RANSOMWARE THREATS

Is your agency ready?

Federal and state agency IT leaders are battling a growing array of ransomware attacks. Data recovery capabilities and comprehensive planning hold the most promise for ensuring they don't have to pay.

PRESENTED BY
fedscoop | statescoop

UNDERWRITTEN BY
VERITAS™

EXECUTIVE SUMMARY

In a new survey of federal and state government information technology decision makers, underwritten by Veritas Technologies, FedScoop and StateScoop explore:

- How federal and state government agency leaders currently view the **risks and potential impact** of ransomware and malware attacks.
- How agency program and IT leaders rate their agency's ability to **prevent, detect, protect and recover** from a ransomware and malware attack.
- What proportion of federal and state agency IT executives have been directly affected by ransomware attacks — **and how they responded.**
- How frequently agencies **back up** their critical data — **and test** their data recovery plans.
- What procedures agencies have in place to **mitigate the impact** of potential ransomware and malware attacks.

EXECUTIVE SUMMARY

RANSOMWARE THREATS

Perceptions and preparedness among government IT officials

The mounting costs — and disruptions — of ransomware attacks across the United States are pressuring federal, state and local government agencies to look beyond established IT security measures and focus new attention on emergency cyber preparedness.

Recent estimates predict ransomware damage costs will reach $20 billion by 2021, according to Cybersecurity Ventures, and continueto disrupt public and private enterprises at increasing rate.

This new research study from FedScoop and StateScoop reveals that more than 8 in 10 federal and state government IT officials believe ransomware will continue to be as great, if not a greater threat, in the coming year.

The research, underwritten by Veritas Technologies, reveals a number of new findings to give public officials greater insights about the risks, perceptions and strategies to consider in addressing ransomware attacks. Among the findings ▶

EXECUTIVE SUMMARY

TOP-LINE FINDINGS

Perceptions and preparedness among government IT officials

- Though news coverage about ransomware attacks tends to focus on state and local agencies, **almost the same share of federal agency respondents (30%) have experienced a ransomware attack as state agency respondents (32%).**
- Despite FBI and DHS recommendations not to pay a ransom to recover data, **24% of affected respondents said their agency did so** — often without regaining their data.
- **3 in 4** federal and state respondents affected by ransomware attacks said their agency **did not pay the ransom**. But **1 in 10** also said their agency was **unable to recover their data.**
- Federal and state respondents ranked **phishing, malware and ransomware** as the **three biggest cybersecurity concerns their agencies now face.**
- The impact of data loss to mission varies: **Federal respondents worry most about risks to national security; state respondents worry most about unbudgeted costs to recover from an attack.**
- Only **34% of federal respondents** and **17% of state respondents** said their agency could **fully recover their most critical data within 12 hours** of a ransomware or malware attack.
- **Half of respondents** reported having procedures to **recover or isolate ransomed data. Far fewer** have plans in place to **engage with law enforcement and cyber specialists.**

WHO WE SURVEYED

In August 2019, FedScoop and StateScoop conducted an online survey of 150 prequalified government IT decision makers about their agency's perceptions of ransomware and data recovery capabilities.

RESPONDENT BY TYPE OF AGENCY

FEDERAL GOVERNMENT
74 RESPONDENTS

STATE GOVERNMENT
76 RESPONDENTS

RESPONDENT BREAKOUT BY SIZE OF AGENCY

- **27%** MORE THAN 10,000 EMPLOYEES
- **16%** 5,000 – 9,999 EMPLOYEES
- **29%** 1,000 – 4,999 EMPLOYEES
- **29%** UNDER 1,000 EMPLOYEES

RESPONDENT BREAKOUT BY JOB TITLE

- **20%** C-SUITE / EXECUTIVE LEVEL IT DECISION-MAKER
- **27%** IT MANAGEMENT
- **14%** PROGRAM / PROJECT TEAM LEADERS
- **29%** PROGRAM / PROJECT STAFF
- **7%** GOVERNMENT CONTRACTOR
- **3%** OTHER (ANALYST, ADMINISTRATION, SPECIALIST)

RANSOMWARE ATTACKS AFFECT FEDERAL AS WELL AS STATE AGENCIES

Federal agencies have been affected by ransomware attacks almost as frequently as state and local agencies over the past three years.

▼ RANSOMWARE HAS DIRECTLY AFFECTED ▼

Q: Has your agency been directly affected by a ransomware attack in the last 3 years?

TO PAY OR NOT TO PAY?
AGENCY'S RESPONSE TO RANSOMWARE

PAID

1 in 4 respondents at agencies affected by ransomware said their agency **paid the ransom.**

- **13%** paid, but are in process of recovering their data
- **7%** paid, and did recover their data
- **4%** paid, but lost access to their data

NOT PAID

3 in 4 respondents at agencies affected by ransomware attacks said their agency **didn't pay the ransom,** but **9% of them still lost data.**

- **67%** did not pay the ransom but recovered their data
- **9%** opted NOT to PAY... and lost their data

> **We had to make a determination on whether to pay. We could have literally been down months and months and spent as much or more money trying to get our system rebuilt." - Jackson County, Fla. county manager.**

Q: If affected by ransomware, did your agency pay a ransomware to recover its data?

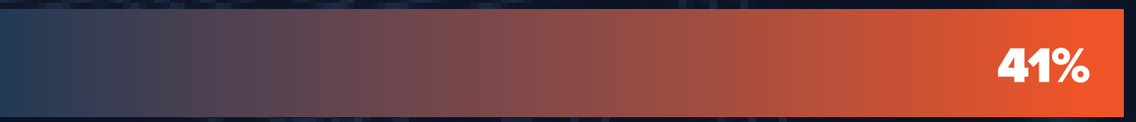
Base - 46

TYPES OF RANSOMWARE AFFECTING AGENCIES

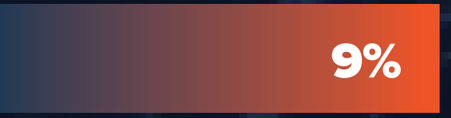
Among those affected by ransomware: Nearly 5 in 10 respondents' agencies were victim to encrypting ransomware; 4 in 10 by non-encrypting ransomware; and 1 in 10 by leakware or extortionware.

FEDERAL AND STATE RESPONDENTS AFFECTED BY RANSOMWARE WITHIN THE LAST 3 YEARS

ENCRYPTING RANSOMWARE
Encrypts files; requires a key to decrypt and restore operations



NON-ENCRYPTING RANSOMWARE
Restricts access to files and data, without encrypting them



LEAKWARE OR EXTORTIONWARE
Attacker exfiltrates and threatens to release data if ransom is not paid.

OTHER

PROTECT YOUR NETWORKS

Federal cybersecurity and law enforcement agencies offer guidance on proactive steps organizations can take to protect their networks from ransomware — and tactics to follow when preventative measures fail.
Learn more here ▶

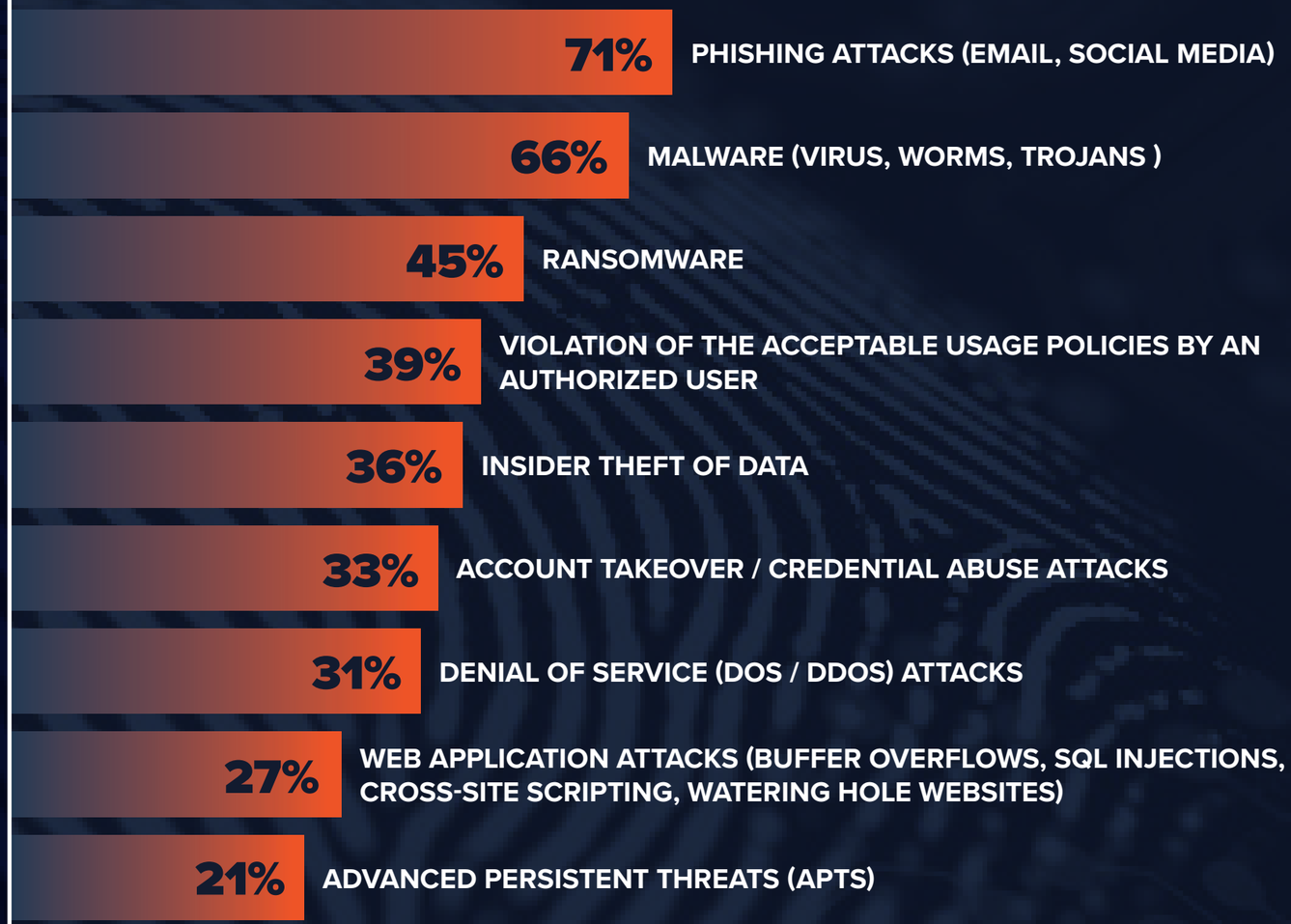
Q: What type of ransomware infected your agency?

Base - 46

BIGGEST CYBERSECURITY CONCERNS

The cybersecurity threats that worry federal and state agency leaders most:

Phishing: attackers deceive people into sharing personal information or passwords to access sensitive information.
Malware: malicious software designed to invade, damage or disable networks or steal critical information.
Ransomware: software that prevents users from accessing their system or files unless they meet ransom demands to regain access.



Q: What are the biggest cybersecurity concerns your agency faces today? (Select up to 5)

Base - 150

CYBERSECURITY CONCERNS FEDERAL VS. STATE

However a higher percentage of state respondents ranked phishing attacks (80%), malware (72%) and ransomware (49%) as a pressing concern compared to federal respondents — most likely reflecting a combination of having more isolated systems and limited resources.

FEDERAL RESPONDENTS		STATE RESPONDENTS
62%	PHISHING ATTACKS (EMAIL, SOCIAL MEDIA)	80%
59%	MALWARE (VIRUS, WORMS, TROJANS)	72%
43%	RANSOMWARE	49%
41%	VIOLATION OF THE ACCEPTABLE USAGE POLICIES BY AN AUTHORIZED USER	36%
39%	INSIDER THEFT OF DATA	33%
Base - 74		*Base - 76*

BEHIND THE FINDINGS

Larger organizations have the resources to participate in cooperatives with a wider range of solutions to respond to attacks. It's the smaller organizations that often need the most help because they don't have dedicated cybersecurity personnel to dedicate to recovery. — **NASCIO Executive Director**

Q: What are the biggest cybersecurity concerns your agency faces today? (Select up to 5)

OUTLOOK: A BIG AND GROWING THREAT

More than **8 in 10 federal and state agency** respondents believe ransomware and malware will continue to be a top concern, if not **a greater concern,** in the next 12 months.

33% think the concern will be larger

45% think the concern will be the same

6% think the concern will be less

11% dont know

MOUNTING THREATS

"Ransomware attacks are only getting worse. The actors are shifting their business models and going to more coordinated attacks like we saw in Texas." **— Chris Krebs, director, DHS Cybersecurity and Infrastructure Security Agency**

Q: In the next 12 months, do you believe ransomware and malware will be a larger or smaller threat to your agency?

Base - 150

THE IMPACT OF DATA LOSS TO THE MISSION
FEDERAL VS. STATE AGENCIES

Ransomware's impact goes well beyond the loss of data. It also compromises service delivery and institutional trust — and results in unplanned costs. For federal respondents, it also presents a serious national security risk.

FEDERAL RESPONDENTS		STATE RESPONDENTS
45%	RISK TO NATIONAL SECURITY	12%
45%	EMPLOYEE PRODUCTIVITY LOSS	47%
39%	PROLONGED LOSS OF SERVICES	49%
35%	UNBUDGETED EXPENSES FOR REMEDIATION	53%
31%	LOSS OF INSTITUTIONAL TRUST	46%
27%	SUBSTANTIAL PROGRAM DAMAGE REQUIRING A RECONSTRUCTION OF DEPARTMENT RECORDS	43%
15%	JOB LOSS	8%
Base - 74		*Base - 76*

COSTLY UNPLANNED EXPENSES

Baltimore faced multiple ransom attacks that disrupted the city's 911 dispatchers in March 2018 and knocked out the city's digital services in May 2019. The collective costs of recovery and lost revenue totaled roughly $18 million. **— Baltimore budget office**

Q: What would be the greatest impact to your program if it suffered a critical loss of data? (Select up to 3)

THE IMPACT OF DATA LOSS TO THE MISSION
VICTIMS VS NON-VICTIMS

Those who have experienced a ransomware attack, however, rank the impact on their mission differently after the fact — compared to those who haven't actually lived through the experience. The findings suggest perceptions about ransomware's potential impact may not align with its actual impact.

RESPONDENTS AFFECTED BY RANSOMWARE		RESPONDENTS NOT AFFECTED BY RANSOMWARE*
43%	RISK TO NATIONAL SECURITY	19%
43%	PROLONGED LOSS OF SERVICES	50%
43%	UNBUDGETED EXPENSES FOR REMEDIATION	47%
41%	LOSS OF INSTITUTIONAL TRUST	38%
30%	SUBSTANTIAL PROGRAM DAMAGE REQUIRING A RECONSTRUCTION OF DEPARTMENT RECORDS	41%
30%	EMPLOYEE PRODUCTIVITY LOSS	53%
24%	JOB LOSS	3%
Base - 46		*Base - 58*

**Does not include those who responded "I don't know" to the question: Have you been affected by a ransomware attack (30% of respondents)?*

Q: What would be the greatest impact to your program if it suffered a critical loss of data? (Select up to 3)

TOP OBSTACLES AND THE NEED FOR A PLAN

Government agencies face a complicated mix of external and internal challenges to guard against ransomware and malware threats. It's critical for agencies to have a response plan — and practice it before ransomware/malware attacks inevitably occur.

PLANNING IS PARAMOUNT

"One of the measures of success comes down to having an action plan ahead of time — not just from the IT side, but working with the enterprise and business sides of government — to evaluate high-value assets, prioritize restoration and coordinate with external partners." **— DHS cybersecurity official who assists state and local governments**

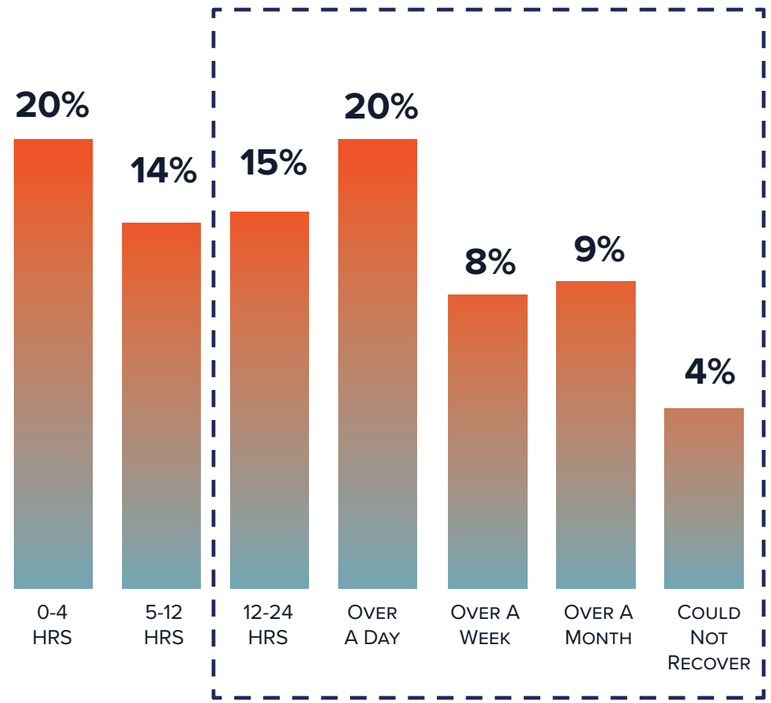
Q: What do you believe to be your agency's biggest obstacles to improving ransomware/malware defense? (Select up to 5)

Base - 150

AGENCIES FACE LENGTHY RECOVERY DELAYS

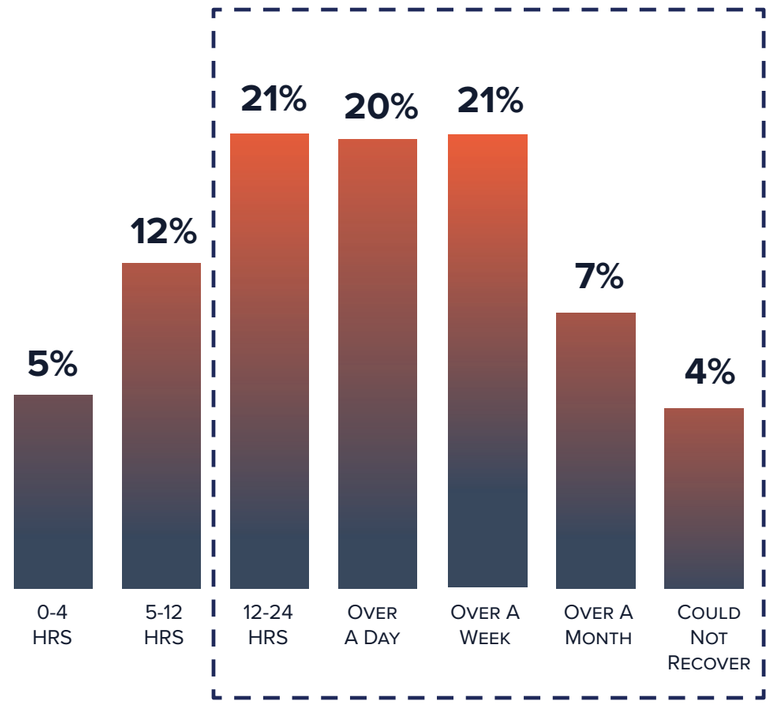
Only **34% of federal** and **17% of state respondents** said their agencies could recover fully within 12 hours from a ransomware/malware attack. As agency services depend increasingly on real-time data, leaders may need to reassess whether their backup and recovery strategies meet emerging threats.

FEDERAL RESPONDENTS



Base - 74

STATE RESPONDENTS



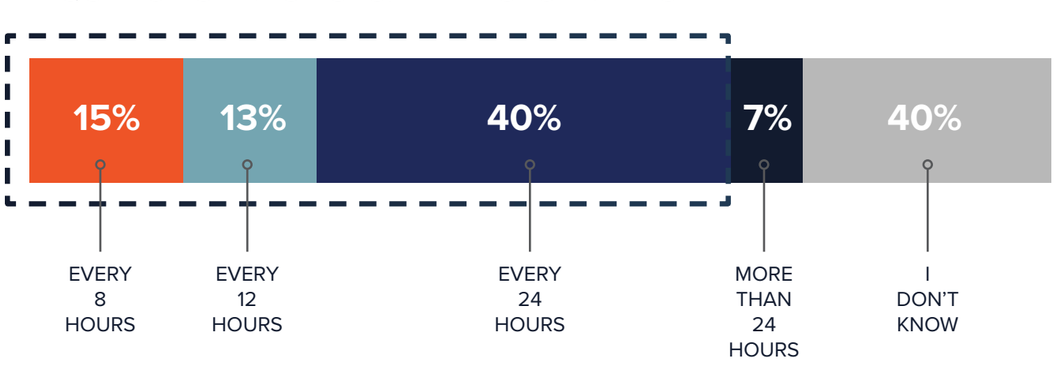
Base - 76

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?

AGENCY PRACTICES
DATA BACKUP AND RECOVERY

Agency back up and data recovery plans vary depending on the data and regulatory requirements. But **7 in 10 respondents** said their agency/program currently backs up its critical data or applications **within 24 hours.**

FREQUENCY OF BACK UPS: ALL RESPONDENTS

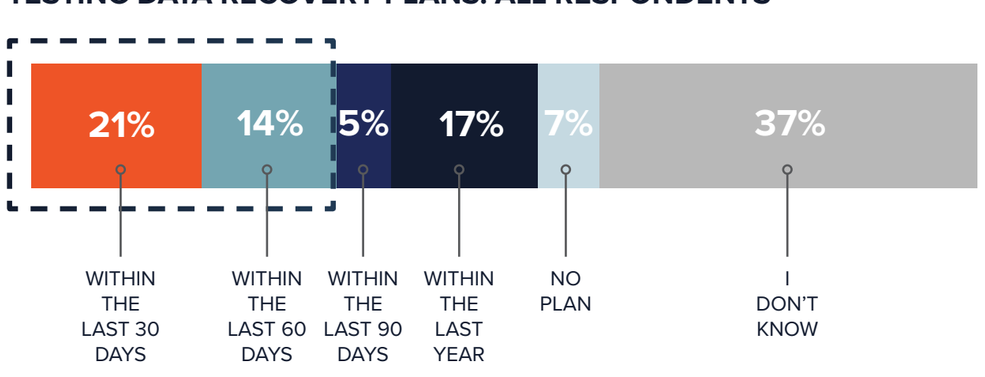


Base - 150

Q: How often does your agency/program backup its critical data or applications?

However only **35% of respondents** said their agency had tested its data recovery plan within the **last 60 days,** suggesting agencies may not have a firm handle on their ability to recover from ransomware/malware attack.

TESTING DATA RECOVERY PLANS: ALL RESPONDENTS

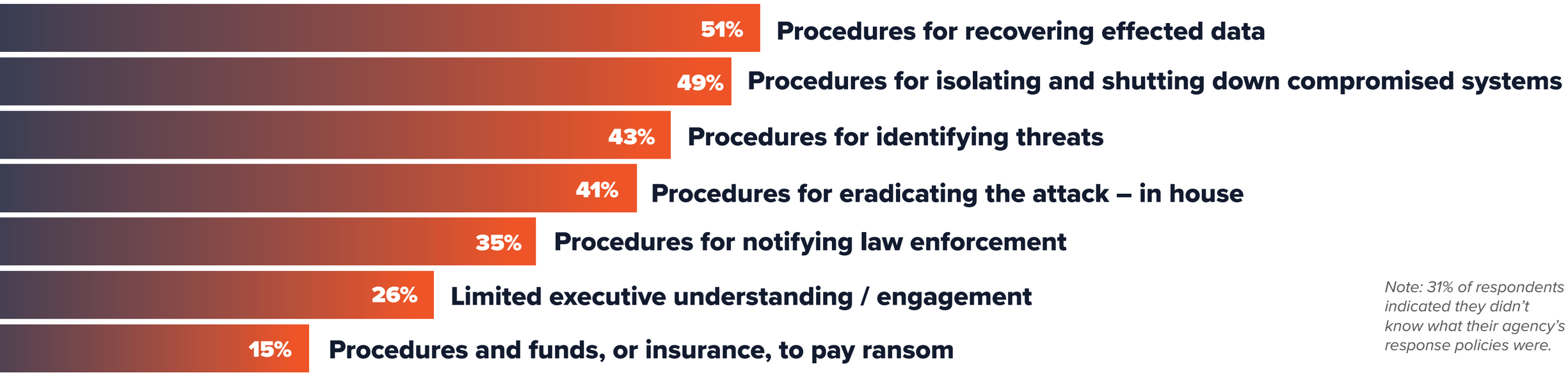


Base - 150

Q: How often does your agency/program backup its critical data or applications?

AGENCY PREPAREDNESS IN THE EVENT OF A RANSOMWARE OR MALWARE ATTACK

Half of respondents said their agencies have procedures in place to recover or isolate data in the event of a ransomware/malware attack. Fewer respondents, however, have procedures to notify law enforcement and engage specialists, suggesting agencies ransomware response plans remain incomplete.



Note: 31% of respondents indicated they didn't know what their agency's response policies were.

ENGAGE WITH CYBER EXPERTS

In the aftermath of Atlanta's ransomware attack, the city accelerated its migration of critical applications to a hybrid cloud service — and developed deeper ties with state and federal governments and cyber first responders. **— CIO of Atlanta**

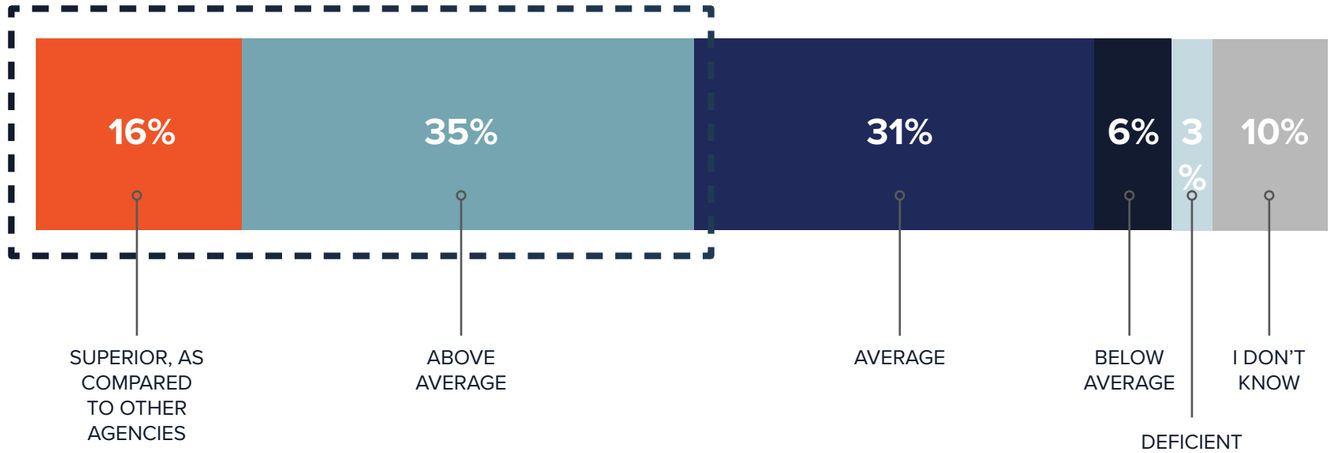
Q: Which of the following policies does your agency have in the event of a ransomware/malware attack? (Select all that apply)

Base - 150

DETECTING RANSOMWARE BEFORE IT COMPROMISES DATA

Half of federal and state respondents 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. However, the broader findings — that agencies may not have sufficient response plans in place — suggest that the ability to detect threats may not be sufficient to prevent attacks.

ALL RESPONDENTS



EMERGENCY RESPONSE

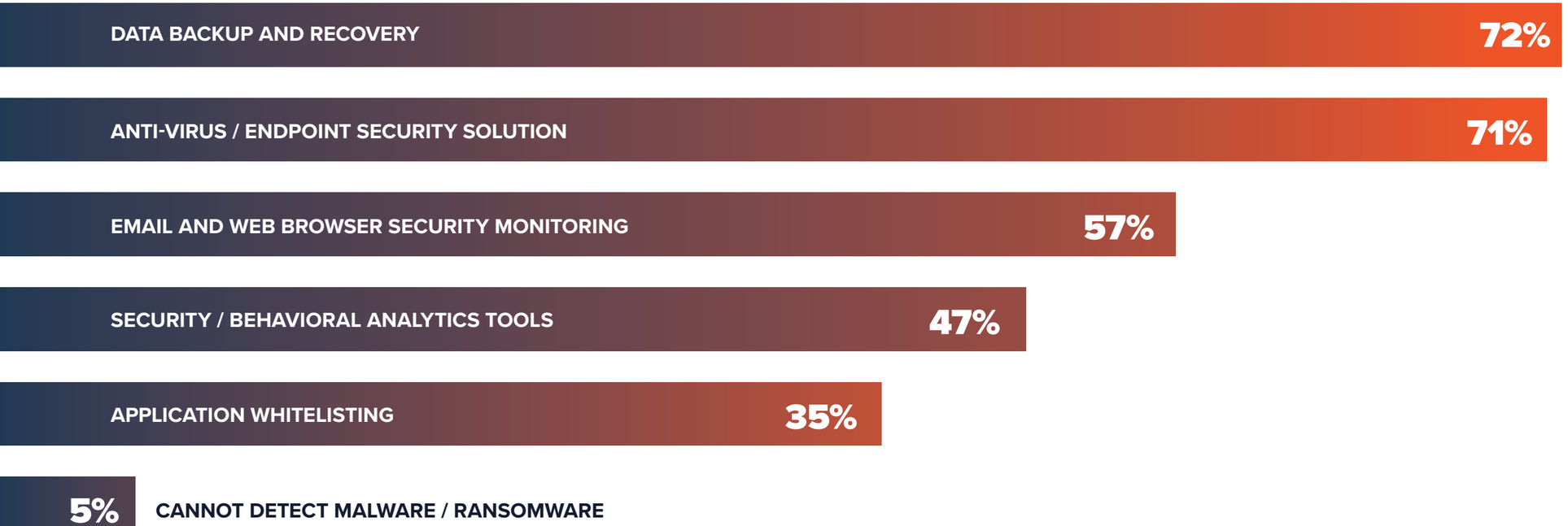
One of the big takeaways from recent ransomware attacks is the need for more officials to train their IT personnel on emergency management principles once threats have been detected.
— National Governors Assn. homeland security program director

Q: How would you rate the current ability of your agency/program to detect ransomware/malware before it locks or encrypts data, compared to other agencies like yours?

Base - 150

COMBATING RANSOMWARE AND MALWARE

More than 7 in 10 agency respondents said their agencies employ data backup and recovery tools and anti-virus and/or endpoint security solutions to combat ransomware and malware threats. But that may not guarantee those tools are being used to full effect or are modern enough to keep up with ransomware threats.



Note: 17% of respondents indicated didn't know what security solutions their agencies employed.

IMPROVING RESILIENCE

To combat the threat of ransomware, federal and state cybersecurity experts stress that agencies should ensure they: 1) Back up critical systems and configurations daily on a separate device; 2) Expand employee training to recognize phishing attempts and suspicious links; 3) Revise incident response plans that treat cyberattacks more like disasters.

Q: What security solutions does your agency currently employ to combat ransomware/malware? (Select all that apply)

Base - 150

RECOMMENDATIONS

- **Need for response procedures**
  Federal, state and local government agencies are wrestling with a complex mixture of internal and external challenges to address ransomware and related cyberthreats.

  Agencies could use more help not only to identify appropriate detection and response technologies, but also in creating appropriate response procedures in the event of an attack.

- **Need for quicker backup and recovery**
  A majority of agencies say it would take more than a day, and up to a month, to recover data in the event of a ransomware attack. This puts agencies increasingly at risk in their capacity to delivery on their mission — especially as they grow more interdependent on real-time and shared data.

  Agencies need more management support and resources to ensure they can back up and recover system data and configurations in shorter time frames.

- **Need for emergency response planning**
  A substantial portion of agency respondents don't know when their agency tested data recovery, or report having incomplete procedures in the event of a ransomware attack.

  Agencies need more help in training IT, enterprise and business leaders on cyber emergency management principles and on developing — and practicing — comprehensive incident response plans.

- **Need for wider training**
  Agencies also need to ensure all employees are better trained to recognize ransomware and malware threats and how to respond.

- **Best practice advice**
  "Immediately and regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and update to the latest version." - Joint CISA, NASCIO, NGA, MS-ISAC advisory

fedscoop

FedScoop is the leading tech media brand in the federal government market. With more than 210,000 unique monthly visitors and 120,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify ways to achieve common goals. With our website, newsletter and events, we've become the community's go-to platform for education and collaboration.

statescoop

StateScoop is the leading media brand in the state and local government market. With more than 100,000 unique monthly visitors and 125,000 daily newsletter subscribers, StateScoop reports on news and events impacting technology decisions in state and local government. With our website, daily newsletter and events, we bring together IT leaders and innovators from across government, academia and industry to exchange best practices and identify ways to improve state and city government.

CONTACT
Wyatt Kash
Senior Vice President Content Strategy
Scoop News Group
Washington, D.C. | 202.887.8001
wyatt.kash@scoopnewsgroup.com

PRESENTED BY

fedscoop | statescoop

UNDERWRITTEN BY

VERITAS™