Cybersecurity has become a central issue for many state officials across the nation. In the past six months, Colorado, Connecticut and North Carolina have all been victims of cybercrime. In today’s world, where so many aspects of daily life depend on data sharing devices that communicate via the internet, state officials are trying to mitigate the damage that can be done by hackers. There is little uniformity among state cybersecurity strategies. However, three states have positioned themselves as potential leaders for enhancing security of the state’s online information.

In Arizona, the cybersecurity operations are coordinated between the state government and a non-profit coalition made up of businesses and universities. Arizona Cyber Threat Response Alliance (ACTRA), grew out of an FBI program launched in the early 2000s that was designed to share information about cyberthreats between the public and private sectors. The group runs workforce development programs designed to help employees identify and fend off a cyberthreat. Convening members from academia, industry leaders, and law enforcement, this program facilitates discussions between businesses, universities and the state government, which allows for a robust state cybersecurity system.

In New Jersey, the state’s Cybersecurity and Communications Integration Cell (NJCCIC), is the state’s one-stop shop for cybersecurity information. As the statewide cybersecurity coordinator, NJCCIC takes the lead on all cybersecurity issues for the state and even serves cities and localities not equipped with the resources to respond to a cyber threat or attack. This consolidation of state and local resources allows for a uniform approach in dealing with cybersecurity. This agency answers to New Jersey Office of Homeland Security and Preparedness, rather than the state information technology office. Placing the chief information security officer under the homeland security office gives the program the authority to expand cybersecurity planning across state agencies.

Rather than establishing a single agency or having a public-private partnership, Washington state coordinates cybersecurity strategies through a chief information security officer but also assigns significant roles to members of emergency management and state military officials. The cooperation between departments has increased the longevity of this program. By incorporating the National Guard into security measures, Washington takes a more defensive approach in securing their online infrastructure. By incorporating the emergency management and military affairs departments, the state expanded their incidence response team in the event a cyberthreat becomes an issue.

Each state must work to find a strategy that is unique to their security needs. The three approaches listed above demonstrate how proper innovation, organization and governance can foster a cybersecurity strategy capable of addressing problems and implementing plans. The one thing in common with these three strategies is coordination across multiple stakeholder groups. Bringing together all stakeholders allows these states to inventory potential partners, leverage existing relationships between agencies and outside entities, blend and braid funding to allow funds to be used more easily and creatively at the point of service and delivery, have a comprehensive definition of success, and easily communicate across cabinets and agencies.