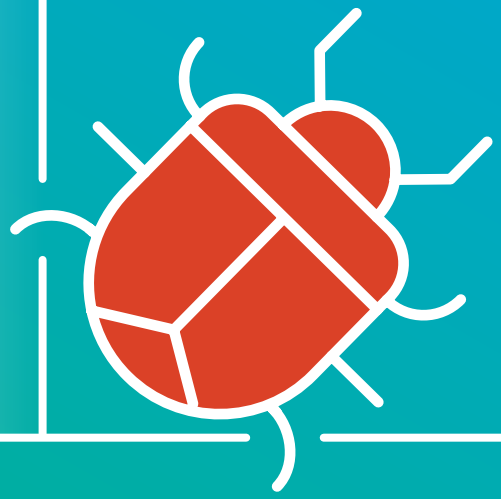
5 Ways to Defend Your Agency Against Ransomware





A GovLoop Playbook

govloop

rubrik

Executive Summary

Government organizations at all levels have been under siege for years now from ransomware attacks, which show no signs of letting up. About 60% of federal, state and local governments reported having been hit by ransomware attacks in Sophos' most recent State of Ransomware report, preventing organizations from providing services and incurring significant costs.

According to a study by Comparitech, 330 individual ransomware attacks were carried out against U.S. government entities between 2018 and October 2022, affecting more than 230 million people and costing about $70 billion in downtime alone — which doesn't account for ransoms paid or recovery costs, the latter of which can mount quickly. Perhaps more important to governments and their constituents, government organizations lost an average of 17 days of operations to downtime.

Ransomware operators are indiscriminate, attacking organizations in virtually every sector — including infrastructure, health care, schools and other institutions involved in public-sector operations. But organizations are not defenseless. There are steps they can take to help prevent an attack from taking hold, protect critical data in the event of an attack and, importantly, recover from an attack quickly while minimizing the damage.

To learn more about what government agencies can do to defend against ransomware, GovLoop partnered with secure data management company Rubrik for this report. We'll examine the challenges governments at all levels face, detail best practices for preventing and recovering from attacks and look at what agencies are doing to mount a united defense.



Need to Know

Government Organizations Are Prime Targets

In its State of Ransomware 2022 report, Sophos' list of the most-targeted sectors includes government organizations, as well as sectors such as critical infrastructure where the response to an attack could include government. Overall, 66% of organizations responding to Sophos' survey reported being hit by ransomware in 2021. The breakdown includes:

- Energy, oil/gas and utilities: **75%**
- Health care: **66%**
- Higher education: **64%**
- Central/federal government: **60%**
- Local/state government: **58%**
- K-12 schools: **56%**

*Source: **Sophos, State of Ransomware 2022***

Senate Report Finds Gaps in Ransomware Response

A **report** in May from the Senate Homeland Security and Governmental Affairs Committee found shortcomings in the government's reporting, data-gathering and response to ransomware attacks.

The report addressed attacks against a range of government entities including schools, local governments and businesses, as well as federal and state agencies. A paucity of data is hindering the response, as the report found gaps in reporting requirements. The FBI's running count of ransomware attacks, which relies on complaints being filed, "drastically underestimates" the number of attacks and the ransoms paid, the report states. The FBI itself considers the numbers to be "artificially low."

Congress passed the **Cyber Incident Reporting for Critical Infrastructure Act of 2022** to generate more complete data on cybersecurity incidents and ransomware payments. The law sets time frames for organizations involved in critical infrastructure to report attacks and payments to the Cybersecurity & Infrastructure Security Agency (CISA). Another goal of the law is to disrupt cybercriminals' use of cryptocurrencies for ransomware payments and to help victims recover quickly.



By the Numbers: Ransomware Attacks on Government

330
individual ransomware attacks on government organizations took place between 2018 and October 2022.

$5 million
was the total payments made in 27 of these 72 cases (though entities are more likely to disclose that they haven't paid the ransom than if they have).

$1,000 to $5.3 million
is the range of ransom amounts demanded.

17 days
was the average downtime government organizations lost, varying from six days in 2022 to over 20 days in 2018.



$36.5 million
was the total demanded in the 72 cases where ransom amounts were revealed.

523,942
individual records have been impacted by the attacks.

230 million
individuals may have been impacted by the attacks.

$70.4 billion
was the estimated overall cost of these attacks.

Source: *Comparitech*

IABs Feed the Ransomware Kill Chain

Initial access brokers (IABs), which breach the networks of organizations, then steal credentials and sell that access to other attackers, are on the rise. Their biggest customers are ransomware operators.

1,300 IAB listings existed on cybercriminal forums in 2021.

$1,000 to $10,000 is the price range for most access offers.

$4,600 was the average price for access.

Source: *KELA Cyber Intelligence Center*

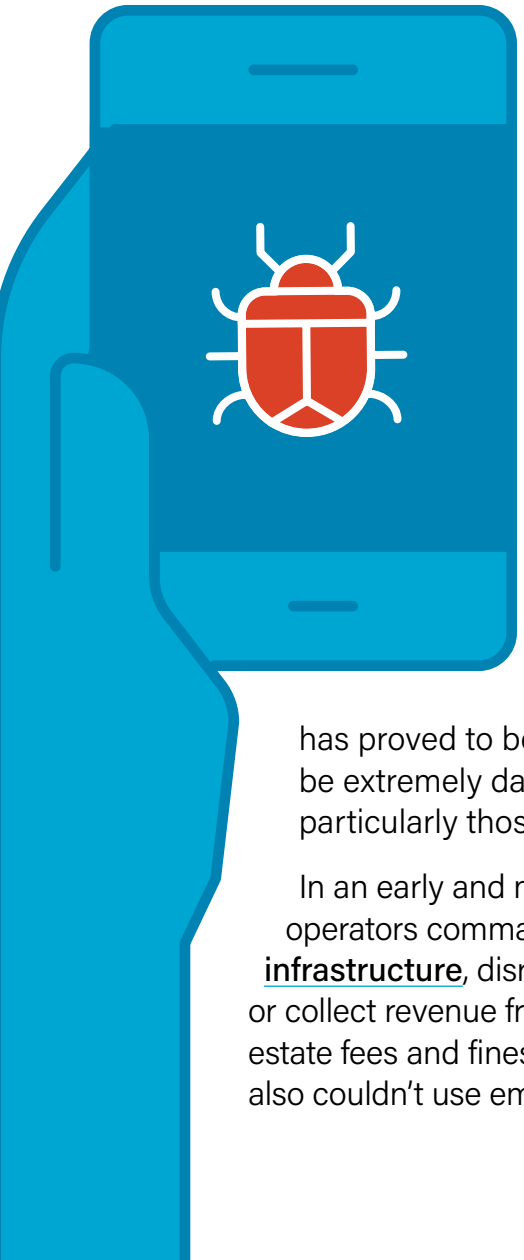
Some New Wrinkles in Ransomware

Ransomware as a service (RaaS): Ransomware operators no longer have to write their own code, but can pay for RaaS, which provides the ransomware code and the operational means to launch an attack.

Supply chain attacks: Ransomware operators multiply the impacts of their attacks via supply chains. A prime example is the Kaseya attack, which affected at least 1,500 of its managed service provider customers.

Double extortion: In a basic attack, ransomware operators encrypt information to freeze systems and demand a ransom in exchange for a decryption key. With double extortion, attackers also hold data for ransom, moving it to a separate location and threatening to make it public or put it to some other use if payment isn't made.

The Playbook: 5 Ways to Defend Against, and Recover From, Ransomware Attacks



Attackers have introduced some new tricks in recent years, but ransomware essentially follows a simple pattern. A user is tricked—via phishing or another tactic—into clicking on a malicious link that downloads a file, and then the user's system secretly executes the file. Ransomware then exploits vulnerabilities to spread throughout the organization, encrypting files as it goes. Finally, the malware displays a message demanding a ransom in exchange for decrypting the files.

Ransomware persists because it has proved to be effective for attackers. And it can be extremely damaging to targeted organizations, particularly those that are unprepared.

In an early and notorious case in 2019, ransomware operators commandeered the **city of Baltimore's IT infrastructure**, disrupting its ability to perform services or collect revenue from water billing, property taxes, real estate fees and fines such as parking tickets. Employees also couldn't use email or voicemail. After the city refused to pay the ransom, which was demanded in Bitcoin and was worth about $76,000 at the time, recovery efforts dragged on for months, amounting to a total cost of about $18.2 million. And in a cruel twist, it was revealed that a software patch **Microsoft had released** months before would have prevented the attack.

"Ransomware is probably the largest threat to organizations of all sizes, including the government agencies that I deal with," said Vice President of Public Sector Sales Engineering for Rubrik Aaron Lewis. And one of the biggest challenges they run into, he said, "is just a lack of preparedness." The question is whether agencies have the manpower and resources to implement the necessary measures. In many cases, they may need a private-sector partner.

Agencies can draw on guidance, such as that offered by the National Institute of Standards and Technology's **Ransomware Protection and Response** resource page and the Cybersecurity & Infrastructure Security Agency's details of the **Zero-Trust Maturity Model**. Agencies may also need to turn to an industry partner such as Rubrik, whose **zero-trust** approach and other services can specifically address the **ransomware threat**.

Government organizations looking to prepare for ransomware attacks can start by focusing on five key areas highlighted in NIST's **Ransomware Risk Management Framework**.

1

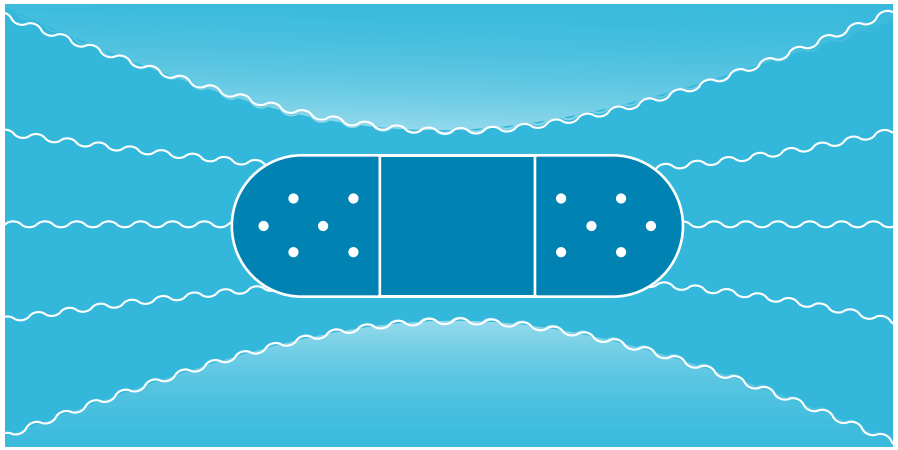


Know Your Risks

Federal, state and local government entities should start by understanding the risks, the business context and other factors involved in cybersecurity. Doing so allows an agency to prioritize its security measures consistently within its risk management strategy, which NIST says is foundational to effectively using the framework.

CISA offers a full slate of downloadable assessment and evaluation tools at its Cyber Resource Hub, including its Cyber Security Evaluation Tool (CSET). CSET includes a Ransomware Readiness Assessment (RRA) tool, which offers guidance to security teams on evaluating their network security practices with regard to ransomware. Drawing on recognized government and industry standards, CSET applies both to IT and operational technology (OT), including industrial control systems (ICS). So it can be used, for example, to assess the security of water and power systems on the municipal level, as well as any connected IT systems.

2

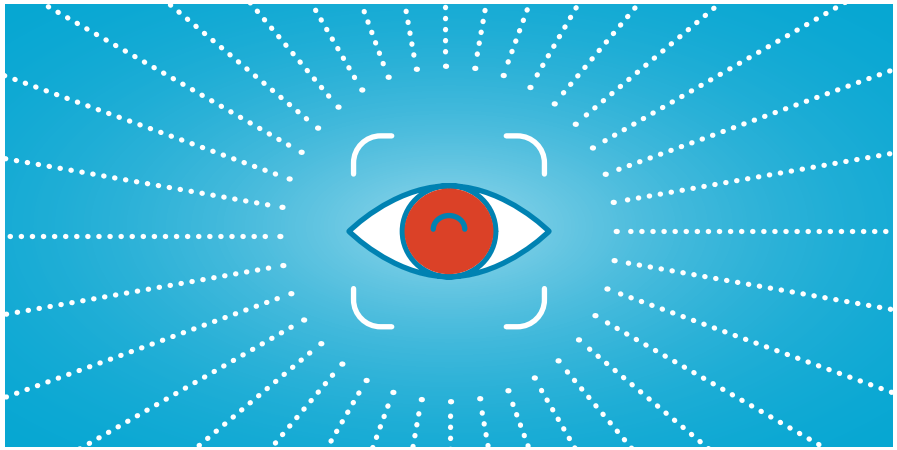


Build Resilience, Plan for Recovery

A recovery plan doesn't have to wait until after an attack; it can begin as soon as the root cause is identified. And it can be enabled by automated tools. Machine learning tools built into backup and recovery systems not only help detect signs of an attack, they can also identify specific files that have been compromised. Those tools can then restore files directly with a single click, rather than having to restore an entire virtual machine, further speeding recovery.

The goal is to build resiliency, coordinating activities among internal and external stakeholders, and making improvements to reduce the probability of future successful ransomware attacks.

3



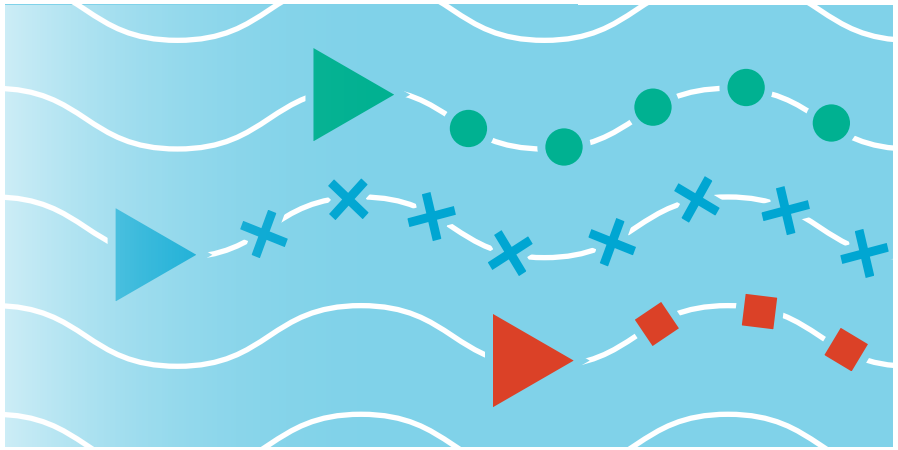
Detect the Signs of an Attack

Many attacks are designed to avoid detection, and can go unnoticed for weeks or months before taking effect. Continuous monitoring of information systems and assets — which is also part of a zero-trust framework — can help detect anomalies in network behavior that could indicate an external attack or an insider threat. It also can help organizations find and close vulnerabilities before an attack occurs.

Because real-time monitoring can help identify intrusions more quickly by enabling a rapid response, it can limit damage from an attack and help an organization swiftly recover. It also can protect backup systems, which are essential to recovering quickly, but which can suffer from failures due to applications, infrastructure, service outages and other factors.

A key component of effective monitoring is automation, including machine learning tools that are adept at identifying anomalies and exfiltration risks, in helping to speed response and recovery.

4



Respond According to Plan

Response is critical in containing the impact of an attack, and it starts with a detailed plan of processes and procedures. The immediate execution of a plan can help stop the corruption or exfiltration of data while preventing the attack from spreading to additional networks and systems. An effective response hinges on:

- **Communication:** Coordinating response activities with both internal and external stakeholders. Roles should be formally laid out in a response plan.
- **Analysis:** Alerts from detection systems should be fully investigated, which can help identify the root cause, understand the potential impact and help shape the implementation of the recovery plan.
- **Mitigation:** Immediately isolating the ransomware can minimize damage to data, prevent the ransomware from spreading and reduce the downtime an agency could potentially suffer from an attack.
- **Improvements:** Incorporating lessons learned from an attack is key to preventing future attacks and/or improving response.

5

Focus on Zero

Agencies need to develop and implement appropriate safeguards to ensure delivery of critical services. There are basic protections agencies should follow, such as always running antivirus software and keeping up to date with patches. There are also a few goals worth highlighting, such as multifactor authentication (MFA) and enforcing least-privilege policies, because they can make a critical difference in security. Ultimately, they should be part of a zero-trust strategy, which is an emphasis of the White House Executive Order on Improving Cybersecurity from May 2021 and the National Cybersecurity Strategy released in March.

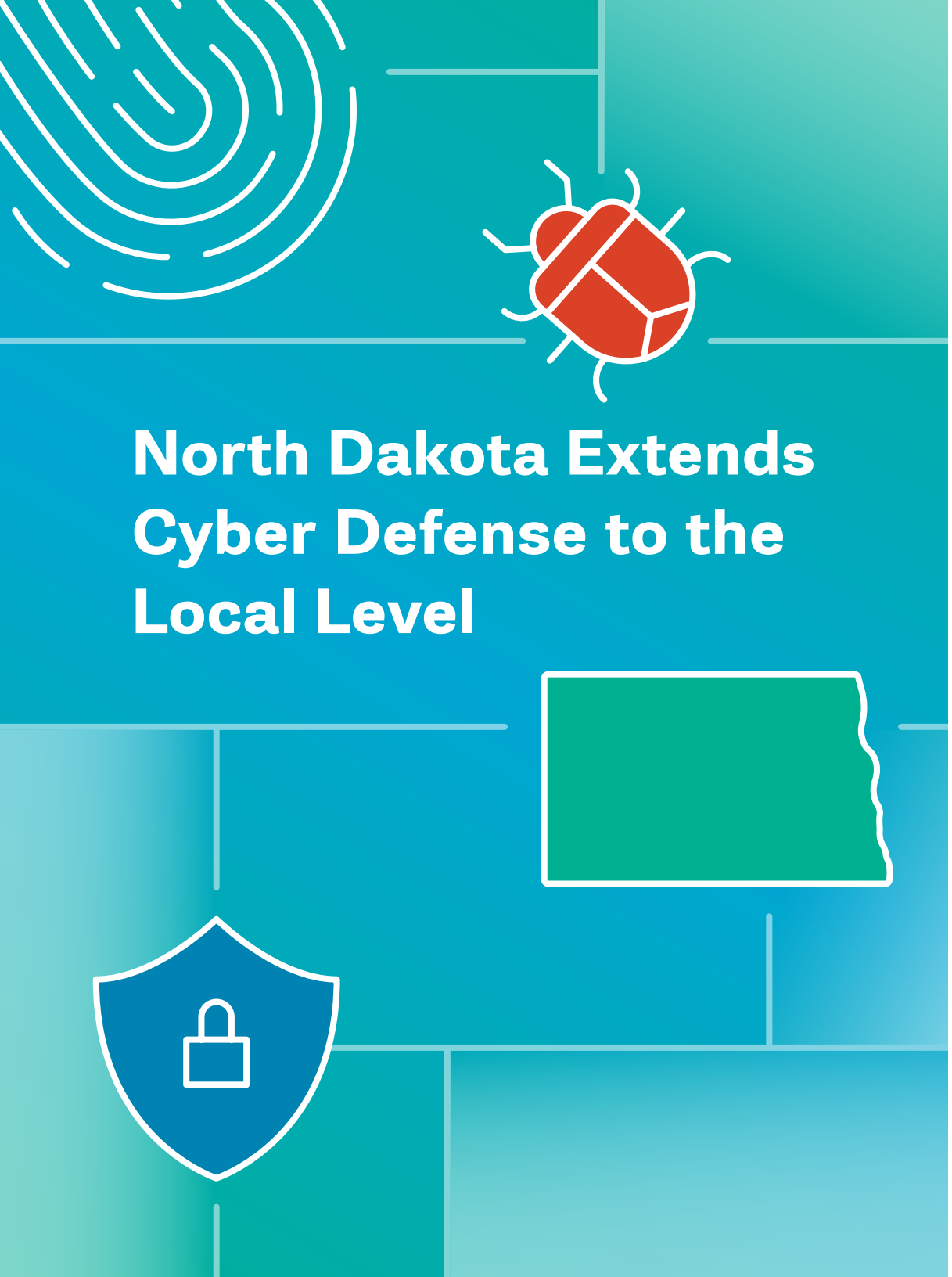
MFA, for instance, should apply to all user accounts, whether they connect on premises or remotely via the cloud. If working with an industry partner, look for a solution that includes features such as a native, time-based one-time password solution that easily integrates with third-party authentication providers. Least-privilege policies also are effective if properly enforced; one way to do that is with role-based access control, which allows administrators to assign users the lowest privilege level they need to do their jobs.

"It's part of the zero-trust framework," Lewis said. "Making sure that those credentials are locked down as much as possible is really key to that."

Zero trust addresses the fact that the network has outgrown the old notion of a perimeter separating in-house systems from what's outside. It seeks to ensure security through the continual verification of all user devices and resources (including applications, services and databases).

Among the other features of zero trust designed to protect data and assets are data encryption, which should always be applied to data at rest and in transit, including connections with third-party platforms. Network segmentation, or more specifically, micro-segmentation, breaks up the network into small, isolated areas of specific workloads. This can limit an attacker's ability to move around the network.





North Dakota Extends Cyber Defense to the Local Level

Defending against ransomware and other cyberattacks is an expensive proposition for state and local governments. Not only are the costs of a successful attack significant, but many agencies don't have the resources to fully protect their systems or respond to and recover from an attack. But in North Dakota, agencies have a place to turn for help.

State CISO Michael Gregg is leading a centralized state security operations center (SOC) that offers cybersecurity tools and services to agencies and political sub-divisions throughout the state free of charge.

"We offer our basic tools such as (endpoint detection and response, or EDR), vulnerability analysis and user awareness training to all agencies," Gregg said. "By deploying these tools, we can get ahead of the curve and work to prevent large ransomware events before there is impact."

It's part of a proactive approach to security that Gregg initiated when he took over as CISO in 2021. "When I started in my role, we were primarily in a responsive mode," he said. "We had a huge backlog of incidents and our team was stretched thin."

Gregg and his team upgraded their approach, quickly adopting automation and machine learning to help clear the backlog. The results have been significant: North Dakota's mean time to respond (MTTR) has been reduced by 90%, and its mean time to detect (MTTD) was reduced by 98%.

"These changes allow the system to handle repetitive tasks and frees up our team to grow, learn new skills and focus on new ways to secure state agencies and our citizens," he said.

‘Whole of State’ Approach

Paving the way for statewide cyber support was the passage in 2019 of Senate Bill 2110, which gave the North Dakota Analysis and Response team the authority to engage with and defend all entities that are part of North Dakota’s Statewide Technology Access for Government and Education (StageNET) network. StageNET covers state and local government, K-12 and higher education, and involves about 250,000 endpoints, Gregg said.

Once built, the North Dakota SOC began immediately working with government entities around the state.

“The key to getting agencies and the PSDs on board was to listen to their concerns and understand what they needed,” Gregg said. “We then adapted our practices to help meet their needs. I call this the ‘whole-of-state’ approach.” The SOC maintains custom dashboards for each entity and sets a minimum standard of security, though each entity is free to pursue higher standards.

The whole-of-state approach has been beneficial, he said. For example, the federal Infrastructure Investment and Jobs Act (IIJA) gave government entities a very tight window to apply for grants. North Dakota partnered with PSDs and submitted the applications and paperwork in less than a month. Not every state got its applications in on time.

Another benefit of North Dakota’s approach is that the agencies and PSDs that adopt the SOC’s tool get a 4% discount from the North Dakota Insurance Reserve Fund (NDIRF), which is significant considering the rising costs of cyber insurance (which has doubled or tripled in the past couple of years, driven by ransomware costs), and how it can help blunt the costs of an attack.

Prevention Is Still the Priority

Insurance can make a difference for state and local agencies, but there are caveats, Gregg said, because the terms of what a policy covers can vary widely.

“The amount actually covered in the policy may be far less than the actual cost of that attack,” he said.

That’s why North Dakota takes a more proactive approach focused on prevention. The SOC promotes basic security hygiene such as backups, endpoint protection and response, disaster recovery plans and vulnerability analysis, he said. “We also have tied our cybersecurity assessment process to our IIJA funding to determine which areas of the state need the most help, so we can focus funding where needed,” Gregg said.

Gregg recommends three best practices:



Plan before an event. “Understand that it’s a case of ‘when,’ not ‘if.’ Part of this preparation means not only having backups but testing your entire disaster recovery plan.”



Have adequate ransomware protection, including having EDR installed on all systems, keeping systems fully patched and using continuous vulnerability scanning. Security awareness training for employees is also critical.



Have a good incident response policy in place and consider a non-cost breach retainer, so if you need outside support, you can get it quickly.

Up to $10M Ransomware Recovery Warranty



Zero Trust. Maximum Data Security.

Enjoy the ultimate assurance from the data center to the cloud.

Rubrik offers up to $10M for the Ransomware Recovery Warranty* for Rubrik Enterprise Edition and Rubrik Cloud Vault.

rubrik

rubrik.com/warranty

*Rubrik warranty brings together the best technology, best practices, and expertise to partner with your IT teams. Terms and conditions apply.

Tap Available Resources for a Complete Defense

An Interview with Aaron Lewis, Vice President of Public Sector Sales Engineering for Rubrik

Building a defense against ransomware and other cyberattacks involves a progression of steps, all of them important. It starts with managing the identities and privileges of users, which can help prevent attacks, and extends to the integrity of the backups necessary for recovery. At each step, agencies must be careful not to overlook any weak links.

Focus on Identities

Ransomware operators most frequently get their foot in the door by stealing or otherwise compromising the credentials of employees. That tactic, in fact, is common among cyberattacks in general, which has led to cybersecurity strategies prioritizing Identity and Access Management (IAM) and zero-trust architectures.

Two essential components of the strategy are multifactor authentication and least-privilege policies. MFA has proved to be extremely effective in deterring credential-based attacks, yet many organizations are lax in applying it. Another important factor is enforcing least-privilege policies.

"Almost all of the recent high-profile cases involve some instance of elevating privileges," said Aaron Lewis of Rubrik. Least-privilege can restrict an attacker's ability to move about the network, but, like MFA, must be part of an enterprisewide policy.

"The most important thing is making sure that that technology is used across the board," Lewis said. An organization may implement MFA and least-privilege for critical workloads, but not for non-essential systems. "That tends to be where attackers can get in," he said, "and then they move sideways within the organization and get into those critical workloads."

Don't Take Backups for Granted

A common theme in security is to "assume breach," accepting the idea that sooner or later every organization will be victimized. That underscores the importance of fast recovery, which often depends on clean backup systems.

Without backups, agencies could be faced with recovering data and systems from scratch. "It can take weeks to months. Some organizations can't do it at all," Lewis said, referring to a county that had to try to recover via paper processes. Backups should be kept separate from the network, since ransomware operators also target backups. A solution that automatically scans backups can ensure they haven't been infected, Lewis said.

Being able to recover quickly is critical, and agencies may not have the resources on their own. Organizations that opt for a solution should find one that guarantees recovery, Lewis said. "And part of the way you do that is by guaranteeing clean backups," he said.

Lean on Your Partners

Performing all the steps required for a ransomware defense can be beyond the capacity of government organizations limited by staff shortages and tight budgets. Partnering with a provider such as Rubrik can ensure defense and recovery because it has resources and expertise that small IT teams may lack.

Lewis recommended that agencies take advantage of available resources, such as those from CISA and NIST, as well as from the private sector. "Make sure you're leveraging your technology partners," he said. "Because we are the experts in it. Make sure you're not leaving that knowledge on the table."

Conclusion

No organization is safe from being targeted by ransomware operators, as many federal, state, local and educational entities can attest. But government organizations can mount an effective defense, starting with a thorough plan for protecting data, devices and systems, and extending to recovery in the event that an attack penetrates their defenses.

A big challenge for government organizations, particularly smaller entities at the state and local levels, is a shortage of resources and manpower to fully implement protections and carry out a response. "Many organizations lack the resources, the people, the procedures and the training to be able to identify and respond when an attack happens," said Rubrik's Lewis.

Agencies can get guidance from federal sources such as NIST and CISA, and some can get help at the state level, as with the North Dakota example. But they also may need to rely on the experience, expertise and considerable resources of their technology partners because the value of services to constituents and the costs of a successful ransomware attack require a thorough and complete defense.







Thank you to Rubrik 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.
www.govloop.com | @GovLoop