Cybersecurity: Protecting our Nation's Counties

Study of Resilience of U.S. Counties

accenture | NATIONAL ASSOCIATION of COUNTIES NACo

The state of county cybersecurity

NACo and Accenture conducted research to better understand the state of county cybersecurity along four dimensions—

- Cyber strategy
- Cyber protection
- Cyber resilience
- Cyber ecosystem

—to gain insight into counties' current risk environments. Our research included a representative sample of county leaders from across the country reached via electronic survey and focus groups.

The findings that follow highlight the urgency of addressing cybersecurity. We learned what keeps county leadership up at night, what types of mounting pressure these leaders face, and how related challenges, such as an increase in remote work, inform their approaches. Perhaps most important, these areas of focus help identify distinct opportunities counties can leverage to mitigate vulnerabilities and protect data, systems, and operations.

Challenges facing county leaders today:

The COVID-19 pandemic forced governments to adapt quickly and shift how they approach and interact with the people they serve. As governments emerge from that context and navigate a new juncture, they have the opportunity to focus on building resilience and creating systems that can withstand any future crisis. One key to creating a resilient government is being prepared to respond to the ever-evolving cyber threat landscape.

Local governments are a desirable target for cyber criminals and nation state attackers because they run critical infrastructure and collect and store valuable resident data. Cyberattacks on county governments can take many forms, such as ransomware attacks that lock down computer systems until a ransom is paid, or data breaches that compromise sensitive information. The consequences of a successful cyberattack can be severe, including financial losses, operational disruptions, and damage to public trust and confidence. According to our survey research, the number of cyberattacks on vital U.S. county services is increasing: **40% of counties report that the number of attempted, unsuccessful breaches has increased since last year (53% stayed the same, 7% decreased).**

County leadership is also contending with more limited budgets than their peers in bigger state, federal, or business enterprises. While new federal funding is emerging (the "State and Local Cyber Grant Program" funds $1B over 4 years), other expenses such as cyber insurance costs have rapidly increased. New guidance including the 2023 National Cybersecurity Strategy calls out county IT leadership's important role in contributing to a defensible, resilient, and values-aligned digital ecosystem. Continuously leveraging emerging technologies in support of this ecosystem is a key force of change that is necessary not only for short-term security, but also for long-term sustainability and growth in government organizations.[1]

The factors above place more pressure than ever on local government technology leaders to quickly improve the cybersecurity of their counties in agile, strategic, and cost-effective ways.

> "I think local governments are increasingly dependent on that technology leadership to keep them safe, to deliver services, to raise the efficiency and effectiveness of entire organizations. **So that's sort of a perfect storm of woe coming to local government at some point if they can't figure out a way to keep technology leadership engaged and at the table and funded and paid appropriately."**
>
> **-Interviewed CIO of medium-size rural county**

Findings:

Cyber strategy

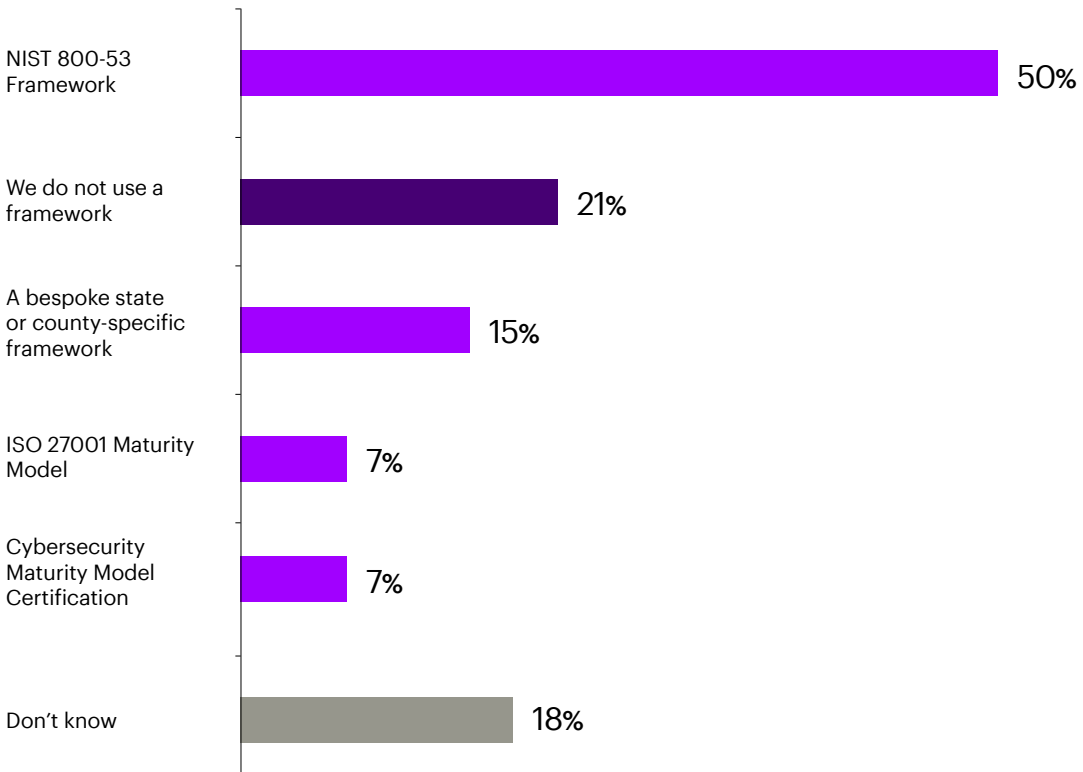
Standards adoption:

County governments employ several frameworks to measure their cybersecurity risk levels. One of the most popular industry standards is the National Institute of Standards and Technology (NIST) 800-53, "Security and Privacy Controls for Information Systems and Organizations." The voluntary standard covers a range of security areas such as access control, contingency planning, incident response, and system and communications protection. While the NIST 800-53 standard was developed primarily for federal information systems, it has become widely used as a best practice framework for securing other types of information systems, including those used by state and local governments, as well as private organizations.

Today, only 50% of counties surveyed are utilizing the NIST 800-53 framework. If they don't use NIST 800-53, responding counties use a bespoke state or county-specific framework (15%), the ISO27001 Maturity Model (7%), or Cybersecurity Maturity Model Certification (7%). A full 21% report that they don't use any framework and 18% don't know which framework they use.

What frameworks do you use to measure your cybersecurity effectiveness?

Multiple responses

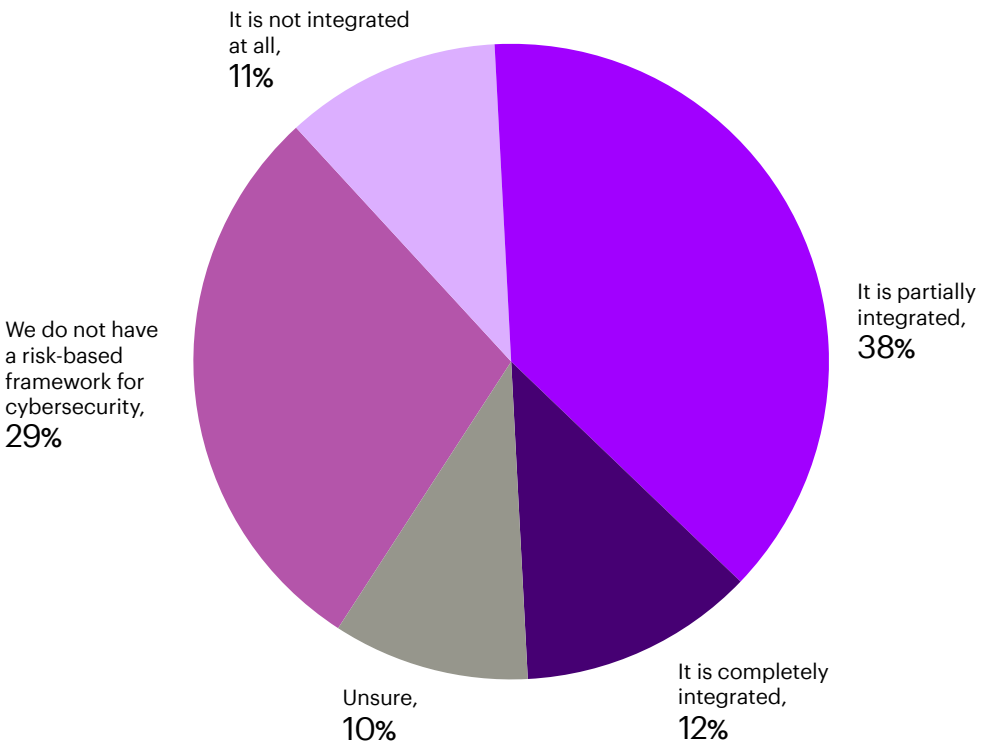


Cyber and risk management security integration:

A cyber risk-based framework is a set of guidelines and principles that organizations can use to manage and mitigate cyber risks. It is a systematic approach that typically includes several components, such as risk assessment, risk mitigation, risk monitoring, and incident response. By integrating a cyber risk-based framework into county-wide enterprise security and resilience plans, county governments can better identify and prioritize the most significant risks, while establishing effective security controls and providing ongoing monitoring and assessment to ensure the effectiveness of those controls.

While 63% of county leaders report having a response and recovery plan for their county's critical infrastructure, just 12% of counties say their cybersecurity risk-based framework is completely integrated into the county-wide enterprise security and resilience plan. 38% of respondents have partially integrated frameworks. 11% have a risk-based framework for cybersecurity that is not integrated, while 29% of respondents do not have such a framework at all.

To what extent is your cyber risk-based framework integrated into your county-wide enterprise security and resilience plan?



"At the end of the night or in the middle of the night, what keeps me up is knowing that we're going to have a cyber incident at some point. And just hoping that our incident response plans are actually going to hold up whenever that happens."

-Interviewed IT Director of a small rural county

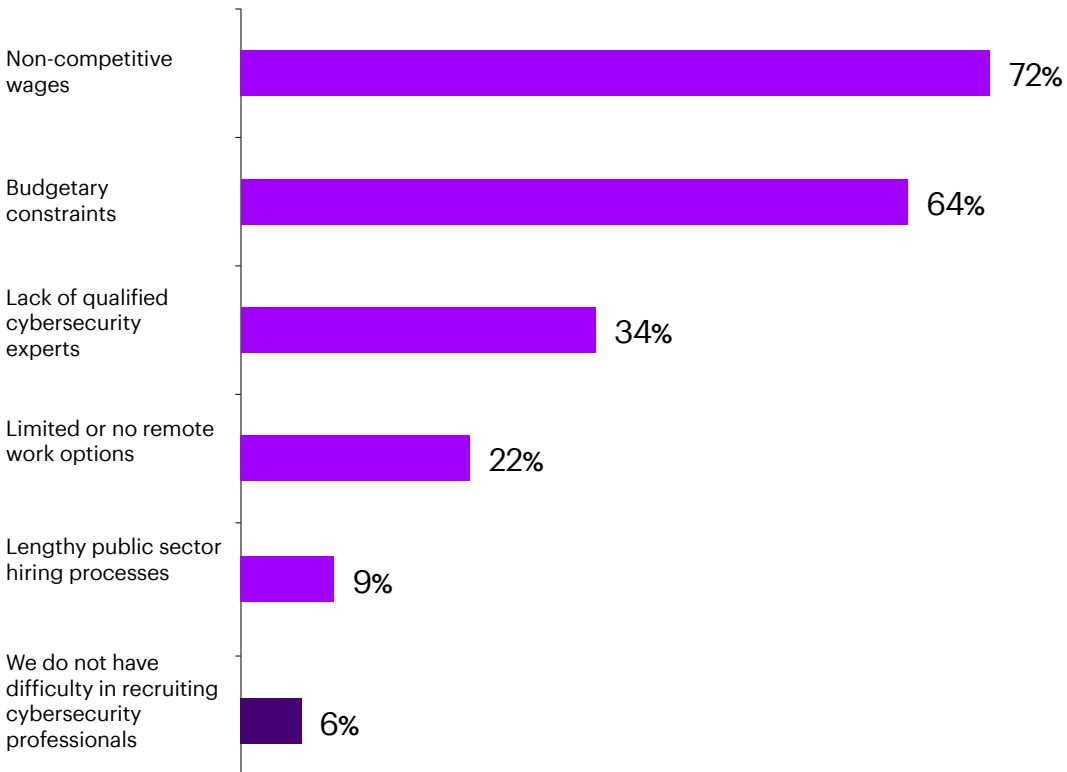
Workforce: Staffing shortages amid increased work

We found that counties are also no exception to the cybersecurity talent shortage felt by private sector and other government employers. Despite adding nearly 63,000 cybersecurity workers in 2022 (bringing the total to 1.2 million workers), the nationwide gap for talent grew to over 400,000 cybersecurity openings (2022 ISC² Cybersecurity Workforce Study).[ii]

County governments have persistent difficulty in recruiting for skilled cybersecurity professionals and face tough competition from other government agencies and private industries. Respondents say non-competitive wages (72%) and budgetary constraints (64%) are the top challenges in recruiting for these roles.

What are the top challenges for your organization in recruiting professionals?

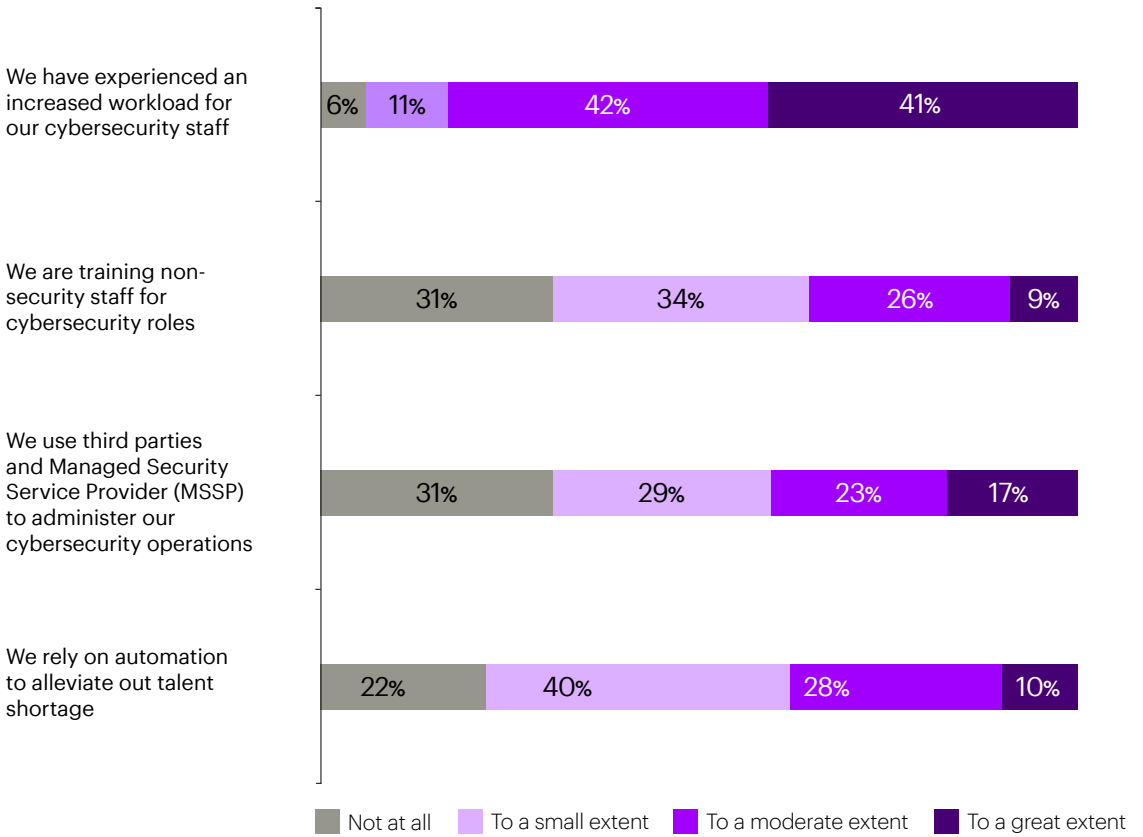
Multiple responses: Select up to three



> "My problem is everybody wants to work remote. And that's a hard sell for some local governments, number one. Number two, nine times out of 10, depending on the skill set I'm looking for, they want to make more money than I do, or the manager that is going to be overseeing them... It took me a year to fill my last position, and I've got a position right now that's open that hasn't had a qualified applicant apply in nine months."
>
> **-Interviewed CIO of medium-size coastal county**

Fewer than a quarter of the counties surveyed report having the right skills in place for effective cybersecurity. To overcome this, counties are creatively upskilling existing talent through new training for cybersecurity roles as well as using Managed Service Security Providers (MSSPs) and relying on automation.

To what extent has your organization experienced the following due to a shortage in cybersecurity talent?



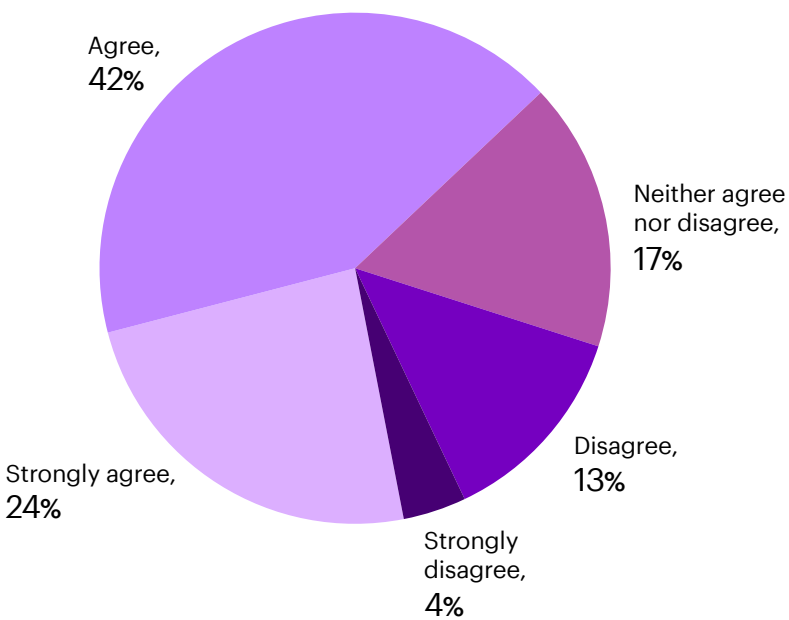
Findings:

Cyber protection

Priority for elected county leadership:

Overall, county governments are aware of the growing threat of cyberattacks and the potential impact they can have on their operations and residents. Nearly two-thirds of respondents (65%) agree that cybersecurity is a top priority for elected county officials. The level of support, however, differs significantly by county size. 86% of respondents feel elected officials in larger counties view cybersecurity as important, compared to 67% in medium-size counties and 57% in small counties.

"Cybersecurity is a top priority for elected county officials."



Self-reported readiness is also impacted by county size. Bigger counties feel more prepared and enjoy more support from their elected officials. 67% of large counties feel ahead of their peers, while 59% of medium-size counties feel ahead of their peers, and only 44% of small counties feel the same (23% feel behind). Counties' confidence levels in their cyber protection can vary depending on factors other than size, such as budget, staffing, technology infrastructure, rural versus urban environment and the level of cybersecurity expertise within the organization.

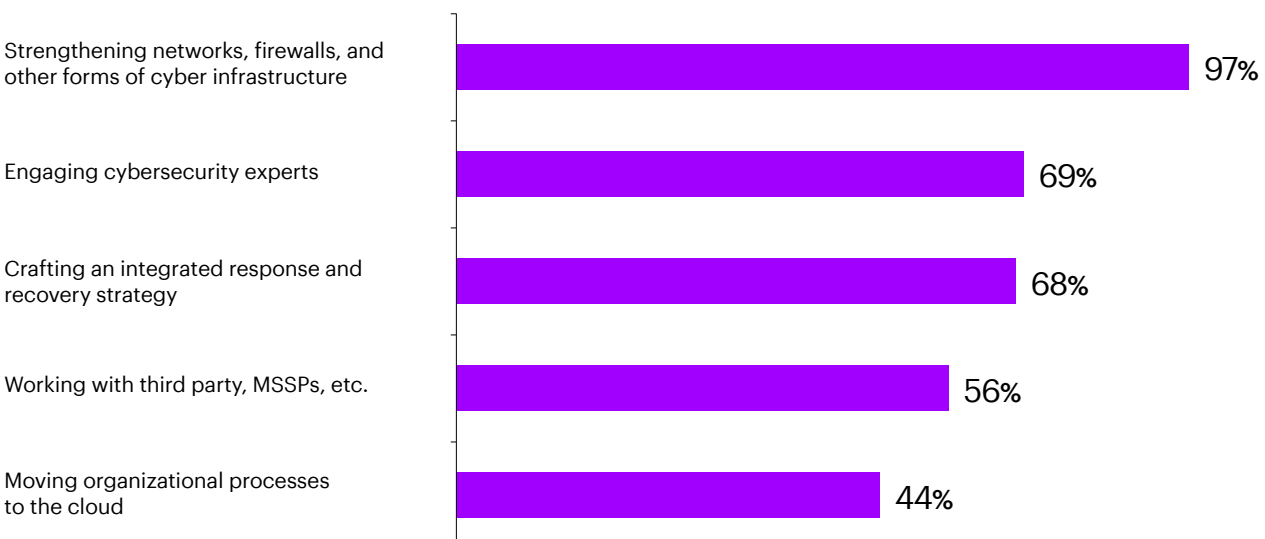
> "It's one thing to buy a tool, it's another to implement it and still run it after the fact. There is no set it and forget it with security. So that is one piece that is difficult. Especially in the smaller counties that can't actually get a security person. So everything is on top of their IT staff, which may be one to two people."
>
> **-Interviewed CISO of large county**

Increasing cybersecurity posture in multiple ways:

To improve readiness and confidence, counties are enhancing their cybersecurity in a number of ways. The top methods that county cybersecurity leaders are using to increase their cyber protection include: strengthening their cyber infrastructure; engaging cybersecurity experts; crafting an integrated response and recovery strategy; working with third party MSSPs; and moving processes to the cloud.

Select which cybersecurity methods your organization is currently utilizing.

Multiple resonses



Difficulty with lagging technology:

Lagging technology presents a serious cybersecurity issue for county governments because outdated hardware, software, and infrastructure are more vulnerable to cyber-attacks. Additionally, older systems may not be able to integrate with newer security technologies and may not be able to keep pace with the evolving cyber threat landscape.

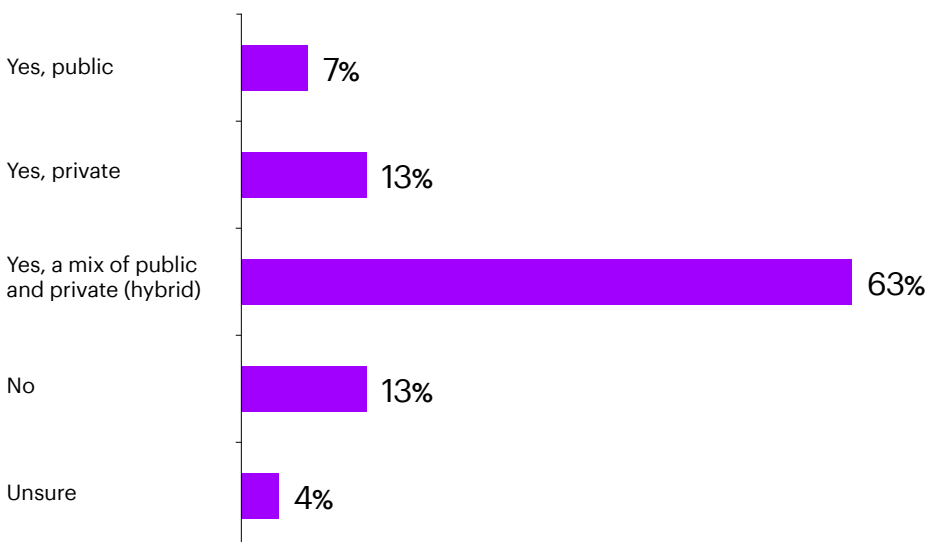
> "And some of the things that concern me, that I spent a lot of my professional energy dealing with, are lagging technology pressures. We have a lot of aging servers, lagging technology that we're constantly trying to stay up to date with."
>
> **-Interviewed CIO of medium-size rural county**

Moving processes and services to the cloud:

County governments are increasingly moving their systems and services to the cloud to improve efficiency, reduce costs, and increase accessibility to their residents. This mirrors the public sector's use of the cloud as a source of competitive advantage. 44% of survey respondents are moving their county's organizational processes to the cloud as a way to increase cyber protection. By using cloud environments, counties can avoid the need to manage the hosting environment themselves and can instead rely on the cloud provider to do the heavy lifting on development, updates, and maintenance.

Many counties are using a combination of on-premises and cloud-based services, known as a hybrid cloud. This allows counties to take advantage of the scalability and flexibility of the cloud while still maintaining control over certain systems and data. Of cloud environments, we found that most counties host operations or data in a mix of public and private cloud environments (63%).

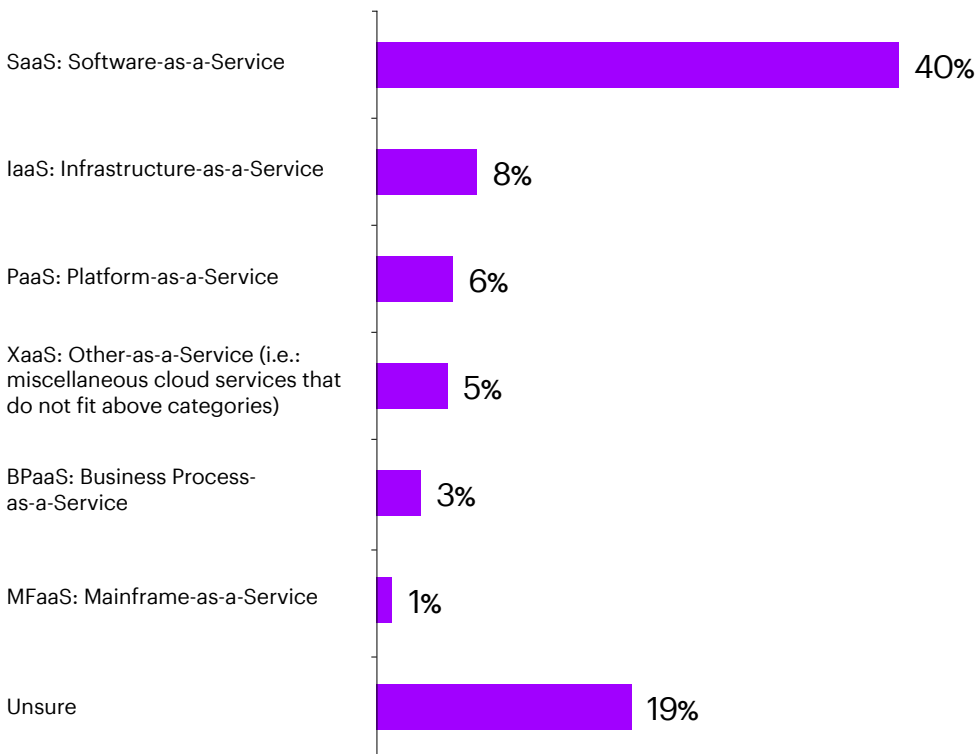
Does your county host operations or data in a public or private cloud?



For those counties that use a cloud environment, Software-as-a-Service (SaaS) is the most popular, making up 39% of their county's total system portfolio. Examples of SaaS products for county governments include workforce productivity, constituent outreach, or geographic information system (GIS) solutions.

> "And now with the cloud, we've actually complicated our security landscape because now we have to protect more. And be aware of where is our data, is it properly configured, and if you lift and shift your infrastructure to the cloud, it's up to us to configure it correctly. And I think it's a real challenge and then think about the skill sets required to maintain these diverse systems."
>
> **-Interviewed CTO of medium-size county**

What percentage of your county's total portfolio currently uses the following cloud services?
Averages



Difficulty with budgeting:

Budgeting for modern cybersecurity products emerged as a theme for county leaders in our research. Of primary concern, the variable operating costs of cloud vendors are at odds with traditional government procurement forecasting and outlays. County CIOs are hesitant to deal with unexpected service spikes or billing fluctuations.

> "One of our challenges here is the procurement side. Our procurement people are used to procuring other services or tangible products; cloud services, not so much. So there's a lot of unknowns, a lot of uncertainty, a lot of fear."
>
> **-Interviewed CTO at large suburban county**

Findings:

Cyber resilience

Security Operations Center (SOC):

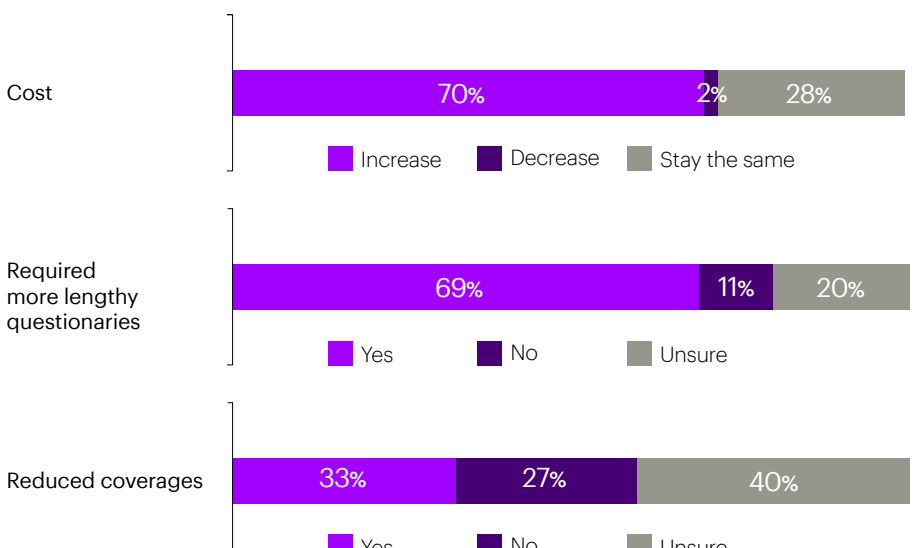
The SOC is designed to be a central hub for cybersecurity operations and is equipped with advanced technology tools that help monitor and protect county government networks, systems, and data. The center is typically staffed by a team of cybersecurity professionals who are responsible for monitoring the county's IT infrastructure, detecting and responding to cyber threats, and ensuring compliance with security policies and procedures. Today, only 41% of counties have a SOC, however they are more likely to appear in larger counties. Our responses showed 73% of large counties, 54% of small counties, and 27% of small counties had SOCs.

Insurance:

When it comes to cyber resilience, cyber insurance is an important element. 86% of counties reported having an external cyber insurance policy, but only 31% are happy with it. Dramatic policy changes contribute to this dissatisfaction. 70% of respondents reported cost increases, 69% noted the questionnaires for coverage increased, and 33% saw coverage reduced. All of this adds up to more costs, more burdens, and decreased coverage.

> "Our cyber insurance tripled from last year to this year in cost. And the requirements are significantly tighter this year. The list of hard no's is getting virtually impossible."
>
> **-Interviewed CIO of medium-size coastal county**

In the last year, has your cyber insurance changed?



"The premium, it's up to 100,000 a year. And the coverage is not enough... So we're also looking to decide, is this annual $100,000 commitment, are we getting anything of value that, should we direct this somewhere else? Our risk manager is definitely studying it pretty sharply to see if it's worth it to renew next year."

-Interviewed IT Director at small rural county

Survey respondents reported that good options for counties without cyber insurance are scarce. 64% of those who don't have cyber insurance have self-insurance, 27% have a contract with a mediating consulting company, and 9% have something else.

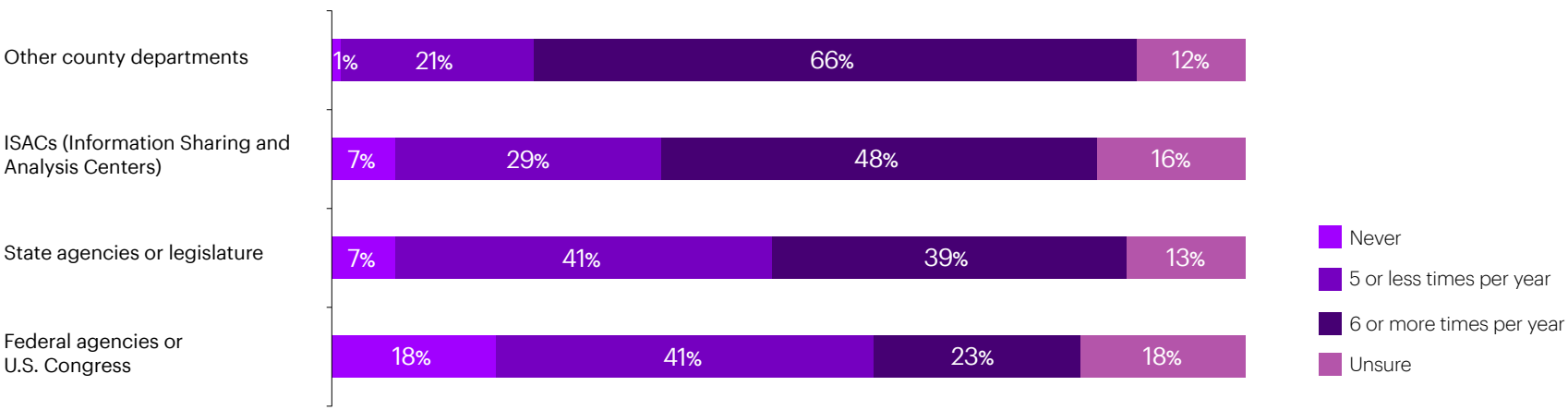
Findings:

Cyber ecosystem

Interconnected peer networks:

County governments often rely on networks that are connected with other agencies and organizations, such as law enforcement, judiciary, public health, or emergency services. This interconnectedness can increase the reach of cyberattack consequences. When it comes to data sharing, we found that, today, most counties are engaging and collaborating with their local government peers and Information Sharing and Analysis Centers (ISACs) more frequently than with state or federal governments.

To what extent is your organization currently engaged in information sharing and collaboration with other agencies?



When it comes to validating security requirements of other local third-party partners like water authorities and recycling centers, counties have mixed success. Today, 19% of county cybersecurity leaders do not require partners to meet any cybersecurity standards. 18% of counties require strict cybersecurity standards for ecosystem partners or vendors. Most (57%) require partners to meet some cybersecurity standards that vary depending on criteria (e.g., the size of organization, amount of data sharing, etc.).

Actions for county leaders

Below are three broad recommendations for improving the cybersecurity position of counties for a stronger digital core:

01 Conduct an industry assessment to determine the county's current state.

Conduct the Nationwide Cybersecurity Review (NCSR) assessment. This free, anonymous self-assessment not only helps measure the maturity of an organization, is also a requirement for new grants through the Department of Homeland Security. Once leaders determine where their organization is today, they can strategically enhance the critical cybersecurity components of people, processes, and technology accordingly. Based on the results of the assessment, counties will better understand their risk profile that can inform a strategic roadmap for cybersecurity risk remediation and maturity.

Implement NIST 800-53 industry standard. Counties should consider developing a road map a road map guided by the NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations." NIST 800-53 is a proactive approach to cybersecurity that helps organizations manage their cyber risks and protect their critical assets from cyber threats. Using this standard will help prioritize programs and funding in the broader context of county resources. Adopting NIST standards can be a cost-savings strategy, as well, as reducing cyber risk in the environment will likely result in lower cyber insurance costs, as less risky counties can potentially enjoy lower premiums.

"...Cyber insurance is now driving the investment side of cyber, right? We all know it's only a matter of time. We all have to pay, you're gonna pay me now or you're gonna pay me later, right? So my cyber insurance premium's gonna triple if I don't get funding to do these two or three things I need to do in my environment."

-Interviewed CIO of medium-size rural county

02 Develop a cybersecurity strategy that includes a focus on workforce.

A key component in a county's cybersecurity strategy is the enabling cyber talent strategy. This plan should identify which capabilities to hire for, upskill, or outsource. Barriers to change can include a lack of cultural readiness to change, leadership capabilities and alignment, and functional silos. Implementing a Cyber Program Management Office (PMO) to manage the plan execution is important for success.

Targeted recruitment to an expanded pool: County CIOs face stiff competition from other organizations that are also clamoring for cybersecurity talent amid the global talent shortage. To address the challenges of limited budgets, generally lower compensation packages, and complex hiring processes, CIOs need to have a targeted strategy for attracting talent. County governments should consider developing targeted recruitment strategies that focus on building relationships with local cybersecurity professionals and promoting the benefits of working in county government. Employers should also broaden their pool to more historically underrepresented groups in the cyber profession, including women, first-generation professionals and immigrants, neurodiverse individuals, and LGBTQI+ individuals. Hiring and investing in training of junior professionals is another area where counties can effectively grow their workforce.

Continuous Reinvention: Recent research from Accenture found a strong digital core to be foundational to all other strategic needs of the county (Total Enterprise Reinvention, 2023). Amplifying the role of technology for the county means shifting from a technology landscape of static, standalone parts to interoperable pieces intentionally integrated and leveraging the cloud. The digital core consists of three layers:

1. An infrastructure and security layer: A modern, cloud-based IT foundation that is automated, agile and secure by design.
2. A data and AI layer: Where enterprise data becomes accessible at scale, with domain-specific, AI-enabled applications and platforms generating insights for decision-making.
3. An applications and platforms layer: Where new experiences and ways of operating come alive—through modernized and new, custom applications and platforms or replatforming on SaaS.

> "We're not competitive on pay here in this area... So for us to compete in cyber we have to grow who we need through training. I'm currently I'm looking for a manager, but I can't afford a manager, so I need to hire a more junior person and shape them."
>
> **-Interviewed CISO of large county**

Managed security service providers (MSSP): County CIOs should examine where managed security services can be helpful as an extension of their internal workforce. Overall, MSSPs can provide county CIOs with the specialized cybersecurity expertise, efficiency gains, 24/7 service, and increased compliance needed to effectively protect county government networks and systems. We found two-thirds (68%) of counties are using third parties and MSSPs to administer their cybersecurity operations. And with only 41% agreeing they have a Secure Operations Response Center, counties should look into managed SOC, Incident Response retainers, and Managed Detection & Response services specifically.

Automation of routine tasks: Cybersecurity automation can help county CIOs alleviate talent shortages by allowing existing cybersecurity staff to focus on higher value-added activities, while automating routine tasks (such as vulnerability scans, patch management, and log analysis). We found that automation (78%) is popular for alleviating the current talent shortages. CIOs should look to modern cloud and SaaS-based security services with options for automation that comply with standards.

03 Take advantage of security provided by ecosystem partnerships.

Cloud adoption: For many CIOs, the target destination operating environment is a hybrid cloud. Moving systems and services to the cloud can offer several key benefits, including cost savings, scalability, reliability, and security. Perhaps most immediately important for county CIOs is the increased security provided by government cloud providers. Many popular cloud providers and ecosystem tech providers (Microsoft, Amazon, Google, Oracle, Workday, SAP, etc.) have evolved and joined the defense industrial based (DIB) companies. Sharing risk with these vendors, with their many advantages including automated security updates, is a faster way of decreasing risk in a county CIO's cyber environment.

> "Microsofts and Oracles and all the companies that do the hosting [like] Amazon, they spend more probably in one day than we could hope to put into cybersecurity as a county probably in a decade. So that was the big selling point... The increased security of the data, our citizens' data, their tax information, all of the information is what was really what I think helped us turn the corner."
>
> **-Interviewed CIO at large coastal county**

Relationships with vendor networks: By working with technology providers and implementers, county governments can access the latest cybersecurity solutions and expertise, reduce risk, and better protect their operations, data, and constituents. County governments can partner with vendors to get the latest understanding of the current cybersecurity trends and best practices. Technology vendors can also help implement security solutions, conduct risk assessments, provide training, and manage security systems on behalf of counties.

> "I would add vendors and outside experts and consultants have been a great resource for us.... It can bring some best practices or state of the art leading solutions to you that it's hard to stay on top of individually or as a small team."
>
> **-Interviewed CTO at large suburban county**

Peer partnerships with state and federal governments: By partnering with state and federal governments, county governments can enhance their cybersecurity posture and better protect their systems and data against cyber threats. Engagement with government peers usually exists today with formalizing data sharing guided by regulatory standards (e.g., HIPPA or CJIS).

In addition to sharing information and collaborating on incident response, counties can take advantage of the standards, federal and state funding, and training resources of other government entities. New and exciting federal funding such as the recent $1b "State and Local Cyber Grant Program" will hopefully catalyze engagement between states and counties. Organizations including the Center for Internet Security and Cybersecurity and Infrastructure Security Agency (CISA) provide free or low-cost services, including: Malicious Domain Blocking and Reporting (MDBR), Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), Multi-State Information Sharing and Analysis Center (MS-ISAC), and other government resources.

> "So there are a lot of resources out there that we can avail ourselves of. MS-ISAC, EI-ISAC, CISA, FBI, they've all got great resources for us to use about trends and so forth."
>
> **-Interviewed CIO of medium-size rural county**

Conclusion

IT Leadership in U.S. counties can improve cybersecurity by increasing standards adoption, developing and implementing a strategy with a focus on talent, and taking advantage of the benefits offered by ecosystem partnerships and vendors. As cyber risks that threaten to disrupt services, compromise data, and lead to severe financial losses continue to increase, attention to this matter for jurisdictions of all sizes is urgent. To improve cybersecurity and reduce risk within tight budget constraints, we noted two key motivating factors to compel stakeholders to act: Positioning cyber as a strategic business decision and focusing on the high-risk environment of county infrastructure. Two county leaders we interviewed had the following to say on those points:

> "I go back to cyber becomes a business decision because really helping leadership understand the risks and the benefit of investing, and helping them understand that it really becomes a business decision—how much risk are they willing to fund or reduce?"
>
> **-Interviewed CTO of medium-size county**

> "What I think really got their attention or has had their attention and focused them on this effort are concerns about providing services, especially life emergency support services and the risk from a cyber event, whether it's a ransomware attack or other type of cyber event, or just some sort of disaster. Not being able to provide fire, safety, rescue, police rescue, or 911 services is critical."
>
> **-Interviewed CTO at large suburban county**

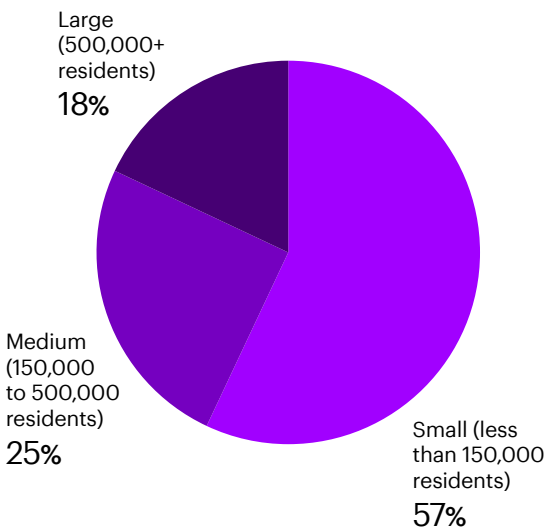
Private companies are responding to a number of external challenges by amplifying the role of technology through a strong digital core that includes cloud and security layers. In the context of county governments, attention to and strategy around cybersecurity is paramount. As counties examine the above strategies to enhance their cybersecurity and safeguard their operations, it's important to remember cyber threats are evolving rapidly. To keep pace, counties need to view the information here in the context of continuous improvement. Successful cybersecurity isn't a "one-and-done" project. Done right, it's an agile, long-term strategy that facilitates optimal resilience in the face of any threat or disruption.

About the research

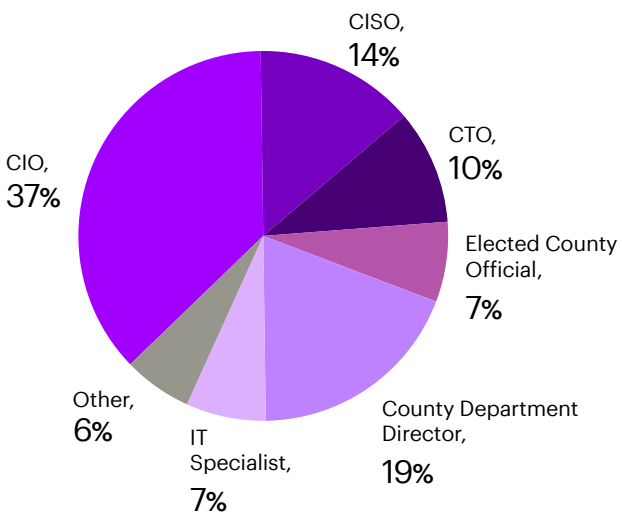
To best understand cyber resilience of U.S. counties, Accenture conducted qualitative and quantitative research initiatives. Accenture also conducted two focus groups of NACo members. Each focus group of five included representatives from a diversity of counties pulled from NACo's IT standing committee.

Accenture conducted an electronic survey of NACo's IT-affiliated members in December 2022 and January 2023. The survey yielded 134 responses. Survey respondents included a variety of IT leaders: 60% were county technology executives, including: 37% CIO, 14% CISO, 10% CTO. The remaining included 7% elected county official; 19% County Department Director; and 7% IT specialist role. Survey respondents varied by size of county: over half (57%) of responses came from small counties (less than 150,000 residents); a quarter (25%) came from medium-size counties (150,000 to 500,000 residents); and the remainder (18%) came from large counties (500,000+ residents).

County Size



Role



Authors

Rita Reynolds
Chief Information Officer
at NACo

Michele Myauo
North America Public Services
Security Industry Lead at Accenture

Jenny Brodie
Global Lead, Health and Public
Service Research at Accenture

Phil Pollman
Public Sector Research
at Accenture

Contributors:

Ed Blomquist Cybersecurity
Research Principal at Accenture

References

i https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

ii https://www.isc2.org/Research/Workforce-Study

About NACo

The National Association of Counties (http://www.naco.org) strengthens America's counties, including nearly 40,000 county elected officials and 3.6 million county employees. Founded in 1935, NACo unites county officials to advocate for county government priorities in federal policymaking; promote exemplary county policies and practices; nurture leadership skills and expand knowledge networks; optimize county and taxpayer resources and cost savings; and enrich the public's understanding of county government.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at **www.accenture.com**

About Accenture Research

About Accenture Research Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity.

For more information, **visit www.accenture.com/research**