county using the cloud for hosting data and applications and how is that protected?

10 Why do we need cyber insurance and what are the current challenges?

DIG DEEPER

Phase two will include the tracks below which will contain additional questions county leaders can use in dialogue with the county IT support.

Track 1

More in-depth questions for elected officials

Track 2

An IT track for county CIOs, IT Directors, outsourced IT support

Track 3

A track for county executives and administrators

Track 4

A track for department directors

For more information on the guides or on NACo Technology resources, visit
County Tech Xchange (naco.org), or reach out to Rita Reynolds, NACo CIO at rreynolds@naco.org

FB.COM/NACoDC
TWITTER.COM/NACoTWEETS
YOUTUBE.COM/NACoVIDEO
www.NACo.ORG/LINKEDIN

NATIONAL ASSOCIATION of COUNTIES NACo®

660 North Capitol St., NW · Suite 400 · Washington, D.C. 20001 · 202.393.6226 · www.NACo.org