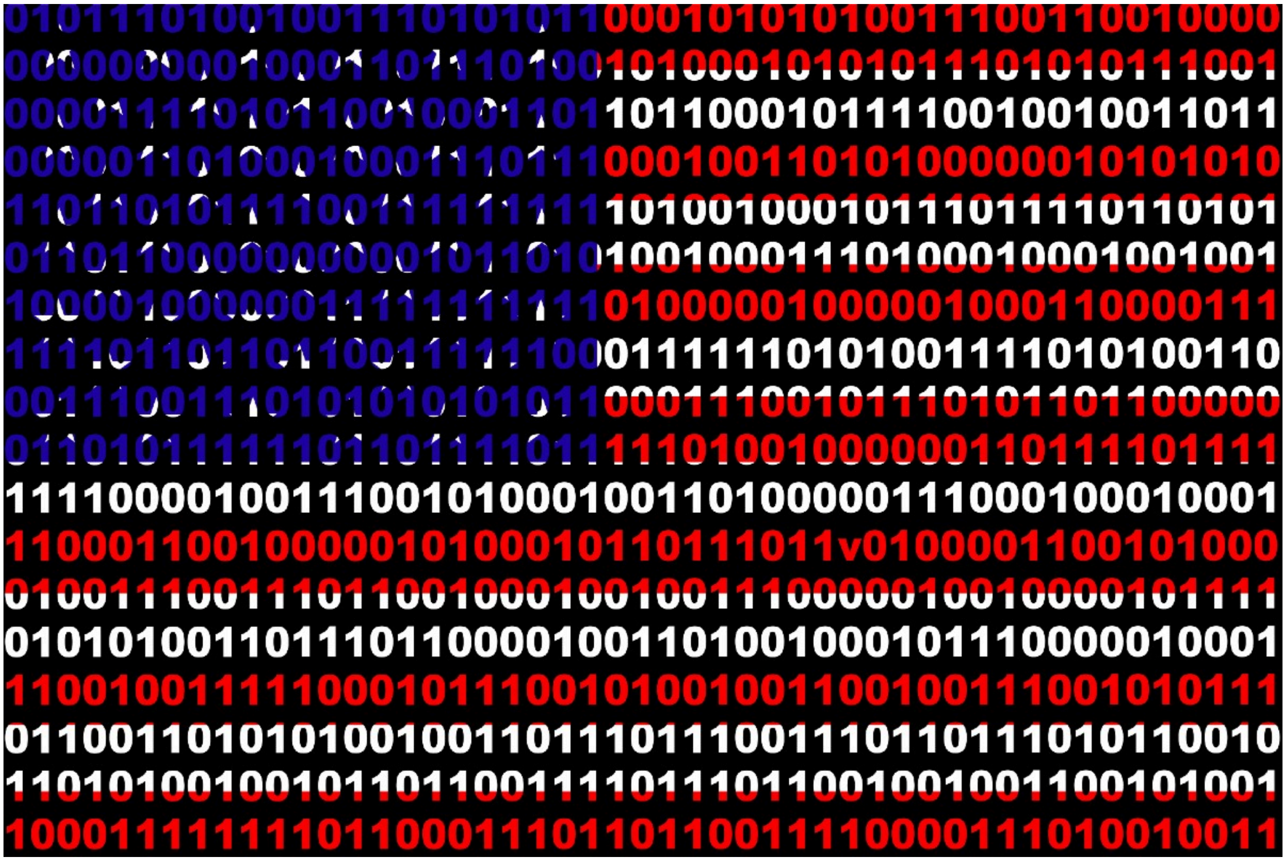
(https://fastfuture.org/)

Deloitte cybersecurity study highlights good and bad trends for state CISOs Edit

(https://fastfuture.org/wp-admin/post.php?post=502379&action=edit)

October 25, 2022



(https://fastfuture.org/wp-content/uploads/2022/10/State-cybersecurity.jpg)

Photo: Fernando Astasio Avila/Shutterstock

Does your state have a CISO? Are they getting the funding and backing they need? Deloitte and the National Association of State Chief Information Officers (NASCIO) released their 2022 Cybersecurity Study, “State Cybersecurity in a Heightened Risk Environment (https://www2.deloitte.com/us/en/insights/industry/public-sector/2022-deloitte-nascio-study-cybersecurity-post-pandemic.html).” The survey asked questions of chief information security officers in all 50 states and three territories about cybersecurity trends, challenges and opportunities.

State CISOs throughout the U.S. gained considerable strength and authority over the past few years, as they rapidly migrated government operations and services to a virtual environment and expedited digital transformations to meet the needs of people and families. State agencies were able to continue providing quality service to their constituents, despite the challenges of a global pandemic.

The report also highlights some other challenges and successes:

Talent: In 2022, the demand for high-skilled workers has grown even more acute for public and private-sector employers. The lack of cybersecurity professionals and other staff remains among the top five barriers cited by state CISOs. Headcounts for state cybersecurity professionals remain about the same as in 2020, and more than 6 in 10 CISOs report gaps in competencies among their staffs.

Embracing the entire state: CISOs made progress in enhancing their stature and visibility at the state executive and legislative levels, and they are continuing to get the institutional support and resources they need. All 50 states now have a CISO, and many are establishing new positions for chief privacy officers, chief risk officers and identity program directors. More state legislators are codifying the role of the CISO into state law and funding the position.

Emerging technologies: Post-pandemic, CISOs have an even more critical role to play in guiding the evaluation and implementation of new technologies.

State CISOs confirm that many applications have migrated to the cloud. With remote work, digital and mobile platforms have become part of the fabric of daily life.

“The complexity of cyber challenges that the state CISOs tackle is increasing with the need to take a whole-of-state approach involving multiple jurisdictions and stakeholders,” said Srini Subramanian, principal, Deloitte & Touche, and Deloitte’s global risk advisory leader for government and public services. “To address these challenges, state CISOs are increasingly laying the groundwork to adopt emerging technologies, promoting more collaboration with local government agencies and higher education institutions, upskilling state employees and transforming employment practices to attract the next generation of highly capable cyber talent.”

Additional takeaways from the 2022 Deloitte/NASCIO survey include:

- Thirty states increased their cybersecurity budgets from 2021 to 2022. And for the first time, CISOs report that a handful of states are allocating more than 10% of their IT budgets to cybersecurity, in alignment with federal government levels. However, most states still only allocate between 2% and 10% of their budgets to cybersecurity efforts.
- Many state CISOs identified the drafting and implementation of the Zero Trust framework as a key initiative.
- CISOs say that malware, ransomware and phishing attempts continue to present security challenges.
- CISOs found that the three leading causes of cyber incidents remain web applications, malicious code and financial fraud. However, CISOs note a rise in cyber incidents involving foreign state-sponsored espionage, zero-day attacks and attacks against cloud platforms.
- Nearly one-third of state CISOs say that state agencies manage cyber incidents on their own, rather than working with a central state IT security group.
- More than half of CISOs report outsourcing security operations center tasks, which require 24×7 monitoring, and more than 60% of CISOs report having confidence in the cybersecurity services of third-party vendors.
- State CISOs are starting to incorporate diversity, equity and inclusion (DEI) practices, such as designating a DEI leadership position or teams to foster a culture of inclusion. However, many CISOs say they do not know if they have such practices in place.

Have you met your state’s CISO? What is their contribution to your state? Even small states with lower populations need lots of cybersecurity to prevent catastrophic malware attacks.

Posted in ITSR Newsletters (https://fastfuture.org/category/newsletters/itsr-newsletter/), Tech Trends (https://fastfuture.org/category/tech-trends/)

About Fast Future

Mission and Team (https://fastfuture.org/mission-and-team/)

Contact Us (https://fastfuture.org/got-a-story/)

More Ways to Connect

LinkedIn (https://www.linkedin.com/company/fast-future/?viewAsMember=true)

X (formerly Twitter) (https://twitter.com/Fast FutureFuture/)

Terms & Conditions (https://fastfuture.org/terms-and-conditions) | Privacy Policy (https://fastfuture.org/privacy-policy/)