Telos

# Modernizing State and Local Government Cybersecurity

**Ransomware is a "threat to national security."**

—**Alejandro Mayorkas** | Secretary | Department of Homeland Security

Mike Matchett | Principal Analyst

September 28, 2021

Small World Big Data

In partnership with

Truth in IT


In recent market research here at Small World Big Data, we have noted that ransomware and related cybersecurity threats represent one of the biggest current risks to digitally transforming organizations. The more that organizations leverage data and automate processes within highly connected business functions, the more vulnerable they become to potential data loss and cyber threats. Because of this, it is clear that cybersecurity programs must go hand in hand with all modernization and digital transformation efforts.

Unfortunately, not every organization has the in-house security-related staffing, skills, and expertise or the available resources to ramp up the security capabilities needed to keep pace with fast-evolving, quickly growing cyber threats. In particular, state and local governments, including education (and higher education, for that matter), are especially vulnerable. They need to modernize and adopt digital solutions for many reasons, ranging from aging infrastructure to meeting the challenges of remote workers and classrooms. However, state and local organizations are greatly challenged to assemble the significant resources necessary to implement adequate security protections. In fact, often the executive leadership at this level simply does not have the technical expertise necessary to direct cybersecurity programs and ensure that they are being satisfactorily implemented.

TruthInIT hosted a high-interest online event recently on this topic, *"Modernizing State and Local Government Cybersecurity"* (sponsored by Telos Corporation; see sidebar), featuring an expert panel of guest speakers. In this report, we attempt to extract and lay out the key takeaways and recommendations for action.

## Modernizing State and Local Government Cybersecurity

### Event Host

**David Littman**, TruthInIT

### Panel Host

**Richard Stiennon**, Principal Analyst and CEO with IT Harvest, author of the annual cybersecurity industry IT Security Yearbook

### Panelists

**Nick Leiserson**
Chief of Staff and principal advisor on cybersecurity for US Congressman Jim Langevin

**Derek Root**
former CTO of Charlotte Mecklenburg School District, advisor/consultant to DHS, DoD, and DoT

**Vince Scheivert**
Director of Technical Strategy, Telos

## Cybersecurity Is a Growing Problem

Hackers have long targeted government entities for many reasons, but historically the reasons were mainly political or espionage/hostile nation-state oriented. There are plenty of examples of government entities being targeted by bad actors. Recently, infamous breaches have leveraged insidious vulnerabilities, like the Solarwinds supply chain attack, which affected more than 18,000 organizations, including federal, state, and local agencies; and the Kaseya ransomware attack, which victimized thousands of businesses and public agencies by exploiting their managed service providers. But according to our event panel, it was the 2021 Colonial Pipeline ransomware attack that finally convinced many at the U.S. federal level regarding the "real" cyber threat to national interests.

At the federal level, cyber is becoming the fifth domain of warfare, with a national strategic level of discussion about election security, ransomware, and other pressing issues, as well as growing concern about the increasing globalization of cyber crime. In response, the federal government is now working more actively on programs to provide assistance to state and local governments (see CISA sidebar).

*Cyber is becoming the fifth domain of warfare.*

According to our panel, local agencies need help from the federal government in the form of ongoing partnerships, providing continuing cyber expertise and resources, not just regulation and one-time grants. Local school boards, for example, are often made up of former local teachers, who cannot be expected to be experts in cybersecurity.

A related issue facing local and regional agencies is the scarcity of cybersecurity professionals available for hire in their markets. This nationwide (and perhaps global) security challenge will hopefully also be addressed at the federal level with programs to motivate and recruit more talent into security-related careers.

### Introduction to the US CISA

**https://www.cisa.gov/about-cisa**

CISA leads the nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and the American way of life.

## SLED attracting hackers

When bad actors using ransomware choose targets, they look for the most vulnerable, potentially profitable institutions. While larger global corporations might have deeper pockets to pick, there is some evidence that state and local governments are also profitable—but easier—ransomware targets. (For example, see Donald Norris's in-depth report, *"A Look at Local Government Cybersecurity in 2020,"* in the July 2021 issue of ICMA's Public Management magazine.) SLED organizations are certainly less risky to attack and threaten than a cyber-hardened, professionally staffed federal agency with potentially global reach (e.g., Department of Defense).

During the online event, there was some discussion about the need for cybersecurity to be as important today as physical security. If you store sensitive information and financial instruments in a locked safe, then you also need to protect digital assets analogously with encryption and unmodifiable backups. If you have to be authorized to access private records on paper, then you should be digitally authenticated and authorized (i.e., multi-factor authentication, zero-trust infrastructure) for similar data online.

## Recommendations

During this event, the panelists were asked for their key recommendations. The underlying message was that the best cybersecurity strategy may be to first partner with a reputable, expert cybersecurity firm that can guide and fully manage cybersecurity programs.

Another key takeaway: Don't just fix the vulnerability that pops up. Cybersecurity needs to be a continuous practice, with ongoing monitoring, recurring assessments, and evolving protection measures. It's like the need to maintain your house in good condition. There is always going to be something more to do to keep digital data safe and secure.

We've summarized a few more key recommendations listed by the panelists:

- As a personal action, consider helping elevate the cybersecurity risk issue locally. Digital life is becoming as important to society as physical life, and that approach needs to start with kids when they are students.
- Eat the "cybersecurity elephant" one bite at a time. Use a qualified service provider partner to get started, and realize that this will be an ongoing process.
- First, admit that there is a cybersecurity problem and real vulnerabilities. Ignoring the risks until they actually manifest themselves is not a good strategy.
- Like most activities, it pays to start with planning. Outline a good initial plan; then look for grants, guidance, and partners to help implement it.
- Last year's (U.S.) defense policy bill created an official cybersecurity advisor in each state to help access federal programs and resources. Thirty-three states have already hired advisors, providing a great go-to resource for organizations in those areas. There is much more to be done, but it is not too early to get connected.
- Tell your state and local representatives to look into and connect with CISA and their cybersecurity advisor!


## Summary

If you are interested in the broader state of the cybersecurity IT industry, check out the panel host Richard Stiennon's latest annual Security Yearbook 2021. In addition to some background education on cybersecurity trends and domain-specific security acronyms, you can learn the history and current focus of key cybersecurity solution vendors. You'll get a bigger picture of the threat landscape through the lens of the solutions being actively marketed to address them.

We also highly recommend that interested individuals download and open the interactive CISA services catalog found here: https://www.cisa.gov/publication/cisa-services-catalog. Its interactive features enable organizations to determine their current cybersecurity posture and needs (through dropdown selections), and help highlight the set of CISA resources and services aligned with their current situation. If nothing else, the inherent self-evaluation and subsequent resources offered will help create a baseline of what types of cyber programs and services to pursue next.

Finally, we fully agree and reiterate that the best course of action when starting out is to engage the assistance of an expert cybersecurity solutions and services provider. When evaluating service providers, look for expertise and experience in the relevant compliance standards and regulations for your organization, along with some evidence of demonstrated client success. It makes sense to select a provider that will become a true partner over a longer time frame. Cybersecurity requires cohesive ongoing attention and active management, and is not simply acquired through a series of independent projects.

Small World Big Data

truthinIT

**About Small World Big Data**
Small World Big Data creates insightful technology analysis and research for IT, Cloud and Data markets. In addition to incisive market research and opinionated analyst reports, we specialize in producing popular, consumable, expert analyst-hosted video content and podcasts. As a small agile firm with deep experience in IT and vendor marketing, our constantly refreshing research calendar provides ongoing and cost-effective opportunities for market awareness, education, demand generation, lead nurturing and more. For schedule and information about current research and advisory services, visit SmallWorldBigData.

**About Truth in IT**
Truth in IT has published independently created informational and educational content for the IT professional since 2009. We partner with independent analysts and bloggers to create unique seminars, webinars, videos and market research reports. We also invite sponsors to further help educate our audience about best practices and trends to help the IT professional succeed in their daily jobs and careers. Our goal is to amplify the subject matter expert's expertise, insight and voice so our audience is able to cut through the hype to get to the Truth in IT.



aws partner network

**Advanced**
Technology Partner

Government Competency
Security Competency
Public Sector Partner