Deloitte.

2020 Deloitte-NASCIO Cybersecurity Study

Key Findings & Recommendations

Deloitte. Insights

NASCIO Representing Chief Information Officers of the States

2020 Deloitte–NASCIO Cybersecurity Study

States at risk: The cybersecurity imperative in uncertain times

A JOINT BIENNIAL REPORT (6TH EDITION) FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

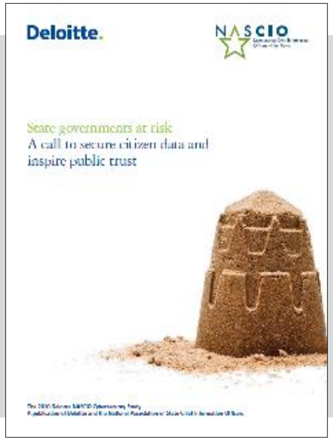
December 16, 2020

2020 Deloitte-NASCIO Cybersecurity Study – *Background and Overview*

States at risk: The cybersecurity imperative in uncertain times

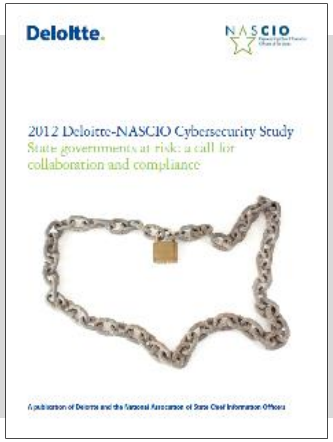
- 2020 survey report marks Deloitte and NASCIO’s sixth joint, biennial state & local government cybersecurity report.
- A record 51 state & territory chief information security officers participated in the 2020 survey, including the NYS CISO.
- 3 key takeaways:
  1. COVID-19 has challenged continuity and amplified gaps
  2. Connecting the cyber dots across state, local, and higher education
  3. Strength, consistency, and enforcement in numbers
- Updated progress on the 2018 survey report’s “Bold Plays:”
  1. Advocate for dedicated cyber program funding
  2. CISOs as an enabler of innovation, not a barrier
  3. Team with the private sector and higher education

2010


Deloitte.
NASCIO
State governments at risk
A call to secure citizen data and inspire public trust

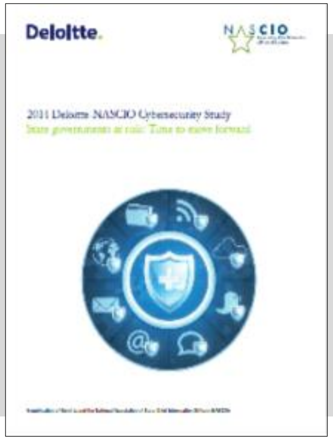
A call to secure citizen data and inspire trust

2012


Deloitte.
NASCIO
2012 Deloitte-NASCIO Cybersecurity Study
State governments at risk: a call for collaboration and compliance

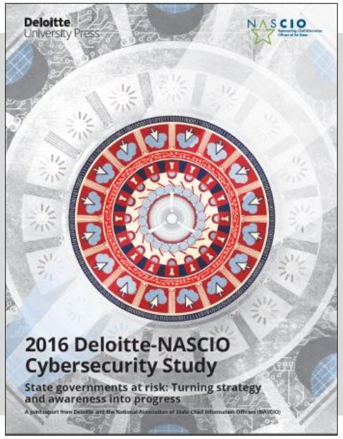
A call for collaboration and compliance

2014


Deloitte.
NASCIO
2014 Deloitte-NASCIO Cybersecurity Study
State governments at risk: Time to move forward

Time to move forward

2016


Deloitte University Press
NASCIO
2016 Deloitte-NASCIO Cybersecurity Study
State governments at risk: Turning strategy and awareness into progress

Turning strategy and awareness into progress

2018

Deloitte. Insights
NASCIO
2018 Deloitte-NASCIO Cybersecurity Study
States at risk: Bold plays for change

Bold plays for change

2020

Deloitte. Insights
NASCIO
2020 Deloitte-NASCIO Cybersecurity Study
States at risk: The cybersecurity imperative in uncertain times

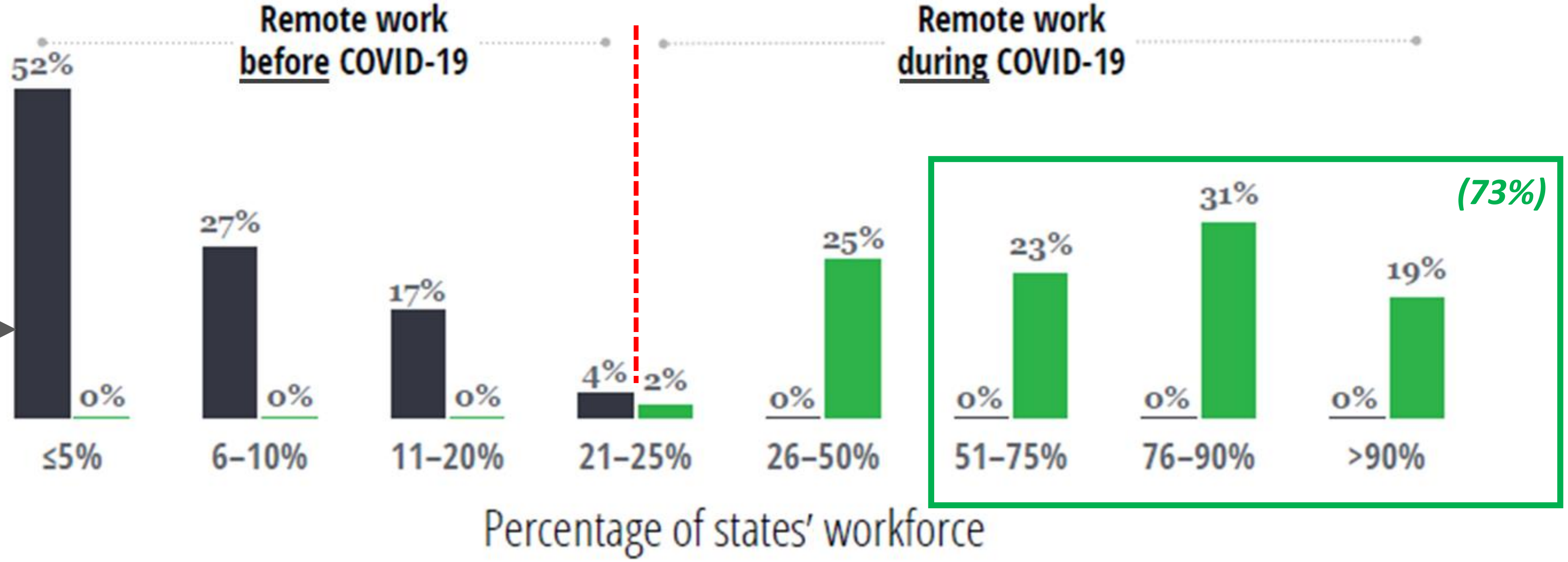
The cybersecurity imperative in uncertain times

Key takeaway 1: COVID-19 has challenged continuity and amplified gaps

The pandemic widened cyber challenges: budget, talent, threats, and the need for partnerships

States' remote workforce before and during COVID-19

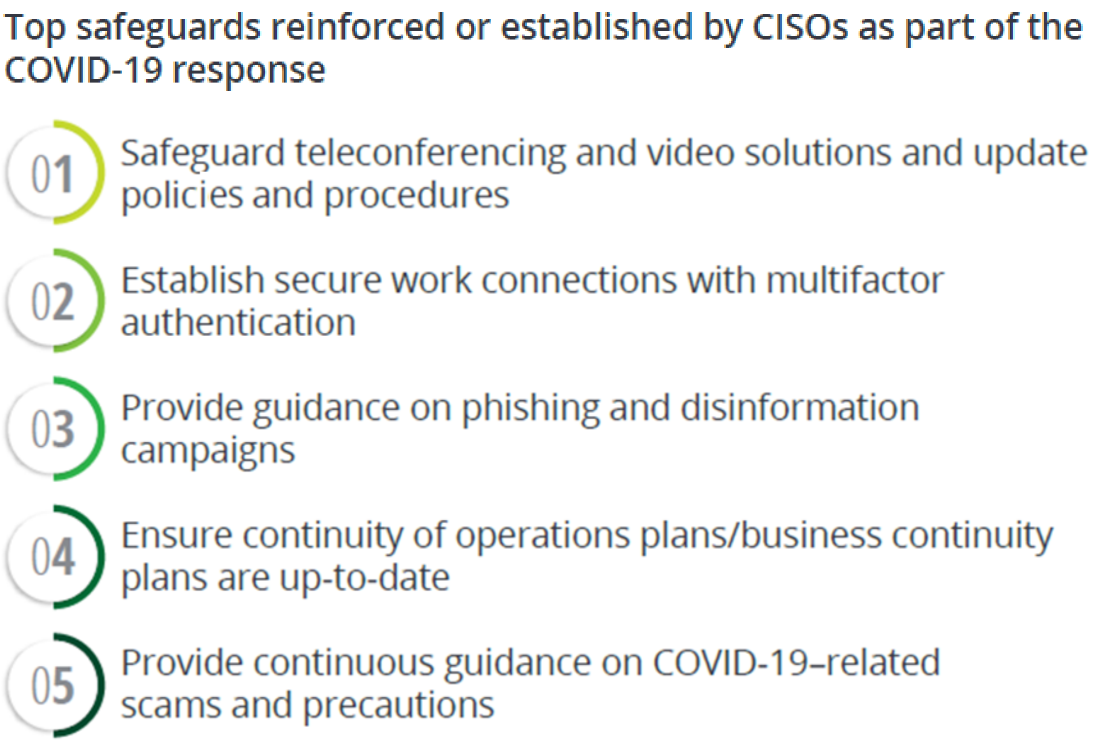
What percentage of your workforce worked remotely ***before COVID-19?*** ***And during?***



Before the pandemic, 52% of respondents said *less than 5% of staff worked remotely*.

Key takeaway 1: COVID-19 has challenged continuity and amplified gaps (cont'd)

The pandemic widened cyber challenges: budget, talent, threats, and the need for partnerships



Top safeguards reinforced or established by CISOs as part of the COVID-19 response

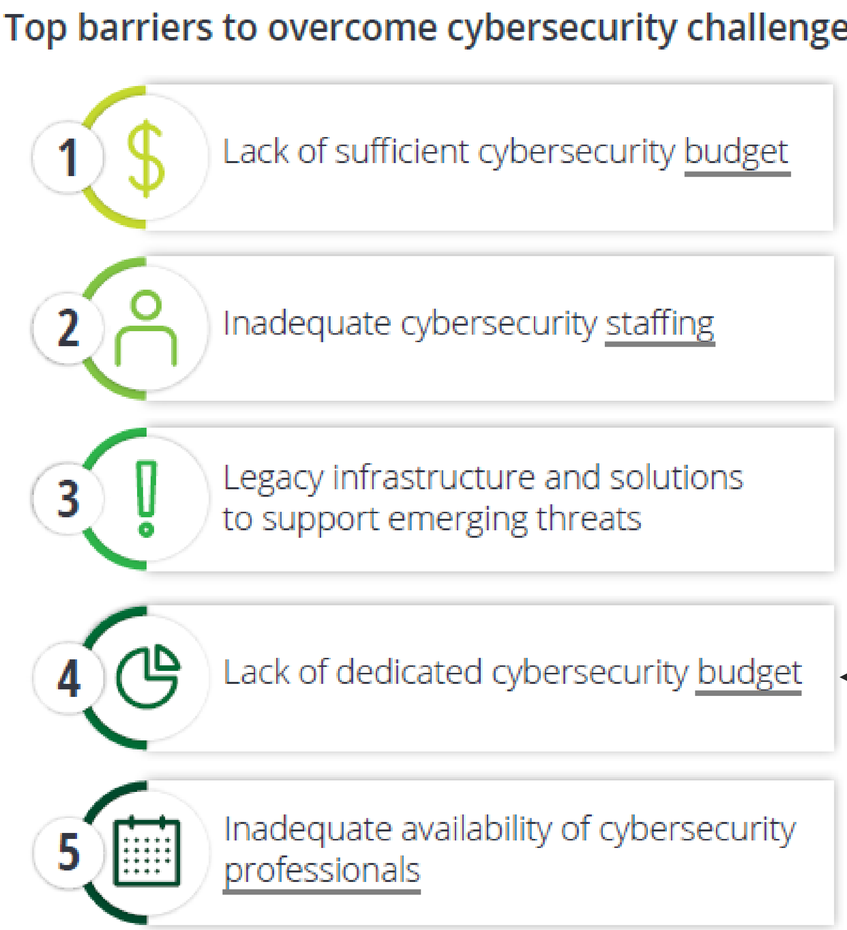
01 Safeguard teleconferencing and video solutions and update policies and procedures

02 Establish secure work connections with multifactor authentication

03 Provide guidance on phishing and disinformation campaigns

04 Ensure continuity of operations plans/business continuity plans are up-to-date

05 Provide continuous guidance on COVID-19–related scams and precautions



Top barriers to overcome cybersecurity challenges

1 Lack of sufficient cybersecurity budget

2 Inadequate cybersecurity staffing

3 Legacy infrastructure and solutions to support emerging threats

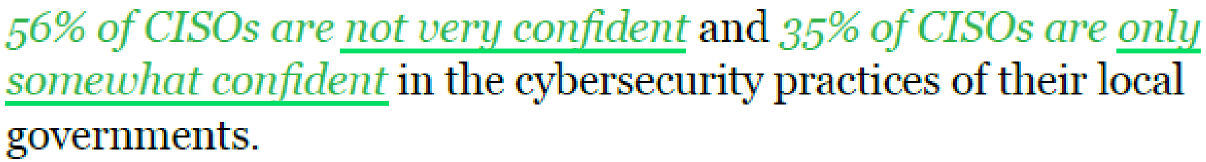
4 Lack of dedicated cybersecurity budget

5 Inadequate availability of cybersecurity professionals

← 2018 report "Bold Play"

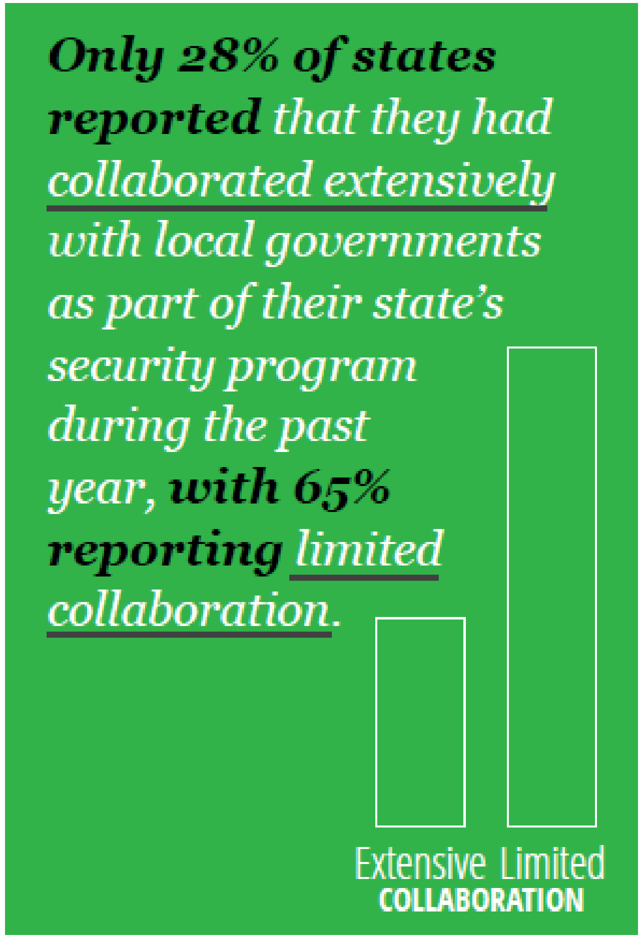
Key takeaway 2: Connecting the cyber dots across state, local, and higher education

Collaboration with local governments and public higher education is critical to managing increasingly complex cyber risk within state borders



56% of CISOs are not very confident and *35% of CISOs are only somewhat confident* in the cybersecurity practices of their local governments.

- A "**whole-of-state-approach**"—one that engages local, city and county governments, legislative and judicial branches of government, and public higher education—could potentially strengthen cybersecurity at all levels of government.
- States should consider increasing their leadership and influencing role in how federal grant funding, provided through the annual Homeland Security Grant Program (HSGP) and proposed *State and Local Cybersecurity Improvement Act* (H.R.5823), etc., is most effectively and efficiently invested to enhance local government cybersecurity.



***Only 28% of states reported** that they had collaborated extensively with local governments as part of their state's security program during the past year, **with 65% reporting** limited collaboration.*

Key takeaway 3: Strength, consistency, and enforcement in numbers

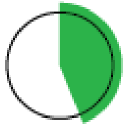
A centralized model may help CISOs position cyber to improve agility, effectiveness, and efficiencies

3 models of cybersecurity governance:

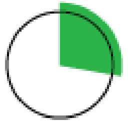
- **Decentralized** model – *Individual state agencies are on their own for cyber services and execution with only policy guidance from the State CIO and/or CISO*
- **Federated** model – *State CISOs are responsible for centralized policy with a mix of centralized shared services and agency-led services specific to each agency*
- **Centralized** model – *Centralized governance structure where State CISO is responsible for cybersecurity for all state agencies*

Potential advantages of a centralized model include:

- With the state CISO at forefront, higher agency adoption of enterprise security services
- A centralized cybersecurity budget elevates overall importance of cyber, helping to improve a state's overall cybersecurity posture
- Increased agility and efficiency in deploying scarce cyber resources to the agencies and programs with the highest need
- Improved scale in cross-training and upskilling may lead to more career growth opportunities for cyber staff
- Opportunity to leverage federal funding (e.g. state-level grants) for implementing and delivering cybersecurity services in a shared model to benefit all agencies
- If all states were to follow a *centralized model*:

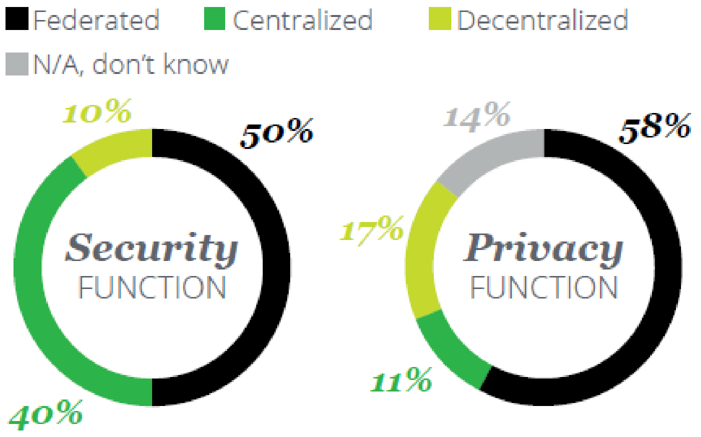


44% of states would have more than 51 full-time employees

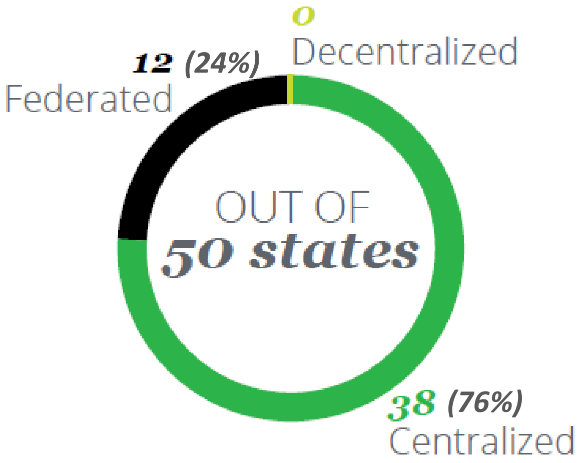


28% of states would have 26–50 full-time employees

Cybersecurity and privacy functions: Operational model



Most states indicate that a centralized operating model can best reduce cybersecurity risk



Bold Play 1: Advocate for dedicated cyber program funding

There has been limited progress since 2018 on dedicated state cybersecurity budget line items

(36%)
Only 18 states have a cybersecurity budget line item.

Average cybersecurity spend in 2020 (percentage of IT budget)

1–3% Most state governments

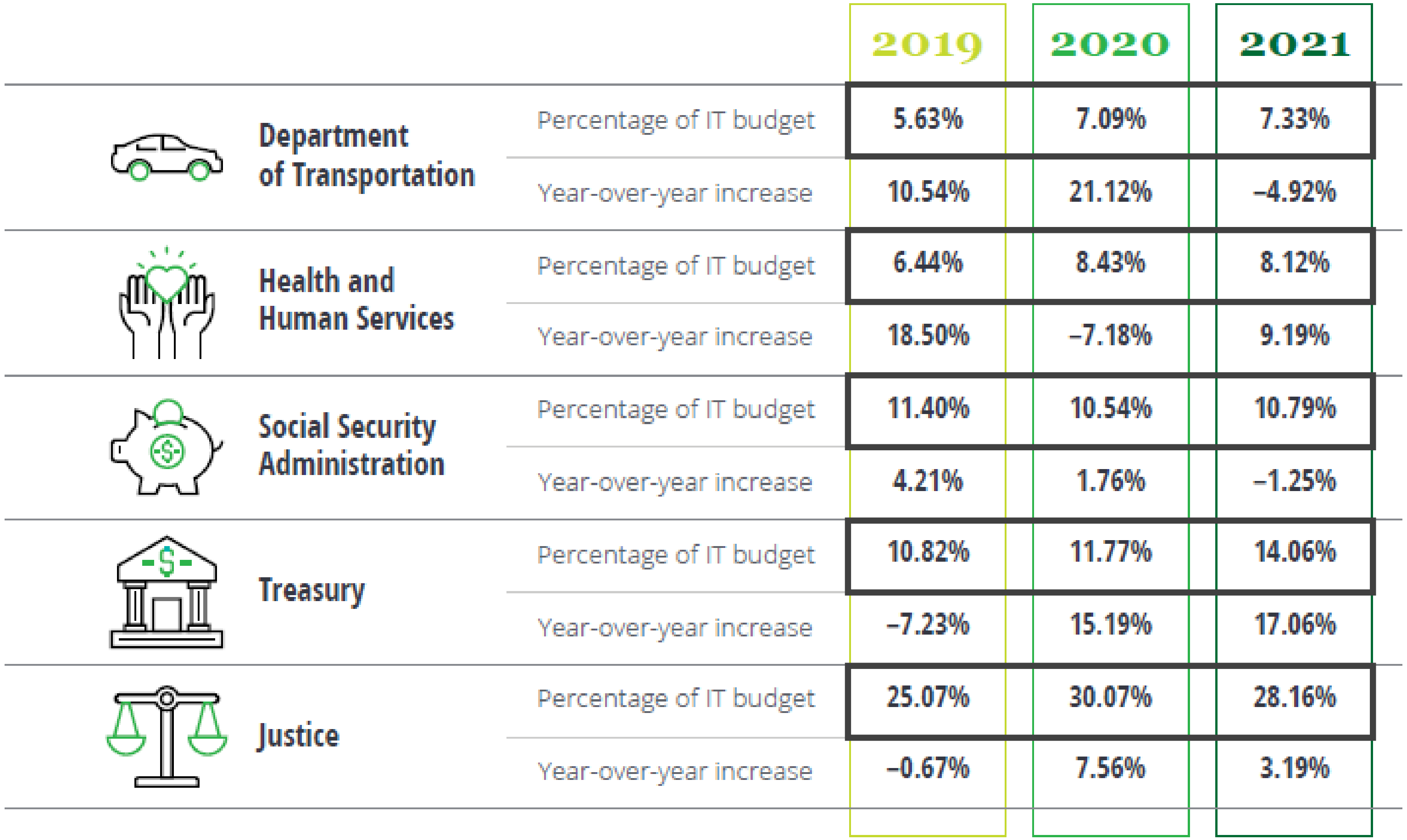
16.3% Federal agencies*

10.9% Financial institutions

*Federal civilian agencies under the CFO Act of 1990.

Federal agencies spend a greater percentage of their IT budgets on cybersecurity than many states

Federal agencies' cybersecurity budgets as a percentage of total IT budget and year-over-year growth

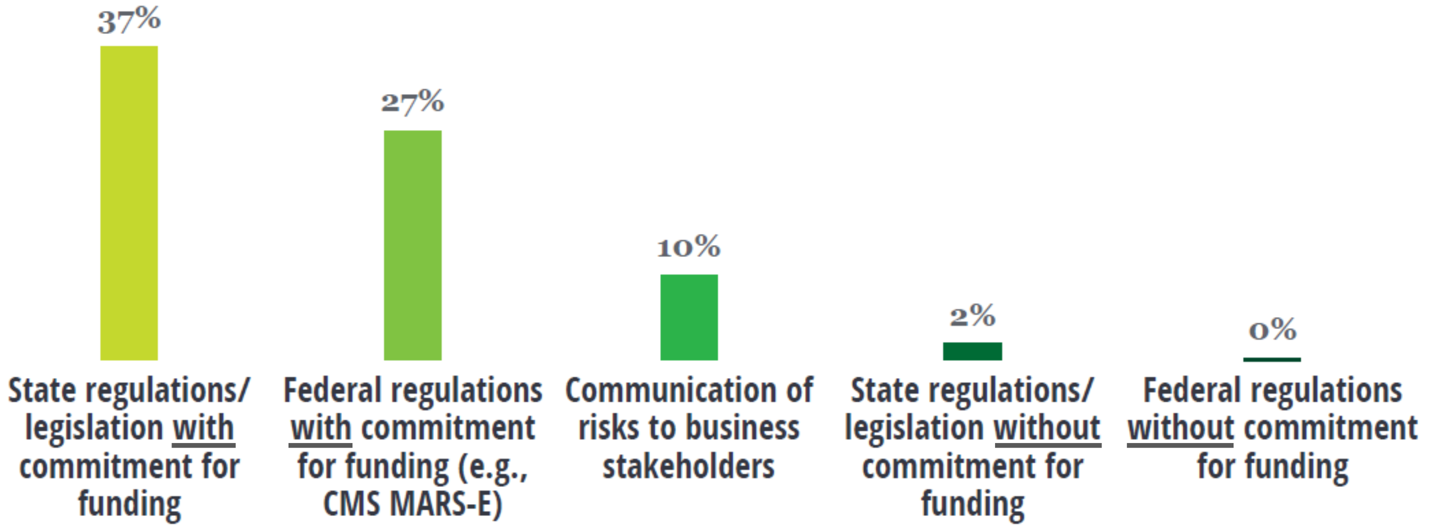


		2019	2020	2021
Department of Transportation	Percentage of IT budget	5.63%	7.09%	7.33%
	Year-over-year increase	10.54%	21.12%	–4.92%
Health and Human Services	Percentage of IT budget	6.44%	8.43%	8.12%
	Year-over-year increase	18.50%	–7.18%	9.19%
Social Security Administration	Percentage of IT budget	11.40%	10.54%	10.79%
	Year-over-year increase	4.21%	1.76%	–1.25%
Treasury	Percentage of IT budget	10.82%	11.77%	14.06%
	Year-over-year increase	–7.23%	15.19%	17.06%
Justice	Percentage of IT budget	25.07%	30.07%	28.16%
	Year-over-year increase	–0.67%	7.56%	3.19%

Bold Play 1: Advocate for dedicated cyber program funding (cont'd)

Added challenges of unfunded and non-harmonized cyber regulatory mandates

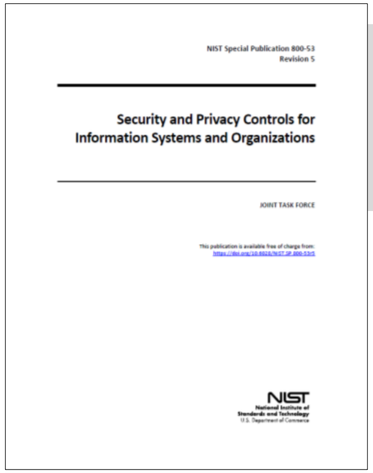
Which regulations are most effective at improving cybersecurity posture and reducing risk?



There are several federal regulations that require States receiving federal information to implement specific security controls and comply with associated compliance audits. These regulations often include conflicting security requirements and inconsistent levels of financial assistance to help offset compliance costs.

Examples of such regulatory compliance standards include:

- IRS Publication 1075
- FBI Criminal Justice Information Services Security Policy (FBI-CJIS)
- CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Agencies Exchanging Electronic Information with the Social Security Administration


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

From NASCIO President testimony to the House Oversight Committee, Intergovernmental Affairs Subcommittee (7/18):

Federal Regulation:	IRS Publication 1075	FBI-Criminal Justice Information Services	SSA Electronic Information Exchange Security Requirements and Procedures
Unsuccessful logins	Information system must enforce a limit of 3 consecutive invalid login attempts by a user during a 120 min period, and automatically lock account for at least 15 mins.	Where technically feasible, system shall enforce limit of no more than 5 consecutive invalid attempts, otherwise locking system for 10 mins.	SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information…SSA recommends no fewer than three (3) and no greater than five (5).

From U.S. GAO Report (5/20): "Among the four federal agencies (IRS, FBI, CMS & SSA) [with requirements to secure data that states receive], the **percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent**.

Coordinating with state and federal agencies when assessing state agencies' cybersecurity may help to minimize states' cost and time impacts and reduce associated federal costs."

Bold Play 2: CISOs as an enabler of innovation, not a barrier

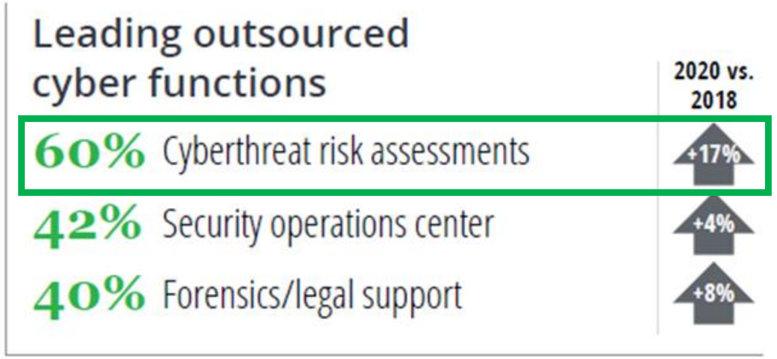
The 2018 study challenged state CISOs to elevate role of cybersecurity by taking a leadership role in digital modernization and embracing Artificial Intelligence, IOT, and Smart Government

- Emerging technologies are still not yet a high priority among state CISOs when compared to operational cybersecurity initiatives.
- As resources allow, state CISOs could look to Financial Services and other industry sectors in prioritizing cybersecurity-focused investments in cloud, data analytics, & robotic process automation (RPA).
- CISO role in tech modernization will likely increase as states accelerate adoption of cloud, RPA, mobile technologies, etc., particularly considering rapid shift to remote work due to pandemic.

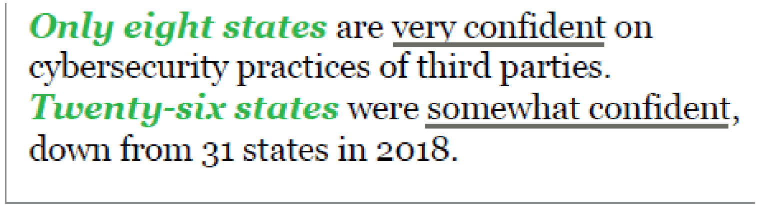
Bold Play 3: Team with the private sector & higher education

State CISOs should consider leveraging public-private sector partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as outsourcing to private sector firms

- Increases in outsourcing of cyber functions are helping States grapple with continued cyber talent shortages
- CISOs should consider partnering with local colleges & universities to develop a pipeline of new cyber talent through internships, co-ops, and apprentice programs, while working together to develop common strategies to improve statewide services



Leading outsourced cyber functions		2020 vs. 2018
60%	Cyberthreat risk assessments	+17%
42%	Security operations center	+4%
40%	Forensics/legal support	+8%

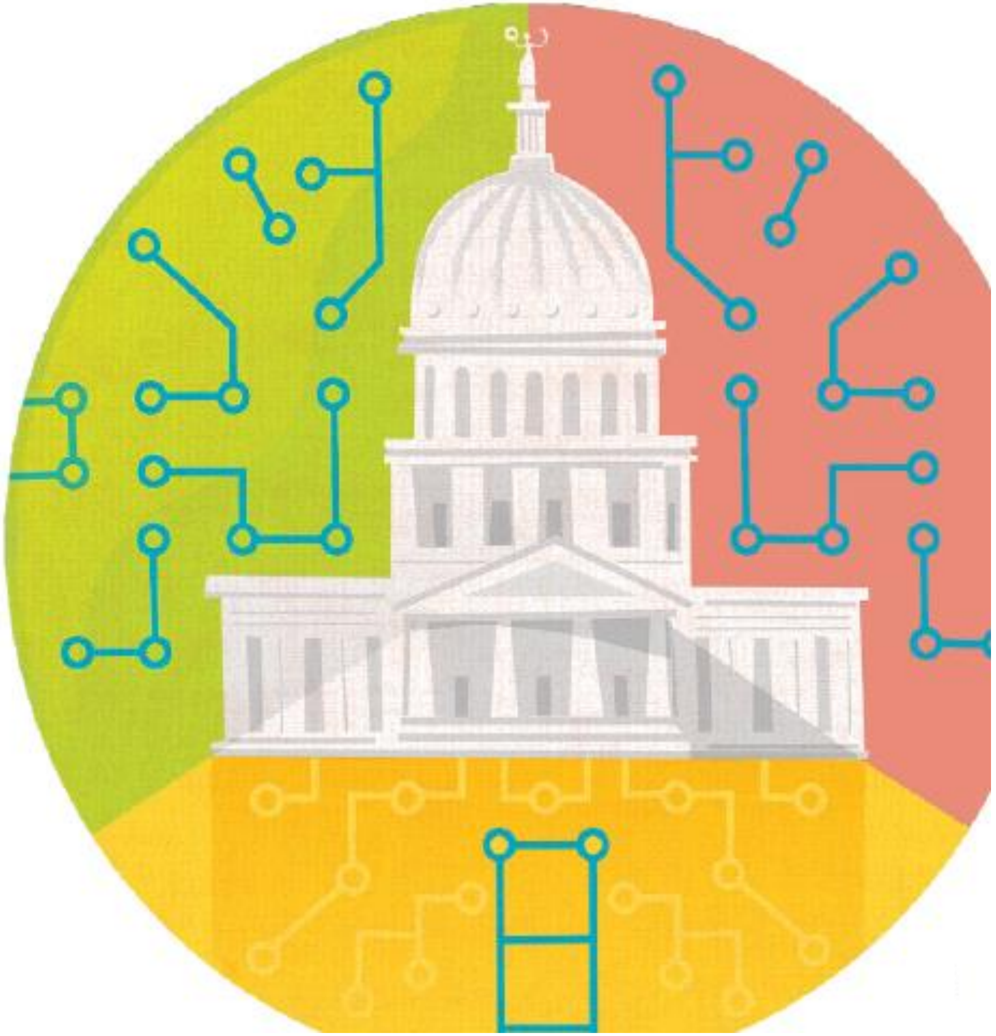


Only eight states are very confident on cybersecurity practices of third parties. ***Twenty-six states*** were somewhat confident, down from 31 states in 2018.

It is concerning that *confidence in third parties has decreased*. Standardizing governance and adherence to leading practices and policies can help increase confidence in these third-party partnerships.

Survey data analysis deep dives

In the following section, we take a detailed look at the survey findings.



Survey data analysis deep dive: Strategy and governance

Only 10 states:

- → Have appropriately aligned on cybersecurity initiatives with the goals and initiatives of business/program stakeholders.
- → Have legislation in place that provides funding to support the role and authority of the enterprise CISO or equivalent.

CISOs receive input on cyber strategy from:

01 State technology decision-makers | 47 states

02 State business decision-makers | 39 states

03 Private sector | 23 states

04 Higher education | 16 states

Declining trend on periodic executive cybersecurity report

2018–2020

To governor: **24** to 22 states

To legislature: **27** to 16 states

(-41%)

Enterprise security services adopted by state agencies

57%	Security awareness
57%	Security operations center
47%	Incident response
35%	Risk and vulnerability assessments
14%	Identity and access management

Top cyber services provided to the state, local, and public higher education entities

01 Incident management

02 Awareness and training

03 Investigation and forensics

04 Security operations center

05 Vulnerability management

CISO's role in procurement of hardware, software, and service providers

01 Establish security policies and guidelines (**90%**)

02 Evaluate a security questionnaire that vendors need to complete for procurement opportunity (**67%**)

03 Prohibit procurement of specific manufacturers/ vendors/products (**38%**)

Risk and privacy leadership in states

16 States with chief **privacy** officer

13 States with chief **risk** officer

Survey data analysis deep dive: More on cyber budget

Budget continues to be the top barrier

01 Lack of sufficient cybersecurity budget (46%)

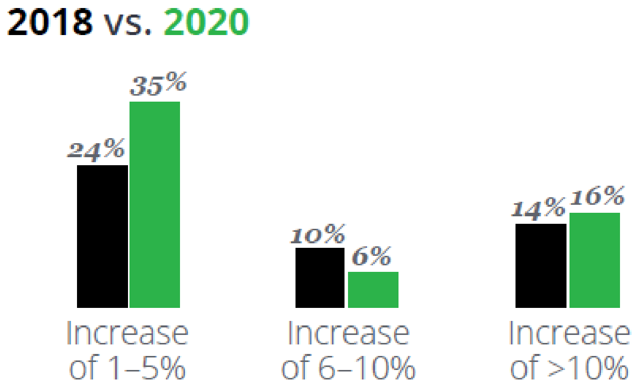
02 Inadequate cybersecurity staffing (42%)

03 Legacy infrastructure and solutions to support emerging threats (34%)

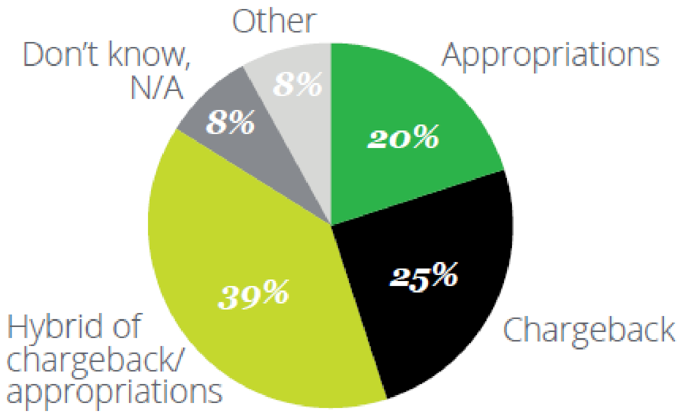
Top five areas covered in the cybersecurity budget

		2020 vs. 2018
86%	Audit logging and security information and event monitoring	+16%
84%	Security operations center	+18%
76%	Cybersecurity strategy and road map	+4%
76%	Threat intelligence and analytics	+6%
76%	Compliance and risk management	+10%

Only a few states reported a budget increase since 2018



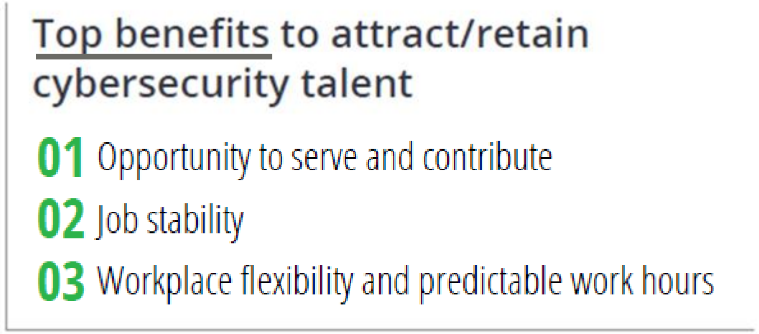
Cyber funding charge back versus appropriations



Additional cyber funding sources

		2020 vs. 2018
46%	US Department of Homeland Security	+13%
40%	Interagency collaboration	+2%
23%	Other state funding from legislature	+15%
19%	Business or program stakeholders	-16%

Survey data analysis deep dive: Cybersecurity workforce

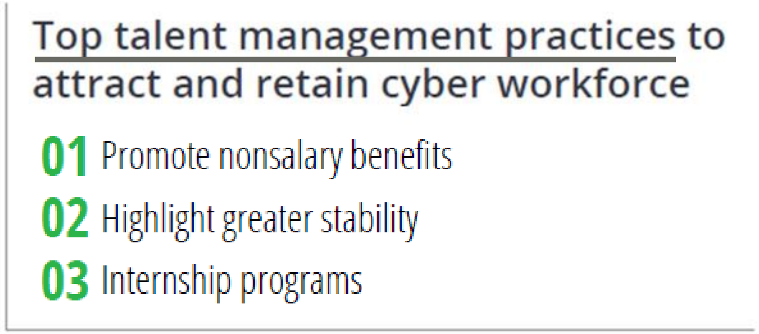


Top benefits to attract/retain cybersecurity talent

01 Opportunity to serve and contribute

02 Job stability

03 Workplace flexibility and predictable work hours

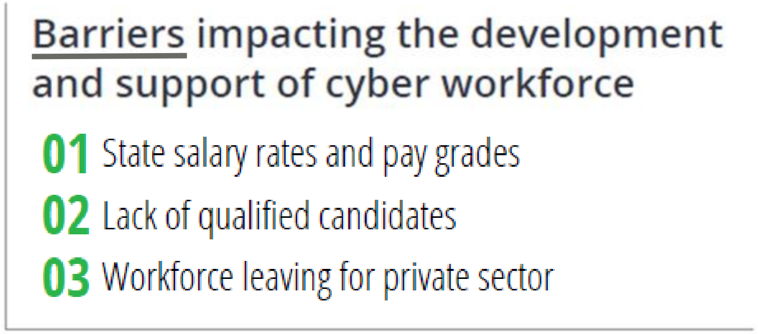


Top talent management practices to attract and retain cyber workforce

01 Promote nonsalary benefits

02 Highlight greater stability

03 Internship programs

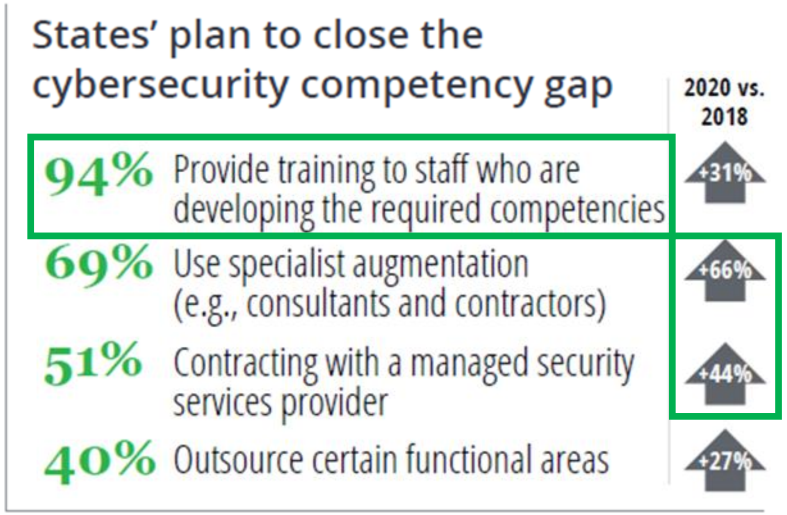


Barriers impacting the development and support of cyber workforce

01 State salary rates and pay grades

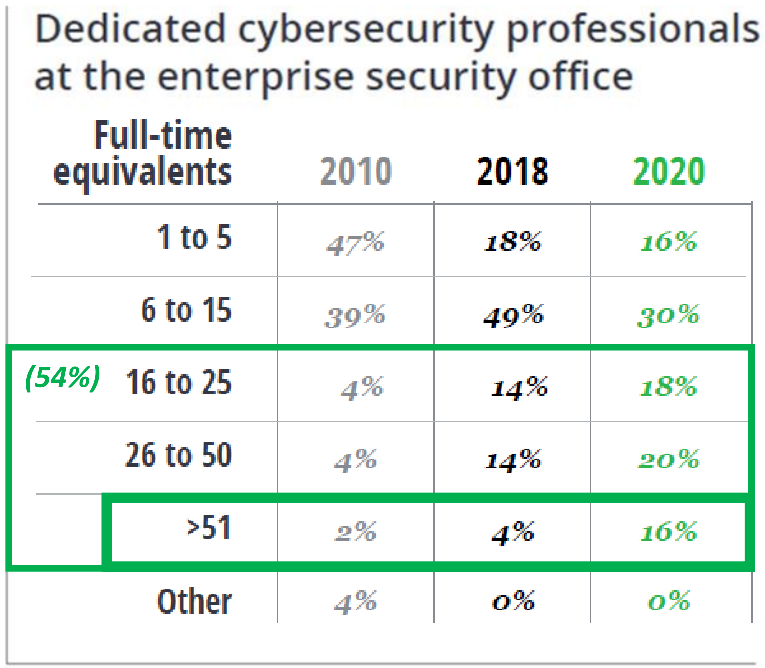
02 Lack of qualified candidates

03 Workforce leaving for private sector



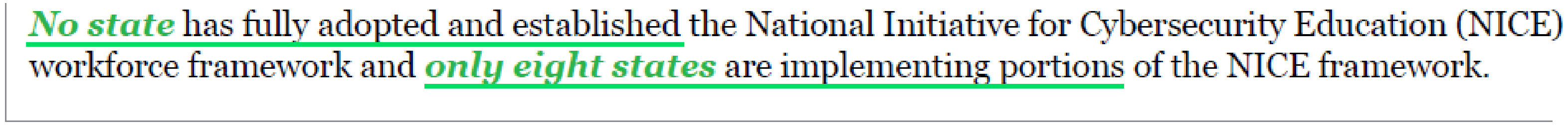
States' plan to close the cybersecurity competency gap

		2020 vs. 2018
94%	Provide training to staff who are developing the required competencies	+31%
69%	Use specialist augmentation (e.g., consultants and contractors)	+66%
51%	Contracting with a managed security services provider	+44%
40%	Outsource certain functional areas	+27%



Dedicated cybersecurity professionals at the enterprise security office

Full-time equivalents	2010	2018	2020
1 to 5	47%	18%	16%
6 to 15	39%	49%	30%
(54%) 16 to 25	4%	14%	18%
26 to 50	4%	14%	20%
>51	2%	4%	16%
Other	4%	0%	0%

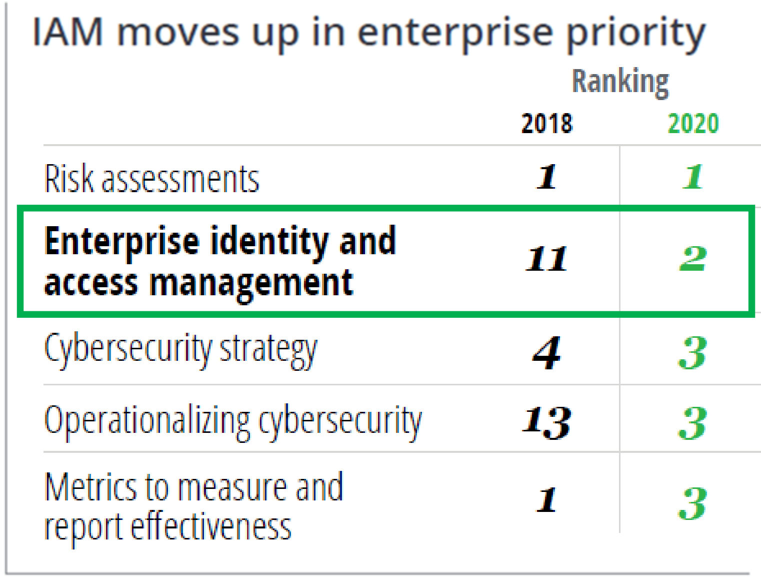


No state has fully adopted and established the National Initiative for Cybersecurity Education (NICE) workforce framework and ***only eight states*** are implementing portions of the NICE framework.

https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

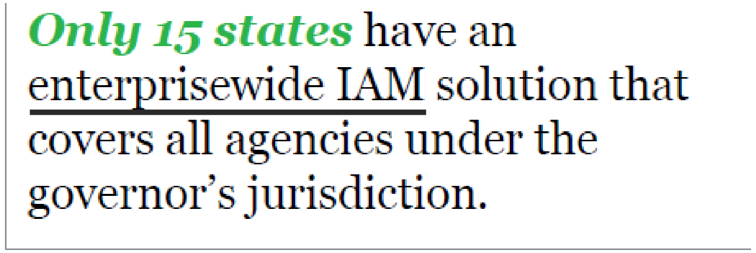
https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Survey data analysis deep dive: Identity and Access Management (IAM)

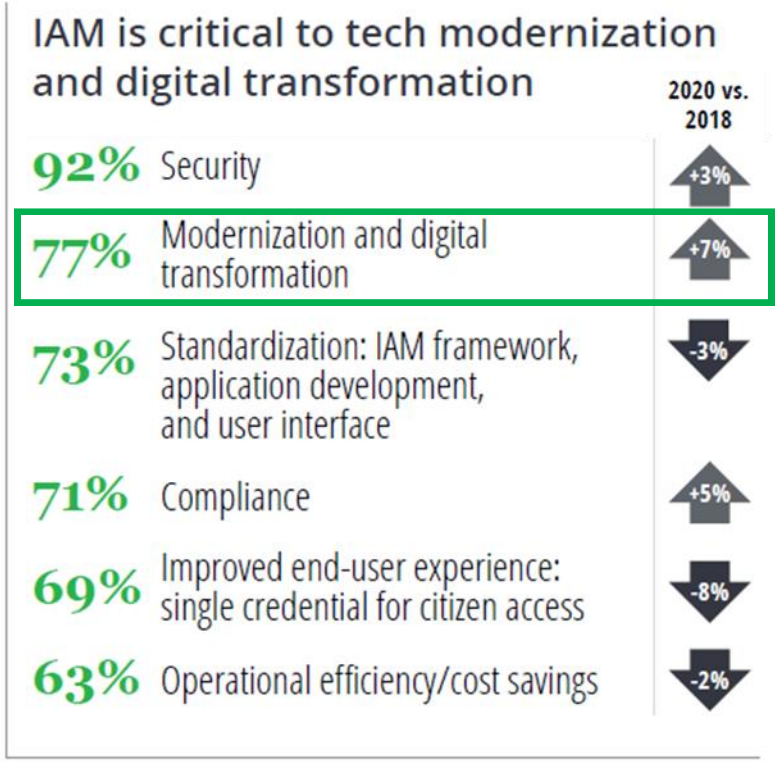


IAM moves up in enterprise priority

	Ranking	
	2018	2020
Risk assessments	*1*	*1*
Enterprise identity and access management	*11*	*2*
Cybersecurity strategy	*4*	*3*
Operationalizing cybersecurity	*13*	*3*
Metrics to measure and report effectiveness	*1*	*3*

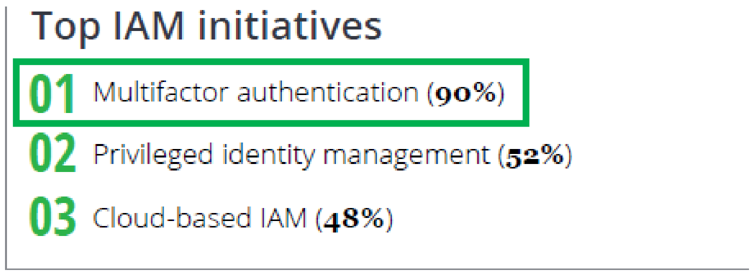


Only 15 states have an enterprisewide IAM solution that covers all agencies under the governor's jurisdiction.



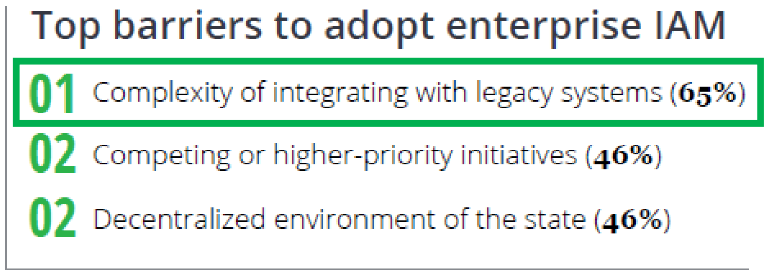
IAM is critical to tech modernization and digital transformation

		2020 vs. 2018
92%	Security	▲ +3%
77%	Modernization and digital transformation	▲ +7%
73%	Standardization: IAM framework, application development, and user interface	▼ -3%
71%	Compliance	▲ +5%
69%	Improved end-user experience: single credential for citizen access	▼ -8%
63%	Operational efficiency/cost savings	▼ -2%



Top IAM initiatives

01	Multifactor authentication (**90%**)
02	Privileged identity management (**52%**)
03	Cloud-based IAM (**48%**)



Top barriers to adopt enterprise IAM

01	Complexity of integrating with legacy systems (**65%**)
02	Competing or higher-priority initiatives (**46%**)
02	Decentralized environment of the state (**46%**)

Survey data analysis deep dive: Cyber operations

Financial fraud ranked higher as an external threat

01 Malicious code | **26 states**

01 Web applications | **26 states**

03 Financial fraud involving information systems | **22 states (only 5 states in 2018)**

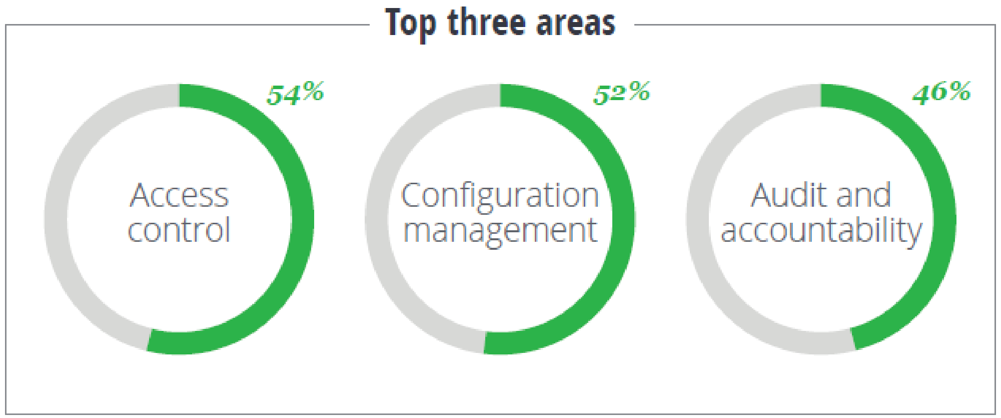
Only 22 states use DMARC* for their state's enterprise email systems.

**Domain-based Message Authentication, Reporting, and Conformance*

States improving on performing regular cyber assessments

		2020 vs. 2018
67%	Security events monitoring/security operations center	▲ +2%
63%	Annual disaster recovery exercises and tests	▲ +3%
60%	Application security testing and code review	▲ +6%

Areas where external audit findings have identified gaps in the past year



44%	Identification and authentication
42%	Risk assessment
40%	System and services acquisition
40%	Contingency planning
38%	System and communications protections
31%	Security assessment and authorizations
29%	Incident response
27%	System and information integrity
25%	Planning
23%	Physical and environmental protection
23%	Media protetion
21%	Personnel security
21%	Maintenance
19%	Awarness and training
17%	N/A, don't know
15%	Privacy
4%	No internal/external audit findings

Survey data analysis deep dive: Cyberthreats

54% of the states are not confident in their ability to address threats from emerging technology.

30 states said financial fraud was a leading cause of breaches in the past year compared to ***10 states in 2018***.

Leading causes of breaches continue to be from external sources: ***malicious code*** (68%), ***web applications from external sources*** (81%), and ***"hacktivism"*** (86%), which is on the rise.

Twenty-two states perform a periodic election security assessment.

In 29 states, the enterprise CISO and agency CISO are the officials responsible for coordinating and responding to cyber incidents.

CISO confidence in tackling types of threats ("very confident" and "extremely confident" combined answers)

		2020 vs. 2018
6%	Threats originating from use of emerging technologies (e.g., Internet of Things)	▲ +2%
10%	Threats originating from business partners/vendors	▲ +4%
15%	Threats originating from local government and public higher education entities	New in 2020
19%	Threats originating from cloud platforms and solutions	▲ +9%
19%	Threats originating internally	▼ -4%
23%	Threats originating from applications	▲ +11%
42%	Threats originating externally	▲ +5%

CISOs' top concerns for potential breaches have seen increases since 2018. Other notable changes:

74 to 85%	Phishing/farming
59 to 70%	Ransomware/malware
47 to 54%	Exploits of unsecured code

Leading cybersecurity standards that states use:

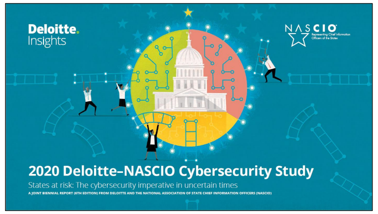
01 National Institute of Standards and Technology (NIST) Special Publications (88%)

02 Center for Internet Security (73%)

03 NIST Cybersecurity Framework (63%)

2020 Deloitte-NASCIO Survey Report & 2019 Nationwide Cybersecurity Review (NCSR)

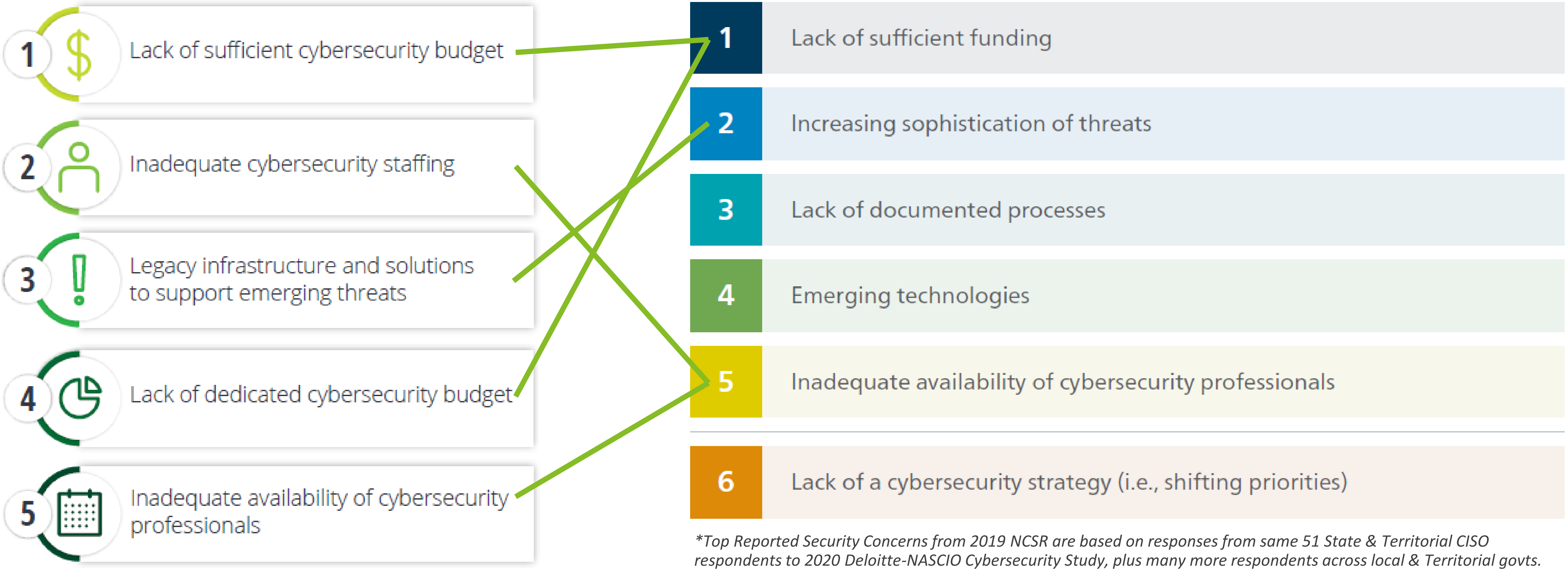
Parallels in top cybersecurity challenges and concerns


Deloitte. Insights
NASCIO
2020 Deloitte-NASCIO Cybersecurity Study
States at risk: The cybersecurity imperative in uncertain times

NCSR Info.: https://www.cisecurity.org/ms-isac/services/ncsr/

Top barriers to overcome cybersecurity challenges

2019 NCSR*
Top Reported Security Concerns



1. Lack of sufficient cybersecurity budget
2. Inadequate cybersecurity staffing
3. Legacy infrastructure and solutions to support emerging threats
4. Lack of dedicated cybersecurity budget
5. Inadequate availability of cybersecurity professionals

1	Lack of sufficient funding
2	Increasing sophistication of threats
3	Lack of documented processes
4	Emerging technologies
5	Inadequate availability of cybersecurity professionals
6	Lack of a cybersecurity strategy (i.e., shifting priorities)

**Top Reported Security Concerns from 2019 NCSR are based on responses from same 51 State & Territorial CISO respondents to 2020 Deloitte-NASCIO Cybersecurity Study, plus many more respondents across local & Territorial govts.*

Managing Cyber Threats through Effective Governance:

A *Call to Action* for Governors and State Legislatures

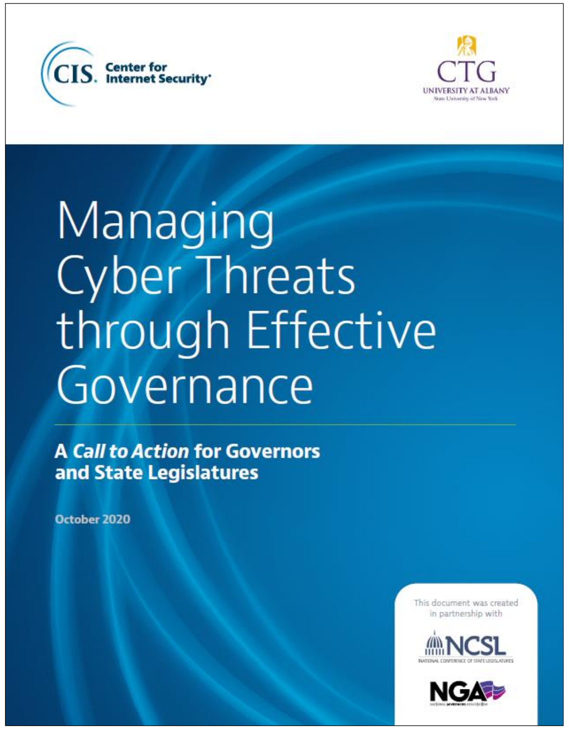
- A collaborative effort between many leading government- and security-focused organizations:
  - Center for Internet Security (CIS)
  - Center for Technology in Government at the University at Albany (CTG UAlbany)
  - National Governors Association (NGA)
  - National Conference of State Legislatures (NCSL)

- A Centralized Approach to Cybersecurity Governance
  - "Many organizations, including NASCIO, strongly recommend a centralized approach to cybersecurity governance.
  - While full centralization may be out of reach for many states given their current culture and structures, evolving away from fully decentralized toward centralization is highly recommended."

- Building a Whole of State Risk Management Program
  - "Increasingly, success will correlate with the extent to which states are able to expand the scope of their cybersecurity governance across all of a state's public and private critical infrastructures.
  - This implies incremental expansion from executive level agency assets to a "whole of state" perspective that engages stakeholders across all branches, jurisdictions, and sectors in a collaborative process of risk management."

Recommendations consistent with Deloitte-NASCIO Study report

- 4 Actions Steps for Governors and State Legislatures:
  1. **Establish Authorities through Executive Order & Legislation** – "Executive orders and legislation are being used by governors to formally establish the entities and authorities required to govern cybersecurity. Such authorities are being designed to overcome existing fragmentation in cyber governance and, where possible, are leveraging strong existing governance structures."
  2. **Formalize Key Processes** – "An effective governance framework formalizes key processes, including financial, procurement, technical standards, and risk assessment, necessary to effectively identify and manage cyber risks."
  3. **Assign Roles and Responsibilities** – "An effective governance framework includes an assignment of roles and responsibilities for designing and implementing the state's cybersecurity program as directed by the governor and/or legislature."
  4. **Monitor Indicators for Decision-Making and Adaptation** – "An effective governance framework requires the use of relevant indicators, beyond incident reporting, in decision-making processes to guide cybersecurity governance strategies and execution."



CIS. Center for Internet Security

CTG UNIVERSITY AT ALBANY State University of New York

Managing Cyber Threats through Effective Governance

A *Call to Action* for Governors and State Legislatures

October 2020

This document was created in partnership with

NCSL

NGA

https://www.cisecurity.org/white-papers/managing-cyber-threats-through-effective-governance/

2020 Deloitte-NASCIO Cybersecurity Study: *Related and Supporting Activities*

- The Deloitte-NASCIO Study report is available to state CISOs, CIOs and other cyber and IT leaders in state and local government, as well as their partners in the federal government, private industry and academia, as a resource providing State CISO-survey-based information on challenges and opportunities in S&L government cybersecurity.
- The Senate Homeland Security and Governmental Affairs Committee’s Federal Spending Oversight and Emergency Management Subcommittee held a hearing on 12/2/20, which included findings from the Deloitte-NASCIO survey report:
    - Hearing: “State and Local Cybersecurity: Defending Our Communities from Cyber Threats amid COVID-19”
    - Denis Goulet, New Hampshire CIO and current NASCIO President, continually noted in his testimony the report’s “whole-of-state” approach and advocated for much-needed State & Local government grant funding.
    - Senator Margaret Wood Hassan, D-NH, Ranking Member, also accentuated need for federal grant dollars for S&L Cybersecurity.
- Deloitte continues to collaborate with organizations such as NASCIO and the National Governors Association (NGA) in their efforts to help advance the importance and need for federal support of state and local government cybersecurity.

Deloitte. Insights

NASCIO Representing Chief Information Officers of the States

2020 Deloitte–NASCIO Cybersecurity Study

States at risk: The cybersecurity imperative in uncertain times

A JOINT BIENNIAL REPORT (6TH EDITION) FROM DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

To learn more or to take steps to rethink your cyber strategy, please contact us:

Rick Comeau
Senior Manager | Government & Public Services (GPS) Cyber Risk
Deloitte & Touche LLP
ricomeau@deloitte.com
+1.518.598.5391

Vik Bansal
Principal | GPS Cyber Risk
Deloitte & Touche LLP
vbansal@deloitte.com
+1.773.960.6143

https://www2.deloitte.com/content/dam/insights/us/articles/6899_nascio/DI_NASCIO_interactive.pdf

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this presentation contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.