From Ransomware Vulnerability to Resilience

GOVLOOP
E-BOOK
2020

rubrik

PURESTORAGE®

Executive Summary

If you've never encountered ransomware, imagine this: Malicious software threatens to publish or block access to your data unless you pay the attacker a ransom. For agency officials, ransomware presents a painful choice between spending precious funds or jeopardizing sensitive citizen data.

But ransomware isn't some bad dream – it's a harsh reality. Even worse, ransomware ranks among the fastest-growing cybersecurity threats facing today's governments. State and local agencies are particularly vulnerable to ransomware because, having smaller budgets and workforces than their federal peers, they are perceived as "soft" targets. Nationwide, agencies are finding that ransomware presents a clear, present danger to their missions.

If you work at a state or local agency, don't lose hope. Although ransomware creates serious challenges, solutions exist for weathering them. Agencies can strengthen their defenses by backing up their data, creating a rapid recovery plan and simplifying their security process management. Collectively, these steps can help agencies prepare for, survive and heal from ransomware incidents.

In "From Ransomware Vulnerability to Resilience: A GovLoop E-Book," we'll discuss the challenges of ransomware, identify the building blocks of a strong cyber defense, and share best practices for responding to and recovering from ransomware incidents, no matter your agency's size.

Although ransomware can hurt any agency, it isn't unstoppable. The insights the state and local thought leaders provide in this e-book will help your agency stay healthy whenever a ransomware attack strikes. More importantly, the cybersecurity resilience our e-book describes will help your agency achieve its mission.

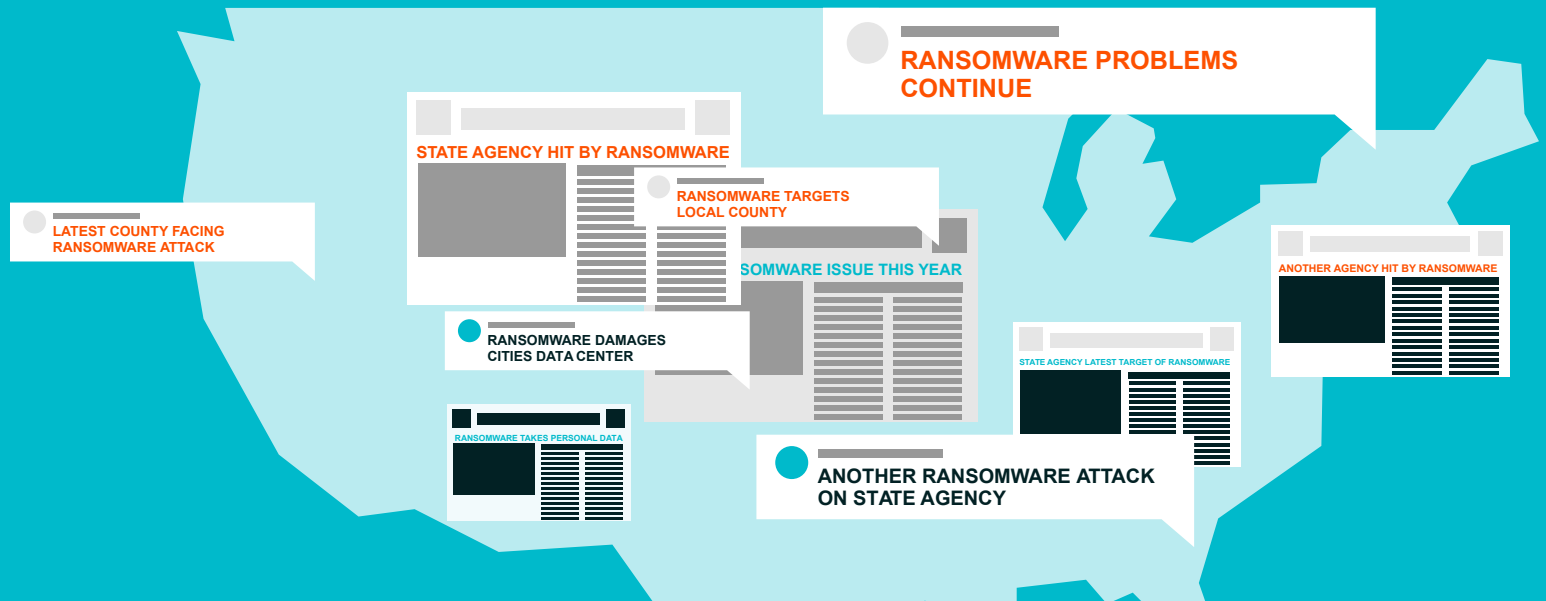
Contents

In the News

Ransomware attacks are happening nationwide. From the tiniest town to the largest state, no government appears safe from this cyberthreat.

One reason ransomware ranks among the most popular attack methods is it potentially generates large rewards for cybercriminals with little effort. And although federal agencies such as the FBI recommend against paying ransoms, some agencies can't resist. Ransomware creates an unprecedented disruption for these agencies, and they're willing to bet that addressing it sooner will aid them later.

The following pages recount some recent major ransomware incidents. They also detail the fresh ways agencies respond to this problem.



Reliving Near-Term Ransomware Events

Durham, North Carolina

On the evening of March 6, Durham, North Carolina suffered a ransomware attack. After the initial damage, the city announced that someone had opened an attachment containing ransomware, which infected 1,000 computers on Durham's network before the breach was detected. Ultimately, Durham's Department of Technology Solutions (TS) temporarily shut down the city's network to prevent further damage.

Although city officials acted quickly, Durham estimated that recovering all its systems would take four to five weeks. In a FAQ published after the mishap, Durham warned its employees against clicking unusual links in the future.

New Orleans, Louisiana

On Jan. 10, New Orleans announced it had restored functionality to its website after it lost many of its digital services on Dec. 13, 2019, when ransomware struck.

Mayor Latoya Cantrell said that recovering from the attack had cost New Orleans more than $7 million by Jan. 15. New Orleans could recoup $3 million from a cybersecurity insurance policy the city purchased before the incident, she added, but the event's cost demonstrates how expensive ransomware can be for agencies.

Louisiana

Louisiana's response to an attempted attack on Nov. 18, 2019 shows why ransomware can become so difficult for agencies. Soon after ransomware was detected, Louisiana's Office of Technology Services (OTS) began rapidly shutting down state networks. On one hand, the decision prevented a widespread ransomware infection. On the other, it interrupted many state services for more than a day.

Gov. John Bel Edwards also reacted rapidly to the attempted strike. During the incident, he used Emergency Support Function 17, a statewide emergency declaration that reassigned Louisiana's cybersecurity experts to affected agencies. Collectively, Louisiana's response shows the coordination agencies may need to stop potential intrusions.

Texas

On August 16, 2019, ransomware spread across Texas. That morning, at least 22 agencies statewide reported that ransomware had victimized them.

Four days later, the Texas Department of Information Resources (DIR) announced that every affected agency was recovering. According to the department, evidence pointed to a "single threat actor" behind the incident.

Ransomware has no limit on the number of people needed to deploy it; events like this one suggest that attacks might grow more coordinated over time.

Ransoms: A Tough Choice

US Mayors: No More Ransomware Payments

In 2019, the U.S. Conference of Mayors took a bold position against ransomware during its 87th annual meeting in Honolulu, adopting a resolution against making ransomware payments.

"NOW, THEREFORE, BE IT RESOLVED, that the United States Conference of Mayors stands united against paying ransoms in the event of an IT security breach," the resolution reads.

The conference cited a steep uptick in ransomware attacks during 2019 as the resolution's basis. At least 170 county, city or state government systems had experienced ransomware attacks since 2013, with 22 incidents happening in 2019, according to conference data. The group listed Baltimore and Albany, New York as two of the cities hit by ransomware that year, and Fisher County, Texas and Genesee County, Michigan as two counties targeted.

According to its website, the conference is the official nonpartisan organization of cities with populations of 30,000 people or more. With more than 1,400 cities currently meeting that benchmark, mayors could be crucial for America's efforts against ransomware.

New York Considers Anti-Ransomware Legislation

Two bills proposed in New York's Senate suggest a way for state and local agencies to stand together against ransomware.

State Sen. Phil Boyle's S7246 and Sen. David Carlucci's S7289 would prohibit New York's state and local agencies from paying ransoms to cyberattackers.

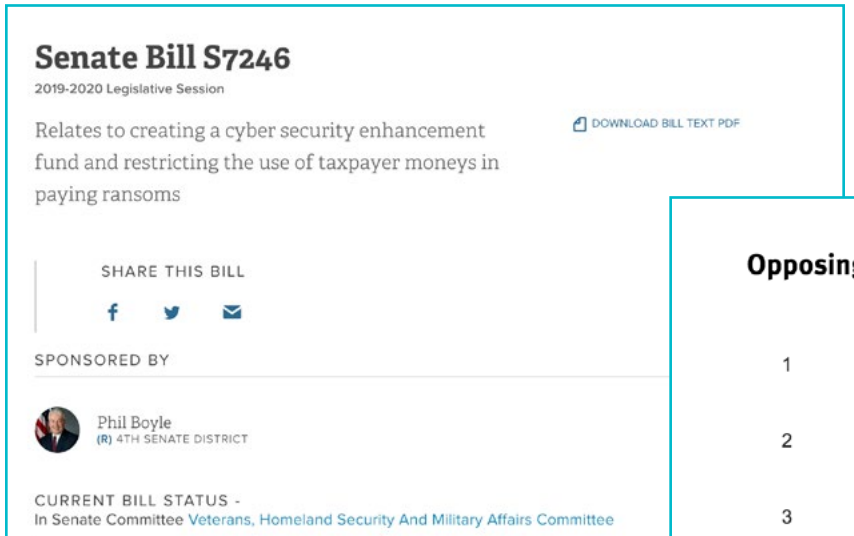
"This bill establishes that no local or state taxpayer funds shall be used to pay ransoms for ransomware attacks after January 1, 2022," S7246 reads.

"When municipal corporations and government agencies comply with these ransoms, they incentivize cyber-attackers looking to make a quick buck," S7289 states. "Prohibiting these entities from complying with ransom requests will remove this incentive and safeguard taxpayer dollars."

S7246 goes further than S7289 by imagining a state fund that would provide aid to local agencies for stronger cyberdefenses.

"This bill creates the Cyber Security Enhancement Fund that will make available grants and financial assistance to villages, towns, and cities with a population of one million or less for the purpose of upgrading the cyber security of their local government," S7246 states.

Collectively, this proposed legislation implies that agencies are trying to make ransomware less profitable for cybercriminals.



Senate Bill S7246

2019-2020 Legislative Session

Relates to creating a cyber security enhancement fund and restricting the use of taxpayer moneys in paying ransoms

DOWNLOAD BILL TEXT PDF

SHARE THIS BILL

SPONSORED BY

Phil Boyle
(R) 4TH SENATE DISTRICT

CURRENT BILL STATUS -
In Senate Committee Veterans, Homeland Security And Military Affairs Committee

Opposing Payment To Ransomeware Attack Perpetrators

1 **WHEREAS**, targeted ransomware attacks on local US government entities are on the rise; and

2 **WHEREAS**, at least 170 county, city, or state government systems have experienced a ransomware attack since 2013; and

3 **WHEREAS,** 22 of those attacks have occurred in 2019 alone, including the cities

Need to Know: Types of Ransomware

Broadly, ransomware appears in three forms: Encrypting, non-encrypting and extortionware or leakware. Regardless of the category, ransomware can cause serious problems for agencies and damage devices, networks and services.

Generally, each kind of ransomware differs in how it attempts to force payments from its targets. For agencies, it's a distinction without a difference. Once ransomware hits, it creates anxiety and confusion for workers.

Encrypting Ransomware

Encrypting ransomware encrypts its victim's data, leaving it unavailable without a key. It can freeze personal files and folders, locking up documents, pictures, spreadsheets and videos.

Generally, victims realize there's an issue only when they try to use a corrupted file. At times, this ransomware presents users with a "lock screen." Typically, this is a set of instructions for payment that launches once someone clicks on a formerly accessible file.

Additionally, encrypting ransomware pressures victims to rely on their attackers for a solution. Cybercriminals use encrypting ransomware to convince people that only their key will solve the problem.

Non-Encrypting Ransomware

Non-encrypting ransomware blocks access to data and files without encrypting them. Consequently, it can appear simpler than encrypting ransomware because no key is involved.

However, non-encrypting ransomware can become just as difficult for agencies. Non-encrypting ransomware often generates a full-screen image that blocks out all other windows and demands payment to remove.

Sometimes, non-encrypting ransomware changes a device's master boot record (MBR) rather than its screen. When this happens, the device's normal boot process disappears. A message seeking money replaces the startup screen.

Extortionware or Leakware

Extortionware or leakware may be the most frightening ransomware. It steals data or files and then threatens to release them. Governments must either spend tight budget dollars or expose sensitive citizen data.

Overall, cybersecurity is a top concern for agencies because of citizen data. Government employees who mishandle this information may lose public trust, pay fines or face criminal charges. With such severe consequences, agencies may rush to pay extortionware or leakware ransoms rather than suffer embarrassing data breaches. Although tempting, it's not a painless solution for agencies encountering this ransomware.

Need to Know: Ransomware's Impact

Manual Labor

Once ransomware blindsides agencies, they might feel like they've returned to a time before modern technology.

Consider the world that existed for agencies before the internet. In that era, agency employees relied on paper rather than digital forms. Communication couldn't occur across large distances via chat or email systems. Most noticeably, public service involved strictly in-person encounters between citizens and government employees.

Ransomware can temporarily resurrect these pen-and-paper days. For agencies used to conducting business with contemporary conveniences such as websites, it can be a jarring transition for any length of time.

Public Outrage

Citizens rely on their governments for everything from fishing licenses to paying utility bills. When those capabilities vanish, citizens may become increasingly disappointed with the agencies serving them.

The fallout only worsens when the services agencies provide directly influence people's lives. Ransomware can delay critical functions such as emergency services, health care and electricity. Gradually, ransomware can erode the delicate trust between agencies and the citizens they engage with.

Resource Drain

Ransomware can leave agencies with dwindling resources.

Government budgets are stretched thin enough without ransomware. With some attackers demanding tens of thousands of dollars, the price tag for this obstacle may grow too steep for agencies.

The workforce is another hurdle. Agencies can hire only so many personnel, including IT staff. As a result, ransomware attacks can morph into all-hands-on-deck affairs.

Finally, ransomware saps valuable time from agencies they could spend on their missions. Agencies rarely have enough hours in the day to meet objectives as it is.

Feeding Crime

No agency wants to cause more crime, but ransomware can do just that. When agencies pay ransomware attackers, they're potentially funding more cybercrime later.

Like legitimate businesses, cybercriminals need money to survive. For these bad actors, ransomware payments can become a valuable revenue streams. Cybercriminals who repeatedly profit from ransomware can use their ill-gotten gains for more attacks.

Building Blocks

Cybercriminals are notorious for hitting agencies when they're down. They won't hesitate to unleash ransomware during unrelated crises. Pandemics, natural disasters and even terrorist attacks are opportunities for cybercrime. As a result, agencies should always be ready for ransomware.

What does ransomware preparedness look like? Initially, constant vigilance can help agencies foil possible attacks. After that, agencies must implement the right tools to shield their data and heal it after successful breaches.

Best Practices for Detecting, Stopping and Recuperating from Ransomware

1 Streamline Data Storage

Agencies' data is often scattered across both legacy and modern IT. Agencies that use cloud computing have distributed IT that is mostly non-physical. Regardless of their IT arrangements, agencies must determine the most effective way to store their data.

To streamline their data storage, agencies can adopt policy-driven platforms. Policy-driven platforms ease data management and recovery. First, they assist agencies with complying with all applicable data privacy and security regulations. Second, policy-driven platforms simplify data storage by improving information transfers between physical and cloud environments.

2 Backup Data With Native Immutability

Data backups are often agencies' last line of defense against ransomware. These backups are valuable as they can effectively restore data attackers blocked. Frequently backing up data can reduce the power ransomware wields over agencies.

But data backups aren't invincible. Ransomware can still encrypt, paralyze or delete any backup. And protecting data backups only grows harder for agencies while they're identifying or recovering from attacks.

Native immutability can offer agencies a way out by making their data backups harder for external forces to read, change or erase.

3 Recover Rapidly

Ransomware attacks are a question of when, not if, for agencies. No matter how much they want to, agencies can't fend off breaches forever.

Fortunately, agencies that rapidly recover from ransomware can come back swinging after incidents. Rapid recovery involves quickly identifying the most recent uninfected version of agencies' data. Such version control helps agencies regain information that might have seemed lost.

4 Get Granular Visibility

Agencies can't fight ransomware blindly, and granular visibility helps them see all their data clearly. Data visualizations can help agencies understand which applications and files ransomware are affected. Afterward, agencies can roll back corrupted assets to unaffected backups.

Granular visibility can also give agencies before and after snapshots of their data, exposing any alterations ransomware makes. These insights boost agencies' ability to recover from and respond to ransomware.

Additionally, granular visibility reduces the risk of data loss from mass restores including uncompromised data.

Cyber Resiliency, Ransomware and COVID-19

The details sound like apocalyptic fiction: During an unprecedented viral pandemic, cyberattackers repeatedly batter overwhelmed agencies. Sadly, that sequence of events remains a legitimate possibility during the ongoing COVID-19 crisis.

In late 2019, COVID-19 infections began spreading worldwide from China. Highly contagious and potentially fatal, the virus led most global governments to encourage quarantining and social distancing.

In the U.S., agencies from the top down are preoccupied with fighting the virus, and cybercriminals are eager to exploit targets that are more vulnerable than usual. The subsequent threat landscape is more elevated for all agencies, but especially state and local ones with fewer personnel and resources.

How can agencies battling COVID-19 – or similar catastrophes in the future – prepare for ransomware? Here are some tips:

Expect the Worst

Agencies shouldn't expect mercy from cybercriminals during dire circumstances. After painful events, agencies should look for ransomware attacks.

Consider employees who are anxious about COVID-19. Cybercriminals may use false information about the virus to trick them into downloading ransomware or other cyberthreats.

Tighten Cyber Hygiene

Robust cyber hygiene is vital for sturdy security defenses. It is a mentality that only grows more important during emergencies such as the COVID-19 outbreak.

To improve cyber hygiene, agencies should frequently teach their workforces about cyberthreats and how to handle them. For example, ransomware is less likely to fool employees who are familiar with it. Even better, trained employees can find and stop ransomware attacks. During uncertainties such as pandemics, this knowledge can save agencies valuable energy and time.

Take Advantage of Data Backup, Recovery

Tools aren't useful if they aren't used. Data backup and recovery solutions are no different, so agencies must teach employees to use both. Although recruiting data experts can help, agencies must also train existing employees for better data literacy.

Workers who practice data backup and recovery are more prepared when any calamity emerges. Obstacles such as COVID-19 loom, but agencies can fortify their data against other hurdles such as ransomware. By making data backup and recovery second-nature, it is less likely ransomware can catch agencies unaware.

Ransomware Readiness With Data Backup and Recovery

An interview with David Siles, Global Field Chief Technology Officer (CTO) at Rubrik; and David Huskisson, Director of Rapid Restore Solutions at Pure Storage

Ransomware's prevalence is rising. Cybercriminals can quickly and easily profit from it and they crave the control ransomware gives them. Using ransomware, cybercriminals can force any agency to do their bidding. And cybercriminals often target state and local agencies because of their smaller budgets and workforces.

Despite this, David Siles, Global Field Chief Technology Officer (CTO) at Rubrik, and David Huskisson, Director of Rapid Restore Solutions at Pure Storage, say state and local governments can survive these cyberattacks if they have a good data backup and recovery strategy in place.

Huskisson and Siles shared three ways agencies can leverage Rubrik, a cloud data management provider, and Pure Storage, a data storage hardware and software provider, to back up their data and recover from ransomware attacks.

1. Make data snapshots immutable

Data backups are agencies' first line of defense against ransomware. After attacks, they can recuperate by restoring their data with backups untouched by ransomware.

Unfortunately, cybercriminals are now attacking backup data to prevent this. Immutable data snapshots can solve this dilemma by frequently copying agencies' data in real-time. By repeatedly cloning their data, agencies create too many clean versions for ransomware to infect. Immutability, meanwhile, ensures no one can alter any data after it is snapshotted. "**It's written once, and it can only be appended to," Siles said of each snapshot.** "It can't be modified. It should never be changed once it's taken."

Although nothing is invincible from ransomware, immutable data snapshots can help fortify agencies against it.

2. Recover rapidly

Ransomware's power comes from its impact on citizens and governments. For agencies, ransomware can prevent them from completing their missions. For citizens, ransomware can disrupt crucial public services for unpredictable amounts of time. "**Agencies aren't able to deliver critical services if their IT infrastructure isn't up and running," Huskisson said.** "Every second you're down, it might cost you money."

Rapid data recovery, however, removes some of ransomware's sting by recovering any lost data nearly instantly. Rapid recovery tools can boost agencies' agility while strengthening their business continuity; meaning agencies can resume normal operations in hours rather than days or weeks.

3. Simplify data management

Although immutable snapshots and rapid recovery are helpful, they aren't the only chapters in the government data story. With modern tools needing increasingly large amounts of data to operate, agencies need a platform capable of managing big data stockpiles. "It's the classic more with less approach," Huskisson said of solutions such as the ones Rubrik and Pure Storage provide. "Our tools allow administrators to manage more data per administrator."

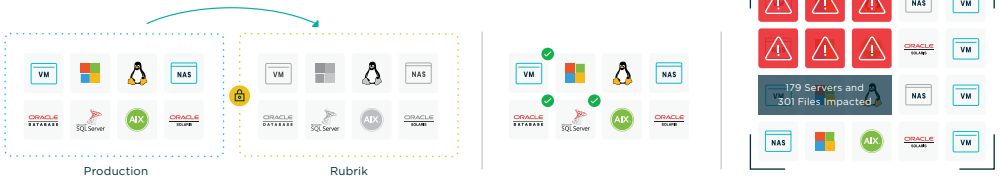
No cure exists for ransomware, but simple data platforms are the first step for overcoming it. Agencies that add immutable snapshots and rapid recovery to their data capabilities are well shielded for whenever ransomware strikes.

COMBAT RANSOMWARE WITH RUBRIK

Native Immutability
Safeguard Backups

Fast Recoveries
Minimize Downtime

Granular Visibility
Reduce Data Loss



Backups are often your last line of defense against ransomware attacks and can be an effective way to restore data that has been locked or encrypted by the attacker.

https://www.rubrik.com/en/products/polaris-overview/polaris-radar

rubrik | public sector

THIS GUY IS HUNTING FOR YOUR BACKUPS

Hackers spend over 200 days on your network **before** encrypting data.

Make sure your agency is ready.

PURESTORAGE®

Exploring New Mexico's Ransomware Defenses

Many of New Mexico's ransomware defenses are built from the ground up. With 33 counties spread across the fifth-largest state in the country, local governments are major players in the state's collective cybersecurity.

Taylor Horst, Risk Director for New Mexico Counties (NMC), a nonprofit association that serves every county statewide, said ransomware is a daunting obstacle for state and local agencies such as New Mexico's.

During an interview with GovLoop, Horst explains what he has learned about ransomware working in New Mexico.

This interview has been lightly edited for clarity and length.

GOVLOOP: How does cybersecurity insurance help protect agencies from ransomware?

HORST: One of the coverages available in cyber liability policies is called "bricking coverage," and it's called "bricking" because once your computer's been encrypted, it's as useless as a brick. So, there are some property damage coverages available in different policies to basically take your computers, go put them in the dumpster and buy new ones, vs. trying to unsnarl the ransomware.

From an insurance perspective, it's an interesting coverage. That's because it includes first-party coverage, third-party coverage and typically some compliance coverage. There's starting to be bodily injury coverage in there too, which is a part of third-party coverage. But it's the only insurance product that has all these coverages in one package.

And it is a young product. I don't think the insurance carriers fully understand the risks that they are trying to underwrite with it. Basically, they're collecting five-figure premiums for this coverage and paying out six- and seven-figure ransoms. That's not going to go on very long before they sublimit the coverage for ransomware events, the premiums go up dramatically or both.

How does ransomware affect an agency's budget, its workforces and the citizens it serves?

There can be many impacts. With the cyber liability policy that we have in place here, there's a $25,000 self-retention. So, there's the impact of any claim. And there's a lot of costs in employee time because the IT people work all weekend long – you have some disruption because of that. If there isn't a quick resolution, then there are other departments that can't operate.

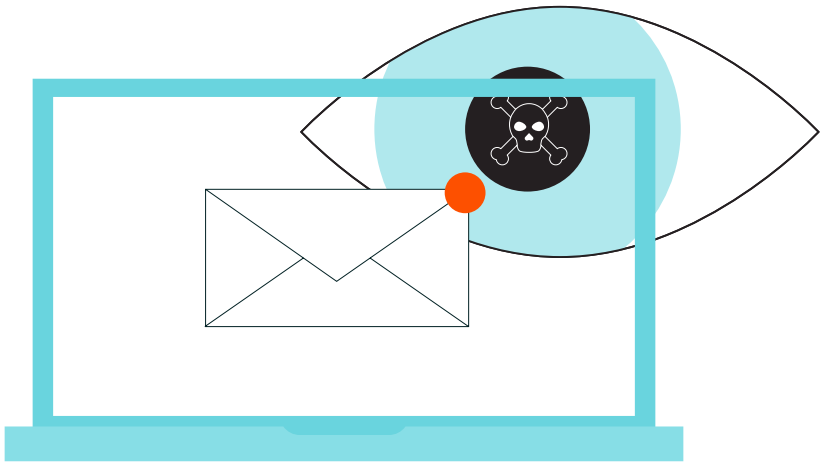
I'm thinking first, though, about the public-facing services. Depending on how sophisticated the county is, there's probably a system in place that they use to help them manage their public works efforts. It is snow removal, road repair and things like that. So, there are all these services that county governments provide that can't be avoided. They must keep the roads clean. It varies by county, but some counties, for example, are responsible for trash pickup.

What's the main takeaway that people should have after learning about ransomware?

The main takeaway is you just can't be too careful. Another major point is isolating your actions. You can either isolate your network or the actions that you take on a computer. Don't be using Facebook in one tab on your browser, and then be using business systems on the other tab in your browser. Isolate what you're doing to try and cut it into smaller pieces.

Ransomware is not unlike COVID-19. With COVID-19, there's people traveling all over the world now all the time. We've just got all this social interaction. And COVID-19 and ransomware are some of the bad results from us having all this social interaction.

I think we're going to have to learn how to have faith in social interaction. Right now, we call it social distancing. I don't know what the computer equivalent of social distancing is, but it might help with the ransomware.



Georgia CISO Talks Ransomware Readiness, Disaster Prep

As Georgia's Chief Information Security Officer (CISO), David Allen has seen many ransomware attacks. In some cases, agencies have bounced back in days. In others, they've been reduced to using pen and paper.

In any case, Allen says that preparing for ransomware can teach agencies important lessons that they can apply in many ways, including to other cyberattacks, pandemics or something else.

During an interview with GovLoop, Allen describes how bracing for ransomware can equip agencies for many setbacks.

This interview has been lightly edited for clarity and length.

GOVLOOP: How do situations like the COVID-19 pandemic affect ransomware preparedness, especially with so many agencies working remotely?

ALLEN: If our attention is on other things, it provides an opportunity for adversaries to step up attacks. Everybody's awareness of ransomware was heightened over the past year and we saw a decrease in a lot of issues or incidents. Or, at least we saw a decrease in the severity of them when they occurred because there were people taking definitive action to make sure that ransomware attacks didn't happen to them.

I think cybercriminals are relying on us to take our eye off the ball in that regard. They're seeing it as a potential opportunity to cause some damage and extort additional payments. And we have seen an increased spike in activity out there.

The No. 1 thing with working remotely is to maintain vigilance. Typically, our home networks are not as secure as the ones we use in the office. So, the second piece is stressing to our employees that they should practice good cyber hygiene at home. It's using complex passwords, being mindful of specific policies about bringing your own devices, etc. As far as the IT staff, if they're monitoring net flow, they need to pay extra attention.

We're just going to have to stay diligent from a security perspective. We must be mindful not to roll back any security protocols out of convenience. We should be able to adjust to this new normal.

What can agencies do to prevent ransomware attacks?

For prevention, I would say pay attention to our first line of defense: Our users. In Georgia, our Governor, Brian Kemp, leaned forward very hard on mandating training for all executive branch employees. We were able to give about 95% of our executive branch employees training within a 90-day period, which was significant for us. And that's gone a long way to mitigate things.

When we talk to administrators, a big problem around ransomware has been that once cybercriminals get in, they've been able to compromise someone's account that had elevated privileges. So, we focus a lot on making sure these administrative credentials and passwords are of the appropriate complexity by transitioning to multifactor authentication. It's at a minimum at the admin level, but we're pushing to get it implemented across the board for all users.

The third component is putting a lot of focus on our data backups and making sure we're verifying the integrity of those backups continually. I've seen backups that have been compromised because the firewalls or some of the applications they were using weren't configured properly. They didn't provide the defense that they were supposed to.

How can recovery tools such as data backups help protect agencies from ransomware?

If you can completely restore your critical systems and the files that personnel work with, you're going to be up in hours or days as opposed to weeks and months where you don't have backups to restore to.

Without those backups, you're basically building your entire IT environment from scratch. And that can cost you hundreds of thousands of dollars in equipment and new licensing, not to mention the personnel you need to help you architect the environment and set it up. If you're a small shop with only two or three IT personnel supporting a lot of locations, you're not going to be able to do that without a lot of contracting help.

Being able to restore those critical systems that keep your doors open and allow operations to flow, you can manage some of the lower-level stuff. But knowing what those critical systems are and having them on a secure backup that's verified will go a long way to ensure that you can quickly recover from an operational perspective.

Conclusion and Next Steps

Agencies of any shape and size shouldn't feel helpless against ransomware. Although state and local budgets and workforces make those agencies extra vulnerable, they shouldn't give up. Combating ransomware is objectively hard, but it's a battle that agencies can win. Here's how:

Make Awareness an Anchor

As with any threat, agencies can gain strength in numbers to fight ransomware. Agencies in close contact with one another can swap information about potential ransomware risks. They can also trade insights into possible cybercriminals and how they operate.

Perhaps most importantly, friendly agencies can boost a victim's recovery time after attacks. And by monitoring the news for ransomware incidents, agencies can learn not to repeat one another's mistakes.

Learn the Language

Jargon gives cybercriminals advantages over agencies. Agencies that can't discuss what ransomware is, how it works or the topics related to it may stumble against it.

First, agencies should familiarize themselves with common cyberthreats such as ransomware. Ransomware is a form of malware, or malicious software. Agencies that can recognize ransomware and its malware relatives are prepared for these cyberthreats.

Second, agencies should study concepts such as cryptocurrency and the dark web that are linked to ransomware. Cryptocurrencies are digital currencies such as Bitcoin that users securely exchange using encryption. The dark web includes parts of the internet that are accessible only with specific authorizations, configurations and software. Understanding these can help agencies communicate with cybercriminals.

Review the Options

Ransomware attacks often seem like either-or predicaments: Agencies can either pay a ransom or they can rebuild their damaged assets independent of attackers.

Both scenarios are usually true, but other avenues also exist. For some agencies, negotiating with attackers might be possible. It can lower the ransom or help them recover more assets. This route can even give agencies more time to recover or thwart their attackers.

Cyber insurance is a fourth solution that's increasingly available to agencies. This relatively new form of insurance protects agencies by insuring some of their assets.

Practice Personal Cybersecurity

Public servants can push their agency's cybersecurity to the next level. Individually, government employees can protect their agency by avoiding any emails, social media posts or websites that seem suspicious.

When working remotely, public servants can help shield their agency by using protected Wi-Fi networks so sensitive information doesn't land in the wrong hands.

Lastly, government workforces can reinforce their cybersecurity with recurring awareness training that teaches employees how to spot and avoid potential hazards.

Together, these steps can make the shields agencies have against ransomware and other cyberthreats exponentially harder.

Thank you to Pure Storage and 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**.

govloop.com | @govloop