Knowledge. Advice. Clarity.

THE CYBER AWARE WORKFORCE

How state and local agencies can create a stronger line of defense against ransomware and other threats.

GOVLOOP
E-BOOK
2020

DLT
A TECH DATA COMPANY

CROWDSTRIKE

TABLE OF CONTENTS

INTRODUCTION

In the blink of an eye, the coronavirus pandemic has forced state and local governments to the forefront of the work from-home (WFH) movement.

With government offices closed to the public, shelter-in-place orders executed, and draconian budget cuts and layoffs looming because of the pandemic-spurred economic downturn, cybersecurity professionals at all levels have faced unprecedented demands to protect their networks and keep their agencies functioning in new ways. Meanwhile, internet traffic volume has soared more than 40%, straining network throughput and resilience.

This new landscape also increases the threat landscape as bad actors seek to take advantage of hastily implemented technologies to support telework. More than ever, agencies' employees are the first line of defense. From case workers to police officers, and every role in between, employees accustomed to having tech support close at hand are now part of the frontline cyber protection workforce. Whatever their usual job responsibilities, employees are now also responsible for some level of cybersecurity, or at least security awareness.

Concepts such as phishing, malware and ransomware may not be new to these workers, since governments at all levels provide basic cybersecurity awareness training, alert them to the dangers of opening unexpected email attachments, require them to change passwords frequently and take other security precautions.

But working from home ratchets up the stakes, even as new threats and new actors emerge, and one slip can have catastrophic consequences in this new environment.

State and local agencies are working hard and taking action to raise employees' awareness of cybersecurity threats and better protect themselves.

IN THE NEWS

With the arrival of the COVID-19 pandemic, news and information regarding cyberthreats at the state and local levels have focused on the vast expansion of telework as agencies scrambled to keep providing services to the public even as workers sheltered at home. Many news stories also focused on the dangers to the health care sector — hospitals, clinics, research institutions, pharmaceutical companies and the myriad elements that comprise the supply chain.

Cyberattacks that were little more than nuisances have suddenly become potentially life-threatening problems during the pandemic. In some instances, particularly loathsome criminal groups use the fear of COVID-19 to spread their malware.

ALERT AND WARNINGS

For instance, U.S. cybersecurity agencies issued a pandemic-related cyberthreat warning in early April 2020 about cyber criminals and malicious groups that had begun to use the crisis as their lure.

"We urge everyone to remain vigilant to these threats, be on the lookout for suspicious emails and look to trusted sources for information and updates regarding COVID-19. We are all in this together. And collectively, we can help defend against these threats," Bryan Ware, Assistant Director for Cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA), said in the warning.

CISA warned about phishing emails with embedded malware masquerading as pandemic information from legitimate sources such as the World Health Organization. U.S. agencies also have tracked increased activities by cyber rings scanning for and exploiting known vulnerabilities in remote- working tools and software, such as the attacks reported on the video conferencing platform Zoom.

These kinds of attacks, and the alerts they've engendered, show that all levels of government recognize the need to hypercharge cybersecurity protections. But doing so requires funding at a time when states, cities and localities are reeling from the loss of tax revenue.

STATE SEARCH FOR FUNDING

At the end of April, a coalition of a dozen of the largest and most influential state governmental associations — including the National Governors Association (NGA), National Association of Counties, National League of Cities and the National Association of State Chief Information Officers (NASCIO) — asked Congress to include funding for cybersecu rity and IT infrastructure in pandemic financial aid legislation:

"COVID-19 has required our workforces, educational systems and general way of life to quickly move remotely, exerting greater pressure on cybersecurity and IT professionals and increasing the risk of vulnerabili- ties and gaps to state and local networks. These gaps are exacerbated by systems requiring modernization that do not foster remote work, which also increases the risks to employees supporting these systems."

Likewise, increased traffic to unemployment portals and health insurance marketplaces has created additional risks as systems are being modified or created to handle the exponential increase in demand. This surge on our information technology infrastructure requires additional investment in both funding and manpower to keep up with the mas- sive usage. Additionally, malicious cyber actors have used attention on COVID-19 to their advantage, further targeting government infrastructure, the healthcare sector, and individual citizens for internet crimes, such as ransomware, phishing, and computer-enabled financial fraud.

CURRENT ATTACK LANDSCAPE

In January 2020, NGA and NASCIO jointly released a report, Stronger Together: State and Local Cybersecurity Collaboration, which specifically identifies ransomware threats targeting states and municipalities. It notes that although some ransomware attacks have been reported publicly — such as those against Atlanta and Baltimore — it should be presumed there have been other such attacks.

In late May 2020, CISA warned that malicious actors are mounting cyberattacks against health care policymakers and researchers. Many of these attacks use passwords spraying techniques, applying the most common passwords to the email accounts of individuals at targeted organizations. For state and local officials, those could be health departments, public research universities and public hospitals.

LESSONS FROM TEXAS

In a recent interview with GovLoop, Texas Chief Information Security Officer (CISO) Nancy Rainosek explained how agencies can survive cybersecurity incidents before, during or after events such as COVID-19. As part of that discussion, she shared some preventative and response measures that agencies can learn from the coordinated ransomware strike against various Texas agencies in 2019:

- Build a cybersecurity-aware culture.
- Create security policies and plans, including incident response plans, continuity of operations plans and acceptable use agreements.
- Know where your data is, the priority of what needs to be recovered and in what order.
- Ensure that contracts for managed IT services include cybersecurity and liability protections.
- Perform regular, automated backups and keep them separate and offline.
- Modernize legacy systems and ensure that software is as current as possible.
- Limit the granting of administrative access.
- Segment networks and install and tune effective firewall technologies.
- Keep software patches and antivirus tools up-to-date.
- Ensure that users properly manage passwords.
- Enable multifactor authentication, especially for remote logins.

NEED TO KNOW: WHY CYBER AWRENESS MATTERS

State and local IT professionals find themselves in the center of a storm created by a confluence of events, including having to implement agencywide teleworking plans with little advance notice and seeing financial and manpower resources melt away because of the ongoing economic crisis.

To make matters worse, all of these challenges are occurring while state and local municipalities are facing an increased threat environment that bad actors are using as cover to hide their malicious activities. In some cases, criminals are even leveraging the chaos of the situation as an opportunity to strike. A viral pandemic may not have been the disaster that most state and local cybersecurity professionals were planning for, but their concerns about preparedness have been growing for some time.

Cybersecurity and risk management have been state and local CIOs' top priority for seven years in a row, according to NASCIO. Included in this broad description are governance, budget and resource requirements, security frameworks, data protection, training and awareness, and third-party (contractor) risk.

NGA has an online resource center to help states boost their cybersecurity programs.

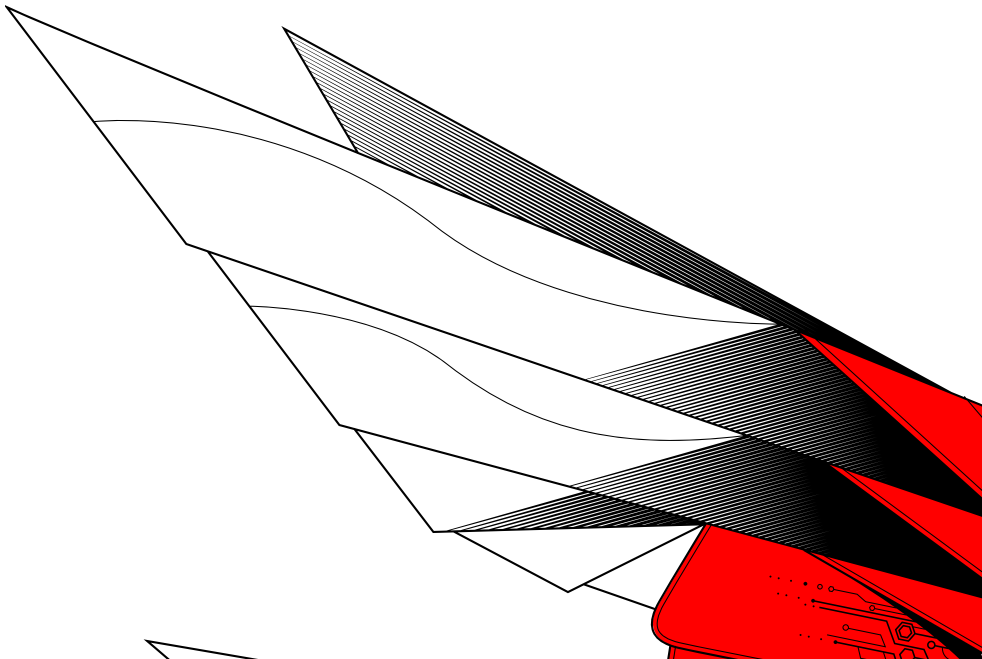
PAIN POINTS

The Information Technology Laboratory (ITL), one of the research laboratories within the National Institute of Standards and Technology (NIST), issued a bulletin in March 2020 that outlines the key pain points that were driving many of the concerns state and local officials expressed about their cybersecurity operations. They included:

- A lack of physical security controls. During normal times, client devices are used in a variety of locations outside of the organization's control, such as coffee shops and hotels, where they can be lost or stolen. Stay-at-home orders minimized that risk, but it is rising again as employees leave their homes.
- Unsecured networks are used for remote access. These networks, whether broadband or wireless, are susceptible to eavesdropping as well as man-in-the-middle attacks to intercept and modify communications. They are also generally less, or not at all, controlled or monitored by agency officials or any structured cybersecurity program.
- Providing external access to internal-only resources. Allowing remote users to access sensitive servers that handle internal traffic increases the risk that servers could be compromised. Normally, these resources can be blocked to all outside traffic, but that is not possible with most of a workforce using them from their homes and remote locations.

The research institute offered several suggestions for enhancing cybersecurity for remote workers, such as incorporating encryption for storage on remote devices, which also has the benefit of providing some protection from eavesdropping, interception and modification of data transmitted via external networks.

NIST suggested that cybersecurity managers should assume that employee-owned devices used for teleworking will become infected with malware at some point. Possible strategies to address this include using anti-malware technologies, network access control solutions that verify the device's security posture before allowing access and having a separate network at the organization level for telework devices brought in for internal use.



HUMAN BEHAVIOR IS KEY

NIST ITL focuses only on the IT part of the equation; what is outside its purview is the human element.

Colin Bastable, CEO of Lucy Security, a security awareness training company, said agencies' employees need to be trained to identify social engineering attacks, such as phishing.

"A strategy of patching people, by simulating ransomware attacks on staff and running 'what if' system tests to identify systemic vulnerabilities, would be far more effective in reducing damage...than solely focusing on plugging holes below the IT waterline after a hit," he said. "Many IT security people regard non-IT folks as part of the problem. CISOs need to treat their colleagues as potential allies in the fight against cybercrime, engage [human resources], departmental heads, and make the whole organization defense-ready."

'WHALE-OF-STATE' STRATEGIES ARE EMERGING

Well before the pandemic, states were moving toward a whole-of-state" approach to cybersecurity, building partnerships among agencies, local governments, colleges and universities, utilities, private industry, health care, and other sectors to strengthen cybersecurity protections among all the participants.

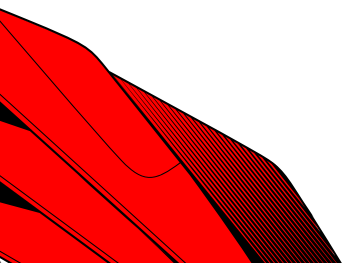
The foundation for this approach is elected officials' and agency professionals' recognition that cybersecurity is far more than an IT responsibility. "It is a critical business risk, homeland security and public safety threat, voter confidence issue, and economic development opportunity," according to NASCIO and NGA's state and local collaboration report.

In many cases, state governments are providing services to counties and municipalities, including endpoint protection, shared service agreements for cyber defense tools, incident response, and cybersecurity awareness and training. A survey presented in NASCIO's 2020 Tech Forecast found that 25% of respondents said their states had implemented a whole-of- state cybersecurity strategy, while 39% said one was is in progress. Less than a quarter (22%) said they were not implementing it.

The NASCIO and NGA report outlines numerous examples of states' approaches to broadening the reach and scope of their cybersecurity efforts to protect their interconnected elements.

"Many CISOs believe that increased engagement with locals has strengthened the state's overall cyber posture, and they have made it a top cybersecurity priority," it states.

But "if you've seen one state, then...you've seen one state," the report adds. Each has its own legal and regulatory framework for this kind of collaboration.



BUILDING BLOCKS FOR IMPROVED CYBERSECURITY STRATEGIES

State CIOs and CISOs can take concrete steps to strengthen cybersecurity, whether or not they are implementing a whole-of-state approach.

Cyber summits targeting cybersecurity offices and broader education programs aimed at stakeholders at all levels, including elected officials, corporate officers and health care IT professionals can build awareness of services that are available to localities.

Additionally, there are municipal and county leagues at the state level where state CIOs and CISOs can build trust and identify the needs of groups including entire counties and towns. It can be just as helpful to have a strong coalition of cybersecurity efforts centered on cities and municipalities as a blanket, state-run program. If you have the luxury of talented cybersecurity professionals at the local level, it might even be more efficient to design defenses and awareness programs as close to the users as possible.

Creating umbrella purchasing agreements for products and services can also help states and localities save budget resources. What's more, an umbrella buy could provide smaller entities access to services they otherwise might not be familiar with or have access to without volume pricing. Consulting with localities during the contract planning process again builds trust, while taking into consideration the broadest gather- ing of requirements.

The NASCIO and NGA report outlines the various steps NASCIO members are taking. Although each prioritizes a slightly different aspect of cybersecurity based on the needs and resources available to that state, when looked at as a whole, it covers many of the concerns state and local governments nationwide have.

The report has many examples of state and local governments working quickly and efficiently to develop new protections and programs to address the current environment. The following four are among the most impressive and demonstrate the highest levels of intra-agency cooperation.

NORTH CAROLINA: NATIONAL GUARD STEPS INTO THE BREACH

The North Carolina Department of Information Technology (NCDIT) formed a partnership with the National Guard and the North Carolina Emergency Management agency. A memorandum of understanding allows NCDIT to activate the National Guard for cybersecurity assessments and other cyber duties, without requiring a declaration from the governor.

The partnership can be activated immediately to help local governments, school systems and community colleges remediate and recover infrastructure and data compromised during a cyberattack. The partnership also provides training for those same groups to help prevent future incidents. Additionally, NCDIT deploys tools to support the monitoring of county infrastructure and local network traffic, further helping to keep threats at bay.

LOUISIANA: 1-800 HOTLINE FOR LOCAL GOVERNMENT

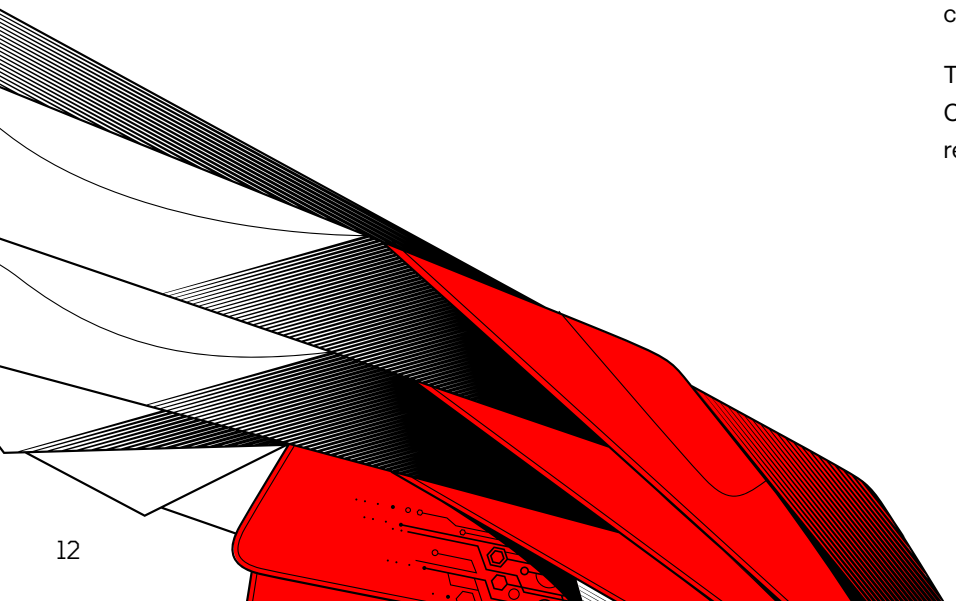
Louisiana has established a statewide Information Security Team, which provides an escalation point for incident response via a 1-800 hotline for local government entities. State responses range from providing remote assistance and direction over the phone to full onsite incident response. The state is looking for ways to engage with all entities on preparedness, to improve prevention — or at least improve detection — and make sure critical audit log data is captured and maintained.

In addition, the governor established the Louisiana Cybersecurity Commis- sion via executive order to address a range of cyberthreats and integrate cyber responses into the larger emergency management framework. The commission's Emergency Support Function was activated in July 2019 by a gubernatorial emergency declaration to respond to a multitarget ransom- ware attack on local school districts. Local entities promptly reported the incident, and the state conducted a forensic investigation and prevented the attack from spreading.

PENNSYLVANIA: COLLABORATION WITH COUNTY COMMISSIONERS

The commonwealth has been partnering for five years with the County Commissioners Association of Pennsylvania through PA CyberSafe, a col- laborative workgroup of county CIOs and IT directors. They meet quarterly and focus on security education, collaboration with the state CISO and security standardization. The partnership created a pilot program with a cyber forensic provider to help counties identify and remedy security gaps.

The group also provides statewide access to phishing exercises and computer-based security awareness training through a cloud-based learning management system. In 2018, the Pennsylvania Office of Administration joined with the association to provide training and phishing exercises to all 150,000 county and state employees and contractors through a single service.



IOWA: PITCHING CYBER SERVICES, TRAINING

The state of Iowa began assisting counties with cybersecurity in 2012. The Office of the CIO's Information Security Division realized that county resources were — and continue to be —limited. It started expanding services to counties, first with in-state conferences and workshops on the importance of cybersecurity and then marketing its services and educating counties on its capabilities. Currently, all 99 counties in the state participate in at least one offering.

Iowa's Homeland Security Grant Program funds licensing, appliances, hardware and tools, such as vulnerability scanning for counties to focus their patch management efforts, for localities. The state also offers online security awareness training, incident response, anti-malware tools and an intrusion-detection service that continuously monitors networks.

The state has pilot programs for other services that will extend to all counties looking for assistance, plus it is piloting projects with local schools, cities and county hospitals.

The state pays particular attention to the human side of the equation. Iowa's Cybersecurity Services Coordinator stresses that building the state/local relationship is important even if a county opts not to use state services.


STRENGTHEN RANSOMWARE DEFENSES AND BUILD CYBER RESILIENCE
Read More

HOW TO STRENGTHEN RANSOMWARE DEFENSES AND BUILD CYBER RESILIENCE

An interview with James Yeager, Vice President, Public Sector and Healthcare, CrowdStrike

Ransomware has proven to be an unrelenting, volatile and evolving threat. Malicious actors continue to find new methods and new threat vectors for infiltrating government systems. Meanwhile, the ability of state and local agencies to improve their defenses remains hindered by outdated technology, a shortage of cyber experts, and inadequate funding.

Despite all of that, agencies can take steps to prevent ransomware attacks. To learn more, GovLoop spoke with James Yeager, Vice President for Public Sector and Healthcare at CrowdStrike, which provides cybersecurity services and solutions. Yeager highlighted three methods that are key to ransomware protection.

EXPLOIT BLOCKING

In many cases, malicious actors get into a system by taking advantage of a known vulnerability that an agency has failed to address. An unpatched vulnerability is the cyber equivalent of leaving a window open or a door unlocked.

In part, the solution is better cyber hygiene, Yeager said. Agencies need to know what software is installed on their systems, what systems they are connected to peripherally, and what vulnerabilities are part of that mix.

But given the scope of the challenge, agencies also need to assess the risks associated with each system, and leverage patch prioritization and automation solutions to ensure critical systems are always protected.

MACHINE LEARNING

Adversaries are operating with tremendous speed these days, Yeager said. Cyber defenses that look for the signatures of known attacks will always be running behind. "To match the speed of defense with the speed of the attack, we need to be operating at machine-speed levels," he said.

Machine learning leverages operational data from across the network to detect anomalies and identify malicious intent without relying on signatures. But this method requires massive datasets and sophisticated data models. Ultimately, most agencies will need to partner with cloud-based technology providers to make a machine learning-based approach feasible.

INDICATORS OF ATTACK

How do you know that a ransomware attack is underway before it is too late? The problem is that malicious actors have gotten good at obfuscating their activity.

Often their attacks comprise a series of steps, each of which is seemingly innocuous. Yeager compares it to recognizing that a bank robbery is in process. The person walking around the building might be out for a stroll, or they might be "casing the joint." The person entering the bank wearing a mask might have health concerns, or they might be hiding their identity, and so on.

"If interpreted on their own, they are not necessarily indicative of a potential breach," Yeager said. "But when you stitch them together with a pattern of behavior, they begin to tell the story."

CrowdStrike recognizes that there's no simple solution for ransomware. Instead, "it's about having a committed, sustained and truly modern approach to the three fundamental aspects of a security program: people, process and technology," said Yeager. "These three aspects must really work in concert if you want to tip the scales in your favor."

As challenging as it sounds, cyber resilience is an achievable goal, he said. "It can be done, and frankly, it's got to be done."

CULTIVATING CYBER AWARENESS DURING REMOTE WORK

A Q&A with Connecticut CISO Jeff Brown

Connecticut Gov. Ned Lamont signed an executive order that went into effect March 23 telling residents to stay home. It also ordered nones- sential businesses to close, except for telework. Most of the state's government offices also closed, swelling the number of teleworkers who needed remote tech support and cybersecurity protections. Jeff Brown, the state's new CISO, said making the switch wasn't easy but went smoothly.

"I joined the state in the middle of the COVID-19 pandemic and was working remotely from Day One. Connecticut moved the vast majority of our employees from being office-based to being fully remote in a matter of weeks. We were able to accelerate our efforts with [virtual desktop infrastructure] technology to get employees up and running very quickly and without a lot of problems. The technology group really did an amazing job getting everyone productive in a short time.

"Of course, any change of this magnitude comes with new challenges like patching, bring-your-own-device and the use of remote technology. Maybe the bigger challenge was getting people who were used to working in an office used to working from home. We managed to leverage solutions like group chat and 'cameras on' videoconferencing to help people feel more connected. I've worked at some big companies like GE and Citigroup with over 300,000 employees and understand how important it is to make people feel connected no matter where they are physically located."

To ensure that state employees were conscious of cybersecurity and could identify possible phishing or other malicious schemes, the state took several steps, Brown said.

> "We released SecurityMentor's 'Working Remotely: Anywhere, Anytime' training to all our employees and the agencies. We also set up a series of general IT checkpoints spanning the agencies where any concerns or glitches could be reported, including security issues. I had to quickly release some guidance around Zoom conferencing and other issues that arose. We also increased our general communications to make sure that everyone is aware that there are plenty of people willing to take advantage of this situation. I consider training and awareness a critical element of our security program. We've used tools like SecurityMentor for some time, but the big change is the volume of our other commu- nications. Since I'm new to the role, I've also tried to put a face to the program and security team despite not being able to meet everyone in person. This means one-on-one introductions with our stakeholders over videoconferencing and making sure that people knew how to engage our team."

Bad actors could consider the new telework environment target-rich, Brown said. Although some states have reported more phishing and malware attempts, Connecticut state employees have seen a different kind of threat.

> "Our fusion center is reporting that ransomware and phishing have been relatively stagnant, but I am definitely seeing an uptick in outright fraud as a concern. The Department of Labor across all states has been a target, so we are keeping vigilant and looking at identity-proofing technology to minimize successful fraud attempts. I think more CISOs will find fraud, be it cyber fraud or traditional fraud, landing on their agendas."

Just as the state had to scramble to implement a vastly expanded telework environment, counties and municipalities faced the same challenges. Brown said the state has tried to help wherever it can.

> "We are working closely with our agency partners. I think that
>
> security issues are pretty universal no matter what your business model looks like. I find that security professionals in general are very quick to share and collaborate. We have forums set up where concerns can be raised, and we can discuss solutions. One concrete area of assistance we provided is that our emergency management organization held regional security awareness training for local government partners that was really well received. We hope to do more like that. I intend to keep our collaboration level very high and leverage the state's ability to make more enterprise decisions that could benefit everyone."

The state has been moving toward a whole-of-state cybersecurity strategy for a few years, Brown said. This has been the foundation for much of the work undertaken in response to the pandemic.

> "We were one of the first states to have a formal cybersecurity strategy under Gov. [Dannel] Malloy back in 2017. To a degree, I am building on the work done by Arthur House, who was the Chief Cybersecurity Risk Officer of Connecticut at that time. The state is home to critical infrastructure, financial services, insurance and defense. We have two nuclear power plants, defense contractors like Sikorsky and a naval submarine base. We are also one of the few states — that I am aware of — whose state police under the Department of Emergency Services and Public Protection is trained up to help respond to cyberattacks that are not plausible for response from the federal agencies. These are the small and medium businesses that typically don't make it to their radar."
>
> "While all of these concerns are priorities, my initial charter is to make sure that security concerns that are directly under our control are addressed first. I've lived in Connecticut for years and security is a small industry, so I do intend to work with my fellow CISOs across the state in both public and private sectors."

WHEN THE THREAT ENVIRONMENT GETS PERSONAL

Conversation with Washington Sate CISO Vinod Brahmapuram

The state of Washington was the first publicly reported U.S. location of a COVID-19 outbreak and the first reported case of community spread.

Vinod Brahmapuram became the state's CISO in October 2019. He got caught 3,000 miles away when he returned to South Carolina to close up his house — he's been there ever since, teleworking.

> "One thing that helped Washington in this process was the policy the governor's office put in place two years ago that encouraged telework. Through NASCIO, we've heard that other states have found it very challenging. Our folks already were prepared in a way; the mindset was already there."

Even though state employees were generally ready for the shift, doing it all at once had a major impact on agencies' networks, from both performance and capacity standpoints.

> "When we went into this, we really had to increase our capabilities from a technology perspective. We use [virtual-private network] technology to allow them to connect back in; that number skyrocketed. [Before the pandemic,] remote working hovered around 4,000 or 5,000 people; even in bad situations it was around 6,000 or 7,000. But right now it's close to 30,000. There was somewhere between 35,000 and 40,000 employees where we had to create accounts and get them in place."

"There are a couple of things I'm very proud of. From the moment we had the early indication that there's a virus situation spreading fast, and some [concerns] this could lead to telework, that led to planning. We re- viewed our infrastructure architecture end to end and said, if everything changes and everyone is teleworking, what does that do to our capacity? We put measures in place: 'If this appliance hits this threshold, we'll do this. If that network reaches that level, we'll do that other thing.' And [second], what we saw immediately was that we had very good partners in our vendor community. Some offered things for free, like expanded capacity for 100 days, folks who offered things for three months, then extended them for six months. So between our plan and help from our partners, we were able to transition very well."

As the spread of the virus sped up, one issue states had to contend with was ensuring that employees had devices at home to work remotely. This was less of a concern for Washington state employees; anyone who uses a computer for work had already been issued a laptop.

"Even though we had to enable people to work remotely, everybody who was connecting back to the state network was on state devices, not personal devices. So we had a secure [setup] for access. Based on discussions I've heard within NASCIO, states that had already planned for these things, as in Washington, a lot of [them] are providing laptops whether the person wanted to work at home or not. States that didn't have a telework arrangement before coronavirus, their employees didn't have state-provided devices. [In many cases,] their personal devices were laptops from China. So, many of these states allowed employees to take their desktop PCs home, since they're better, trusted devices.

Certainly, our help desk met with big challenges. The questions started coming up extensively, not about connecting, but about applications. We had to pull resources from other areas [of our organization] and augment them."

Brahmapuram said the threat environment definitely changed because of the pandemic.

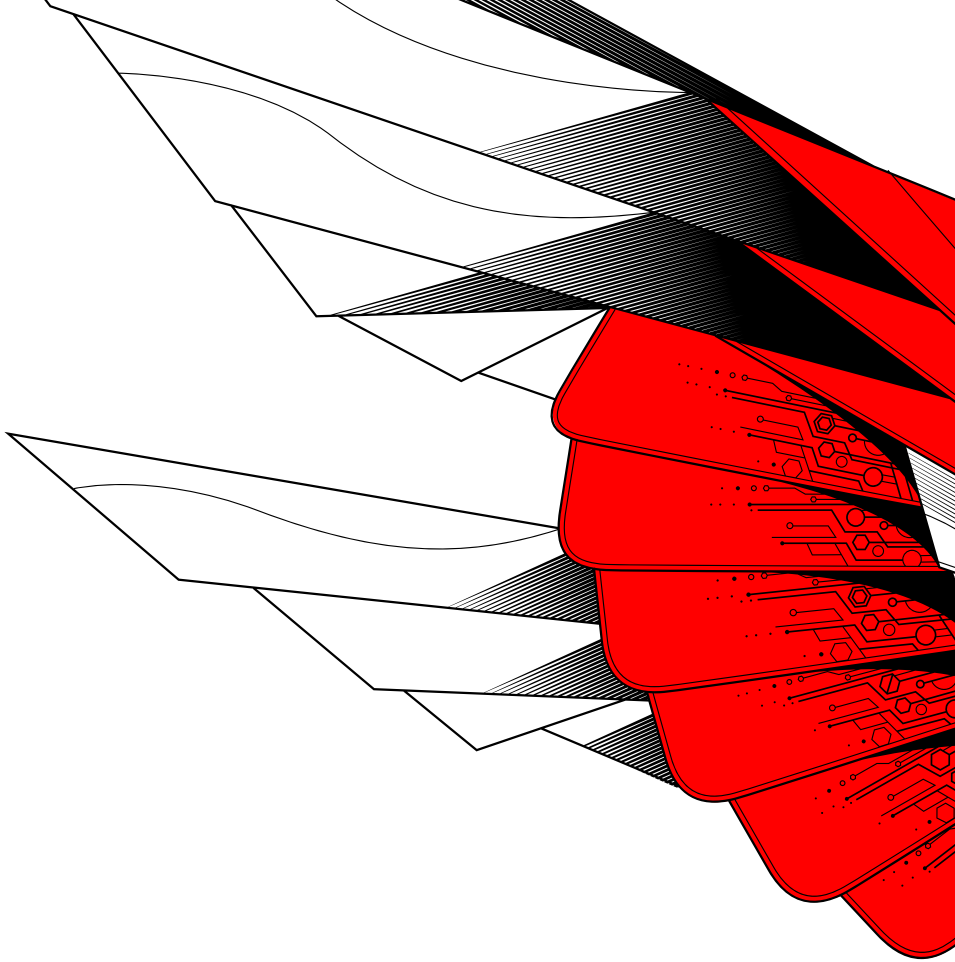
"The sad part is, any time there's...a topic of high importance, the bad guys are going to exploit that. They either want to make money or have another motive, like impacting the function of [an agency]. There were some actors that launched a [distributed denial-of-service] attack — they just wanted to create some tension and confusion.

"What we saw, what was heartbreaking to me — I consider it inhuman — was that people were worried and scared about their loved ones, and the bad actors started to take advantage of that fear. For instance, 'If you want to know if there are any active cases in your neighborhood, download this app,' which means they download malware or compromise their computers. There was so much unknown...people were hungry for

that information. They started exploiting them with financial scams, like 'donate to COVID research.' Threat actors are always looking to exploit an ongoing situation. Their attacks come from two angles: exploit human weakness or exploit technology weaknesses.

The state has been using its threat intelligence platform to share information and answer counties' and localities' questions, working through state and regional chapters of ASIS International, an organization for security professionals.

"These smaller organizations really can't afford to gather all the information they need, [so] we started putting the technology intel information on the threat intelligence platform. If there were things they saw, or if they needed other help, they could contact us and ask for it — we were providing that kind of support. Right now we're setting up additional resources with ASIS, the group that brings [together] all the counties in Washington state. We communicate a list of services we can provide. They said, 'Out of these 10 things that you offer, these three things would be helpful.' My team will be setting up educational meetings [through them]."



CONCLUSION

State and local governments are slowly beginning to reopen their offices, but now that agencies have wrestled through many of the challenges of telework, it's likely that some will continue to allow more workers to remain at home, at least on a partial basis.

This is not happening only because the pandemic is far from defeated, but also because, in many cases, having a high number of teleworkers has gone very smoothly. Governments that were reluctant to increase teleworking numbers have seen little downside to the new programs, especially as cybersecurity concerns have been mitigated.

That means cybersecurity professionals will need to stay vigilant about keeping their telecommuting workforce safe for at least some time to come, and perhaps on a more permanent basis. But armed with the lessons learned during the early days of the pandemic and tools and resources from groups such as NASCIO, NGA, NIST and others, that no longer seems as daunting as it had. Even after COVID-19 is a distant memory, telecommuting may be the new way that state and local governments efficiently conduct their business.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon®platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike:
We stop breaches.

THANK YOU TO CROWDSTRIKE AND DLT FOR THEIR SUPPORT OF THIS VALUABLE RESOURCE FOR PUBLIC SECTOR PROFESSIONALS.

ABOUT GOVLOOP

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to **info@govloop.com**.

govloop.com | **@govloop**