2020 Deloitte-NASCIO Cybersecurity Study

States at Risk: The Cybersecurity Imperative in Uncertain Times

Meredith Ward

12.3.2020

2010

A call to secure citizen data and inspire trust

2012

A call for collaboration and compliance

2014

Time to move forward

2016

Turning strategy and awareness into progress

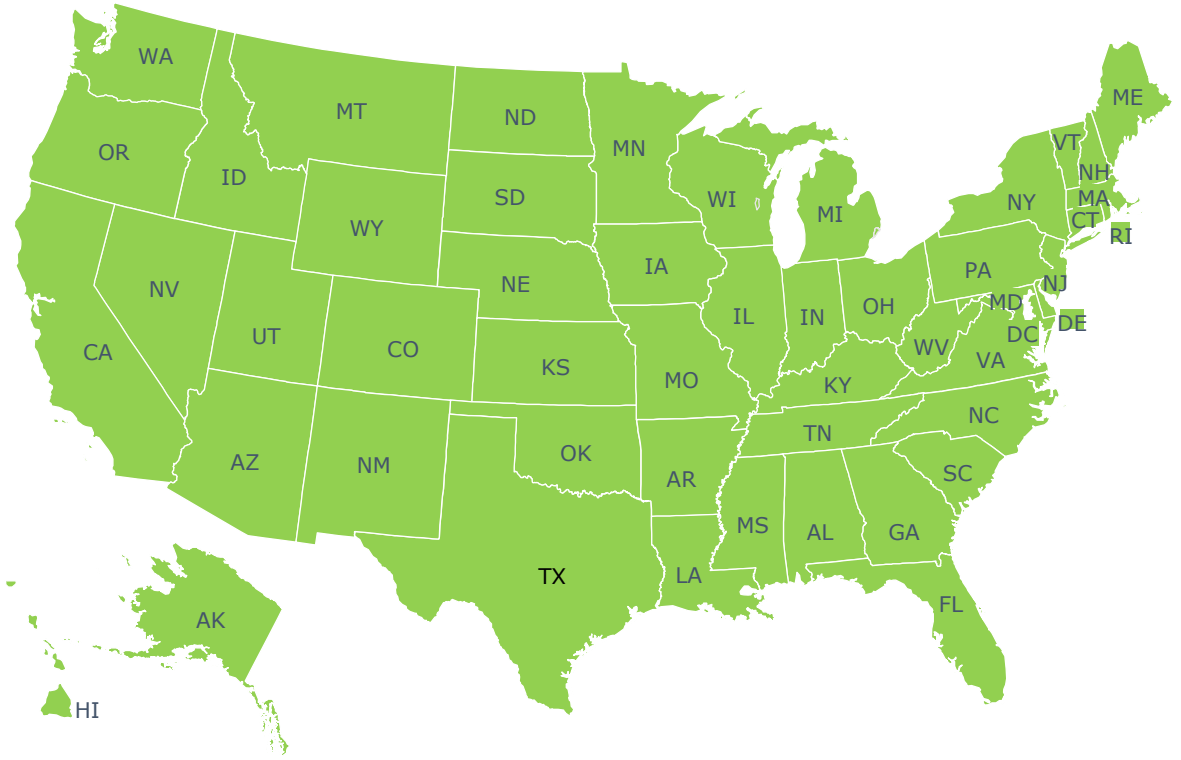
2018

Bold plays for change

2020

The cybersecurity imperative in uncertain times

All 50 States and D.C. Participated



COVID-19 Challenged Continuity and Amplified Gaps

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

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.

***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 1 2 3

Centralized Operating Model Reduces Risk

A centralized structure helps CISOs position cyber in a way that improves agility, effectiveness, and efficiencies

Advantages of a centralized structure

1. A centralized model should help to increase adoption of essential enterprise security services.
2. States have an opportunity to leverage federal funding for implementing and delivering cybersecurity services in a shared model to benefit all agencies.
3. The ability to manage a centralized cybersecurity budget is likely to help evaluate the overall cyber posture
4. Cross-training and upskilling can also be simplified and more easily scaled, providing more career growth opportunities for cyber staff.

Identity & 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

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%)

Cyberthreats

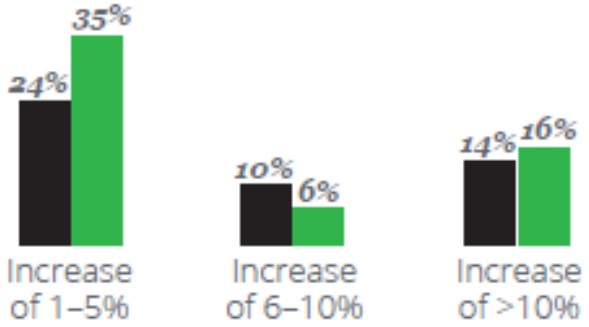
30 states said financial fraud was a leading cause of breaches in the past year compared to ***10 states in 2018***.

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.

Budget

Only a few states reported a budget increase since 2018

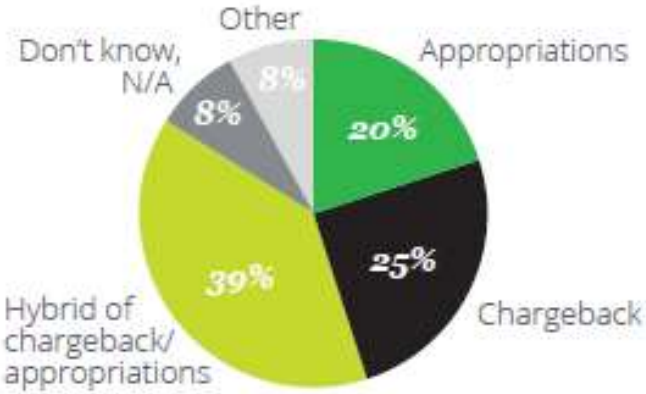
2018 vs. **2020**



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%

Cyber funding charge back versus appropriations



www.nascio.org/stateofcyber

mward@nascio.org