UNDERSTANDING THE CYBER THREAT

A Policy Guide for Legislators

Contents

AT&T

NATIONAL CYBERSECURITY ALLIANCE

Produced by: GOVERNING INSTITUTE

DAVID KIDD

It's Time for Action

AT&T and the National Cyber Security Alliance are leading a long-term strategy to increase cybersecurity awareness among elected officials. As part of that effort, we commissioned the Governing Institute—an organization that helps public sector leaders govern more effectively through research, decision support and executive education—to survey 103 state legislators and their staff to understand how lawmakers view their role in this critical issue. The results, published at **www.governing.com/cyberfindings,** show that awareness is growing. A vast majority of respondents said protecting state computer networks is a priority. But the findings also indicate awareness isn't necessarily turning into action, at least not yet.

Given the growing concern over cyber threats, we wanted to dig deeper into state cybersecurity challenges and show legislators how they can make an impact on this critical issue. We asked a wide range of experts—legislative thought leaders, government chief information security officers and industry security professionals—to interpret key data points from the survey, and offer practical advice and ideas. The result is this policy guide.

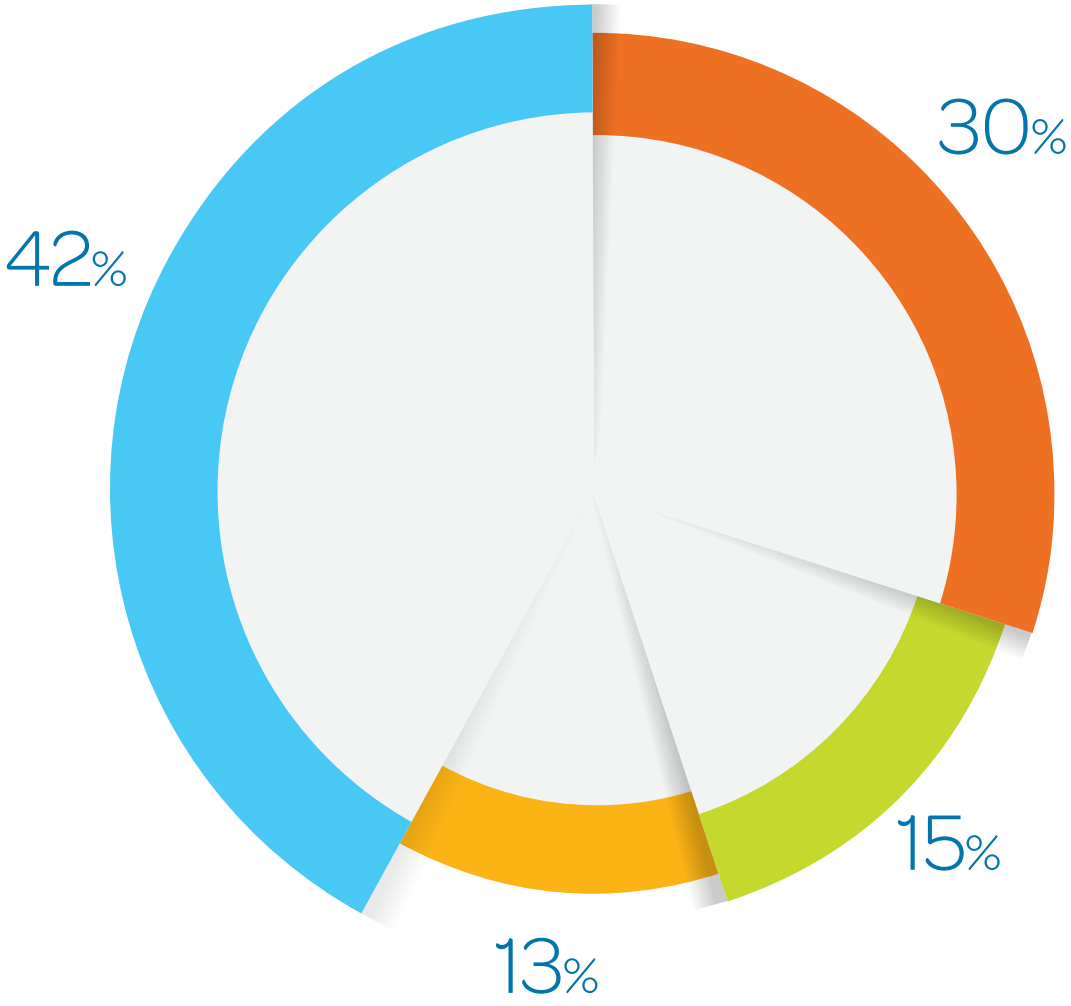
If there's a common thread running through the interviews presented here, it's that lawmakers and senior government leaders must engage more deeply on cybersecurity. Although technology is involved, this isn't a technology issue. Cyber threats represent a serious business risk to government operations. Attacks have the potential to cripple vital government services and damage public infrastructure.

Legislators have a central role to play in addressing these risks—from budgeting for adequate security resources, to overseeing policy development and implementation, to monitoring agency security compliance. These tasks can't be delegated or ignored. They are issues on which elected leaders need to lead.

Yes, the survey shows progress is being made, but it also indicates that more work needs to be done. Governments are more reliant on computer networks than ever before, and they are amassing soaring amounts of valuable citizen information. Meanwhile, cyber attackers are growing more bold and sophisticated by the day.

The time for action on cybersecurity is now.

Nearly 1/3 of respondents said their state's current level of cyber risk is high.



Assessing Cyber Risk

You're More Vulnerable Than You Think

Although almost one-third of survey respondents said their state's cyber risk is high, far too many others underestimated the threat to their systems and data. More than half ranked their cyber risk as moderate or low, while 13 percent didn't know.

In reality, all government agencies hold some type of valuable or sensitive material, whether it's citizen records, financial information or procurement data. Therefore, everyone is a target. And in today's highly interconnected world, each agency—no matter how small—is a stepping stone to another. So even a seemingly minor breach can have wide-ranging implications.

"It's not just your value, it's the value of all of your customers, all of your partners and all of your partners' partners," says Terry Hect, AT&T's director and chief security strategist for government. "If I can get into your computer, that information can get me into 5 more computers, and they can get me into 25 more."

Searching for Weakness

Unfortunately, agencies also are under nearly constant assault. Hackers know that state and local governments often lag behind commercial entities in cybersecurity readiness. Consequently, the number of attackers probing your systems for vulnerabilities is exploding—everyone from small-time crooks equipped with black-market ransomware kits, to nation states and organized crime syndicates armed with sophisticated cyber weapons.

The threats are all over the map. Small towns and school districts are hit with ransomware that shuts down computer systems until they make a payment. Thieves steal citizen identities and financial information from state agency databases. Water authorities endure surgical strikes that use specialized computer code to destroy water pumps.

Perhaps most concerning is that the seeds for future attacks are quietly being sown into government networks through a technique known as advanced persistent threats. "Advanced persistent threats will be the biggest problem we face for a long time," says James O'Dell, a senior fraud manager at AT&T. "This is malware code that can be planted in a device today, and even if you remove the device, the malware stays embedded in your network and data. It can be used by cyber criminals for years."

Fighting Back

How can agencies help to protect themselves in this dangerous environment? With multi-layer cyber defenses, Hect says. Traditional cybersecurity gear—like firewalls and secure email—remains important for blocking known threats. But today's attacks evolve so rapidly that these tools must be augmented by real-time intrusion detection capabilities that quickly spot abnormal network behavior and shut down suspicious activity.

Finally, agencies need to truly understand their cyber risk. A comprehensive security assessment, performed by a qualified third party, is a vital step toward addressing your organization's vulnerabilities.

"You can't put your head in the sand. You need to understand these issues," says Hect. "Everyone thinks their risk is low until they've been breached."

Terry Hect

Director and Chief Security Strategist for Government, AT&T

James O'Dell

Senior Fraud Manager, AT&T

The top 3 cybersecurity threats that pose the greatest risk are:

Criminal organizations outside the U.S.

70%

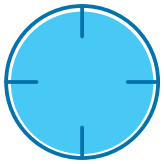
Political hacktivists

54%

Criminal organizations within the U.S.

54%

Other threats identified include:



Nation states' espionage

40%

Inside employees

39%

Inside contractors

27%

Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

Identifying the Source of Threats

Your Biggest Threats

When legislators were asked which cybersecurity threats posed the greatest risk to their states, organized crime topped the list, followed by political hacktivists. Are these truly the biggest dangers roaming the cyber landscape? Perhaps not.

"I was a bit surprised at the ranking," says Michael Singer, executive director of technology security for AT&T. He says policymakers may be overestimating the power of hacktivists, and underestimating the danger of several other potential adversaries.

He pointed to hostile nation states—ranked fourth by survey respondents—as the biggest threat to state and local government computer systems because of their resources and sophistication. "Nation states will have the most skilled people; they're trained professionals and they're being paid to work a shift."

Next, according to Singer, are insider threats—both employees and contractors—because of their potential access to sensitive systems and data. It's also important to note that nation state actors use the credentials of insiders, making the focus on insider threats doubly important. However, these two groups were ranked among the least dangerous by legislator survey respondents.

Course of Action

The discrepancy between threat perception and reality points to the need for stronger relationships between policymakers and their security teams. Essentially, senior executives need to lean on security experts who are plugged into constantly evolving cyber crime trends and understand how to respond to them.

"You need to build a team of talent at the CIO level," says Singer. "You can look to them to recommend what to do first, second and third. Also, you need to work with them to identify critical data that would be most valuable to attackers—you can't protect it if you don't know what it is."

Mitigating the risk also demands multiple layers of protection—and security tools and techniques are improving to help governments manage the threat.

For instance, email scanning technology combs through the incoming messages to find harmful attachments or links to dangerous websites. These solutions can help agencies weed out phishing emails and other scams before they reach employees. Next-generation anti-virus software helps governments stay ahead of rapidly mutating malware attacks by spotting suspicious behavior instead of looking for known virus signatures. As attackers improve their ability to mask the identity of dangerous software, behavior-based protections grow more important.

And data loss protection solutions can help guard against insider threats by automatically preventing end users from removing critical data from systems. "You need to assess your most sensitive information, and then put this type of extra protection around it," says Singer. "Make that information the hardest data to get to."

Always Watching

In addition to these tools, governments must implement monitoring capabilities that constantly examine network and system behavior. Far too many organizations—public, private, large and small—have been victims of long-term data breaches that allowed attackers to steal valuable information for weeks or months before anyone discovered it. Security monitoring is designed to quickly spot unusual data movement or other suspicious activity so it can be investigated and stopped.

"It's absolutely essential to know what's going on," says Singer. "The last thing you want is an attacker in your network long term, stealing your sensitive information and you don't know about it."

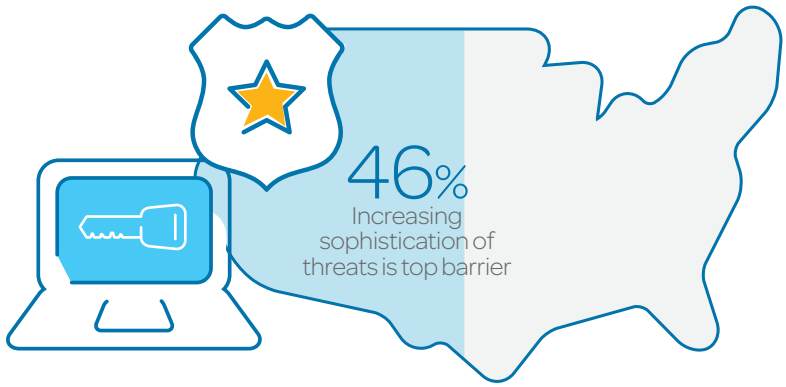
Large government entities may opt to build and operate their own security operations centers. But running such a facility—which requires expensive monitoring equipment and 24/7 staffing—is a heavy lift for many public agencies. Monitoring services offered by commercial security providers may be an effective alternative.

Ultimately, a combination of risk assessment, sophisticated tools, careful monitoring and constant vigilance is key to managing cyber threats, regardless of whether the danger comes from nation states, malicious insiders or politically driven hacktivists. "The goal," Singer says, "is to find and address your weaknesses before one of these adversaries does."

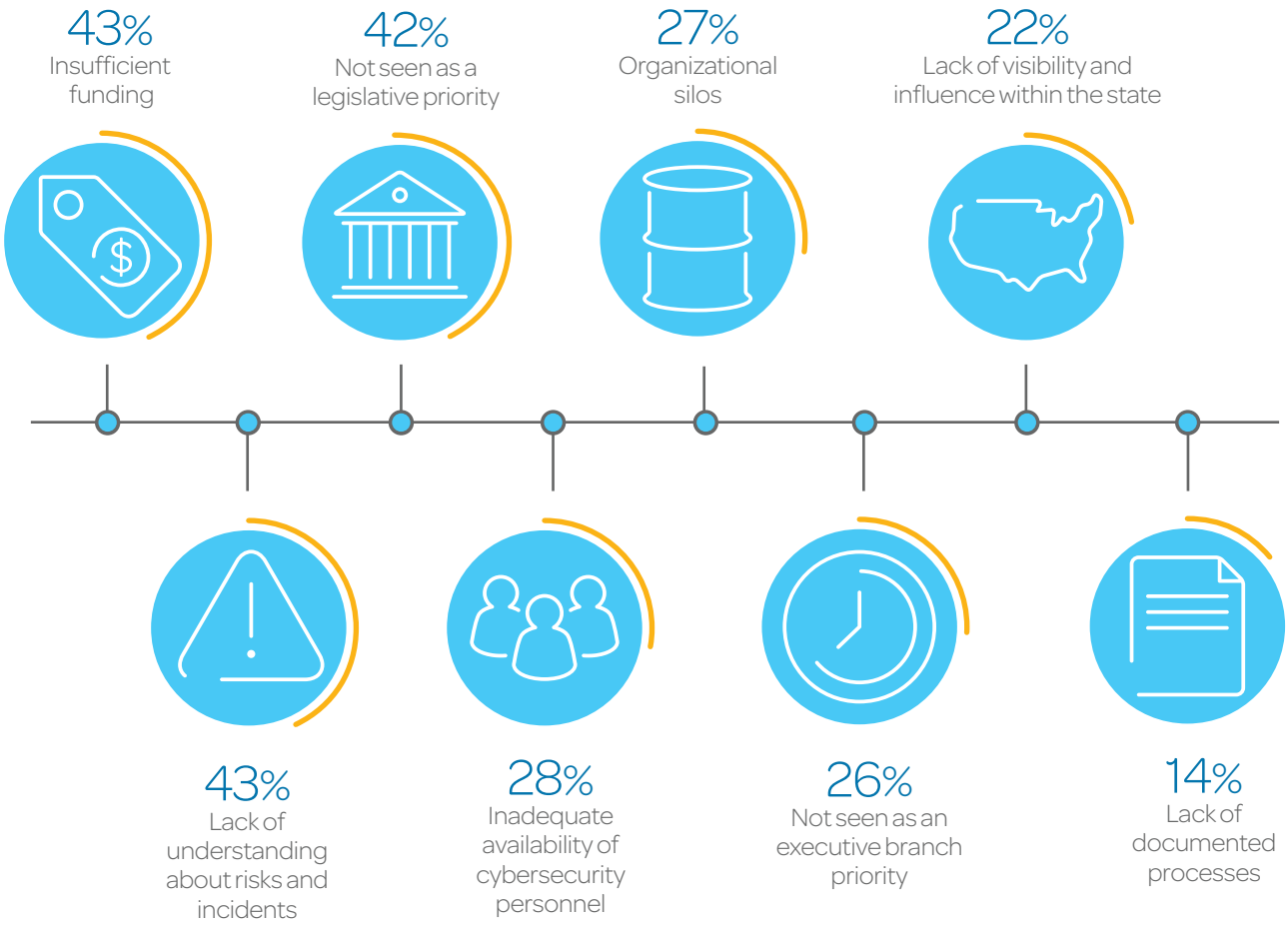
Michael Singer

Executive Director of Technology Security, AT&T

The increasing sophistication of threats (46%) was identified as the top barrier to appropriately protecting states from cyber threats.



Other barriers include:



Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

Strengthening Internal Awareness

Building Support for Better Security

Over the past five years, the state of Missouri has built a multi-layered cybersecurity strategy. It includes the latest technology—from next-generation firewalls that track programs running on state networks to security analytics that monitor evolving threats—and a wide-ranging awareness campaign targeting everyone from top executives to rank-and-file employees.

Missouri is a model for engaging stakeholders and building support for cybersecurity initiatives. Unfortunately, it's in the minority.

According to our survey, there are a number of reasons why state and local governments struggle to safeguard sensitive information from cyber criminals. But they tend to point to one overarching issue: Threats are becoming more numerous and complex, and most governments aren't devoting enough attention and resources toward responding to these growing risks.

Our survey findings illustrate both sides of this challenge. Forty-six percent of respondents said growing threat sophistication is their top concern. But that response was followed closely by a trio of answers—insufficient funding, lack of understanding and low prioritization—that indicate many top government officials may not fully grasp their role in addressing them.

Old Scams and New Tools

Missouri Chief Information Security Officer Michael Roling says hackers are continually improving their tactics for sneaking into computer networks and stealing valuable information. Some attacks use sophisticated technology, but many more prey on unsophisticated end users.

"Our adversaries have identified soft targets that don't really require advanced tools," Roling says. "They understand that the average employee is potentially the weakest link, so they are using old-school scams in a high-tech way to get their foot in the door."

Trends like these are pushing the state toward innovative programs for improving security awareness. For instance, Roling conducts fake phishing campaigns that emulate techniques used by attackers to trick unsuspecting state employees. Those who fall for the scam receive more security training.

"A great example is during tax season, they'll send W-2 themed emails asking our employees for Social Security numbers for people in their department," Roling says. "The emails look like they came from the employee's boss."

Missouri also has gamified security awareness by ranking agencies based on their performance in fake phishing exercises, completion of monthly training activities and other factors. "Every month, we send a report on how the agencies are doing," Roling says. "No one wants to come in last. It has really taken off."

Engaging State Leaders

End-user training activities are backed by strong commitment from state leaders. A cabinet-level IT committee meets regularly to discuss new processes and potential security threats. This group—which includes the leaders of key state agencies—also issues statewide policies on technology use and security procedures. Involving these stakeholders in the development of security policies helps to bolster their support as new rules are rolled out across the government enterprise.

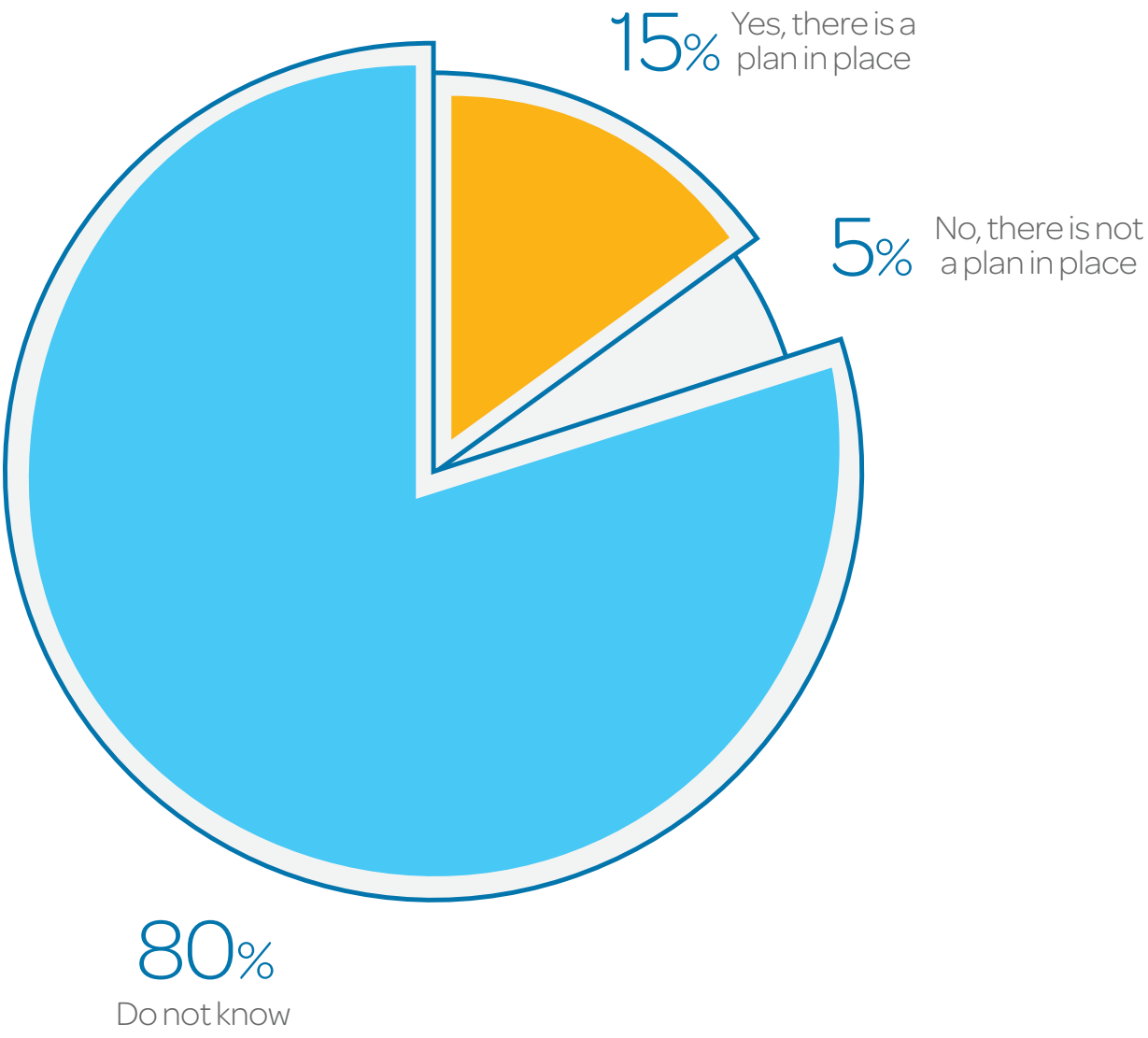
In addition, Roling raised security awareness among state legislators and senior policymakers by giving them a tour of Missouri's security operations center and providing them with analysis reports showing the volume of attacks hitting the state's computer systems.

State leaders have taken the message to heart. "Our decision-makers understand the need to have security ingrained from the top down," Roling says. "We also made sure they were aware of their responsibility to fund efforts required to protect citizens' data. They agreed, and our funding has gone up year over year."

Michael Roling

Chief Information Security Officer, State of Missouri

A majority of respondents do not know if their state has a cyber emergency incident plan in place.



Making Cybersecurity a Priority

The Role of Leaders in Incident Response

There may be no clearer indication of legislative disengagement on cybersecurity issues than this: 80 percent of survey respondents did not know if their state has a formal plan in place to respond to cyber incidents. That's sobering news in an era where most security experts concede that security breaches are a matter of when—not if—for almost any organization.

Even the best defenses can't block every threat as attacks become more frequent and attackers constantly change tactics. So it's imperative that government agencies have plans to quickly respond to security breaches and help minimize their impacts.

"A lot of energy in the security space over the past few years has been around incident response, with the assumption that attackers are going to get in the door," says Chris Boyer, AT&T's assistant vice president of global public policy. "For many governments, as big and complex as their organizations are, they're going to have points of failure. Which means you need a strong incident response plan to deal with it."

Lack of Attention

The survey results don't necessarily mean governments lack cyber incident plans. In fact, most of them certainly have some type of plan in place. What the results show, however, is a troubling lack of attention from top government officials on this crucial issue.

Elected leaders and senior policymakers have a significant role to play in setting priorities around incident response planning, as well as conducting oversight once response plans are in place. "They are working with budgeting and funding, so elected officials need to see to it that resources are aligned to deal with the problem," says Boyer. "And from an oversight perspective, they need to ensure those resources are being fully utilized so their state is prepared for an attack. If they don't even know they have a plan, they aren't performing these roles."

Powerful Tools

Elected officials also are uniquely positioned to lead broader initiatives to strengthen their jurisdiction's response to cyber incidents. Forward-thinking governors and legislators are creating cybersecurity commissions that bring together key stakeholders—technology leaders, public safety officials, senior agency managers and others—to identify and prioritize security efforts.

For instance, Georgia Gov. Nathan Deal issued an executive order last year creating a statewide Cybersecurity Review Board that's chaired by the state CIO and includes leaders of Georgia's Emergency Management/Homeland Security Agency, National Guard and Department of Administrative Services. The board provides a unified and authoritative voice on cyber issues that commands attention from agency commissioners, budgeting officials and others.

Significantly, some of these initiatives reframe cybersecurity as an emergency response or public safety issue, opening up new classes of resources to respond to cyber attacks. One such effort is unfolding in California, where a 2015 executive order from Gov. Jerry Brown created the California Cybersecurity Integration Center within the state's Office of Emergency Services.

The new organization—which includes representatives from the Department of Technology, Highway Patrol, Attorney General's Office, U.S. Department of Homeland Security and the FBI—is charged with building a multi-agency Cyber Incident Response Team that will lead cyber threat detection, reporting and response in coordination with public and private entities across the state.

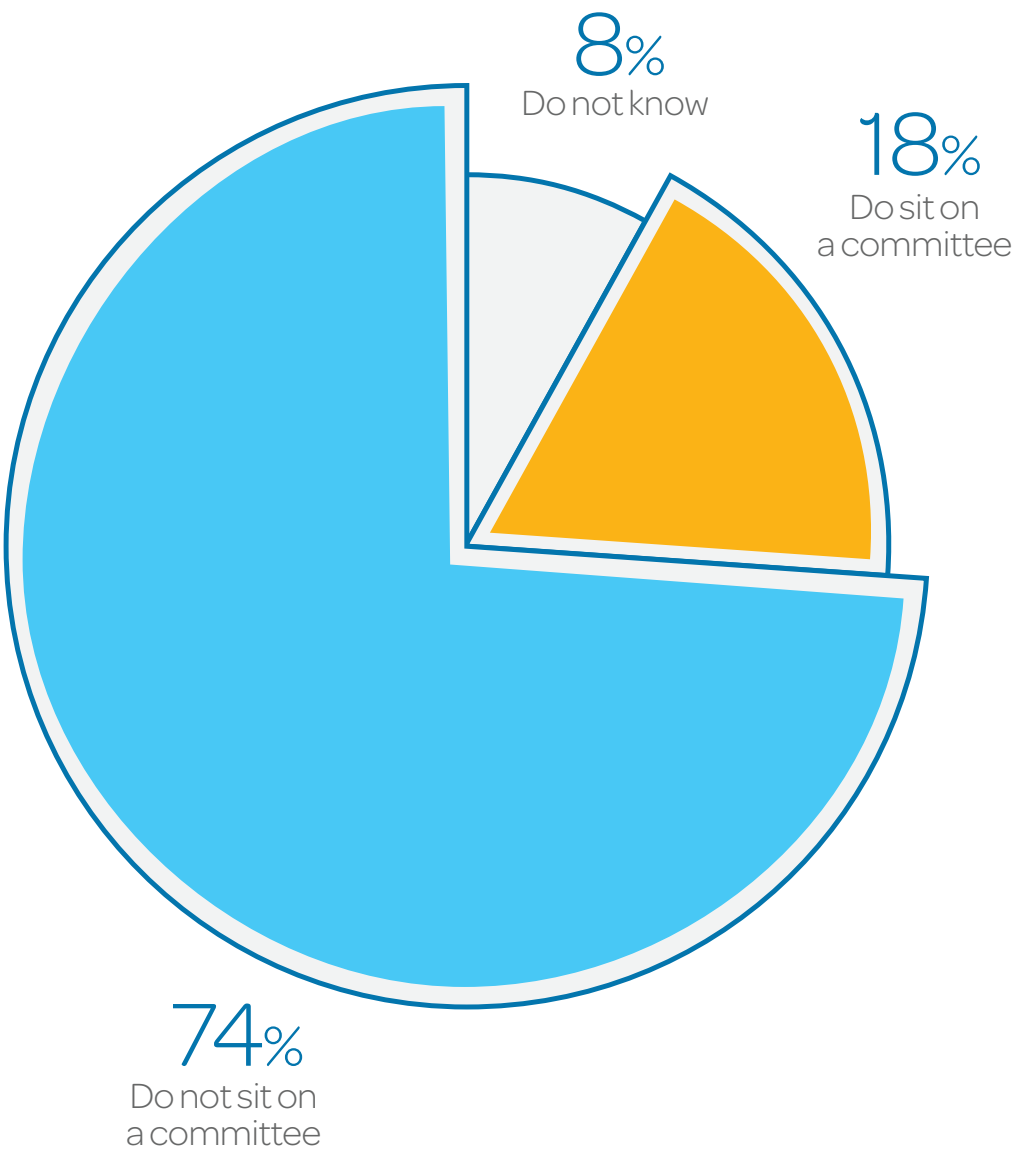
In addition, Boyer notes that the National Governors Association now recommends that state fusion centers—created after the 9/11 attacks to provide counter-terrorism intelligence—be expanded to include detection and remediation of cyber attacks. It's another tool that legislators and senior executives can bring to bear—but only if they engage in the task of building stronger incident response capabilities.

"The message is that lawmakers need to lead on these issues," Boyer says. "These are executive-level tasks."

Chris Boyer

Assistant Vice President of Global Public Policy, AT&T

A majority of respondents do not currently sit on a committee that has cybersecurity as part of its mandate.



Getting Involved in Planning

Committee of None

Most legislators view cybersecurity as extremely important, but our research shows that few of them are directly involved in the issue. Less than 20 percent of survey respondents said they sit on a committee that has cybersecurity as part of its mandate, yet more than 80 percent agreed that protecting government networks is a "critical priority."

Why the disconnect? First, relatively few state and local legislative bodies have dedicated cybersecurity committees. So lawmakers simply don't have an opportunity to join. But more deeply, the paucity of such committees indicates a lack of meaningful interaction between lawmakers and security professionals.

"It's disheartening that there are not more cybersecurity committees," says Ricardo Lafosse, chief information security officer for Cook County, Ill. He says it remains a hard sell to convince officials they need a standalone committee on the issue, despite the fact that data breaches and cyber terrorism events regularly make headlines.

"The response is often, 'You can cover it inside of the technology committee,'" says Lafosse. "This is such an important topic that it needs to stand on its own."

Making It Known

Security professionals bear at least some responsibility for the lack of legislative support for dedicated cyber committees, according to Lafosse. Too many government chief information security officers (CISOs) do a poor job of educating legislators and policymakers on the threats facing government systems and the possible impact of major attack.

He says lawmakers need a regular flow of easily digestible information from security organizations. For instance, dashboards that provide a high-level snapshot of the jurisdiction's security posture can give senior officials situational awareness and a starting point to seek deeper information. Regular newsletters that highlight security activities and provide thought leadership on the topic can also help legislators engage.

"One thing I've been trying to work on is marketing. Why not feed some relevant security information to them on a daily, weekly or quarterly basis," Lafosse says. "Legislators don't need to know the nitty-gritty of technology, but they need to understand which threats are on the rise and what that could mean."

Helpful Hypotheticals

One of the best ways for policymakers and security professionals to engage on cyber issues is to focus on the real-world impact of a major attack. Discussing cyber threats in the context of risk to critical government business operations can be the key to building executive and legislative support.

"For instance, what if someone took down the property tax system? First responders wouldn't get paid. Will they still protect you if they haven't been paid for two months?" Lafosse says. "It's a crazy scenario, but it's something you can visualize. There's a direct public safety impact."

Another way to firm up support for cybersecurity initiatives is to work collaboratively with departmental leadership. When Lafosse joined Cook County three years ago, he spent his initial months on the job networking with elected officials and departmental CIOs.

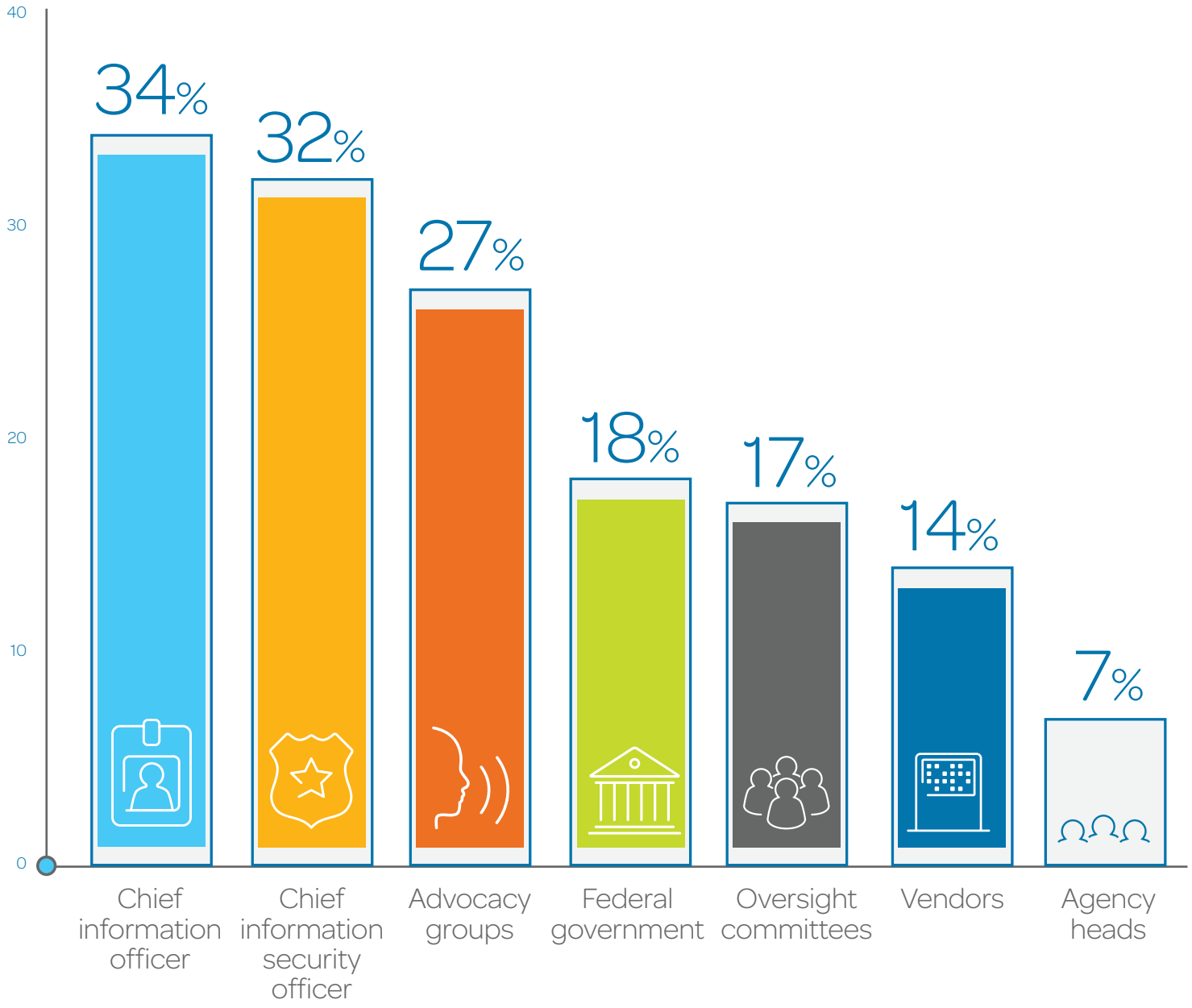
"I found it odd how decentralized we were, yet we all rode on the same network. A breach in one department could impact another department. Really we were all in the same boat," he says. "So I brought them into an inclusive security environment. I didn't dictate what technology to use or the type of passwords. I identified the gaps and said, 'We need to work together to address this.'"

Ricardo Lafosse

Chief Information Security Officer, Cook County, Ill.

Media reports (39%) were the most commonly cited sources for cybersecurity information.

Other sources included:



 Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

Communicating and Staying Informed

Understanding Cyber Issues

The fact that most legislators get their cybersecurity information from media reports doesn't surprise California State Assemblymember Jacqui Irwin. It's human nature to react to sensational news about major attacks, and that tendency can be magnified in a political environment.

"It reflects what typically happens to politicians," says Irwin. "You tend to be very reactionary as opposed to looking at the overall state of security and what needs to be done."

Media coverage isn't necessarily a bad source of cyber information—it can be an effective tool for drawing attention to the issue—but it can't be a primary source of knowledge for policymakers. Instead, public officials need to build strong staff expertise on the issue and cultivate open and honest relationships with technology and security experts.

Focusing on Cyber

The need for deeper legislative engagement on cybersecurity drove Irwin to ask California Assembly leaders to create a committee focused on the issue. The results are the Assembly Select Committee on Cybersecurity, which Irwin now chairs, and several pieces of legislation designed to strengthen information security practices across California state government.

For instance, Irwin authored a new law that tightens lax security assessment practices by requiring state departments to undergo regular risk assessments performed by the California National Guard. She also wrote another piece of legislation requiring California to create a statewide response plan for cybersecurity threats on critical infrastructure by next year.

"Once we started to dig into this issue, we realized we had to make sure the state had its house in order," she says.

Open Communication

Cybersecurity committees like Irwin's are a rarity in state legislatures, but she doesn't expect it to stay that way. "There has been so much change in focus over the last year or two because of high-profile security breaches that I would suspect many legislatures are taking a look at it," Irwin says. "The conversation is just starting."

Another evolving area is the relationship between legislators and CIOs and CISOs. About one-third of our survey respondents listed CIOs and CISOs as frequent sources for cyber information. But Irwin says most states lack consistent communication between lawmakers and technology or security professionals, and that needs to change. Regular briefings, honest updates and meaningful metrics on security issues may lead to better legislative support for security initiatives.

"I want to know how different departments are doing. How many have done security audits? How many have completed assessments?" says Irwin. "Give us the metrics on how departments are complying. And then let us help get the resources."

Making a Difference

With degrees in both systems engineering and applied physics, Irwin is well-equipped to tackle the technical nuances of cybersecurity. But she says lawmakers don't need to be tech wizards to make an impact. Much of their task involves ensuring agencies take appropriate steps to manage risk.

"We hear from departments that want to fix vulnerabilities just by hooking up some sort of hardware," Irwin says. "But when you dig deeper into it, you realize it's more about business management."

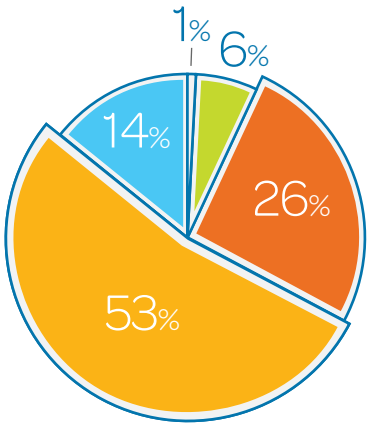
Software and hardware are part of the equation. But so are more familiar concepts like employee training and awareness, along with good safety practices in the workplace. "You don't have to be technical to make a difference," Irwin says. "These are things that legislators can easily master."

Jacqui Irwin

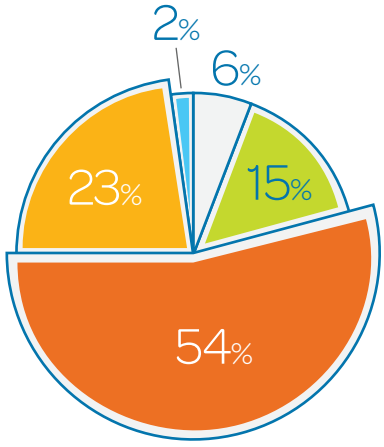
California State Assemblymember

Respondents were asked to **rate their level of agreement** with the following cybersecurity awareness statements.

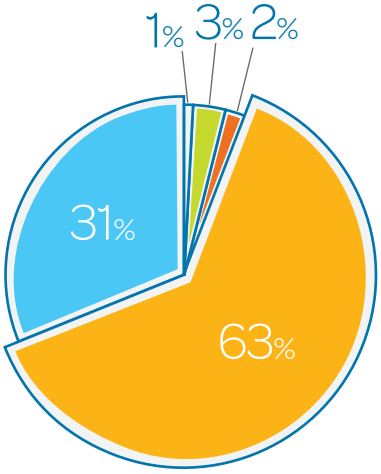
We have good policies in place, but understand it's a matter of when, not if, we will be attacked.



We're one step ahead—our sensitive data isn't all in one place.



Hackers are getting smarter, which means our state could be compromised.



Strongly agree | Somewhat agree | Neither agree or disagree | Somewhat disagree | Strongly disagree

Taking Steps Toward Better Security

Turning Awareness into Action

Survey findings around cybersecurity awareness indicate that a growing number of legislators grasp the seriousness of the threat to government networks and data. Almost 70 percent of respondents acknowledged that attacks are inevitable, and more than 90 percent say malicious hackers are getting smarter.

That's good news, says Michael Kaiser, executive director of the National Cyber Security Alliance. "Awareness of cybersecurity as an issue was quite high, which indicates that there is increasing knowledge about cybersecurity and how it relates to their responsibility to protect their states' networks and citizens."

But awareness must translate into action—and that's where lawmakers still have work to do.

Kaiser cited several pieces of data that aren't so encouraging. First, a majority of respondents (63%) were unaware of the size of cybersecurity investments being made by their states. "This lack of awareness is troubling because it's critical that state networks have good cybersecurity technology in place and invest in upgrading older legacy systems that may be more difficult to secure," he says.

Also, half of respondents said their states don't have adequate cybersecurity personnel. And a similar number admitted they have gaps in expertise and struggle with attracting and retaining cybersecurity talent.

What to Do

What can lawmakers do to help address the risk of cyber attack? A good first step is requiring agencies—and their vendors—to follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Kaiser says. The NIST Framework was developed several years ago by government and industry to provide a roadmap for protecting critical systems and information from cyber threats. "The framework lays out a plan to protect assets, detect if an incident has occurred, and then respond and recover," he explains.

In addition, legislators should fund ongoing security awareness training for state workforces and support the development of statewide cybersecurity plans that spell out in plain language how computer networks will be protected.

One thing policymakers should avoid, however, is mandating or legislating the use of specific cybersecurity technologies, Kaiser adds. "Those technologies may become outdated quickly or offer a narrow solution space and leave out many other promising cybersecurity tactics."

Casting a Wide Net

When it comes to crafting security policies, more input is better. Kaiser urges lawmakers to seek advice from a broad range of sources, including experts from state agencies, the federal government and private industry. Utilities, financial institutions, telecommunications companies and internet service providers can be good sources for insight.

"Cybersecurity is a fast-paced, ever-changing environment, and it is critical to get input from those most plugged in to the threats and best practices to develop sound policy," Kaiser says.

Finally, stakeholder communication is crucial throughout the process. Businesses will need to understand the impact of complying with new or expanded regulations. They'll need both reasonable input and adequate notice of policy changes.

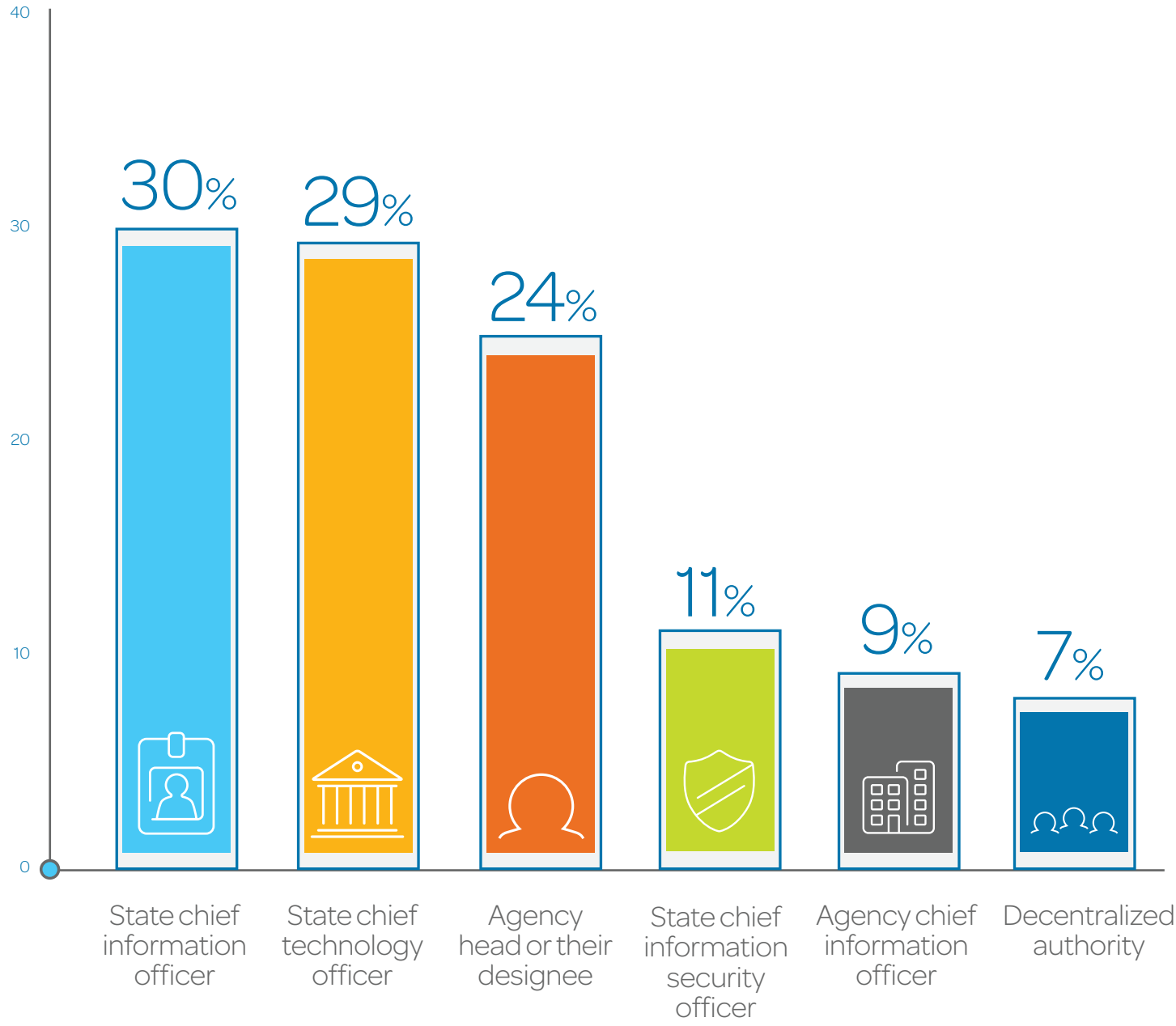
Citizens also should be alerted to cyber protection measures being taken on their behalf. "Transparency is important in cybersecurity," Kaiser says. "Consumers should be regularly informed of the steps being taken to protect their personal information and their state's critical infrastructure."

Michael Kaiser

Executive Director, National Cyber Security Alliance

Over 1/3 of respondents do not know who is responsible for developing their state's enterprise cybersecurity strategy.

Other respondents identified the following as being responsible:



 Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

Crafting Cybersecurity Strategies

Making a Statement on Data Protection

Why is it troubling that more than one-third of legislators in the survey don't know who develops their state's cybersecurity strategy? Because the strategy makes a fundamental statement about how states will protect their citizens' most valuable and sensitive data—and that's a statement senior officials need to own.

"I see it as a huge issue," says Steve Hurst, director of security services and strategy for AT&T. "If you don't know who's responsible for your strategy and policy, you really don't know who is crafting the governance model that you're adhering to."

Among respondents who did know the source of their security strategy, answers were fairly evenly split among the state CIO, CTO and agency heads—perhaps reflecting the diversity of government organizational structures.

But ultimately it's less about who develops the strategy and more about which stakeholders are consulted and how policies are rolled out across the government enterprise. Senior officials—CIOs, CTOs, agency leaders and elected officials—should have input into the enterprise cybersecurity strategy. And they'll need to support and enforce it once it's created.

"These security policies may not be crafted at the top," says Hurst. "But they need to come down from the top to show support for them across the entire organization."

Balancing Act

At a high level, a cybersecurity plan—and the policies associated with it—makes judgments on the value of the various types of data collected and held by governments. Part of the process is inventorying the types of data agencies have and assessing the business risk created by potential vulnerabilities.

Hurst describes security strategy as a balancing act that weighs users' need to access data against the importance of safeguarding it from malicious predators. "You start with what we call the CIA triangle—confidentiality, integrity and availability. That's the basis of all security," Hurst says. "The amount of focus on each of those factors depends on the specific situation and data risks that need to be managed."

He adds that tying security policies to data value—not to specific security technologies—is key to long-term effectiveness. "A well-crafted policy stays relevant even as technology evolves," says Hurst. "You need to be aware of technology changes—and revise where necessary—but the policy itself will remain valid if it's crafted at the data level."

Building Clout

One key cyber policy challenge for governments is getting multiple, independent public agencies and institutions on the same page. Ideally, one high-level policy should be adopted across legislative, executive and judicial branches. This, of course, is easier said than done.

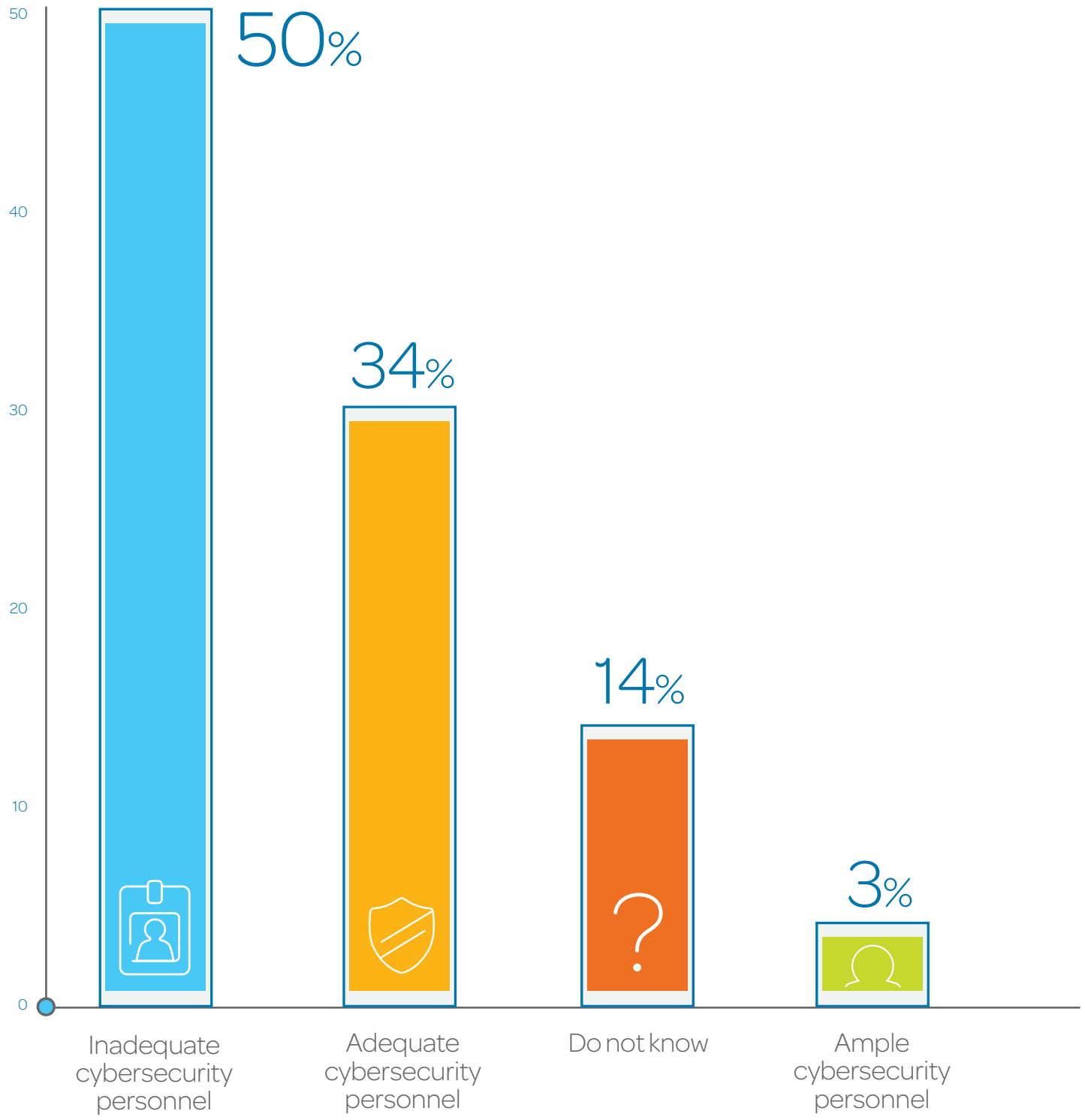
One option for defusing potential turf wars is to work with outside experts on policy and strategy development, Hurst says. "Bringing in a third party can take the politics out of it," he explains. "Even if you have internal expertise, bringing in someone from the outside to do an evaluation adds clout. Leveraging that clout can go a long way toward getting something enacted."

Once policies are developed, senior leaders must drive adoption and compliance. "Officials need to focus on this data as if it were their own," says Hurst. "Holding and protecting valuable citizen data is a public trust."

Steve Hurst

Director of Security Services and Strategy, AT&T

When it comes to cybersecurity staffing levels, respondents said their state has:



 Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

Finding and Retaining Cyber Talent

The Quest for Talent

State governments struggle to attract talented cybersecurity professionals, but they're not alone. Organizations across the globe are scrambling to hire cyber talent from a pool that's simply too small to meet the spiraling demand.

"It's an issue for everyone, but governments have some particular challenges," says Dr. Ernest McDuffie, former leader of the National Initiative for Cybersecurity Education, a federal government-led effort to expand the country's cybersecurity workforce.

Most public agencies can't match private sector compensation packages. And slow government hiring cycles make it tough to compete against companies that can make on-the-spot job offers to highly skilled individuals.

What's more, the task isn't likely to get easier. Although universities are ramping up cybersecurity degree programs, they won't catch up to the demand anytime soon, says McDuffie, who now leads a consulting firm focused on cybersecurity workforce issues. "The studies I've seen predict literally millions of unfilled cybersecurity jobs over the next 5 to 10 years. We're not going to be producing that many students."

Smart Moves

Still, there are a number of moves legislators can make to improve the odds of finding the cyber talent they need, says McDuffie.

Lawmakers can establish special hiring categories to erase some of the private sector salary advantages. They can re-examine HR policies with an eye toward streamlining state hiring processes. And they can work with agencies to offer non-salary benefits that make government service more appealing.

"It's not all about money," McDuffie says. "Flexible schedules, onsite childcare, help with transportation to and from work—those kinds of things can go a long way toward making an attractive package."

Instead of hiring expensive new cyber experts, states can also consider growing their own. It may make sense to launch cybersecurity training initiatives aimed at existing employees interested in making a career change. These workers already understand state business processes, which may allow them to apply security skills more effectively.

New Partnerships

Scholarship programs are another option. McDuffie says the federal CyberCorps: Scholarship for Service program recently was opened to state and local governments. The program pays for students to attend university cybersecurity programs. In return, students must work for government agencies—federal, state, local or tribal—after they graduate.

"States need to be aware that there's this pool of students who are obligated to work for government," McDuffie says. "As a potential employer, states can contact the Office of Personnel Management and get access to their resumes, where they went to school, etc."

Lawmakers also can consider starting local versions of the program by working with universities in their own states and tailoring scholarships to fit their particular needs. "That's an idea I've advocated for a long time," he says. "You form a partnership with a university and let them know exactly the kind of training you're looking for. You provide scholarship money to the university to generate those students who'll come to work for you."

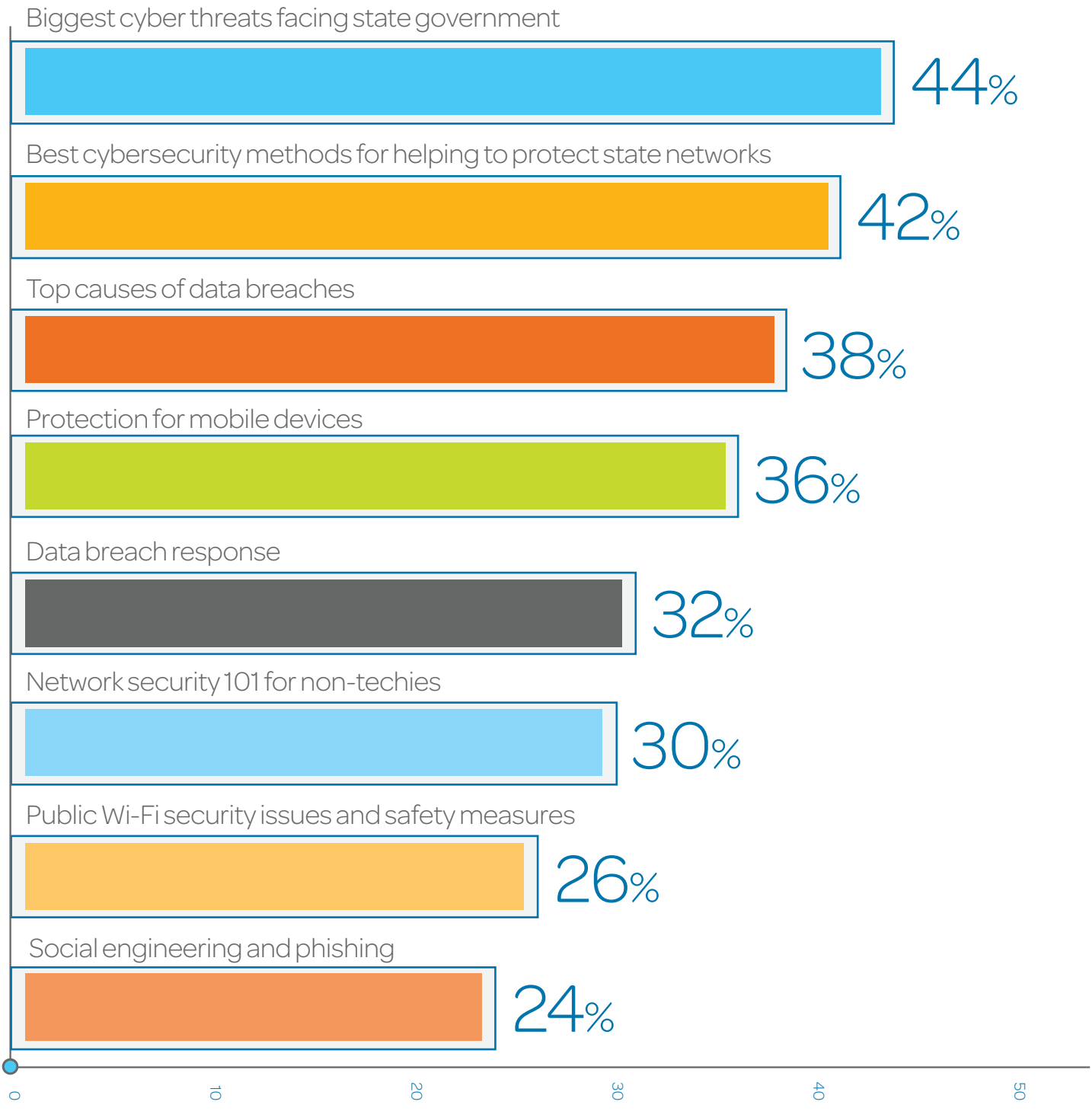
And, McDuffie adds, don't forget to play up the natural strengths of public service. Government jobs offer stability that's hard to match in the private sector, and many still provide attractive retirement benefits. They also appeal to individuals interested in giving something back.

"For people motivated to serve their communities, the state is an excellent place to do that," he says. "The people you serve are your neighbors, and that can be powerful."

Dr. Ernest McDuffie

Former Leader, National Initiative for Cybersecurity Education

Respondents said they would like to learn more about the following cybersecurity topics.



 Because survey participants were allowed to select more than one response, results will not add up to 100 percent.

You Need to Lead

We began this guide by noting that legislators have become keenly aware that cyber attacks pose a serious risk to state governments. And the survey data shows that they want more information on important topics such as the biggest threats, top causes of data breaches and best ways to help protect state networks.

But beyond seeking answers about attackers and technologies, lawmakers and senior government officials must be ready to champion broad cybersecurity initiatives.

"Those are great questions," says Jason Porter, vice president of security solutions at AT&T. "But it's also important to understand what you're trying to protect. A lot of what we talk about is finding alignment from the top down on what are your crown jewels—the resources you most need to protect."

Reaching Consensus

As we've mentioned throughout this guide, this is the type of overarching issue that demands engagement from legislators and top government officials. Achieving consensus on which assets need the highest level of protection involves input from stakeholders throughout the government enterprise. Elected leaders and senior officials must convene these activities and support their results.

Understanding the relative value of state information assets allows legislators and other policymakers to match resources to protection priorities. "So now in the budget cycle you can propose to protect the things that were identified as your most critical resources, and recommend spending X amount to cover them," Porter says. "You're not looking at technical issues like, 'I want to spend $1 million on firewalls.' You're saying, 'We'll spend this much to protect the state's utilities.'"

On a broader level, understanding the value of various state assets and the protection priorities tied to them forms the basis of state cybersecurity strategy. "These are very healthy discussions to have in the course of building your security policies and practices," Porter says. "It's much better to talk about these issues upfront than to establish them after you've been breached."

Next Steps

Ultimately, the advice on these pages is aimed at helping legislators become better informed, more engaged and more proactive. Lawmakers must be able to make smart decisions around a number of critical cybersecurity issues—including which assets to protect, how to provide adequate funding, attaining the right level of workforce training, maintaining appropriate oversight and staying abreast of their state's overall security posture.

Lawmakers clearly grasp the fact that cyber attacks are becoming more numerous and sophisticated. The risk they present to state information assets has never been greater. We hope the ideas, examples and suggestions presented here help you take action on improving your state's cyber-readiness.

Jason Porter

Vice President of Security Solutions, AT&T

Government is where innovation happens.

To learn more, visit
www.att.com/stateandlocal

AT&T