NATIONAL CONFERENCE of STATE LEGISLATURES

Budgeting for Cybersecurity

Introduction

How much does your state need to invest—in terms of money, person-hours, and other resources—to provide adequate cybersecurity to state systems? How can legislators determine whether a budget request is justified and sufficient?

Budgeting for cybersecurity is a challenging process, in part because implementing security measures is not a finite task: it's a series of interrelated, ongoing processes. Providing adequate cybersecurity resources should not be an afterthought; rather, it must inform every step of the process. States need to incorporate security considerations and testing into the entire systems development, acquisition, deployment, maintenance and support life cycle similar to the federal government. For example, the Office of 18F within the federal General Services Administration (GSA) has been working with states on automating security testing as part of the continuous deployment pipeline, ensuring that every new line of code or newly implemented system is automatically subjected to a battery of tests validating that it has not created a new vulnerability. The Office of 18F is part of the Technology Transformation Services, which is within the Federal Acquisition Service.

To successfully understand and budget for cybersecurity needs, state legislators and their legislative staff need to understand cyber terminology, better understand the cybersecurity risks that exist, and develop knowledge of what activities and resources can help them plan for, respond to, and recover from cybersecurity events when they do happen. Legislators and legislative staff need to understand that cyber preparedness is an ongoing process that requires a maintenance of effort and flexibility in budgeting to address emerging vulnerabilities and threats. Specifically, legislators must consider how cybersecurity functions are organized and who, within each state, is responsible and accountable for cybersecurity. This knowledge will directly affect the type, scale, and complexity of governance, organizational, and funding models that must be established.

Several factors—competing fiscal interests, a lack of understanding of cyber vulnerabilities, and legislators' incomplete knowledge of the current cyber "states" of their states—make this process difficult at best. We hope that the following guidance will help state legislators and legislative staff navigate the landscape of cybersecurity readiness and properly assess cybersecurity budget requests.

Sean McSpaden
Principal Legislative IT Analyst
Oregon

Monique Appeaning
Fiscal Analyst/Special Projects Coordinator
Louisiana

The National Conference of State Legislatures (NCSL) is the bipartisan organization that serves the legislators and staffs of the states, commonwealths and territories.

NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues and is an effective and respected advocate for the interests of the states in the American federal system.

NCSL has three objectives:

- To improve the quality and effectiveness of state legislatures.
- To promote policy innovation and communication among state legislatures.
- To ensure state legislatures a strong, cohesive voice in the federal system.

NCSL Executive Task Force on Cybersecurity

Co-Chairs:

- Assemblywoman Jacqui V. Irwin, California
- Senator Thomas C. Alexander, South Carolina

Task Force Members by state:

- Katy Proctor, director of research, Majority Research Staff, House of Representatives, Arizona
- Brandon Bjerke, legislative aide, Office of Assemblymember Jacqui Irwin, California
- Representative Don L. Parsons, Georgia
- Representative Mark M. Nakashima, Hawaii
- Diane Powers, deputy executive director, Legislative Services Agency, Indiana
- Terri Clark, director of technical services, Legislative Office of Information Services, Kansas
- Representative Diane St. Onge, Kentucky
- Senator Whitney H. Westerfield, Kentucky
- Monique Appeaning, fiscal analyst/special projects coordinator, Legislative Fiscal Office, Louisiana
- Representative Barry Ivey, Louisiana
- Senator Susan C. Lee, Maryland
- Representative Angelo J. Puppolo, Jr., Massachusetts
- Representative Pat Garofalo, Minnesota
- Representative Scott DeLano, Mississippi
- Representative Daniel Zolnikov, Montana
- Representative Kelly K. Fajardo, New Mexico
- Representative Jason Saine, North Carolina
- Representative Kent K. Smith, Ohio
- Sean McSpaden, Legislative Fiscal Office, Oregon
- Senator Louis P. DiPalma, Rhode Island
- Representative Stephen R. Ucci, Rhode Island
- Senator Jim Stalzer, South Dakota
- Representative Giovanni Capriglione, Texas
- Mark Humphrey, director, Information Systems Division, Legislative Council, Texas
- Senator Jim Dabakis, Utah
- Senator Wayne A. Harper, Utah
- Senator Todd D. Weiler, Utah
- Delegate Richard L. Anderson, Virginia
- Senator Frank Wagner, Virginia
- Senator Sharon R. Brown, Washington
- Representative Zack Hudgins, Washington
- Representative Cindy S. Ryu, Washington

NCSL Staff:

Susan Parnas Frederick,Washington, D.C.
Danielle Dean,Washington, D.C.
Pam Greenberg, Denver
Heather Morton, Denver

The mission of the NCSL Cybersecurity Task Force is to engage members in policy discussions, educate members and extend networking opportunities to legislative leaders on cybersecurity issues through a series of well-defined programs, webinars on key definitions and critical cyber policy issues as well as supporting private-public networks.

For their generous support of this task force, NCSL gratefully acknowledges these organizations:

- AT&T
- Consumer Data Industry Association
- IBM
- Kaspersky Lab
- Microsoft
- VMWare
- CompTIA
- CTIA-The Wireless Association
- Force Training Directorate, Office of the Assistant Secretary of Defense Readiness, Department of Defense
- MasterCard Worldwide
- Toyota Motor North America
- University of Phoenix
- Walmart

NCSL thanks the 18F Office of the General Services Administration, the states of Texas, Oklahoma, Oregon, Louisiana, Mississippi, Connecticut, Michigan, Illinois, and the National Association of State Information Officers (NASCIO) staff for assisting with this document.

Jacqui V. Irwin
California State Assemblywoman
Co-Chair, NCSL Task Force on Cybersecurity

Thomas C. Alexander
South Carolina State Senator
Co-Chair, NCSL Task Force on Cybersecurity

Cybersecurity Governance, Responsibility and Accountability

Cybersecurity governance is a nuanced term. It refers to the decision-making processes surrounding and oversight of the roles, responsibilities, processes, and practices state executives use to establish and maintain effective statewide, branch-wide, or agency-specific cybersecurity programs.

Ultimately, the state executives responsible for cybersecurity governance must provide the leadership, oversight, organizational structures and resources needed to protect state information, networks and information systems. State executives are also responsible for achieving cybersecurity objectives in a way that is compliant with statutory and contractual obligations.

Risk management plays a large role in cybersecurity governance. According to ISACA, previously known as the Information Systems Audit and Control Association, an especially useful definition for risk management is, "a process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss. This is usually accomplished by ensuring that the impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost."

Before considering actual budget numbers, legislators and legislative staff should consider the two following factors needed for successful cybersecurity measures:

1. The continuous and efficient operation of systems, networks and infrastructure, is vital to protect and serve the people of and businesses operating within each state. Unfortunately, state government information systems, networks and critical infrastructure are threatened by increasingly sophisticated cyber attacks.

2. The clear identification of cybersecurity needs and governance in each branch of government (legislative, judicial and executive) is essential. State legislators and legislative staff responsible for oversight and budget decisions must be familiar with governance policies, which state leaders are responsible for making relevant decisions, and which specific individuals or organizations are responsible and accountable for ensuring that the information, systems, networks and infrastructure under state government control are appropriately protected and secured.

In some states, responsibility and accountability for cybersecurity (at least at the branch level) are vested in single state officials (for example, with the state chief information officer who exclusively serves the executive branch) or with a centralized information technology (IT) organization (for example, a state Department of Information Technology). In other states, responsibility and accountability are decentralized and dispersed across, and sometimes within, each branch. It is essential, within each branch or at the agency level, to have clear, direct responsibility and accountability for cybersecurity programs and operations; this will help ensure strategic alignment, policy, and standards compliance, while minimizing the "pointing of fingers" when something bad happens and reducing the unnecessary duplication of scarce cybersecurity resources.

Further, in decentralized environments, risk-management decisions—whether to avoid, transfer, mitigate, or accept cyber-related risks—are often made at the agency level. This practice can be problematic. Independent, uncoordinated decisions made using different criteria or based on different risk tolerances may work at the agency level, but could expose multiple agencies, or perhaps the entire enterprise, to increased risk. This practice could also complicate budgeting decisions, as different agencies address cybersecurity concerns differently.

State legislators and legislative staff must take steps to understand the governance, accountability, oversight, and operating environment within which cybersecurity-related budget requests are being formulated. Armed with that knowledge, they will be better positioned to ask better questions about, and to identify and evaluate the specific merits of those requests.

Cybersecurity Strategy, Program and Assessments

The foundation for effective risk management is a comprehensive risk assessment, based on a solid understanding of the state's risk universe. It is not possible to devise a relevant risk management program if there is no understanding of the nature and extent of risk to information resources and the potential impact on the organization's activities. Risk management, the development of business impact assessments, the creation of an IT asset inventory, and risk analysis are fundamental prerequisites to developing a meaningful security strategy. ISACA - 2015 Certified Information Security Manager Review Manual 14th Edition, ISACA, 2015

Business Impact Analysis (BIA) – An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. Source: National Information Assurance Glossary, Committee on National Security Systems (CNSS) Glossary Working Group, CNSSI 4009, 2010.

Ideally, cybersecurity strategy needs to change as quickly as new information about a system is obtained. Statewide and/or individual state agency cybersecurity-related budget requests should support the implementation of formal cybersecurity strategies developed and updated over time in response to formally conducted risk, vulnerability and business-impact assessments.

State legislators and legislative staff should expect those responsible for cybersecurity to have, and regularly update a formal cybersecurity strategy. In decentralized states, agency strategies and plans should align with and support the statewide cybersecurity strategy. Alignment and coordination of strategy is key to establishing a strong cybersecurity foundation for your state.

Regular risk assessments are key to maintaining cybersecurity. The National Institute of Standards and Technology (NIST) defines risk assessment as the process of identifying risks to the operation of an organization's information systems through its functions, assets, mission, image, reputation and individuals. The assessment incorporates analyses of threats and vulnerabilities and considers how security controls can mitigate those threats.[1] Qualified internal staff or third-party staff should conduct them at least once per biennium, if not more frequently. Statewide and agency officials may be reluctant to share detailed risk assessment findings. That said, those responsible for cybersecurity should be able to disclose when their last comprehensive risk assessment was conducted, whether the risk assessment was conducted internally or with the assistance of skilled third parties, and, at an appropriate level

---

[1] National Institute of Standards and Technology (NIST) Special Publication ***800-53,*** Special Publication 800-53A; Special Publication 800-37.

of detail, what key risks will and will not be addressed based on whether the current budget request is approved or denied.

Vulnerability assessments of key facilities, data centers, networks, or specific information systems, and more should be conducted based on priority (i.e., mission criticality) on at least a monthly or quarterly, if not continual, basis. In contrast to a risk assessment, a vulnerability assessment requires a systematic examination to determine the adequacy of security measures, identifies security weaknesses and deficiencies and provides data from which to predict the effectiveness of proposed security measures for information systems or products. (NIST SP 800-53A; Committee on National Security Systems (CNSS) Glossary, CNSS Instruction No. 4009 (CNSSI No. 4009) (Apr. 6, 2015) (CNSSI-4009)).

For mission-critical information systems and/or those systems for which critical vulnerabilities have been discovered, those responsible for cybersecurity should consider conducting more detailed and thorough penetration testing, usually via contract with specialized cybersecurity firms. Penetration testing simulates real-world attacks to identify different ways hackers could use to circumvent the security features of an application, system or network. (NIST SP 800-115)

People responsible for statewide or agency-centric cybersecurity should make initial and ongoing budget requests to ensure that a regular regimen of risk assessments, vulnerability assessments, and penetration tests (as warranted) is incorporated into the statewide and/or agency-based budget moving forward.

Statewide and agency officials may be understandably hesitant to share detailed vulnerability assessment or penetration test findings, even though this information is needed to support specific budget requests. In many states, this kind of information is clearly exempt from public disclosure because the disclosure itself could constitute a security incident. With the legitimate need to balance seemingly competing interests, state legislators and legislative staff should work closely with those responsible for cybersecurity to establish so-called “rules of engagement.” These rules should provide the legislative branch with the information it needs for appropriations and oversight while protecting access to and disclosure of sensitive cybersecurity-related information.

Cybersecurity Education and Training

IT Security Education – Seeks to integrate all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and proactive response.

SOURCE: NIST SP 800-50

IT Security Awareness and Training Program – Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed.

SOURCE: NIST SP 800-50

It has been said that cybersecurity is a team sport. Data on cybersecurity incidents from the past few years shows that the level of employee cybersecurity awareness and cooperation can dramatically help or hinder an organization’s overall cybersecurity efforts. With that in mind, those responsible for statewide, branch-wide, or agency-centric cybersecurity efforts should formulate one-time and ongoing budget requests for consistent, standardized employee cybersecurity awareness training.

At the technical level, the cybersecurity landscape is constantly shifting. The cybersecurity workforce within state governments are often outgunned and outnumbered, with limited reinforcements available on the horizon. Cybersecurity professionals with the requisite knowledge, skills, and abilities are scarce and in high demand across the public, private, and nonprofit sectors. Although faced with a daunting task, those responsible for cybersecurity must create meaningful and relevant technical training programs and opportunities for their information security and information technology staff. Specialized cybersecurity training can be costly or hard to access, which makes creating program-, state- or agency-specific training even more important.

People responsible for cybersecurity should be prepared to make justified budget requests for cybersecurity training and should be able to communicate the importance of employee awareness and technical training in contrast to other pressing state priorities.

Relatedly, state legislators and legislative staff should be open to reasonable rationale for cybersecurity-awareness and -training budget requests, and should work, to the best of their abilities, to support adequate funding for these important activities. NCSL's list of state-specific trainings provides examples of training resources in state governments, and is a good place to begin identifying resources for your organization. Please note that most of these trainings are for executive-branch staff.

Hardware and Software

Well-constructed budget requests should include money for hardware, software, and professional services costs related, but not limited, to the following:

- IT asset inventory
- Vulnerability scanning
- Firewalls that limit access between networks and systems following a specific security policy
- Intrusion detection systems (host-based, network-based)[2]
- Intrusion-prevention systems[3]
- Anti-virus, anti-spam/spam-filtering software and anti-malware software

[2] Intrusion Detection Systems (IDS) – (Host-Based) IDSs operate on information collected from within an individual computer system. This allows host-based IDSs to determine exactly which processes and user accounts are involved in an attack on the operating system. Host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks. SOURCE: SP 800-36; CNSSI-4009. Intrusion Detection Systems (IDS) – (Network-Based) IDSs, which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment. SOURCE: SP 800-36; CNSSI-4009

[3] Intrusion Prevention System(s) (IPS) – System(s) can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. SOURCE: SP 800-36; CNSSI-4009

- Log management and monitoring software[4]

Some of these specialized hardware and software tools are best deployed within a centrally managed IT environment; others can effectively be deployed within local IT environments.

The acquisition of hardware and software often calls for initial and ongoing investments. With that in mind, those responsible for statewide, branch-wide, or agency-centric cybersecurity efforts should coordinate their budget requests, acquisitions, and subsequent deployments related to these specialized hardware and software tools. Cybersecurity-responsible employees will leverage existing enterprise hardware and software investments, follow established standards, and avoid requesting funding that is redundant to current investments in hardware, software, and professional services, unless these requests are absolutely justified.

Third Party-managed Services

States are strongly encouraged to "in-source" cybersecurity as a core state government function. In some instances, those responsible for cybersecurity at the statewide, branch-side, or agency-centric level cannot realistically hire, train, and retain the requisite number of skilled and experienced cybersecurity staff. In those situations, the agencies involved may make budget requests for the acquisition and use of third-party cybersecurity consulting and managed services in, but not limited to, the following areas:

- Security operations center (SOC) services
  - An information security operations center (ISOC) includes the people, processes, and technologies involved in providing cybersecurity situational awareness through the detection, containment, and remediation of cybersecurity-related threats. A SOC manages incidents for the enterprise by properly identifying, analyzing, communicating about, acting on/defending against, and reporting them. A SOC is typically a facility where cybersecurity experts monitor, assess, and defend enterprise information systems, including websites, applications, databases, data centers and servers, networks, desktops, and other endpoints. A SOC should be managed internally but, in the absence of internal capabilities, could be managed by a third-party contractor specializing in providing managed cybersecurity services.

- Firewall services
  - A managed firewall service provides 24/7 firewall administration, log monitoring, and response to security and device-related events.

---

[4] A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant to a particular system. Virtually all software applications and systems produce log files. Log management is the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an information system.
Effective log management is essential to both security and compliance. Monitoring, documenting and analyzing system events is a crucial component of security intelligence (SI). Regarding compliance, regulations such as HIPAA, have specific mandates relating to audit logs. Log management software automates many of the processes involved.
http://searchitoperations.techtarget.com/definition/log-management

- Intrusion detection system (IDS) and intrusion prevention system (IPS) services
    - IDS/IPS services monitor state networks, servers, and information systems for suspicious traffic and offer near-real-time surveillance of the data traffic flowing through state networks. Managed IDS and IPS services use these systems to scan for unauthorized access attempts and provide the tools needed to help defend the enterprise.

- Incident and breach response services
    - Service providers help organizations plan for, manage, and recover from data breaches and other attacks to information systems and networks. Response services can be provided remotely or onsite and are, typically, bundled as part of a cybersecurity firm's monitoring, assessment, and alerting service offerings.

- Monitoring, detection, and alerting services
    - Cybersecurity firms provide 24/7 network, server and application monitoring, log management, and alerting services to protect against threats and ensure compliance with regulatory requirements. They also provide comprehensive security reports detailing critical security events, threats, and vulnerabilities. In addition, firms may provide or offer to manage an organization's security information and event management (SIEM) solution to more efficiently and effectively detect and apply countermeasures to advanced threats.

- Forensic investigation and analysis services
    - Some cybersecurity firms provide forensic investigation and analysis services designed to identify, collect, examine, analyze, preserve the integrity of and maintain a strict chain of custody for any computer-related evidence and data related to an incident or breach regardless of whether it may lead to criminal investigation or prosecution.

- Cyber Analytics
    - Cyber analytics applies big data tools and techniques to capture, process, and refine network activity data; applies algorithms for near-real-time review of every network node; and employs visualization tools to easily identify anomalous behavior required for fast response or investigation. Cyber analytics tools allow security analysts to more easily recognize patterns of activity that represent network threats. (National Association of State CIOs (NASCIO) Advanced Cyber Analytics: Risk Intelligence for State Government, 2016, page 3).

Cybersecurity-related Audits

The goal of any cyber-related audit is to understand and evaluate an agency's ability to identify, manage, and mitigate the risks facing the agency's facilities, networks, information systems, and data. State legislatures have a fundamental role in ensuring that security protocols are established and communicated effectively and efficiently. Legislators can ensure accountability in agency compliance with the states' established security framework. Several state legislatures have created offices to conduct research studies and audits to evaluate enterprise-wide policies and programs and identify gaps, suggest improvements, and reduce costs. Where possible, costs for these audits for the auditing entity and for affected agencies should be budgeted for in advance. To budget for audits, legislators should understand the process, as it may help legislators identify funding priorities.

Internal Audits

Step 1: Ensure regular auditing of cyber-related activities. Ensuring that current audit offices or boards in your state include a cybersecurity review component is an essential first step in evaluating cybersecurity-related audit functions. How are audits initiated in your state? Are audits conducted based on legislative request, or is there a required annual audit?

Step 2: Require actionable improvements. Audits should assess and identify opportunities to strengthen enterprise security. Internal audits have a duty to inform—are the controls in place and functioning correctly?

Step 3: Understand each agency's multi-year strategy. Understand the agency's current operational state, where the agency is going, and the minimum expected cyber practices needed. The audit will tell you where the agency currently stands and what changes it needs to make within the next one, two or five years. How often is an audit needed? Some agencies will need more frequent oversight based on the type of information they are storing and how the agency information systems interact with the rest of the network.

Executive/Legislative Audits

In some states, a joint legislative audit committee or a joint legislative committee on information management and technology may have explicit statutory authority to conduct cyber-related studies and audits. In other states, responsibility for these kinds of studies and audits are placed with the secretary of state or some other agency that serves as the state's independent auditor.

State legislators and legislative staff should work to gain a clear understanding of legislative authority and responsibility for cyber-related studies and audits. As needed and appropriate, responsible legislative committees should develop an audit plan to be implemented by internal or contracted staff. Alternatively, if statutory authority and responsibility for cyber-related studies and audits is placed within another state agency, legislative committees with oversight responsibility should ensure that the state's independent auditor develop a cyber-related audit plan to be implemented by internal or contracted staff.

- Does your state have a legislative auditing office or committee with statutory authority to evaluate, validate, and report on the security practices of state government?
- Is the statutory authority placed with another entity within state government (perhaps the secretary of state)?
- Can the auditing entity perform comparable evaluations for all three branches of government and for other public bodies (for example, local governments, schools or special districts)?
- Are the costs for cyber-related audits budgeted for in advance or are they unexpected/unbudgeted expenses?

Federal Government Audits

State governments partner with the federal government to administer federal programs and deliver services to citizens, such as Internal Revenue Service (IRS) compliance, Health Insurance Portability Accountability Act compliance and Family Educational Rights and Privacy Act compliance. Because of this partnership, the state becomes subject to rules that govern the use and security of data that is shared by federal programmatic agencies. For example, state departments of revenue commonly use federal tax information (FTI) and are thus subject to the regulations contained within IRS Publication 1075. Exchanging criminal justice information with the federal government subjects states to compliance with Federal Bureau of Investigation

Criminal Justice Information Services (CJIS) Security Policy. The list of federal regulations and laws with which states must comply is numerous and diverse, and affect most state government program areas.

The federal compliance regime also requires auditing, which occurs in regular intervals (e.g. once every two years). If federal auditors reveal "findings," the state must address and remediate those findings within an established timeframe (e.g. 30 days or 60 days). State CIOs, chief Information security officers (CISOs), and affected agencies have faced some difficulty with the federal regulatory process because of the complex and duplicative nature of the federal compliance regime and inconsistent audit outcomes.

Achieving and maintaining compliance with these regulations, as well as preparing for, participating in, and responding to findings from these required audits can have operational and budgetary implications for affected agencies.

State legislators and legislative staff should work with those responsible for cybersecurity to better understand the potential operational and budgetary impacts associated with these federal cybersecurity regulations and associated audits, and should work, to the best of their abilities, to support adequate funding for these important activities.

Audits of Third Party Hosting Facilities

State governments across the nation are increasingly considering the use of third party "Cloud" service providers to augment or replace internal systems or service offerings currently provided within an agency, branch-wide, or statewide data center. These companies typically provide: Infrastructure as a Service (IaaS); Software as a Service (SaaS); Platform as a Service (PaaS); and, more recently, Data as a Service (DaaS); to public, private and non-profit sector clients within a state, regionally, nationally or internationally. Note: This shift from capital expenditures to operational expenditures may or may not reduce overall costs. In some instances, this shift may improve cybersecurity of state data and systems. In some instances, this shift may make securing state data and systems more complicated and costly.

State legislators and legislative staff should work with those responsible for cybersecurity to better understand how extensive the use of a "Cloud" services platform is at the agency, branch-wide, or statewide levels. Those responsible for cybersecurity should be expected to communicate to state legislators and legislative staff the measures being taken to ensure that state data and information systems, and the systems, infrastructure and services provided by the third party "Cloud" services provider for state use remain secure over time. Further, they should provide state legislators and legislative staff with assurances that chosen, third party "Cloud" services providers meet state and federal cybersecurity requirements, are conducting and sharing with the state the results from regular cybersecurity assessments and audits, and that the state's "right to audit" the "Cloud" services provider's hosting facility (where possible and appropriate) has been preserved.

Cybersecurity Insurance

Cyber insurance may be helpful to your state because it places a dollar value on your state's cyber risk. The underwriting process can help your state identify cybersecurity gaps and opportunities for improvement. Understanding how cyber insurance works and the costs associated with it will assist policymakers in making sound budget recommendations in this area.

Some initial questions to consider and ask:

Does your state have cyber insurance? How is the yearly cost calculated?

> According to the National Association of State Information Officers' (NASCIO) 2017 CIO Survey, 38 percent of respondents indicated that their states have obtained cyber insurance. This represents an increase of 18 percent from 2015. In a decentralized state, cost may be determined on an agency-by-agency basis.

What is covered under your state's cyber insurance policy?

> In the event of a breach, coverage usually includes public relations, mailings to impacted constituents, and forensics.

If your state has cyber insurance, ask to see the underwriting document to see which agencies are insured and the cost.

> States can pick and choose which agencies should carry cyber insurance; in most cases, departments/agencies that house sensitive information are candidates for insurance.

Where is your state on the NIST scale?

> Insurers will look at existing state frameworks. If a state has something akin to the NIST protocol and has tested all systems, cyber insurance costs will be lower.

Conclusion

Benjamin Franklin once said that, "an ounce of prevention is worth a pound of cure." Just like fire safety at the local level, states must exercise a reasonable level of due diligence and due care when it comes to identifying cyber risks and vulnerabilities, and employing reasonable measures to protect state networks, information, and information systems. We hope this Budgeting for Cybersecurity Guide will help you better understand and evaluate budgeting priorities for appropriate cybersecurity expenditures in your state. This Guide is meant to be a starting point for you as you discuss and respond to cybersecurity-related budget requests in your jurisdictions and is meant to help you properly assess and address your state's unique cyber risks and vulnerabilities and their associated costs.