Cybersecurity is Infrastructure

With the passing of the Infrastructure Investment and Jobs Act, state and local governments are moving to secure themselves against rampant cyberattacks.

When President Joe Biden signed the $1.2 trillion Infrastructure Investment and Jobs Act into law in November 2021, we saw a celebration of bipartisanship that emphasized the importance of the legislation. The bill's journey to passage drew on support from Democrats and Republicans to create jobs across the country by dispersing billions of dollars to state and local governments to help amend decades of neglect.

The bill targets the country's crumbling bridges, tunnels, roads and railways. In addition, it expands broadband internet access to millions of Americans and gives state and local governments the means to enhance and expand local cybersecurity.

Why worry about cybersecurity?

Although cybersecurity has always been a part of all-things-internet, the recent massive rise in malware and other threats has forced the world to sharpen its attention on cybersecurity in ways we never thought necessary.

In the first half of 2020, there were 4.4 million attacks against government customers. However, as reported in the mid-year update to the 2021 SonicWall Cyber Threat Report, during the same period in 2021, that number rose to 44.6 million — a staggering *917% increase* and the most significant jump of any industry examined by SonicWall.

In SonicWall's follow-up report, The Year of Ransomware, the attacks showed no sign of slowing. After posting a groundbreaking high in June, the third quarter saw 190.4 million ransomware attempts, the highest ever recorded in a single quarter by SonicWall. In contrast, there were 195.7 million total ransomware attempts logged during the first three quarters of 2020.

Big Squeeze

State and local governments are under pressure from hackers on one side, work from home on another, and the push toward digital government on another. How can they meet these competing needs while maintaining a sound cybersecurity posture? Explore the technology in-depth by reading the executive brief: State and Local Government: The Big Cybersecurity Squeeze.

What does the infrastructure bill do for cybersecurity?

The $1.2 trillion Infrastructure Investment and Jobs Act allocates about $2 billion for cybersecurity. About half of that amount is set aside for the State, Local, Tribal and Territorial (SLTT) Cyber Grant Program and distributed over four years.

The Department of Homeland Security (DHS) will administrate funding. Therefore, SLTTs must present comprehensive plans that fully and accurately describe new resource procurement, implementation and management to access the financing. The bill provides $200 million in 2022, $400 million in 2023, $300 million in 2024, and $100 million in 2025.

How does the infrastructure bill specify what qualifies as cybersecurity?

The Infrastructure Investment and Jobs Act's language offers a much-needed definition for state and local governments on the types of investments they are expected to make. But, more than likely, DHS will provide additional compliances and rules as a condition for funding.

Specifically, the bill identifies firewalls (on-prem and virtual), secure mobile access (on-prem and virtual) and advanced software that provides endpoint threat detection and response. That means funding rules will focus on technology that offers operational capability or services, including computer hardware, software and related assets that enhance operators' ability to protect themselves against threats.

What kind of broadband spending does it offer?

The legislation identifies $42.45 billion for an initiative called "Broadband Equity, Access, and Deployment." This portion of cyber activity will expand grants available to underserved communities. The Assistant Secretary of Commerce for Communications and Information will soon announce funding details.

Still, this funding is expected to touch on local cybersecurity considerations. Expansion will likely involve expanding wireless communication and involvement from local utilities (e.g., mobile, broadband).

How SonicWall Fits into the Plan

While the Infrastructure Investment and Jobs Act identifies security technology like firewalls, secure mobile access and endpoint threat protection software, it doesn't specify performance metrics to help state and local governments target their plans more precisely. We won't have funding specifics from managing agencies until early next year.

In the meantime, state and local governments are already forming their procurement teams. Some prepare themselves by establishing early partnerships with the cybersecurity industry to identify technology and best practices for managing local networks.

Among the many considerations:

- **Recognize and address the increased cybersecurity risks from all aspects of your network**. SonicWall helps you uncover hidden dangers with high-level analytics and reporting.

- **Create and maintain robust data policies and procedures.** Network management and policy management tools are built into SonicWall Network Security Manager. NSM allows IT teams to govern centrally, meet compliance rules and regulations, and manage risks as they emerge.

- **Look for automated real-time breach detection and prevention.** SonicWall offers automated TLS inspection, patented Real-Time Deep Memory Inspection (RTDMI), Reassembly-Free Deep Packet Inspection (RFDPI) and Capture ATP cloud-based multi-engine sandboxing. Networks gain added security and resilience with Capture Security Appliance (CSA) on-premises advanced threat detection and Cloud App Security for Office 365 and G Suite applications.

- **Seek out proven efficacy and innovation.** Technological efficiency will be a significant consideration for funding since the kinds and variations of threats are constantly changing. SonicWall's latest threat data included a report of a 73% increase in unique malware variants. The company's patented technology uncovered this significant data point.

- **Plan a layered approach to cybersecurity**. For example, SonicWall solutions offer 'end-to-end' layers of protection, detection and inspection. Our portfolio provides firewalls, switches, secure mobile access, Wi-Fi, email security, cloud application security, endpoint security and control — all orchestrated within a consolidated Network Security Manager through a single pane of glass.

- **Build organizational consensus and ownership.** The best cybersecurity implementation starts with total buy-in from everyone in the organization. Your network security is strengthened when everyone complies with the security measures you've chosen to help keep your network and digital assets safe from hackers.

- **Demand the correct certifications from your vendors.** SonicWall meets federal governmental certification and interoperability requirements (e.g., NIST, FIPS 140-2, CSfC, Common Criteria, DoDIN APL, USGv6 and NSA CNSA Suite B.)

Photo by NASA on Unsplash

Portfolio Sample

Ray Wyman Jr, ray.wyman@raywyman.com

Posted: https://blog.sonicwall.com/en-us/2021/11/state-and-local-government-cybersecurity-is-infrastructure/