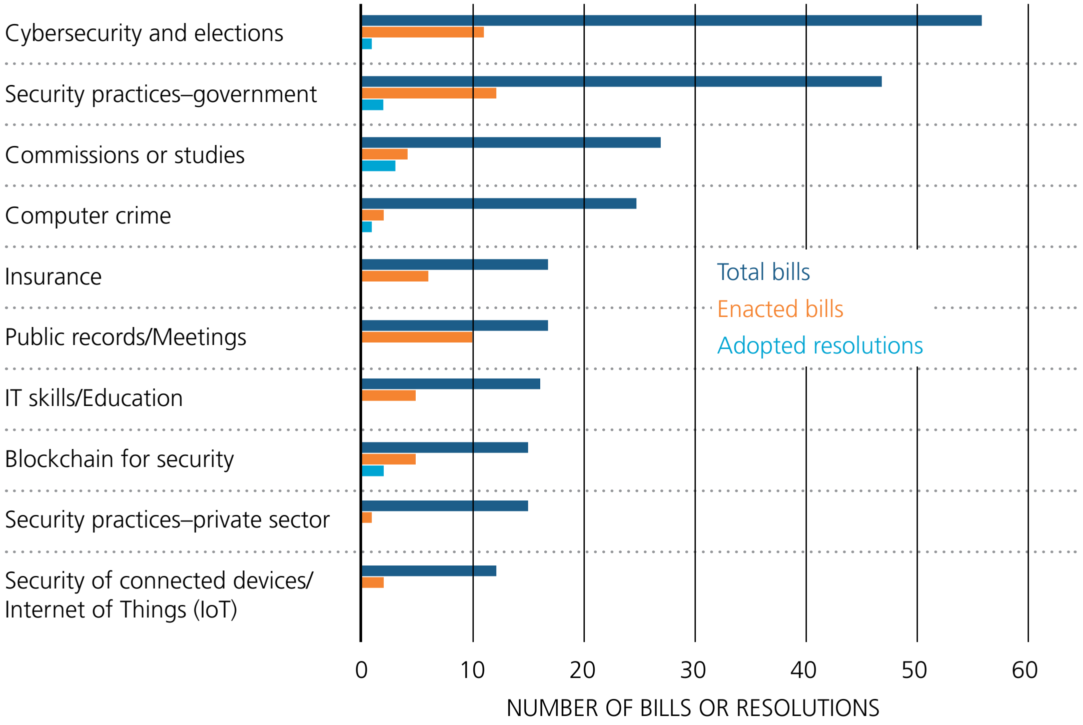
NCSL

LegisBrief

A QUICK LOOK INTO IMPORTANT ISSUES OF THE DAY

NOV. 2019 | VOL. 27, NO. 40

Top 10 Issues in 2019 Cybersecurity Legislation



Source: NCSL, 2019

Did You Know?

- All 50 states have a statewide chief information security officer (CISO) or equivalent, with about a third established by statute and others through executive action or executive order.
- Ransomware attacks against state and local governments increased sharply in 2018, and that surge seems to be continuing into 2019.
- A survey of top IT security officers in the 50 states identified three top issues affecting states' cybersecurity: budget, talent and increasing cyberthreats.

State and Federal Efforts to Enhance Cybersecurity

BY SUSAN FREDERICK, PAM GREENBERG AND ABBIE GRUWELL

States face several significant obstacles to sound cybersecurity practices. These include a lack of resources to meet the challenges of an ever-evolving cyberthreat landscape, workforce and education issues, and development of sound resiliency practices to keep state systems safe and protect privacy.

As states grapple with these issues, the federal government is also looking for ways to assist states and address cybersecurity issues on a national level. When it comes to cybersecurity, there is no question that states cannot address cyberthreats in a vacuum.

State Action

State legislatures' biggest priority in recent years—outside of election security—has been focused on improving cybersecurity practices within state government and increasing resources and training to combat cyberthreats. For example, more states are now requiring agencies to have a statewide, comprehensive approach to security and security oversight. Often, chief information security officers are charged with creating statewide security policies and IT standards, establishing information security plans with annual assessments or reporting, creating cyber incident response or readiness plans, and requiring security awareness training for employees.

■ **2019 Bill Introductions.** At least 43 states and Puerto Rico introduced or considered close to 300 bills or resolutions that deal significantly with cybersecurity, including appropriations for cybersecurity. The top 10 categories of cybersecurity issues, other than appropriations, range from elections to connected devices (see graphic).

■ **2019 Enactments.** In at least 31 states, more than 80 cybersecurity-related bills were enacted or adopted in 2019. Key trends in enacted legislation this year fell into the following areas:

- Improving government security practices.
- Addressing cybersecurity threats to elections.
- Providing for the confidentiality of government cybersecurity plans and practices by exempting them from public records laws.
- Addressing cybersecurity insurance, including enacting laws based on the NAIC Insurance Data Security Model Law, which establishes a comprehensive regulatory framework requiring insurers to implement information security programs.
- Approving studies or task forces to investigate the use of blockchain/distributed ledger technology for cybersecurity.

Federal Action

The executive branch received its congressional mandate in November 2018 when President Donald Trump signed H.R. 3359 into law. Public Law No. 115-278 reorganized the Department of Homeland Security's (DHS) cyber division and created a new DHS agency called the Cybersecurity and Infrastructure Security Agency (CISA). CISA is a full-fledged DHS agency and has assumed responsibility for providing technical assistance to protect and mitigate cyber vulnerabilities and guidance on how to best use federal resources. It also assesses potential cybersecurity risks and facilitates information sharing with states and other entities. In August 2019, CISA released the agency's strategic intent document, which lays out its strategic vision, operational priorities and guiding principles. They include leadership and collaboration, risk prioritization, results orientation, respect for national values and creating a unified mission and agency.

Congress has also recently introduced cybersecurity legislation that seeks to help states by providing grants to improve cybersecurity at state and local levels. S. 1065 and its companion bill, H.R. 2130, the State Cyber Resiliency Act, would assist states and local governments in coordinating resources, better responding to cyberthreats and enhancing cyber resiliency through a series of state grants administered by DHS. Similarly, S. 1846, the State and Local Government Cybersecurity Act, provides funding to states for improved security measures and opportunities to collaborate with federal officials on cyber risks, defensive measures and threat indicators.

The administration has also issued several significant executive orders on cybersecurity. In May, the president issued the Executive Order on America's Cybersecurity Workforce. It introduces new programs to expand and improve the skills of the cybersecurity workforce through cross-government information sharing, academic and workplace incentives, and accelerated learning. The order also aims to facilitate moving cybersecurity professionals between the government and private sector and establishes a rotational assignment program for cybersecurity experts within the federal government.

That same month, the president issued the Executive Order on Securing the Information and Communications Technology and Services Supply Chain. The order set an October deadline for the Department of Commerce to release a rule on information and communications (ICT) supply chain security, including banning the purchase of specific products from "foreign adversaries." The federal government will assess the risk of purchasing certain ICT equipment based on a three-part test and CISA has created a risk assessment used by the Department of Commerce in its rulemaking. DHS also has an ICT supply chain risk management task force within CISA to address hacking, criminal attacks and foreign interference of ICT supplies, products and services.

Additional Resources

- NCSL Cybersecurity Task Force
- Digital Privacy and Security: Overview of Resources

NCSL Contacts

Pam Greenberg
303-856-1413

Susan Frederick
202-624-3566

Abbie Gruwell
202-624-3569