RISE IN RANSOMWARE ATTACKS

at federal agencies prompts growing need for smarter backup and recovery strategies

FedScoop Report

How modern enterprise data platforms provide greater insights and stronger safeguards on mission-critical data.

Thirty percent of federal IT leaders report their agencies have experienced ransomware attacks within the past three years, according to a survey by FedScoop. While the pace of attacks — and their devastating impact — have federal agency officials concerned, the new study also suggests a larger fear. Ransomware not only threatens to disrupt government services; it also has the potential to take down critical infrastructure, creating a national security crisis.

Those fears have taken on added urgency in the aftermath of the January 2020 killing of Iran's top military general. Agencies and critical infrastructure operations should "pay close attention to your critical systems," from *potential retaliation* by Iran's state-sponsored hackers, warned Christopher Krebs, a top security official at the Department of Homeland Security. *U.S. Treasury officials* and cybersecurity experts also warned of increasing ransomware campaigns from state-sponsored actors such as North Korea, in part to fund the country's missile programs.

Federal agencies may appear to have an advantage over state and local governments in having larger budgets and more sophisticated processes for implementing cybersecurity best practices. However, federal IT officials often face the same challenges as their state and local counterparts in being able to recover from malware and ransomware attacks quickly. The latest edition of StateScoop's interactive *Ransomware Attacks Map* shows more than 270 known public sector ransomware attacks have left state and local agencies with costly recovery bills.

Only about 34 percent of federal IT executives said their agency would be able to recover all of their critical data within 12 hours of a ransomware attack, according to the *FedScoop survey*, underwritten by Veritas Technologies. The report also found that more than 8 in 10 IT officials in federal and state government surveyed believe ransomware will continue to be a leading or greater threat in the coming year.

Agency officials already follow strict cybersecurity guidelines — including the National Institute of Standards and Technology (NIST) *National Risk Management Framework* — when considering strategies for enterprise data protection and backup capabilities. However, attackers continue to find new ways to compromise federal data systems, forcing agencies to give heightened importance to what has traditionally been seen as a back-office task to ensure continuity of operations.

> "Ransomware developers realized they needed to hide their tracks [so] a lot of the modern day ransomware actually looks for backup workloads first...before it unleashes its payload into the environment.
>
> **– Rick Bryant, Veritas Technologies**

"Requirements are critical to how to protect things within a risk management framework," said Mike Malaret, Director of Sales Engineering for the Defense and Intelligence communities at Veritas Technologies. "We are trying to follow the security technical implementation guidelines that are published and developed by NIST and the National Security Agency. By ensuring that our products meet the requirements out of the box, we make it less risky for our government customers to actually choose their costs."

The challenge is that ransomware developers continue to refine and improve their capabilities for targeting government agencies. "Ransomware developers quickly realized that they needed to hide their tracks and ensure that the agencies couldn't back up," said Rick Bryant, National Healthcare Architect and Ransomware Expert at Veritas Technologies. "As a result, a lot of the modern day ransomware actually looks for backup workloads first, attacks that before it even unleashes its payload into the environment."

Discover, backup, recover — at scale

Understanding the dangers of modern ransomware is essential to realizing the importance of modernizing data protection and backup and recovery capabilities.

It is essential to safeguard data against two primary types of ransomware: crypto ransomware and locker ransomware. Crypto ransomware encrypts the data on a computer and the attacker demands a ransom for the keys that will unlock the data. Locker ransomware does not encrypt the data; rather, it locks the victim out of their system. A particularly malicious attack involves a random key generator that is used to generate unique keys for each file and no digital record is kept of the keys. Even if a ransom is paid, the data cannot be decrypted. The data is left essentially inaccessible with no way to decrypt the files, requiring a complete restore from backup.

Although the federal government leverages the Department of Homeland Security's Einstein situational awareness program to detect, analyze and protect against malware, it hasn't prevented some agency data from being hijacked by ransomware attackers.

Among the nearly one-third of federal and state IT officials in the FedScoop survey who said their agencies had been directly impacted by ransomware, 1 in 4 reported their agency opted to pay the ransom — and not always with

WHERE LOSS OF DATA FROM RANSOMWARE POSES GREATEST RISKS FOR FEDERAL AGENCIES

Percent of federal IT executives who said:

45%

Risk to national security

45%

Employee productivity loss

39%

Prolonged productivity loss

35%

Unbudgeted expenses for remediation

31%

Loss of institutional trust

27%

Substantial program damage requiring reconstruction of department records

Source: ***FedScoop Survey***

success. Ten percent of those who said they paid the ransom still were unable to recover their data.

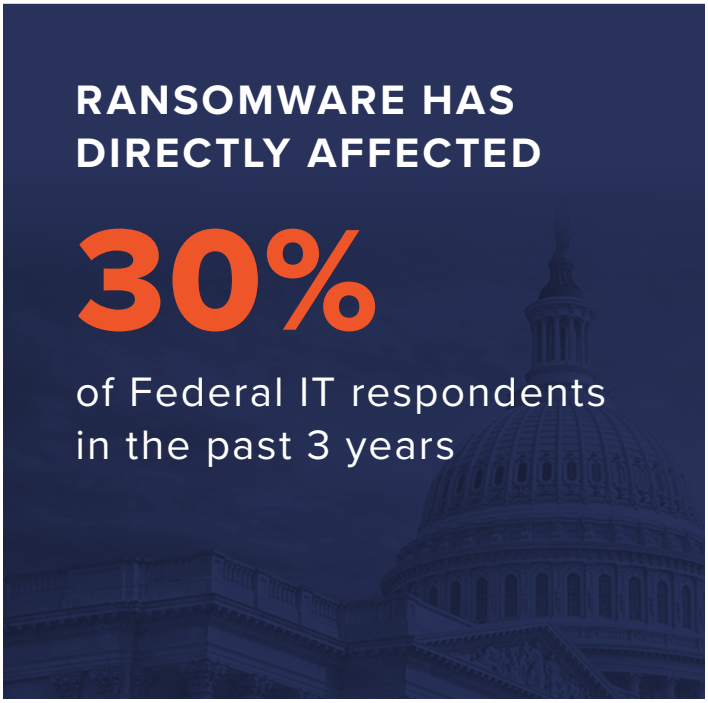
Typically, attackers look to lock up agencies' backup data ahead of blocking users from their primary systems, leaving them little choice but to gamble on paying off their attackers.

Avoiding that scenario is just one of the reasons agencies need to put greater emphasis on modern enterprise data systems that can help ensure alignment with the NIST Cybersecurity Framework, safeguard data when attacks occur and protect against national security threats.

Given the evolution of ransomware, there are inherent advantages to adopting systems like Veritas' ***NetBackup*** (recognized by ***Gartner*** for 14 years running), as well as Veritas' Resiliency Platform and ***APTARE IT Analytics*** tools to help agencies achieve greater resiliency, according to Bryant. These capabilities have been engineered specifically to protect against unexpected losses in citizen services and employee productivity and reduce risks to national security in ways that future-proof an agency's IT investments.

Data discovery

For federal agencies, putting defenses in place against ransomware is only one piece of the puzzle. It's also critical to capture and build upon data management insights as a means to develop a comprehensive data protection strategy.



> So if we can detect anomalies within the environment and remediate them prior to actually worrying about them getting caught in the backup site, agencies are in a much better place.
>
> **– Rick Bryant, Veritas Technologies**

The first step toward building that strategy, Bryant suggests, is to fully discover what data your agency has, where it lives and its value to the mission. "Knowing what's important, where it's located and who has access to it is paramount to being able to effectively protect it," he said.

Solutions such as Information Studio provide agencies the visibility and analysis tools to identify where their data has the greatest value, is most at risk or represents a source of unnecessary added storage costs, he said. It also gives agencies greater power to organize data and take informed action to handle security concerns, new regulations and continuous data growth to ultimately regain control of their data.

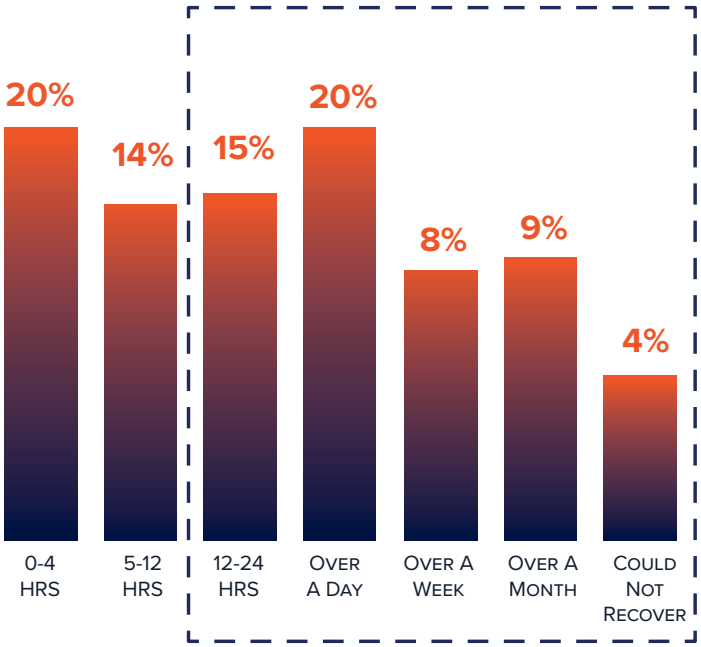
Veritas' Information Studio or Insights products "have the ability to actually collect metadata about all of the files that exist within an agency's organization," explained Malaret. "So if we can detect anomalies within the environment and remediate them prior to actually worrying about them getting caught in the backup site, agencies are in a much better place," he said.

"The Insights technology component is very important for being able to add that extra layer of security, give agencies insights into the data that shouldn't be there — and, should be deleted — and also help give them insights into where their critical data actually exists," said Bryant. "Our predictive Insights components can actually help you proactively scan your environment for malware or ransomware types of extensions to eliminate it before it activates."

Additionally, Bryant recommends agencies take steps to appropriately tier their data based on the relative value of that data. "If data hasn't been accessed in six months, move it to a lower tier, a lower accessibility level or delete it," he said. "Maybe even move it to the cloud; but understand where it is and manage the cost associated with it.

AGENCIES FACE LENGTHY RECOVERY DELAYS

Federal Respondents



Q: If your most critical data was affected by a ransomware/ malware attack, how long would it take your department to fully recover without paying the ransom?

Source: ***FedScoop survey***

Just putting everything in a file share that everybody has access to is foolhardy and rife with problems."

Secure your backup

Another recommendation, said Bryant, is to deploy backup appliances that protect the backup workload itself. Malaret suggests that agencies make multiple copies of data, backed up in multiple locations.

That's especially important as agencies consider their choice of backup solutions because of the need to restore a large-scale environment in a reasonable amount of time in the wake of a ransomware attack. "That's where backup becomes critical," Malaret said.

Bryant recommended agencies look for features, like those offered by Veritas' NetBackup appliance, which includes application whitelisting, "so ransomware can't get into it — and only allows what's been specifically programmed to interact with your data center," he said. "If you build your backup systems yourself, you still need to put in good safeguards to protect those backup workloads, or you can just use our purpose-built appliance," he said. "We can literally recover thousands of systems at the same time."

Investing in better backup controls can also help agencies future-proof their ransomware protections. "They can use it today to protect on-prem workloads. And if later they get a backup data center, it will work in that environment as well," Bryant said. "It can even back up to the cloud."

Recover at scale

Ransomware's impact goes well beyond the loss of data. As ransomware victims in the FedScoop survey indicated, it also compromises service delivery, institutional trust and results in unplanned costs. For federal agencies, it also presents a serious national security risk.

Government agencies face a complicated mix of external and internal challenges to guard against ransomware and malware threats. Forty-two percent of agencies cite lack of budget as a major obstacle to their efforts to defend against ransomware, according to the FedScoop survey. Consequently, it's critical for agencies to have a response plan and practice it before ransomware and malware attacks inevitably occur.

While half of federal respondents in the FedScoop survey rated their agency's ability to detect ransomware or malware (before it locks or encrypts data) as "superior or above average" compared to comparable agencies, the broader findings suggest that the ability to detect threats may not be sufficient to prevent attacks.

And that speaks to Veritas' unique value proposition, according to Bryant. "We can help them by protecting those backup workloads, we can help them recover at scale and we can help them address their number one concern, which is budget overruns and protecting our national critical data," he said.

Learn more about how Veritas Technologies can safeguard your agency's data from the perils of ransomware attacks.

This FedScoop report was produced for, and sponsored by, Veritas Technologies.

fedscoop VERITAS