Innovations in State and Local Cybersecurity

GOVLOOP
E-BOOK
2020

SAP NS2
NATIONAL SECURITY SERVICES

Executive Summary

Improving government cybersecurity never ends — it can't. Every day, cybercriminals hunt for new weapons, such as ransomware, that can give them an edge. State and local agencies must be particularly wary, as they typically have fewer personnel and resources devoted to cybersecurity than their federal counterparts. Despite advances in cybersecurity strategies and tactics, agencies nationwide are constantly looking for fresh advantages.

But change isn't easy, and many state and local agencies discover that continuously upgrading their defenses is painful. Most agencies have tight budgets and can't afford to waste money on unsatisfactory solutions. Additionally, the number of tech-savvy government employees is limited, making engaging workforces and filling skills gaps a frequent challenge for agencies. Collectively, these obstacles can slow any progress toward an agency's mission.

Necessity is the mother of innovation, however, and agencies are dreaming up original ways to make cybersecurity exciting for the workforce. They're also brainstorming ways technology can make cybersecurity cheaper, stronger and more efficient.

In "Innovations in State and Local Cybersecurity: A GovLoop E-Book," we'll examine groundbreaking tools and techniques for healthy cybersecurity in the years ahead, describe the building blocks and best practices that can help your agency survive the latest cyberthreats, and spotlight several state and local thought leaders who have reinvented cybersecurity at their agencies.

Ultimately, our e-book demonstrates what dynamic cybersecurity is and how agencies can use it to stay one step ahead of today's risks.

Contents

In the News:

Need to Know:

Building Blocks:

Thought Leadership:

In the News

In December 2019, COVID-19 began spreading throughout China. Soon after, the coronavirus reached the U.S., and since March 2020, many government workers have been teleworking to support social distancing efforts to slow the illness' spread.

That shift to remote work dramatically transformed cybersecurity. It created new problems for agencies, but equally original solutions for addressing them.

Ahead, you'll learn about the cybersecurity challenges COVID-19 created and how agencies have learned to deal with future disasters.

COVID-19 Exposes Security Cracks

Cybercriminals use crises to their benefit. In April, ransomware struck the Assessor's Office in Orleans Parish, Louisiana. A growing threat, ransomware blocks access or threatens to leak victims' data unless they pay a ransom.

According to the agency, attackers didn't compromise its website or email operations. More importantly, the parish's cyber defenses prevented the ransomware from impacting citizens' personal information or disrupting public services.

COVID-19 Misinformation Spreads

The coronavirus outbreak gave cybercriminals another way to menace agencies. Besides using traditional attacks, cybercriminals could also capitalize on anxiety about the illness to trick employees into giving them what they wanted.

Recognizing this, the Cybersecurity and Infrastructure Security Agency (CISA) warned agencies in April that bad actors could scam them with false COVID-19 information. CISA also advised governments at every level to exercise elevated caution during COVID-19 because cybercriminals were hiding malicious software — or malware — in fraudulent emails.

Agency Attack Surfaces Grow

Broadly, an agency's attack surface includes all its cybersecurity risks and vulnerabilities. Unfortunately, teleworking typically expands these perimeters by adding new flaws such as unsecured network connections.

CISA cautioned agencies about their growing attack surfaces as employees began working from home. According to CISA, cybercriminals sought gaps in agencies' teleworking software and other tools — something state and local agencies might be particularly susceptible to because they might be unable to afford secure teleworking solutions.

Cyberattack Pain Lingers

In March, a cyberattack interrupted city services, including email accounts and server functions, in Torrance, California. More than a month later, the incident continued to plague Torrance in new ways.

Initially, city officials said the breach had not impacted public personal data, but a month later, they said data had appeared on the internet, possibly because of the attack. Leaders said the leaked information potentially included personal details about city employees and others.

Press Release: Torrance Experienced A Cyber Incident To City Servers

POSTED BY CITY OF TORRANCE IN COMMUNITY MATTERS, NEWS ≈ LEAVE A COMMENT

For most recent news, please visit www.CityOfTorranceCA.com.

A BALANCED CITY
INDUSTRIAL · RESIDENTIAL · COMMERCIAL
TORRANCE
©1984

TORRANCE EXPERIENCED A CYE
INCIDENT TO CITY SERVERS

TORRANCE, Calif., March 1, 2020 –
2:30 a.m., computer systems at th
of Torrance experienced a digital
compromise interrupting email acc
and server function. Safety operati
continue to have access to
communications. However, certain
business services are compromised

CISA
CYBER+INFRASTRUCTURE

MAY 2020

CISA INSIGHTS

COVID-19 Disinformation Activity

False and misleading information related to the coronavirus (COVID-19) are a significant challenge. This CISA Insight provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

COVID-19 DISINFORMATION

After the initial outbreak of COVID-19, disinformation campaigns appeared online. Information manipulation and fabrication about COVID-19's origin, scale, government response, and/or prevention and treatment surged as creators leveraged people's increased uncertainty.

Virus Origin

China and other authoritarian governments have promoted false claims about the origins of the virus in an attempt to shift blame overseas and divide free societies against themselves. Common tactics they use include censoring news, injecting false narratives onto social media platforms, and promoting slick government-produced videos.

Prevention and Treatment of COVID-19

False information about COVID-19 treatments continue to circulate on social media, including potentially extremely harmful suggestions to drink bleach or chlorine dioxide, to use vitamin C or boiled garlic, or that illicit drug activity can "cure" the virus.

PROTECT YOURSELF

There are simple steps you can take to minimize the likelihood of amplifying disinformation.

1. Go to trusted sources of information like www.Coronavirus.gov. FEMA has also established a coronavirus rumor control website at www.FEMA.gov/

COVID-19: Lessons Learned

National Guard Aids Maryland With Cyber

Cybersecurity is a team sport, but agencies can always play it in new ways. As COVID-19 spread in April 2020, Maryland's Information Technology Department (DOIT) joined with the state's National Guard (MDNG) for an unprecedented partnership.

The ensuing joint cybersecurity task force was the first of its kind to be launched because of COVID-19, MDNG said. Its job was twofold: monitoring Maryland's government websites to ensure they functioned properly and watching the information on these portals to verify their accuracy.

Collectively, the task force's efforts ensured that critical information about public services such as unemployment reached people continuously.

Virginia Fights COVID-19 Fraud

Cybercriminals quickly took advantage of the coronavirus by using it to fool victims. Launched in March, the Virginia Coronavirus Fraud Task Force aims to halt deception and exploitation related to COVID-19. Since then, the group has countered numerous scams. For instance, the task force warns that some scammers have posed as major health authorities to gain financial and personal information.

Cyber Insurance Shields New Mexico County

San Miguel County, New Mexico, encountered what could have been a worst-case scenario in January 2020, when ransomware hit the county's IT systems.

According to Taylor Horst, Risk Director for New Mexico Counties (NMC), cyber insurance quickly resolved the predicament. NMC is a nonprofit that assists all of New Mexico's 33 counties.

Ultimately, cyberattackers demanded $250,000 from county leaders after negotiations. The insurance policy paid that amount to unlock the county's IT.

Although cyber insurance may cost agencies upfront, it is a life raft after attacks.

Lawmakers Float New Funding

Recognizing the need for stronger state and local cybersecurity, four House lawmakers urged Congress to pass $400 million in assistance in April 2020.

Reps. Bennie Thompson (Mississippi), Cedric Richmond (Louisiana), Dutch Ruppersberger (Maryland) and Derek Kilmer (Washington) cited escalating risks from remote workforces in their funding request. The group addressed a letter to Speaker Nancy Pelosi (California) and Minority Leader Kevin McCarthy (California).

If passed, the funding would be available to public- and private-sector organizations. The request suggests that federal interest in aiding state and local cybersecurity may be rising.

COVID-19 Fraud

The Virginia Coronavirus Fraud Task Force

The United States Attorneys for the Western and Eastern Districts of Virginia, the FBI, and the Virginia State Police are working to protect the residents of Virginia from fraud and exploitation arising from the current coronavirus pandemic through the formation of the Virginia Coronavirus Task Force.

The Virginia Coronavirus Fraud Task Force is a joint federal and state group that will be led by Assistant United States Attorneys from both the Eastern and Western Districts of Virginia, in partnership with experienced fraud investigators from the FBI and the Virginia State Police. The mission of the task force is to identify, investigate, and prosecute related to the ongoing coronavirus pandemic in Virginia.

New Mexico agencies on edge amid rising ransomware attacks

Need to Know: 2020's Cyberthreats

Agencies can't predict how cybercriminals will attack, but unprepared agencies are the most vulnerable.

The following examples are some of the most popular tools and tactics cybercriminals use. Some of these threats emerged more recently, but other, older ones are finding new life as cybercriminals use them in unexpected ways.

Ransomware

It's easy to see why ransomware is all the rage with cybercriminals — they can reap large profits with little effort or risk. Plus, it gives them immense power.

Broadly, agencies have struggled to stop ransomware's three most common forms: encrypting, non-encrypting and extortionware, also known as leakware.

Encrypting ransomware encrypts victims' data, blocking access to it without a key. Non-encrypting ransomware, meanwhile, impedes resources without impeding access to data. Lastly, extortionware, or leakware, threatens to publish sensitive data unless a ransom is paid.

Regardless of the variety, ransomware can cause serious problems for agencies by disturbing their devices, networks and services.

Phishing

Phishing involves attempts to obtain sensitive information through deceptive electronic communications. Using phishing, cyberattackers can gain private details such as credit card numbers via email or other mediums. As far as cyberattacks go, it's one of the oldest tricks in the book.

But time has not made people less susceptible to phishing. Instead, cybercriminals have repeatedly reinvented phishing to hoodwink new prey.

Take social media platforms, such as Facebook. As these services have grown more popular, cybercriminals have started phishing their users. The resulting crimes are modern twists on longstanding hardships for agencies.

Remote Risks

People are often the weakest link in a cybersecurity chain. With that in mind, practicing robust cyber hygiene is never a given for agencies' employees.

Cyber hygiene only grows more complicated with telework. Remote workers frequently use applications, devices and networks that aren't as secure as their office equivalents. Many teleworkers also rely on home technologies such as outdated printers and other home technologies that may expose sensitive information.

Solutions: The Next Generation

Whenever hurdles first appear, agencies race to find ways to overcome them. One way is through emerging technologies, which are tools that aren't fully developed or widely embraced. In terms of cybersecurity, scores of emerging technologies show great promise for helping defend agencies.

Artificial Intelligence

Artificial intelligence (AI) mimics human cognitive functions such as reasoning, making their applications seemingly limitless.

AI is already making inroads for cybersecurity. Once deployed, AI can monitor and stop cyberthreats without humans.

Best of all, AI can free up employees for more engaging, complex work. At state and local agencies, AI can become a valuable force multiplier that augments their workforces.

Blockchain

Blockchain is a software-based distributed ledger for keeping records. Participating users can constantly monitor any stored information, ensuring that no one uses it illegitimately. Because adding blockchain records requires complex math, manipulating them is extremely difficult.

According to advocates and experts, this infrastructure makes blockchain extremely resistant to corruption and hacking. Used properly, blockchain could boost government records' accuracy, cybersecurity and transparency.

State and local agencies are optimistic. Agencies nationwide have launched pilot projects to experiment with blockchain.

Robotic Process Automation

Robotic process automation (RPA) software creates digital bots that can perform manual tasks with little to no human involvement. Using RPA, agencies can relieve their employees of many simple, repetitive chores.

Consider cybersecurity, which involves such mundane responsibilities as resetting passwords. After embracing RPA, agencies can assign unexciting operations to tireless electronic employees. In turn, human workers can focus on more fulfilling, high-level labor. Productivity then grows in tandem with employee satisfaction.

For state and local agencies, RPA offers help amid shrinking budgets and talent pools.

Building Blocks

At its heart, innovation is about injecting novelty into established concepts. For agencies, cybersecurity isn’t disappearing — it’s changing. And agencies that approach cybersecurity with open minds will uncover innovation during the process.

Nationwide, agencies that are creative about their cybersecurity efforts are thriving. Whether it is their procedures, personnel or partnerships, these agencies are netting victories from surprising strategies.

The following case studies highlight the cybersecurity creativity across state and local governments.

Getting Creative With Cybersecurity

1. Escape Room Cyber Training

At most agencies, cybersecurity training isn't exciting, engaging or applicable to employees on the receiving end. It isn't "alive" for them. But Washington's Office of Cybersecurity (OCS) proves cybersecurity doesn't need to be a chore. Since November 2018, OCS has conducted part of its annual cybersecurity training through an escape room competition. OCS teams race to solve puzzles and earn the clues necessary for accessing information on a laptop. The exercise illuminates some of the bad practices people commonly use to secure their digital information.

2. Awareness Campaigns

OCS isn't just reinventing cybersecurity training — it is also increasing its workforce's cybersecurity awareness. Every October, OCS celebrates vigorous cybersecurity with its Hacktober campaign.

In October 2019, OCS marked Hacktober's fourth anniversary. The 2019 exercise included an escape room excursion with more than 250 people representing 24 agencies across Washington and featured a new cybersecurity quiz that nearly 14,000 of Washington's employees took online. Additionally, OCS debuted a "careless cube" at its headquarters in Olympia. About 180 state workers examined the display, which listed common workplace security mistakes.

3. Shared Security Services

In recent years, ransomware and other cyberthreats have shown they can upend any agency at any time. But what if state and local agencies teamed up against their common cybersecurity enemies?

North Dakota's IT Department (NDIT) is exploring that possibility, said Kevin Ford, the state's Chief Information Security Officer (CISO). Ford says NDIT is considering whether it could host a shared security operations center (SOC) that would cover state and local agencies outside North Dakota.

SOCs are centralized units that oversee organizational and technical security. If NDIT shared its SOC, its intelligence and resources would be available to partner agencies. As a result, agencies both inside and outside North Dakota's borders could benefit from one another with their security knowledge and tools.

"We understand that we're all connected," Ford said. "Our cybersecurity boundaries aren't the same as our physical boundaries. The cyber risks one state is facing are the same risks other states are facing or will be facing in the future."

4. Vulnerability Disclosure Programs

Vulnerability disclosure programs improve cybersecurity by offering the public forums for reporting potential security gaps to agencies. Maintaining open channels, agencies not only find flaws they may miss, but connect with the public, too.

Delaware's Information and Technology Department (DTI) has an active vulnerability disclosure program. Using a form on Delaware's website, users can inform the state government about any potential security issues involving its resources or websites. DTI permits submitters to note possible shortcomings, such as access to data that exceed their expected or specified permissions.

DTI's cybersecurity program — and others like it — forge a valuable link between agencies and the communities they serve.

5. Bug Bounties

Bug bounty programs reward ethical hackers with recognition and cash incentives for finding cybersecurity vulnerabilities and reducing risk. Already well-established at the federal level, bug bounty programs are catching on at state and local agencies, too.

A noteworthy one was a hunt for IT penetration testing services that Memphis, Tennessee, hosted between February and March 2019. According to a request for proposal (RFP) in February 2019, city officials were interested in hiring a vendor that could assess their information security posture by probing for network vulnerabilities.

These partnerships can help agencies detect weaknesses in their IT systems before cybercriminals can. They can also help agencies measure how they're complying with all relevant federal, state, local and global cybersecurity regulations. Perhaps most importantly, bug bounty programs can stop cyberattacks before they affect agencies or the public.

Reaching the Cutting Edge of Cybersecurity

An interview with Bob Palmer, Senior Director, Software Solution Strategy, SAP National Security Services (NS2)

For government agencies, the harsh reality is that cyberthreats never stop evolving. New dangers emerge daily, ranging from hostile foreign nations to cybercriminals. The tactics used by these bad actors are constantly shifting. Whether agencies like it or not, their networks are permanently under siege.

New advances in people, processes and technology are transforming agencies' cybersecurity. Fresh approaches – like behavior analysis and endpoint security – are making agencies' cyber defenses stronger than before.

Bob Palmer is Senior Director, Software Solution Strategy at SAP National Security Services (NS2), an enterprise software provider. Palmer explained how agencies can reinvent their cybersecurity in three steps.

1. Put policy first

Agencies need sound direction and training on cybersecurity best practices, or their workers will end up in treacherous waters. Palmer recommended agency leaders establish clear guidelines for their employees' cyber hygiene.

For example, good policies often include warnings about the latest phishing attempts. Phishing involves imitating trustworthy sources online to obtain sensitive information from users. **"Bad actors know all it takes is one employee to not follow good security practices," Palmer said. "Network users are security's weakest link."**

2. Adopt behavior analysis

Behavior analysis measures the actions happening on an agency's network. According to Palmer, agencies derive the most benefit from it by determining how their networks "normally" operate. Next, agencies can continuously monitor their networks for abnormal behaviors that might indicate attacks. This approach goes beyond traditional anti-virus protection; it can identify new malware for which no digital signature is yet known.

Palmer listed suspicious IP addresses, lateral movement of systems' data, phishing email messages, and anomalous user activities as potential risks agencies encounter. "The whole system's behavior can be analyzed in context," he said. "Then, anomalous actions can be stopped, and the affected equipment quarantined before massive damage is done or data is stolen."

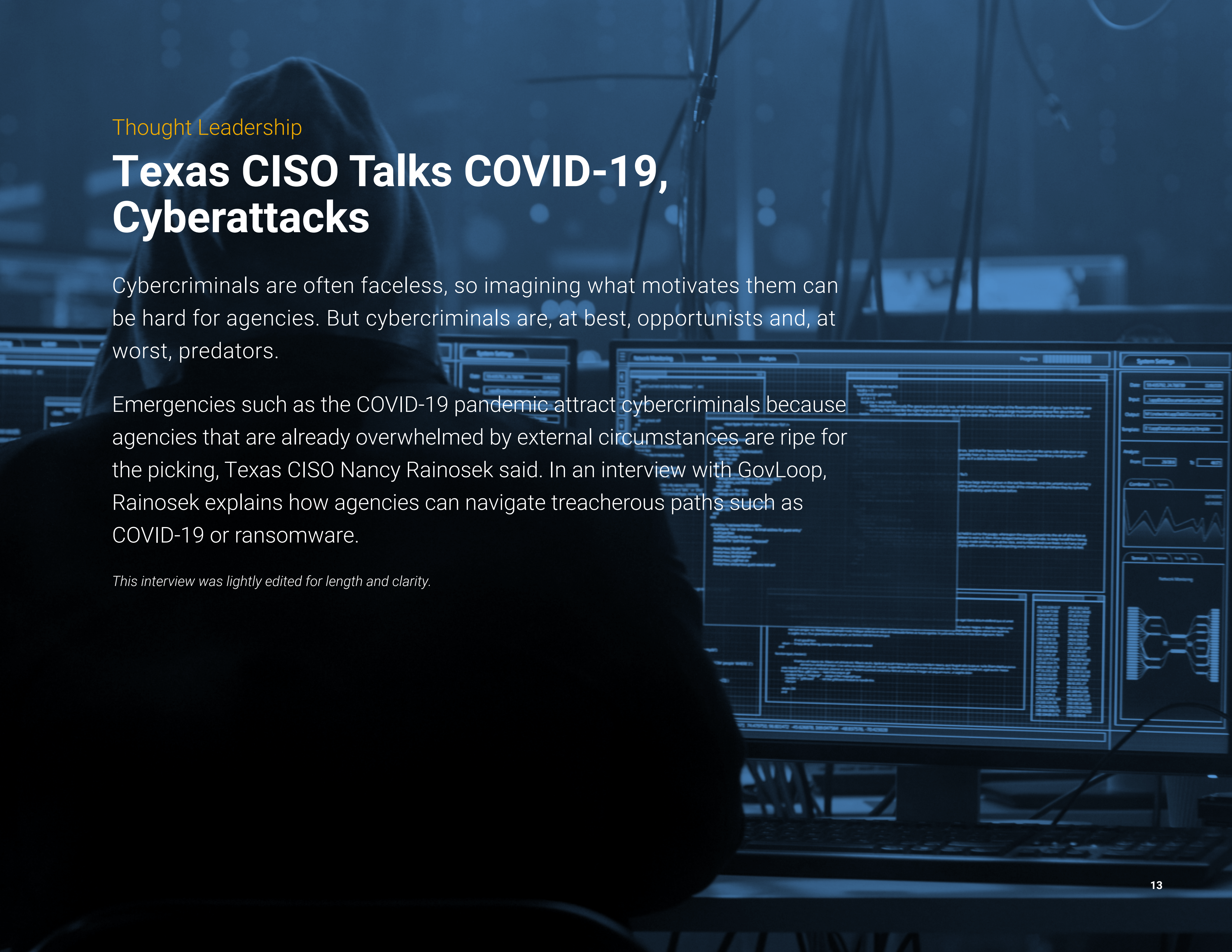
3. Embrace emerging technology

New technologies such as machine learning (ML) can be game changers. ML tools automatically learn from experience and can operate far more quickly with less human involvement. The results are dramatic savings in energy, money and time.

Endpoint detection and response (EDR) gives agencies another set of valuable capabilities. EDR monitors personal computers, servers and mobile devices for suspicious behavior, so agencies fully understand the events unfolding on their networks in real-time.

Inbox detection response (IDR) provides an additional layer of cyber defense. IDR mixes human and machine analysis to continuously monitor email inboxes for potential cyberthreats. For instance, users can conveniently flag suspicious messages for cybersecurity personnel and machine learning scans to examine. "To the extent this process can be automated, it can help organizations keep up with the volume of emails they receive," Palmer said. "It makes the employee part of the solution rather than part of the problem."

Ultimately, cyberdefenses aren't one-size-fits-all. Any agency can embrace the same innovative spirit driving robust cybersecurity, and SAP NS2 can help.



Thought Leadership

Texas CISO Talks COVID-19, Cyberattacks

Cybercriminals are often faceless, so imagining what motivates them can be hard for agencies. But cybercriminals are, at best, opportunists and, at worst, predators.

Emergencies such as the COVID-19 pandemic attract cybercriminals because agencies that are already overwhelmed by external circumstances are ripe for the picking, Texas CISO Nancy Rainosek said. In an interview with GovLoop, Rainosek explains how agencies can navigate treacherous paths such as COVID-19 or ransomware.

This interview was lightly edited for length and clarity.

GOVLOOP: How do state and local agencies' budgets, citizens and workforces affect how they handle ransomware?

RAINOSEK: Many government organizations, particularly at the local level serving smaller portions of the population, are often challenged on how they spend their limited resources. This limits their ability to keep systems current and have the IT personnel on staff to adequately handle ransomware events. Organizations often outsource their IT to a managed service provider that is responsible for their systems' availability and backups. This is what happened in August 2019 in Texas. One managed service provider was impacted, and the ransomware spread through their remote management software, which led to 23 organizations being impacted all at once.

What impact can major problems such as the coronavirus pandemic have on state and local agencies' abilities to fight ransomware?

It can have several impacts. Now, more than ever, hospitals need to have working equipment to save the many lives impacted by this pandemic. Ransomware is not just something that attacks computers; it can attack medical devices as well. Hospitals are highly automated, from patient records to essential medical devices. I cannot imagine what it is like working in a hospital right now, and to introduce malware to impact their ability to serve their patients only complicates things and prevents hospitals from treating at-risk patients.

Telework also increases the attack surface and introduces new levels of risk, because people are using home networks, which may have unknown vulnerabilities.

Finally, a situation such as this pandemic causes fear and increases people's desire for information about the current situation. This creates a situation in which people will be more easily duped into clicking on a link to retrieve information, only to be infected.

How should state and local agencies respond if ransomware strikes their networks?

First, disconnect impacted machines from the internet and their networks. If they can leave machines disconnected but not powered off, there may be evidence in the memory on those machines that law enforcement can use to try to catch the cybercriminal.

Secondly, contact law enforcement. This is a crime and we recommend contacting the local FBI office.

Next, have someone who is experienced in incident response lead the effort to bring systems back to normal. We never recommend paying the ransom. When someone pays a ransom to retrieve their files, they are funding these criminals to perform further attacks and develop more sophisticated tools.

Lastly, I would not have someone immediately log into a backup system to retrieve files. If you have ransomware crawling through your network, you need to be very careful to protect your backups so that they do not get encrypted when you log into the backup system.

What do you want readers' main takeaway to be?

Ransomware is real and can have a major impact on how governments perform their business, and therefore how citizens perform business. People often think cybersecurity is not a main part of their mission. If you can't issue marriage licenses, enable property sales or arrest criminals, you can't perform your mission. Technology is important and involves investment to make sure it is implemented properly and is secured so it works effectively and keeps criminals out.

Thought Leadership

North Dakota CISO on Sharing Cybersecurity

Cybersecurity takes a village. For too long, state and local agencies haven't realized that they can build on the same foundation when addressing their cyber hygiene.

Ford, North Dakota's CISO, says agencies are starting to notice opportunities for cybersecurity collaboration, however. For instance, North Dakota is weighing whether it can launch a powerful SOC that serves any interested agency regardless of geography.

During an interview with GovLoop, Ford detailed how a shared SOC might work for North Dakota and its partners. He also shared what distinguishes North Dakota's cybersecurity landscape from that of its peers.

This interview was lightly edited for length and clarity.

GOVLOOP: What does North Dakota's cybersecurity landscape look like, and how does it compare to others?

FORD: In North Dakota, we're more unified in two ways. First, the state provides a network service to all government agencies in North Dakota. That's the counties, the cities, K-12, libraries, so on and so forth. If you're a local or state government institution, you're welcome to be on the network. NDIT, the organization of which I'm a part, runs that. We can secure that network centrally, whereas other states may have multiple internet service providers at local governments they use. They may not have the ability to secure certain government assets. That's one way we're unique.

Another way in which we're unique is that we have a small state Senate bill, 2110, which provides NDIT strategic authority for cybersecurity for all government entities in the state. So, in addition to the network, we have some ability to issue policies to various institutions around the state for guidelines. We're looking for the "thou shalt" vs. the "thou should" line. That's something the state's looking for us to take the lead on, and that's something we're trying to step up to be able to do.

What are North Dakota's biggest cybersecurity concerns, and how is your state handling them?

My biggest concern that differentiates the state is the people of North Dakota — and the people of any state or federal government — don't have a choice in using your service. They pay taxes, we collect their information. We have an ethical duty to protect their information.

As far as specific threats, I'm concerned with phishing attacks across the state for financial gain. I'm concerned with the potential for ransomware attacks against soft organizations in North Dakota, whether that's human services, hospitals or other services that North Dakota's citizens need.

We don't know what organizations are launching these sorts of ransomware attacks. My intelligence suggests it's both criminal organizations within and outside the U.S. With ransomware, they want to target institutions where having all your data jumbled up and encrypted is the most impactful to the organization or the people who rely on that organization. That way, they can be more certain that people will pay the ransom.

From the state government perspective, what if something happens and the Secretary of State can't register businesses? That could impact commerce in North Dakota.

I'm concerned with critical infrastructure in the traditional sense, like power grids and water supplies. I'm also concerned with things that have negative externalities to our residents, whether it's mortgages, taxes, registering businesses, hunting and fishing licenses, or any of the other services that North Dakota provides.

How would North Dakota share an SOC with other state and local agencies, and what benefits would come from this approach?

It's still early days with that yet. We're working with a lot of interested parties. What we're trying to set up is something that moves the bar a little closer to day-to-day operations to get states more help with cybersecurity events. Our goal is to have a couple partner organizations that can provide support in a day-to-day cybersecurity business operation setting.

Every week, we may have several serious cybersecurity events that we respond to, but they may not reach the level of a statewide emergency where we would pull the lever, the alarms sound and we ask other states to come help us.

What we're trying to do is get some understanding in place. Then, if I have a security event that's not an emergency, but I still need help with it, I can rely on a member of the state to come help me before it reaches the emergency level. It's so we can swarm more effectively and prevent emergencies.

Conclusion

Cybersecurity innovations don’t happen overnight. The hard truth is nothing will make agencies’ cybersecurity permanently innovative.

Instead, cybersecurity innovation requires overhauling agencies’ people, processes, technology, and mindsets. By upgrading these areas, agencies can foster an innovative spirit governmentwide.

Thank you to SAP NS2 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