FEDInsider

DATA SHEET

The Future of Government Cybersecurity: New Money, New Technologies

Recent legislation passed by President Biden has opened new avenues of investment for many agencies to invest in cybersecurity.

The Infrastructure Investment and Jobs Act was recently signed into law, providing a massive amount of funding for state, local, tribal and territorial governments to invest in cybersecurity, infrastructure and other areas. This resource boost for cybersecurity, to the tune of over $1.9 billion, provides local agencies the means to bolster their defenses and make investments that would normally be cost prohibitive. From machine learning and AI to staffing and recruiting, state, local, tribal and territorial governments now have a plethora of options available to them to improve their cyber defenses.

Government and industry experts gathered at a FedInsider roundtable discussion to discuss these developments, and to talk about how states plan to best use this newly available funding to protect their infrastructure. The following are some key points they made during that event.

Develop A Holistic View Of SLTT Cyber Security Needs

Whenever there is a large amount of new funding, the question becomes how to best use that resource. Most state and local governments did not expect a large, new pool of resources, so advanced tools and defenses were not part of their capital budget planning. Because of that, step one for a lot of government agencies will be taking an inventory of needs and then forming a plan about how to best use the new money.

"My tour of the commonwealth, which lasted 60 days and went through 130 localities, was focused on talking to each of those CIOs or CISOs to find out what their needs are," said Aliscia Hernandez, Deputy Secretary of Cybersecurity for the Commonwealth of Virginia. "I talked with them about the gaps we have and how to use the money from the federal government that'll be most beneficial to them."

While Virginia is a populous state with a strong federal presence, and one that is used to working with federal agencies, they are not the only state taking this comprehensive approach.

"The way we're looking at doing this at the state level is by empowering the locals with both technologies and solutions. We are also giving them ideas about how they can better their cybersecurity posture," said Chris Letterman, CISO for the State of Alaska.

By taking the time to develop a holistic overview of all of the locations, applications and users within each local agency's purview, states can better distribute funds to improve cybersecurity across more systems. This allows state, local, and tribal governments to build a strong foundation that provides more deterrents for potential bad actors.

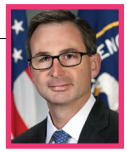
Education & Communication Are Essential

Two of the most important aspects of good cybersecurity posture today are education and communication. Education is crucial since it's not easy to guard against threats if the threats are completely unknown. While there will always be new and evolving threats, it's important for industry professionals to be well-versed on the newest trends.

Featuring:

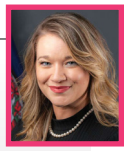
- **Brad Bowers**
  Field Chief Information Security Officer, Global, SHI

- **Michael Mestrovich**
  CISO, Rubrik & *Former CISO* for the CIA



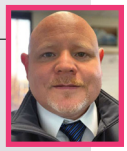
- **Steve Hernandez**
  Chief Information Security Officer, Dept. of Education

- **Aliscia Andrews**
  Dep. Secretary, Cybersecurity, Commonwealth of Virginia



- **Ray Yepes**
  Chief Information Security Officer, State of Colorado

- **Chris Letterman**
  Chief Information Security Officer, State of Alaska



- **Samy Bouhaouala**
  Senior Manager, Security & Cyber Solutions, Accenture Federal

rubrik | public sector

SHI

"I also think there's the deeper side of the education piece," said Brad Bowers, Global CISO at SHI International Corp. "It's now becoming more and more important for the next generation of cybersecurity professionals, and the folks who are in industry today, to understand the risk from a broader perspective." And that requires ongoing study and education about cybersecurity.

Of course, communication about the newest threats and needs goes hand in hand with education. Especially for smaller agencies without a lot of experience, talking about their cybersecurity needs with other agencies, and those in their government structure who are responsible for security, is critically important. Eventually, new tools may be introduced to fill in some of the gaps, but for now, communication is a key to planning good defenses.

"As we go into the future, we'll see more conversation around the trust engine or policy engine," said Steven Hernandez, Chief Information Security Officer at the Department of Education. "We'll get into things like artificial intelligence, machine learning and how we make decisions to enable us to move at the speed of the machines."

But Hernandez added that we may have to wait a bit before that vision can become reality. For now, agencies are best served by focusing on robust education initiatives to identify and recognize new threat patterns that are emerging. Additionally, it is important that agencies realize that knowledge is power, and that sharing their analysis with other agencies can help everyone.

Investments In Hiring & Personnel Are Also Important

It's no secret that governments at all levels are short on skilled cybersecurity employees, and have difficulties hiring good people to fill in those gaps. Unfortunately, this can create quite a problem because having new infrastructure money for cybersecurity investment may not help when there are thousands of open cybersecurity jobs across federal, state, local and tribal governments.

One solution might be to hire people with baseline skills and then train them in more advanced techniques.

"Sometimes it's better to invest in people, even if they don't have all of the latest technical knowledge," said Ray Yepes, Chief Information Security Officer for the State of Colorado. "You have to show that you really care about your people."

Yepes referred to this practice as "leading with the heart" and mentioned how his approach has led to his agency having one of the lowest turnover rates in the state. His plan works by hiring smart people with baseline skills and then training them for increasingly advanced cybersecurity techniques. And because they are given such a great opportunity, for the most part they remain loyal and stick around even after getting advanced training that would qualify them for jobs elsewhere in government or in the private sector.

It might also be possible to recruit young talent by offering them the opportunity to serve their county and communities, especially when combined with other incentives like the ability to telework or to get access to the latest cybersecurity tools.

"Today, there are over five million open jobs in cybersecurity," said Samy Bouhaouala, Senior Manager, Security and Cyber Solutions at Accenture Federal. And finding the right incentives can help to bring those professionals into government service. "There's demand, [and competition to get good talent] but that also means that all of these young stars have opportunities to move." The current climate makes skilled cybersecurity professionals more apt to try new things and new jobs, because they can always find another job quickly if they don't like where they end up.

New Tools Will Assist New Talent

While finding and developing young talent is a great option, it's not always possible, especially if there are thousands of jobs to fill. This has led some agencies to try and find alternative solutions.

"You're not going to be able to bring in enough people and train them up to be the cybersecurity experts you need in the time you have," said Michael Mestrovich, CISO, Rubrik & Former CISO for the CIA. "Historically, that's where we really need advancements in the areas of machine learning and AI."

Adding those technologies can help to make up for shortfalls, Mestrovich said, tasking the machines to filter out all of the low-end, repetitive type security problems that can drain a human workforce, and freeing them up to concentrate on more advanced threats and defenses. And that is another area where the new infrastructure money can be used, to bring on tools and platforms that can assist and supplement an increasingly overloaded human workforce.

The funding coming from the Infrastructure Investment and Jobs Act will be an incredible boon for state and local governments who are trying to defend their networks in the face of an increasingly dangerous threat landscape. The key will be how to invest this massive but limited resource for the best results. The speakers at the FedInsider roundtable admitted that more planning was needed, but were confident that the new funds would be a cybersecurity game changer for state and local governments.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

SHI

SHI
290 Davidson Avenue
Somerset, NJ 08873
Contact: Brad Bowers, Field CISO

(609) 440-9880
brad_bowers@SHI.com
SHI.com
Facebook.com/SHIInternational
Linkedin.com/Brad-Bowers, Linkedin.com/co/SHI-International-Corp
@SHI_Intl