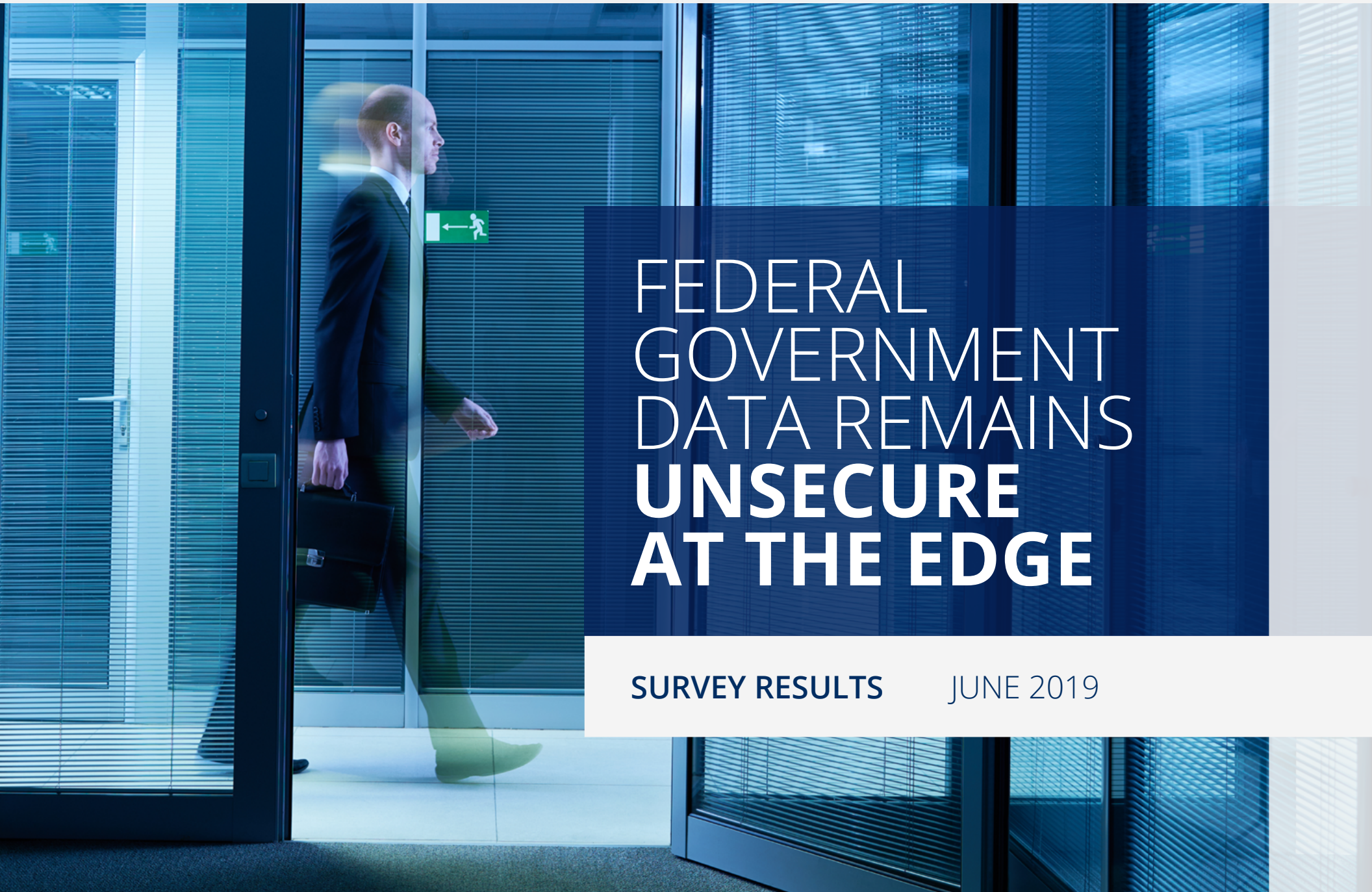
Acronis SCS



FEDERAL GOVERNMENT DATA REMAINS **UNSECURE AT THE EDGE**

SURVEY RESULTS JUNE 2019

Acronis SCS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The rise of the mobile employee in government – and the proliferation of endpoints, battlefield applications and remote branch office networks – requires a renewed approach to securing data, whether it be at the "edge" on an employee's mobile device or within an on-premise data center. Our mobile world is pushing data further and further to the edge, in fact, **IDC research** predicts that at least 40 percent of Internet-of-Things-created data will be stored, processed, and analyzed close to or at the edge of the network.

Historically, however, agencies have prioritized protecting on-premise data centers through methods like log analytics and behavior monitoring, anti-virus software, and standard data encryption.

While such tactics play an important role in security posture, alone they cannot keep edge data truly safe whether for cybersecurity or continuity of operations. How do agencies protect data in the event of a lost or stolen mobile device? A hardware malfunction in a remote office? A ransomware attack that re-encrypts information?

What exacerbates this problem is a clear lack of knowledge when it comes to securing edge data and a clear disconnect in perception about how safe data really is – between senior executives making the budgeting decisions and the IT teams managing the data solutions at the edge.

A recent survey of 200 federal government decision makers and influencers – implemented by Acronis SCS in partnership with Market Connections, a leader with over 20 years of experience of data analysis for the federal government – shows that while most senior executives (42 percent) feel excellent about their security posture, only 21 percent and 31 percent of mid-management and hands-on IT or technical roles respectively feel excellent about their cyber postures at the edge. (See Figure 1)

On top of that, only 12 percent of respondents felt they had any expertise on the subject of securing edge data. (See Figure 2)

Over half of federal government decision makers and influencers surveyed describe their agency's ability to keep data safe and secure at the edge as 'good.' However, only one quarter describe their abilities in this area as 'excellent.'

Figure 1

Agency's Ability to Keep Data Safe and Secure at the Edge

	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
Excellent	42%	21%	31%
Good	45%	66%	49%
Poor	12%	12%	9%
Not sure	0%	2%	11%

Statistically significant difference

EXECUTIVE SUMMARY — CONTINUED

Overall, the research finds that leaders in the federal government are not fully aware of how vulnerable their edge data really is. According to the survey results, 79 percent of senior executives expressed that they were experts in edge security knowledge. However, only 29 percent of hands-on IT/technical experts surveyed expressed that they were experts in edge security knowledge. This signals a clear confidence discrepancy between leadership and those directly on the front lines of security. Leadership may be overstating their levels of edge security knowledge, lacking a true understanding of how vulnerable their agencies may actually be. Additionally, the results demonstrate that IT and security teams are not adequately equipped with the knowledge and resources they need to fully secure information.

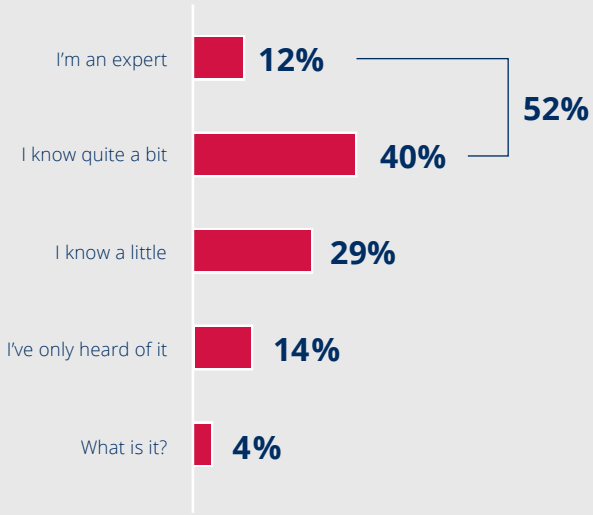
This report takes a deep dive into those survey results, with an overview of the current cyber landscape, the primary concerns over data security, and where agencies can fill the gaps when it comes to implementing data security solutions.

It is clear that the federal government needs dynamic edge data security, which goes beyond the traditional concept of securing networks at the perimeter.

Respondents most often indicate they know quite a bit about edge security. **However just 12% consider themselves experts on the subject.**

Figure 2

Edge Security Knowledge



	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
% I'm an expert/ I know quite a bit	79%	56%	29%

Statistically significant difference

DEMOGRAPHICS: THE DECISION MAKERS OF DATA SECURITY

The report is based on feedback from 200 federal government decision makers (100 from civilian agencies and 100 from defense agencies). (See Figure 3)

The survey results show responses from a wide variety of titles in the federal government including:

- CIO and CTO
- Program Manager and Systems Administrator
- IT Director, IT Manager, IT Specialist, IT Supervisor
- Analyst

Over half of the respondents (56 percent) identify their current job at the mid-management level. (See Figure 4)

Sixteen percent of respondents identified as senior-executives, while over half of the respondents have a role in making decisions or recommendations regarding data security solutions (56 percent). (See Figure 5)

Figure 3

Agency Type

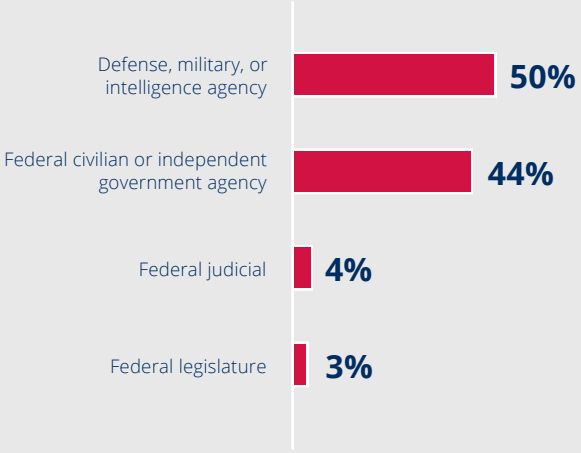


Figure 5

Decision-Making Involvement

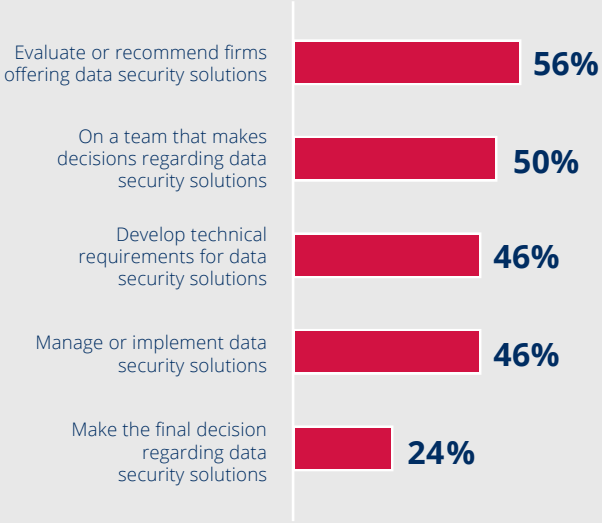
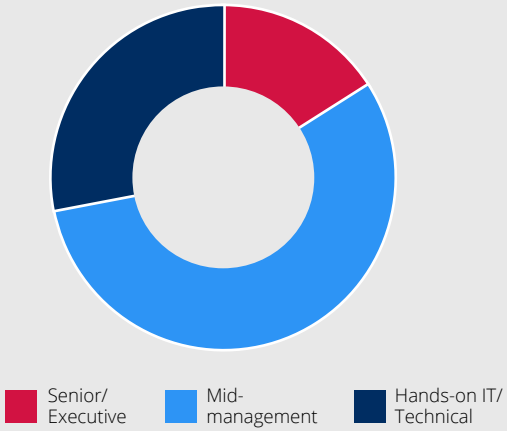


Figure 4

Job Roles and Titles



EXAMPLE JOB TITLES INCLUDE:

- **ANALYST**
- **CIO**
- **CTO**
- **IT DIRECTOR**
- **IT MANAGER**
- **IT SPECIALIST**
- **IT SUPERVISOR**
- **PROGRAM MANAGER**
- **SYSTEMS ADMINISTRATOR**

EDGE DATA SECURITY: DISCONNECT BETWEEN PERCEPTION AND REALITY

For any agency, lack of confidence from IT or security staff should raise a number of red flags. It signals that not only do IT professionals need more knowledge, training, and awareness surrounding edge data security, but also that those towards the top may not understand how vulnerable their agencies actually are to data loss.

What may explain the stark perception gap between those at the higher level and those on the frontlines are different priorities and challenges.

While IT and security teams are on the cyber frontlines of defending data at the edge, senior executives and decision makers face pressures like managing budget constraints and ensuring compliance with the latest policy directives and mandates. As a result, leaders at the top may be unaware that their data backup and recovery solutions are out of date.

Without leaders who understand the challenges of edge data security, those who are directly responsible for securing and maintaining data at the edge (i.e. between remote office locations and mobile environments) are stymied when trying to address a security or operations incident. Meanwhile, federal data remains especially vulnerable to breaches or loss.

EDGE DATA SECURITY: DISCONNECT BETWEEN PERCEPTION AND REALITY — CONTINUED

The research shows that, at first glance, most federal leaders feel confident about their organizations' abilities to keep data safe and secure at the edge. In fact, over half of the senior-level survey respondents (58 percent) feel good about the tools and procedures they have in place, even though some may require updating. (See Figure 1)

The majority of survey respondents also indicated adequate knowledge of edge data security (40 percent said they knew quite a bit and 12 percent considered themselves experts). (See Figure 2)

At the same time, only 27 percent feel excellent about their agencies' abilities to secure data at the edge (See Figure 1). The most significant contrast from the survey results showed that while most senior executives (42 percent) feel excellent about their security posture, only 21 percent and 31 percent of mid-management and hands-on IT or technical roles respectively feel excellent about their cyber postures at the edge. (See Figure 1)

Figure 1

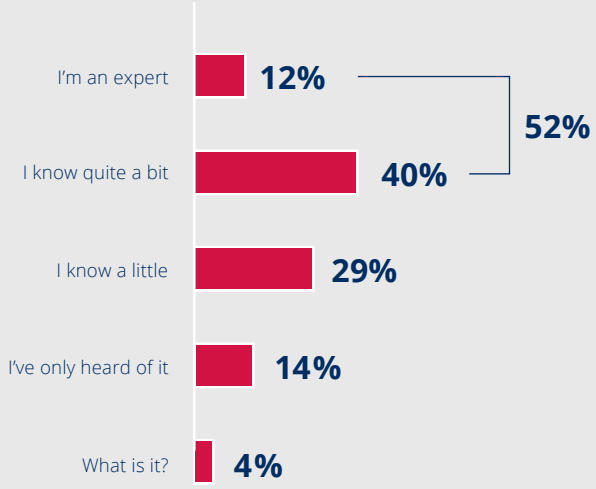
Agency's Ability to Keep Data Safe and Secure at the Edge

	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
Excellent	42%	21%	31%
Good	45%	66%	49%
Poor	12%	12%	9%
Not sure	0%	2%	11%

Statistically significant difference

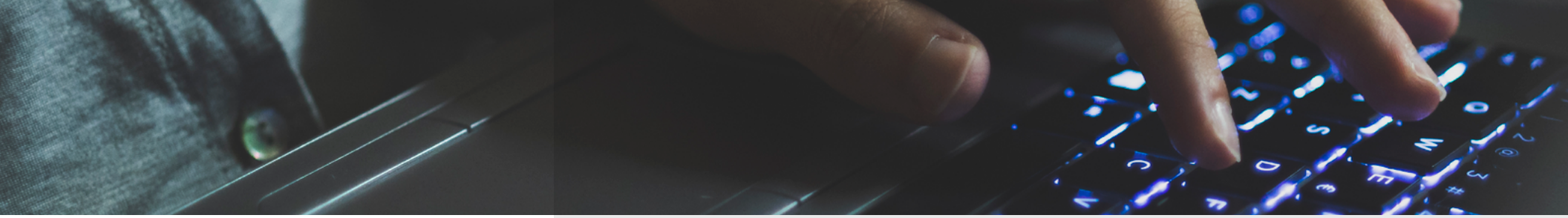
Figure 2

Edge Security Knowledge



	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
% I'm an expert/ I know quite a bit	79%	56%	29%

Statistically significant difference



SECURITY CONCERNS AT THE EDGE

No matter how confident federal leaders may feel about their cyber posture, their agencies may be more vulnerable than they think. Despite the lessons learned from the Office of Personnel Management's data breach nearly four years ago – where 21.5 million records were hacked and stolen – the 2018 Federal Cybersecurity Risk Determination Report and Action Plan determined that **74 percent of federal offices** are still at risk or high risk of a cyberattack.

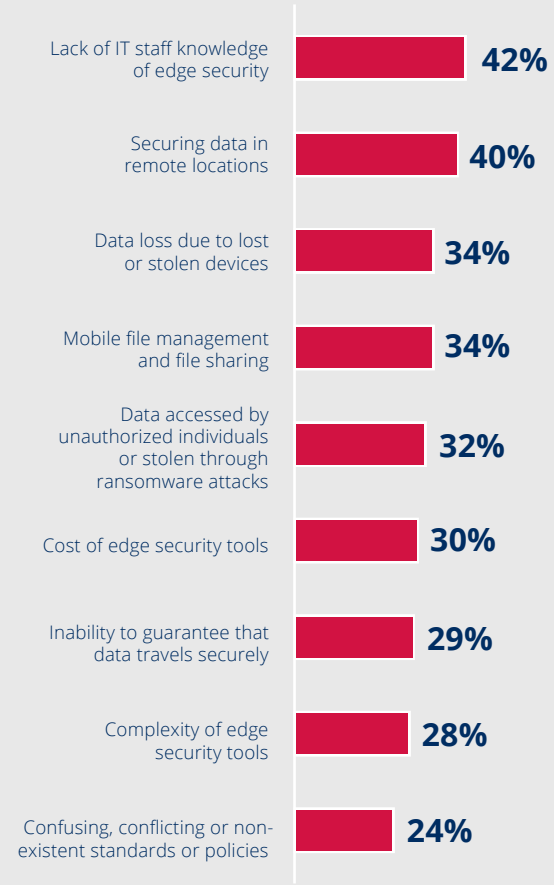
The survey results also showed that despite the majority of senior respondents indicating they feel good about their agency's data security, nearly half expressed concerns with lack of IT staff knowledge about edge data security (42 percent). Such concerns were followed closely by worries about securing data in remote locations (40 percent) and data loss due to lost/stolen devices as well as mobile file management and sharing (both 34 percent). (See Figure 6)

Another defense supply maintenance and contracting chief felt their agency had numerous vulnerabilities,

"**All remote operations are at risk** unless additional resources are introduced to decrease vulnerabilities."

Figure 6

Edge Security Concerns



Note: Multiple responses allowed

	Defense	Federal Civilian
Securing data in remote locations	49%	32%
Confusing, conflicting or non-existent standards or policies	30%	18%

	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
Cost of edge security tools	52%	27%	24%
Mobile file management and file sharing	48%	29%	35%
Data accessed by unauthorized individuals or stolen through ransomware attacks	48%	27%	35%
Lack of IT staff knowledge of edge security	36%	49%	31%

Statistically significant difference

SECURING THE MOBILE WORKFORCE

With the government looking to incorporate more Bring Your Own Device (BYOD) policies for the federal workforce, agencies must confront greater data risks in securing employee or contractor phones, desktops and laptops.

"We might have challenges when my agency leaps into BYOD solutions," one federal IT project manager said.

Many across the federal government share similar concerns. Over half of the survey respondents think their agency's data is most at risk on employee or contractor desktops and laptops (49 percent) as well as employee or contractor-owned mobile devices (42 percent). (See Figure 7)

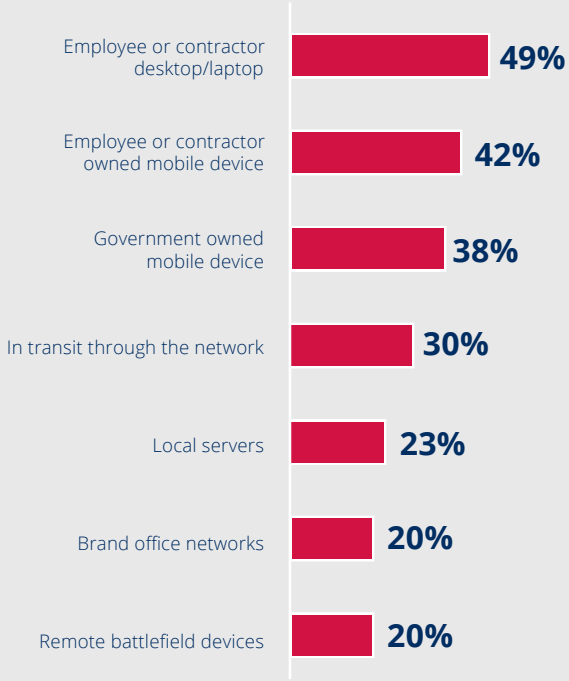
As agencies plunge into cloud migrations and embrace mobility for their employees, leaders and IT must ensure that data – whether it's in an employee's device or in a remote desktop – is fully backed up and can be recovered within minutes of a breach or incident.

Through edge data security, federal IT and security leaders can better secure cloud and mobility efforts by incorporating the golden 3-2-1 rule of data backup and storage. The rule comprises three copies of data (1 production and 2 backups); two types of storage media; and one off-site in the cloud. Additionally, agencies need to secure who has access to sensitive information and have the audit trails necessary to comply with standards and regulations.

Edge data security also entails secure file sharing methods across any device with the ability to encrypt data and monitor privilege and identity access – helping to alleviate concerns and transition to the cloud or bring in BYOD as securely as possible.

Figure 7

Where Data is Most at Risk



	Defense	Federal Civilian
Remote battlefield devices	25%	14%

Statistically significant difference

Note: Multiple responses allowed

THE IDEAL EDGE SECURITY POSTURE
RETHINKING SECURITY PRIORITIES

Despite the importance of data recovery and backup, federal IT leaders still do not align data backup and recovery solutions with their primary cybersecurity investments, compared to massive enterprise solutions that promise to protect all endpoints.

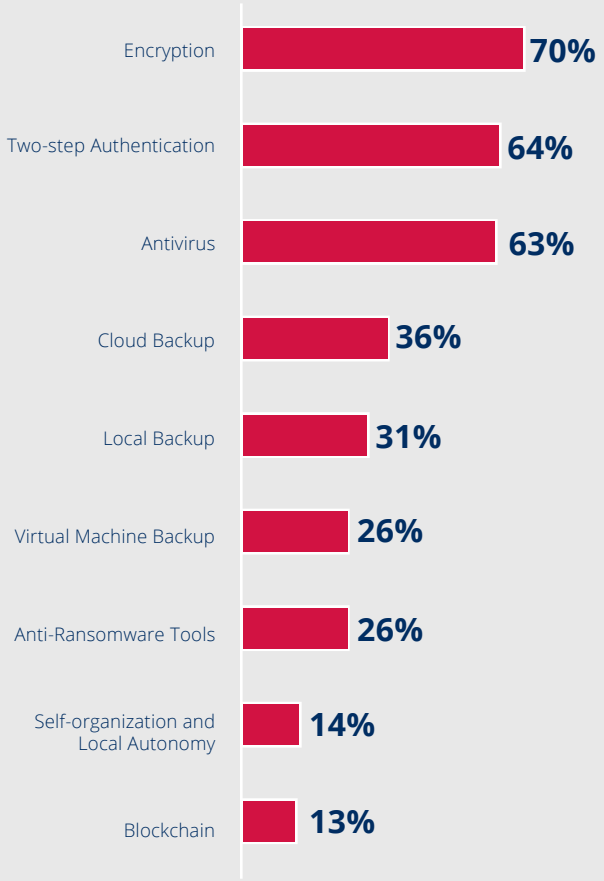
According to the survey results, only about a third of respondents prioritize backup and recovery as integral to securing edge data, including cloud backup (36 percent); local backup (31 percent) and virtual machine backup (26 percent). The results also reveal yet another discrepancy between senior executives and IT practitioners in terms of the perceived tools and techniques used to address edge data security. Whereas 48 percent of senior executives believe cloud backup solutions are how edge data is protected and secured in their agencies, only 25 percent of technical practitioners believe cloud backup solutions are how edge data is protected and secured. Similarly, 42 percent of senior decision makers believe virtual machine backup solutions are how their edge data is protected and secured, only 25 percent of technical practitioners believe the same. (See Figure 8)

But, as established in this report, any sort of downtime can cause unnecessary pain, costs, and lost time for productivity if agencies don't back up their data accordingly.

According to the results, the majority of federal leaders are focused on traditional security methods, with encryption as a primary way to secure edge data (70 percent). This was followed closely by two-step authentication (64 percent) and antivirus software (63 percent). (See Figure 8)

Figure 8

How Edge Data is Protected and Secured



Note: Multiple responses allowed

	Defense	Federal Civilian
Cloud Backup	29%	43%
Local Backup	23%	39%

	Senior/ Executive	Mid-Management	Hands-On IT/ Technical
Cloud Backup	48%	38%	25%
Virtual Machine Backup	42%	21%	25%
Anti-Ransomware Tools	30%	21%	35%
Self-organization and Local Autonomy	30%	13%	7%

Statistically significant difference

THE IDEAL EDGE SECURITY POSTURE — CONTINUED

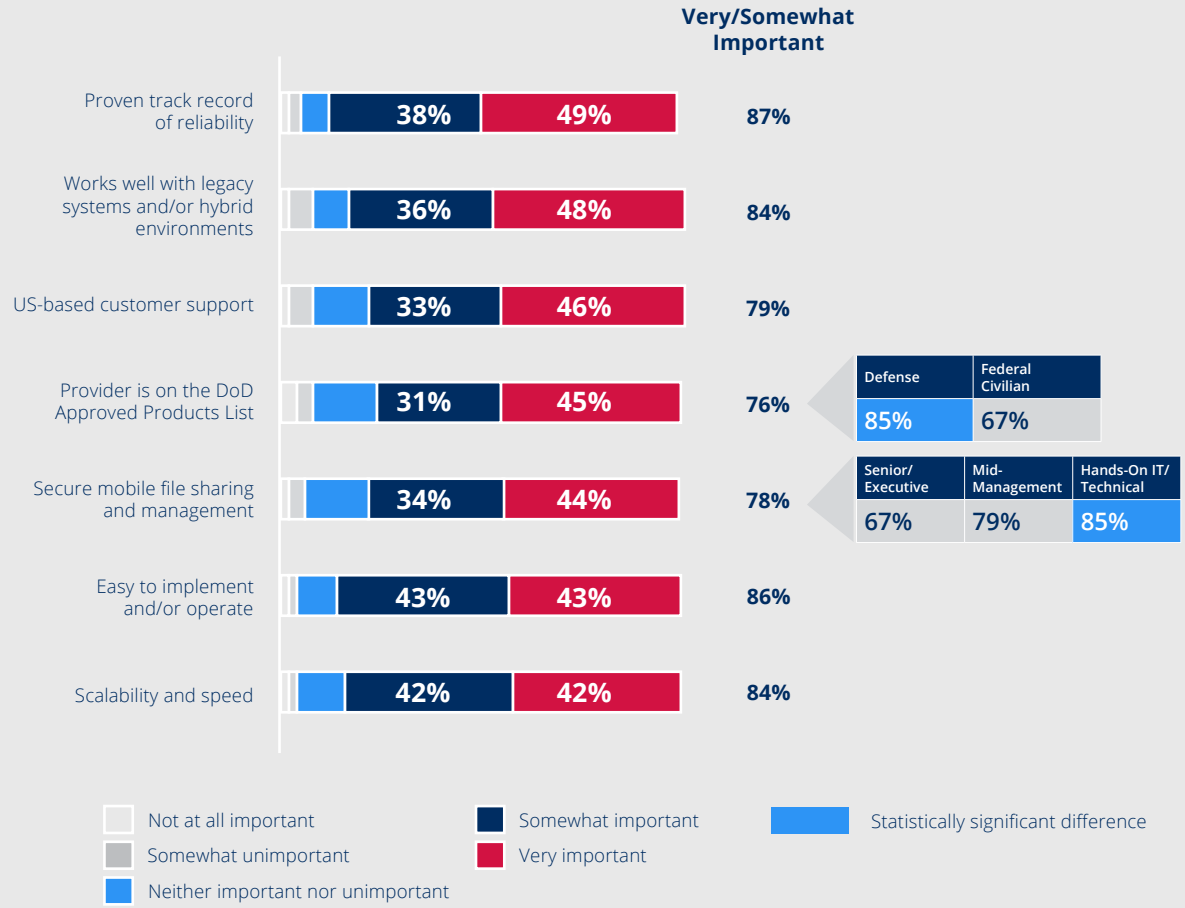
Those managing remote offices or who need to share files and digitally collaborate feel that encryption is imperative to protect data in transit. One Regional Information System Security Manager (ISSM) at a defense agency said, "Ensuring mobile devices and laptops are secure by full disk encryption is critical in my opinion."

However, in cases of a ransomware attacks, where malicious hackers can simply re-encrypt data and withhold it from agencies, encryption, anti-virus software and two-factor authentication can only go so far. That's why the future of government cybersecurity requires self-protecting data; enabling agencies to lock it down, retrieve it back, and encrypt it even after it's already been sent.

For the private sector, disaster recovery and backup have proven to be the difference between surviving a ransomware attack or going out of business. Industry research shows that 93 percent of companies without a data backup and recovery solution who suffered a data disaster were out of business within one year. But 96 percent of organizations with a backup and recovery solution in place were able to fully recover operations, even after a data disaster. This is an especially important lesson for the public sector to learn as well, given the high stakes of public data breaches.

Figure 9

Importance of Edge Security Product Features



THE IDEAL EDGE SECURITY POSTURE — CONTINUED

THE FUTURE-PROOF APPROACH

Edge data security can easily be used to support cloud and mobility efforts for the government workforce. The key is prioritizing data backup and recovery, so that federal IT and security leaders can feel confident in proactively mitigating cyber risks at the edge of their networks – because they're ready for anytime disaster could strike.

Because when a workstation goes down or a device goes missing, disaster recovery and backup enable agencies to take a snapshot of every device – be it a physical machine or server. That image pulls data out of the same file but can be imported into a new machine, operating system, application, or system setting. The data, no matter where it resides, becomes instantly operational – making it as though the data was never lost in the first place.

In terms of actual solutions, respondents most often indicated that a proven track record of reliability is an important product feature when selecting an edge data security solution (87 percent said this was somewhat or very important). (See Figure 9). This makes sense as federal IT and security leaders are responsible for multi-million dollar procurements that can have wide-ranging implications for their agencies.

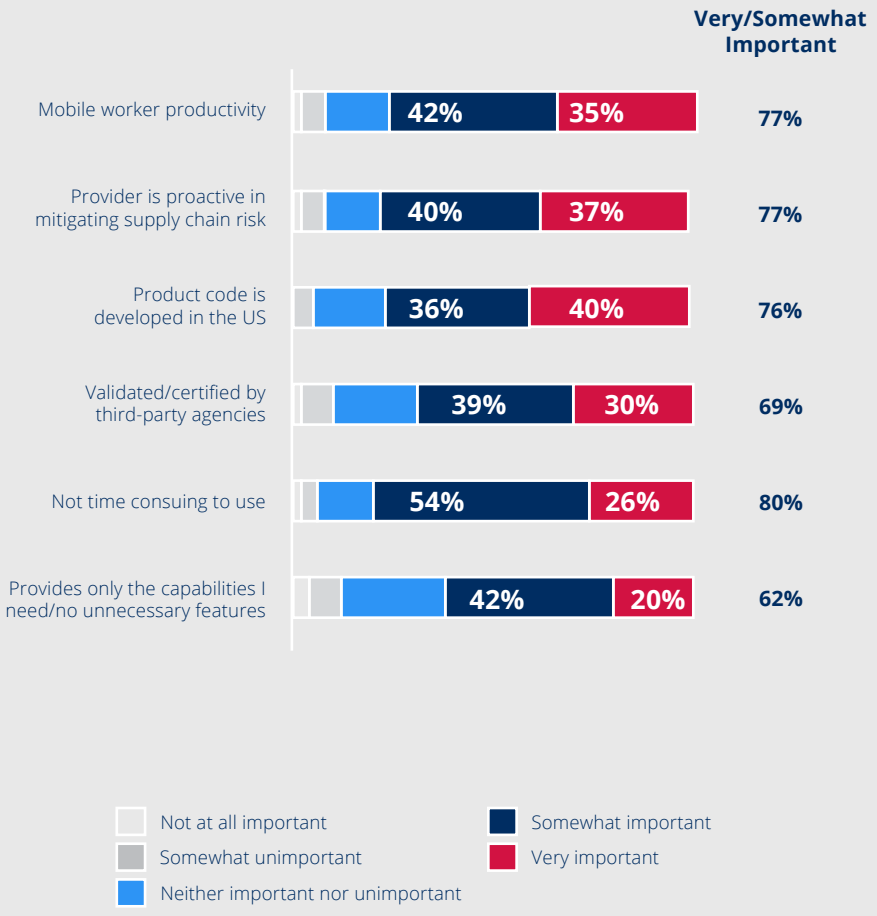
In addition to familiarity and trusted vendors, most federal IT and security leaders prefer buying their solutions knowing they were made domestically. According to the survey results, 76 percent felt that it was somewhat or very important for the product code to be developed in the U.S. (See Figure 10)

This also makes sense given the endless cycle of headlines concerning cyber attacks waged by foreign adversaries and nation-states. Having a trusted vendor solution that is American-made means better ability to deliver on the unique requirements of policy and mandates for the U.S. public sector.

Not surprisingly, federal leaders also prefer products that are easy to use and more proactive in strengthening cyber posture, rather than reactive. At least 80 percent of respondents preferred that their solutions not be time consuming to use; 77 percent wanted solutions to ensure mobile worker productivity; and 76 percent felt that the providers should be proactive in mitigating the supply risk chain. (See Figure 10)

Figure 10

Importance of Edge Security Product Features (Continued)



CONCLUSION

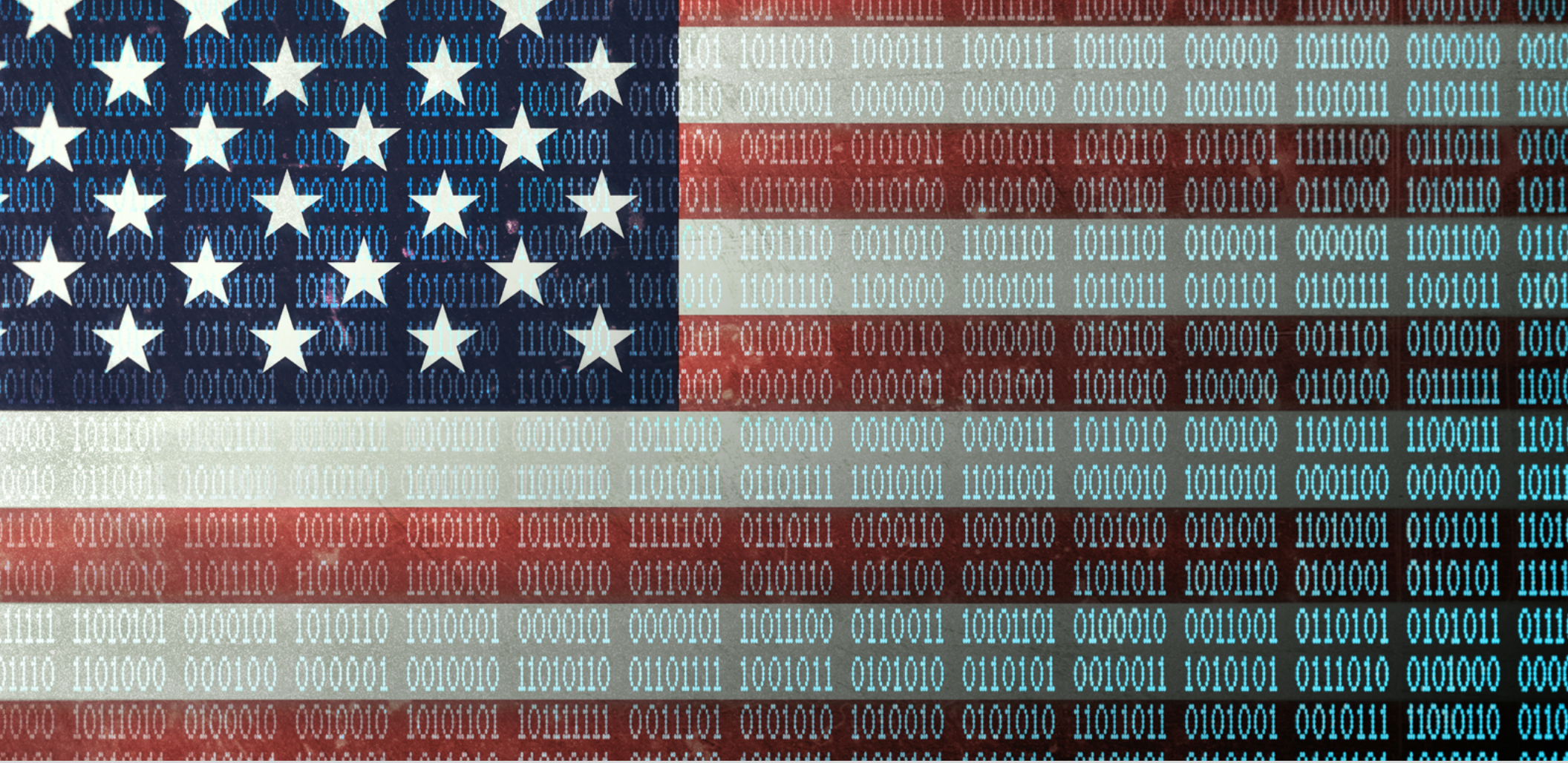
What's evident from this report is that federal agencies risk not only their cyber posture but also falling behind the technology modernization curve by relying solely on traditional methods and solutions for data protection.

Federal leaders and managers must attain a better understanding of securing data at the edge, their agencies' vulnerabilities, and where the knowledge and awareness gaps persist. Going forward will also require rethinking priorities for federal cybersecurity investments. Rather than considering data recovery and backup as a checklist item within operations, federal IT and security leaders should consider this as a critical part of their security strategies.

But leaders and practitioners cannot wait for the next policy mandate to come out. Cyber threats are evolving and getting more sophisticated every day, making government data all the more vulnerable. Scalability is also a critical feature to data solutions as decision makers cannot risk making an acquisition that only meets today's needs but will fail to deliver tomorrow. For the Department of Defense in particular, securing data at the edge and expediting the acquisition process will be especially important to ensure the speed of relevance against peer and near-peer adversaries.

What the Federal Government needs now and for the future is dynamic edge data security, which considers the inevitability of data loss – whether through lost/stolen devices, data breaches, insider threats, system malfunctions, or operator errors.

Whether harnessing the cloud, enabling a mobile workforce, or simply pushing for more digital collaboration, agencies need edge data security solutions that are easy to implement, cost effective, and future-proof – that can integrate with other technology solutions while offering utmost protection now and well into the future.



ABOUT ACRONIS SCS

Since 2005, Acronis SCS products have been successfully protecting US government data, including the Department of Defense and its contractors.

Protecting Federal data requires meeting strict security and compliance standards. Acronis SCS offers the leading data protection and disaster recovery solutions for virtual, physical, mobile and cloud environments. Acronis SCS products help government agencies protect their most valuable data while improving the quality and reliability of their services.

https://acronisscs.com

Acronis SCS