ACHIEVING FEDERAL CYBER RESILIENCE
BEST PRACTICES AND LESSONS LEARNED

ACCENTURE’S THIRD ANNUAL STATE OF CYBER RESILIENCE REPORT
FEDERAL EDITION
Contents

STATE OF CYBER RESILIENCE 7

Where are we now?
- Investment in innovation grows 8
- Cybersecurity basics are improving 9
- Filling the gaps in cybersecurity performance 10
- Progress masks hidden threats 11
- ROI is elusive 13
- Unsustainable cost increases 14
- How to help reduce the cost of a cyberattack 15

BEHAVIOR OF LEADERS 16

- Stop more attacks 18
- Find breaches faster 19
- Fix breaches faster 20
- Reduce breach impact 21

HOW LEADERS SUCCEED 22

- Invest for operational speed 23
- Drive value from new investments
  - Scale more 24
  - Train more 25
  - Collaborate more 26
- Sustain what they have
  - Maintain existing investments 27
  - Perform better at the basics 28

ACHIEVING FEDERAL CYBER RESILIENCE 30

THE CASE FOR MANAGED CYBER RESILIENCE 32

MASTERING FEDERAL EXECUTION 29

ABOUT THE AUTHORS 32
Federal agencies, like all large global organizations, are under attack from bad actors. Though they share many of the same challenges as commercial entities (e.g., deficit of cybersecurity professionals and overabundance of segregated security technologies), they also face unique compliance requirements and acquisition challenges that complicate their approach to cyber resilience.

Existing long-term government procurement processes, combined with a systemic focus on compliance, can hinder effective federal cyber response. This makes it difficult to acquire and implement the right tools while also creating false confidence in the agency’s security.

Yet despite the challenges, results from Accenture’s Third Annual State of Cyber Resilience Report - Federal Edition demonstrate that federal agencies on average perform on par or better than the rest of the global population. But there is room for improvement when agencies are compared to the subset of respondents deemed “leaders” based on their survey responses.

This report yields insights into how federal agencies stack up against commercial peers across the globe, and the results are enlightening and encouraging. It also provides details about how organizations are investing in cyber resilience, the results they are achieving, and the sustainability of current models.

Aaron Faulkner
CYBERSECURITY PRACTICE LEAD
ACCENTURE FEDERAL SERVICES
aaron.faulkner@accenturefederal.com
Executive Summary

Cybersecurity is improving globally, and cyber resilience is on the rise. Accenture’s latest research shows that most organizations, including federal agencies, are getting better at defending against cyberattacks. But as defenses evolve, so too do the threats. Attackers have already moved on to indirect targets, such as suppliers and other third parties. This leads to massive vulnerability for federal agencies that rely heavily on a contractor network to achieve their missions.

And while vulnerabilities continue to shift, cybersecurity costs are reaching unsustainable levels. Despite the hefty price tags, security investments often fail to deliver the desired security outcomes. This is particularly challenging for large federal agencies that cannot implement security solutions consistently throughout their organizations. Proliferation of outdated, hodgepodge legacy security solutions complicate progress.

But there is good news.

Accenture’s analysis reveals there is a group of standout organizations within the public and private sectors that have cracked the cybersecurity code for innovation.

In Accenture’s Third Annual State of Cyber Resilience Report - Federal Edition, we identify what sets leaders apart. 4,644 executives were surveyed, including one hundred federal professionals, and Accenture’s industry experts compiled key findings to benefit commercial and government organizations.

Detailed modeling of cybersecurity performance identified an elite group of leaders — 17% — that achieved significantly higher levels of performance compared to the rest. Federal agencies outperformed the global sample, with 28% qualifying as leaders.

These leading organizations set the bar for innovation.

BEHAVIORS OF CYBERSECURITY LEADERS

- Leaders focus on technologies that provide the greatest benefit.
- They scale, train, and collaborate more.
- Leaders focus on speed for detection, mobilization, and remediation.
For the purposes of this research, we investigated targeted cyberattacks. These have the highest potential to both penetrate network defenses, cause damage, and extract high-value assets from within the organization. This excludes the deluge of hundreds—if not thousands—of speculative attacks organizations face on a daily basis.
WHAT IS CYBER RESILIENCE?

Cyber resilience brings together the capabilities of cybersecurity, business continuity, and enterprise resilience. It applies holistic security strategies to help federal agencies and other organizations respond quickly to threats so they can minimize the damage and continue to operate under attack.

A cyber-resilient federal agency can introduce innovative solutions and operational models securely, strengthen stakeholder and citizen trust, and operate with confidence.
LEADERS OUTPERFORM THE PACK

A group of leading organizations are doing things differently

HOW DO THEY DO IT?

1️⃣ Invest for operational speed
2️⃣ Drive value from new investments
3️⃣ Sustain what they have

Cybersecurity basics are better

Innovation investment is growing

BUT...

- There are hidden threats
- ROI is elusive
- Costs are unsustainable

2x better at reducing breach impact
4x better at stopping attacks
4x better at finding breaches faster
3x better at fixing breaches faster
4x better at stopping attacks
Investment in cybersecurity innovation grows

**Cybersecurity Spending as Percentage of IT Budget**

Surveyed organizations, on average, spend 11% of their IT budgets on cybersecurity programs (10% exactly for federal agencies). Leaders spend slightly more at 11.2%, which is insufficient to account for their dramatically higher levels of performance.

- 11.2% spent by leaders on cybersecurity programs
- 11% spent by non-leaders on cybersecurity programs
- 10% spent by federal agencies on cybersecurity programs

**Cybersecurity Spending on Advanced Technologies**

Most organizations, including leaders, are investing heavily in several advanced technologies to aid in cybersecurity:

1. Artificial intelligence/machine learning
2. Robotic process automation

**Percentage of Cybersecurity Spending on Advanced Technologies**

The percentage of organizations spending more than 20% of budgets on these top two technologies:

- 82% of Leaders
- 89% of Non-Leaders
- 81% of Federal Agencies

Spending on cybersecurity innovation has grown significantly in the past three years.
WHERE ARE WE NOW?

Cybersecurity basics are improving

More than four out of five global and U.S. federal survey respondents agreed that cybersecurity tools have advanced significantly over the past few years and are noticeably improving their organization’s cyber resilience.

Improvements in basic security hygiene back up this finding. Being able to accurately assess the number of cyberattacks against an organization depends on the ability of each organization to detect them.

Global Results

Survey results reveal that the average total number of cyberattacks an organization faced dropped 11% over the course of a year, from 232 to 206 targeted attacks. During the same timeframe, we saw an even larger drop of 27% in the number of security breaches. On average, organizations now face 22 security breaches per year, compared with 30 in the previous year. This indicates the basics seem to be improving.

Federal Results

For federal agencies, the picture is different. The number of year-over-year attacks increased from 211 to 320, a 53% increase, but security breaches are lower, down from 30 to 17 security breaches per year. This marks a 43% reduction. Federal agencies outperform their global counterparts in successfully stopping breaches.

Cybersecurity teams are effectively discouraging cyberattacks and successfully defending against them when they occur.
**WHERE ARE WE NOW?**

**Filling the gaps in cybersecurity performance**

Leaders ranked specific technologies for their importance and effectiveness in addressing a number of requirements for cyber resilience. Non-leaders should use this list to identify potential solutions for current gaps in their cybersecurity program.

<table>
<thead>
<tr>
<th>Technology benefits</th>
<th>SOAR</th>
<th>AI</th>
<th>NGF</th>
<th>RBA</th>
<th>RPA</th>
<th>PAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer successful attacks</td>
<td>#2</td>
<td></td>
<td>#1</td>
<td>#4</td>
<td></td>
<td>#3</td>
</tr>
<tr>
<td>Reduced breach impact</td>
<td>#3</td>
<td>#1</td>
<td></td>
<td>#2</td>
<td></td>
<td>#4</td>
</tr>
<tr>
<td>More precise incident detection</td>
<td>#1</td>
<td>#2</td>
<td>#3</td>
<td></td>
<td>#4</td>
<td></td>
</tr>
<tr>
<td>Reduced inherent risk/shrink the attack surface</td>
<td>#1</td>
<td></td>
<td>#3</td>
<td>#2</td>
<td></td>
<td>#4</td>
</tr>
<tr>
<td>Cost reduction</td>
<td>#1</td>
<td>#2</td>
<td></td>
<td>#3</td>
<td>#4</td>
<td></td>
</tr>
<tr>
<td>Consistent quality of response</td>
<td>#2</td>
<td>#1</td>
<td></td>
<td>#4</td>
<td>#3</td>
<td></td>
</tr>
</tbody>
</table>

**AI**  Artificial Intelligence (Machine Learning/Natural Language Processing)  
**NGF**  Next-Generation Firewall  
**PAM**  Privileged Access Management  
**RBA**  Risk-Based Authentication  
**RPA**  Robotic Process Automation  
**SOAR**  Security Orchestration, Automation, and Response
**WHERE ARE WE NOW?**

**Progress masks hidden threats**

A closer look at the sources of cyberattacks reveals 45% of federal agencies’ security breaches are now indirect, as threat actors target the weak links in their extended operation. This is modestly higher than global responses, where indirect attacks represent 40% of security breaches. This shift to indirect attacks blurs the true scale of cyberthreats.

Organizations should look beyond their four walls to protect their operational ecosystems and supply chains. Fully 85% of federal respondents, in line with the global responses (82%), agreed their organizations need to think beyond securing their enterprises and take steps to secure their ecosystems to be effective.

### Global Hidden Attacks

If we apply the same average number of security breaches to indirect cyberattacks for the global finding, the total number—both direct and indirect—could jump from 232 to about 280, a potential increase of 20% over the prior year.

<table>
<thead>
<tr>
<th>Year</th>
<th>Successful Direct Attacks</th>
<th>Indirect Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>202</td>
<td>30</td>
</tr>
<tr>
<td>2019</td>
<td>184</td>
<td>40% of security breaches from indirect attacks</td>
</tr>
</tbody>
</table>

A potential **20% increase** in overall annual attacks

### Federal Hidden Attacks

For federal agencies, the total number—both direct and indirect—could jump from 201 annual attacks to about 613, a potential 3x increase over the prior year.

<table>
<thead>
<tr>
<th>Year</th>
<th>Successful Direct Attacks</th>
<th>Indirect Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>171</td>
<td>30</td>
</tr>
<tr>
<td>2019</td>
<td>320</td>
<td>45% of security breaches from indirect attacks</td>
</tr>
</tbody>
</table>

A potential **3x increase** in overall annual attacks

---

**Key:**
- Unsuccessful Direct Attacks
- Successful Direct Attacks
- Indirect Attacks
As soon as one breach avenue is foiled, attackers are quick to find other means. With the growth in indirect attacks, the spotlight falls on protecting third parties, including government contractors, grantees, and other partners. But there are enormous challenges in managing third-party cyber risks.

Many federal CISOs feel the sizable number of partners outstrips their capacity to monitor them.

Given finite security resources, there is value in a data-driven, mission-focused, tiered-risk approach to secure the enterprise ecosystem.

Many federal agencies are adopting managed security services to tackle the wider scope and scale of security risks, extending their coverage to trusted third parties.

By collaborating more broadly with others with the common goal of securing the enterprise and its ecosystem, agencies play a responsible role in helping their partners beat cybercrime while also ensuring they are not bolting the front door from attackers while leaving the back door wide open.
WHERE ARE WE NOW?

ROI is elusive

Despite similar spending levels, our research found clear differences in terms of enterprise coverage, detection rate, remediation, and citizen or customer impact. Leaders are able to achieve significantly more return on investment.

With only a little more than half of their organization covered by their cybersecurity programs, non-leaders are at risk of having many areas unprotected. This contrasts with leaders who are able to cover 85% of their organization with their cybersecurity programs.

Across the four risk measures detailed in this table, federal agencies perform better than the average respondent, but not quite as well as leaders.

<table>
<thead>
<tr>
<th>Performance in four measures of security investments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FAILING INVESTMENTS</strong></td>
</tr>
<tr>
<td>Gaps in protection</td>
</tr>
<tr>
<td>Low detection rates</td>
</tr>
<tr>
<td>Longer breach impact</td>
</tr>
<tr>
<td>Customer/citizen data exposed</td>
</tr>
</tbody>
</table>
WHERE ARE WE NOW?

Unsustainable cost increases

Cost increases are beginning to reach what many respondents consider unsustainable levels. Despite rising investments in new cybersecurity technologies, our research highlights many areas where the purchased technologies are failing.

For federal agencies, the three cybersecurity technologies with the largest increases in cost are network security, threat detection, and security monitoring.

SECURITY COMPONENTS RANKED BY BIGGEST COST INCREASES GLOBALLY

2. Threat Detection 8. End-Point Detection And Response 14. Staffing (or People)
5. Firewalls 11. Vulnerability Management 17. Siem and Event Consoles
6. Threat Intelligence 12. OT-Related Security

ANNUAL FEDERAL CYBERSECURITY COSTS INCREASES

55% saw costs increase up to 25%
20% saw costs increase more than 25%
25% saw no increase

60% of federal respondents say increasing costs are unsustainable
Federal agencies can reduce costs—both in terms of the cybersecurity protection cost to the organization and the wider economic impact—by modeling their behavior after that of the leaders.

$380,000us: The average cost-per-attack for non-leaders

$107,000us: The average cost-per-attack for leaders

If agencies perform at the same level as leaders—having the same proportion of attack types and the same time to detect and fix responses—Accenture’s detailed modeling indicates they could reduce the cost per successful attack by 72%.

Replicating the behavior of global cybersecurity leaders can potentially save federal agencies $273,000us per security breach.
WHY LEADERS ARE MORE CYBER RESILIENT

Leaders stop more attacks

Leaders have nearly a fourfold advantage in stopping targeted cyberattacks.

Leaders find breaches faster

Leaders have a fourfold advantage in detection speed.

Leaders fix breaches faster

Leaders have nearly a threefold advantage in speed of remediation.

Leaders reduce breach impact

Leaders have a twofold advantage in containing damage impact.

Leaders are the 17% of global organizations who set the standard for cybersecurity excellence. 28% of federal agencies fit in this category.
Why leaders are more cyber resilient

Detailed modeling and statistical analysis of cybersecurity performance has identified a group of leaders that achieve significantly higher levels of cyber resilience compared with the non-leaders.

The statistical analysis revealed that leaders were characterized as among the highest performers in at least three of the following four categories:

1. Stop more attacks
2. Find breaches faster
3. Fix breaches faster
4. Reduce breach impact

Federal agencies on average perform significantly better than the average survey respondent, though not as well as the global leaders.

Cybersecurity performance characteristics

<table>
<thead>
<tr>
<th>CHARACTERISTICS</th>
<th>LEADERS</th>
<th>NON-LEADERS</th>
<th>FEDERAL AGENCIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop more attacks</td>
<td>1 in 27 attacks breach security</td>
<td>1 in 8 attacks breach security</td>
<td>1 in 18 attacks breach security</td>
</tr>
<tr>
<td>Find breaches faster</td>
<td>88% detect breaches in less than one day</td>
<td>22% detect breaches in less than one day</td>
<td>45% detect breaches in less than one day</td>
</tr>
<tr>
<td>Fix breaches faster</td>
<td>96% fix breaches in 15 days or less</td>
<td>36% fix breaches in 15 days or less</td>
<td>58% fix breaches in 15 days or less</td>
</tr>
<tr>
<td>Reduce breach impact</td>
<td>58% of breaches have no impact</td>
<td>24% of breaches have no impact</td>
<td>35% of breaches have no impact</td>
</tr>
</tbody>
</table>
Why leaders are more cyber resilient

STOP MORE ATTACKS

Leaders globally identify a higher number of direct attacks against them—an average of 239 cyberattacks compared with 166 for non-leaders—while having a higher success rate in defending against them.

Leaders see only nine security breaches per year compared with an average of 22 per year for non-leaders. In the global sample, leaders have nearly a fourfold advantage when dealing with security breaches.

Federal agencies face a higher average number of annual attacks versus the average organization surveyed, but despite facing 320 cyberattacks a year, on average only 17 breaches occur. 5.3% of attempted cyberattacks breach federal defenses, whereas 3.8% breach leaders and 13% succeed against non-leaders.

Key Enabling Technologies
1. Next-Generation Firewall (NGF)
2. Security Orchestration, Automation, and Response (SOAR)
3. Privileged Access Management (PAM)

Average number of security breaches and targeted cyberattacks for leaders, non-leaders, and surveyed federal agencies

<table>
<thead>
<tr>
<th></th>
<th>Average Cyberattacks</th>
<th>Average Security Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaders</td>
<td>239</td>
<td>9</td>
</tr>
<tr>
<td>Non-Leaders</td>
<td>166</td>
<td>22</td>
</tr>
<tr>
<td>Federal Agencies</td>
<td>320</td>
<td>17</td>
</tr>
</tbody>
</table>

Key: □ Average Cyberattacks □ Average Security Breaches
Why leaders are more cyber resilient

FIND BREACHES FASTER

Time is critical when it comes to detecting a security breach, and leaders have distinct advantages, with 88% able to detect a security breach in less than one day on average. The remaining 12% were able to detect security breaches in seven days or less, meaning that nearly all breaches were discovered in a week or less.

For non-leaders, only 22% detected a security breach on the first day, with 83% of breaches detected in seven days or less.

Federal agencies perform better than average, but still shy of leaders. 45% can detect security breaches in less than a day, with 91% of breaches detected in seven days or less.

Key Enabling Technologies

1. Artificial Intelligence (AI)
2. Security Orchestration, Automation, and Response (SOAR)
3. Next-Generation Firewall (NGF)
Why leaders are more cyber resilient

**FIX BREACHES FASTER**

Maintaining mission, business continuity, and rapid recovery speeds are other important aspects of cybersecurity resilience where leaders have clear advantages. Fully 96% of them plug security breaches in 15 days or less.

This compares with only 36% of non-leaders who said they remediate security breaches in 15 days or less on average. This means 64% take 16 to 30 days or more to remediate a security breach.

Federal agencies outperform non-leaders in speed of fixing breaches. 58% are able to fix security breaches in 15 days or less, with 42% requiring 16 to 30 days or more.

**Key Enabling Technologies**

1. Security Orchestration, Automation, and Response (SOAR)
2. Artificial Intelligence (AI)
3. Next-Generation Firewall (NGF)
Why leaders are more cyber resilient

REDUCE BREACH IMPACT

Speed of recovery is essential in minimizing the damage of a security breach and the level of impact on an organization. Leaders stated that 83% of all security breaches resulted in either no impact or a minor impact. Of the remaining security breaches, 10% are moderate impact and 6% are significant. This translates to a moderate security breach every 13 months, on average, and a significant breach every 22 months or so, on average.

Non-leaders have lower levels of performance, with 50% of security breaches delivering a moderate or significant impact.

Federal agencies perform better than non-leaders, but not as well as leaders. 42% of federal security breaches deliver a moderate or significant impact.

Key Enabling Technologies

1. Artificial Intelligence (AI)
2. Next-Generation Firewall (NGF)
3. Security Orchestration, Automation, and Response (SOAR)
HOW LEADERS SUCCEED
Practices and approaches leaders use effectively

Leaders invest for operational speed
Leaders prioritize moving fast and choose turbo-charging technologies to help them get there.

Leaders drive value from new investments
Leaders scale more, train more, and collaborate more to increase the value from innovative technology.

Leaders sustain what they have
Leaders place more emphasis on maintaining existing investments and perform better at the basics of cybersecurity.
Invest for operational speed

PRIORITIZE MOVING FAST

In the current environment of rising costs and growing third-party threats, security investments must work more effectively and efficiently than ever to prove their worth.

The top three measures of cybersecurity success for leaders emphasize speed.

We found that leaders prize how quickly they can detect a security breach, how quickly they can mobilize their response, and how quickly they can get operations back to normal. Beyond these priorities, leaders also measure the success of their resiliency by how many systems were stopped and for how long, and by how accurate they were in finding cyber incidents.

Federal agencies also ranked the same three measures of speed as their top three indicators of success, though they ranked cyber recovery time higher than cyber detection speed or cyber response time.

Top three ways organizations measure the success of cybersecurity programs

1. **Cyber detection speed** (how long it takes to detect an incident)
   - Leaders: 58%
   - Non-Leaders: 41%
   - Federal Agencies: 46%

2. **Cyber recovery time** (how long it takes to restore normal activity)
   - Leaders: 53%
   - Non-Leaders: 39%
   - Federal Agencies: 52%

3. **Cyber response time** (how long it takes to identify and mobilize)
   - Leaders: 52%
   - Non-Leaders: 41%
   - Federal Agencies: 46%
Drive value from new investments

SCALE MORE

The rate at which organizations scale investments across their business has a significant impact on their ability to defend against attacks. Leaders perform four times better than their counterparts at scaling technologies—defined as 50% or more of tools moving from pilot to full-scale deployment. For the leaders, only 5% of cyberattacks resulted in a security breach. For the non-leaders, 21% of attacks resulted in a security breach.

Better security team detection
Security teams are also more effective for organizations who scale more of their technology investments. Leaders’ security teams actively protect three-quarters of all key assets and discover almost three-quarters of cybersecurity attacks against their organizations. Non-leaders are only able to protect one-half of their key assets and only detect one-half of all cyberattacks against them.

Federal performance
Federal agencies scale security tools well. 68% said that more than half of their security tools have been piloted and scaled throughout their organizations, with 22% scaling between one-quarter and one-half of their security tools.
Drive value from new investments

**TRAIN MORE**

When asked about security tools adopted by their organization that require training, 30% of leaders provided training for more than three-quarters of users when it was needed, versus just 9% of non-leaders.

**Faster at discovering and fixing breaches**

The speed with which organizations find security breaches is faster for those who provide higher levels of training. The best at training found 52% of security breaches in less than 24 hours, compared with only 32% for the rest. How long it takes to remediate a security breach is also an aspect of better training. For leaders, 65% of all security breaches are remediated within 15 days.

**Federal excellence in training**

Federal agencies lead the pack in terms of cybersecurity training, surpassing even the leaders in this category. 45% of federal agencies respondents said they provide training for more than three-quarters of users when it was needed.
Drive value from new investments

COLLABORATE MORE

79% of respondents agreed collaborations with other organizations, government bodies, and the wider security community will be one of the essential weapons they will need to combat cyberattacks in the future.

The organizations best at collaborating—the ones using more than five methods to bring together strategic partners, the security community, cybersecurity consortia, and an internal task force to increase understanding of cybersecurity threats—are two times better at defending against attacks than others. Organizations that collaborate more have a breach ratio of 6%, compared to an average of 13% for the rest.

Federal agencies are strong in all aspects of collaboration. Around half (51%) said they collaborate with strategic partners to test cybersecurity resilience and to share threat intelligence (45%). They also focus efforts on maintaining an internal cybersecurity committee/task force (58%).

<table>
<thead>
<tr>
<th>Main ways that leaders, non-leaders, and federal agencies collaborate with partners</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collaborate with strategic partners to share knowledge of threats</strong></td>
</tr>
<tr>
<td>Leaders: 57%</td>
</tr>
<tr>
<td>Non-Leaders: 47%</td>
</tr>
<tr>
<td>Federal Agencies: 51%</td>
</tr>
<tr>
<td><strong>Collaborate with strategic partners to test cybersecurity resilience</strong></td>
</tr>
<tr>
<td>Leaders: 57%</td>
</tr>
<tr>
<td>Non-Leaders: 46%</td>
</tr>
<tr>
<td>Federal Agencies: 45%</td>
</tr>
<tr>
<td><strong>Maintain an internal cybersecurity committee/task force</strong></td>
</tr>
<tr>
<td>Leaders: 56%</td>
</tr>
<tr>
<td>Non-Leaders: 46%</td>
</tr>
<tr>
<td>Federal Agencies: 58%</td>
</tr>
<tr>
<td><strong>Share threat information among the security community within industry</strong></td>
</tr>
<tr>
<td>Leaders: 53%</td>
</tr>
<tr>
<td>Non-Leaders: 45%</td>
</tr>
<tr>
<td>Federal Agencies: 52%</td>
</tr>
<tr>
<td><strong>Contribute to creating cybersecurity standards for industry</strong></td>
</tr>
<tr>
<td>Leaders: 43%</td>
</tr>
<tr>
<td>Non-Leaders: 43%</td>
</tr>
<tr>
<td>Federal Agencies: 40%</td>
</tr>
</tbody>
</table>

Key: Leaders | Non-Leaders | Federal Agencies
Sustain what they have

MAINTAIN EXISTING INVESTMENTS

Leaders understand the need to be brilliant at the basics. They focus more of their budget allocations on sustaining and optimizing what they already have, compared with non-leaders who place more emphasis on piloting and scaling new capabilities.

Federal agencies allocate their budgets similarly to leaders, with an emphasis on testing new capabilities (30%), scaling those capabilities (33%), and sustaining what they already have (37%).

How federal agencies benchmark against leaders in budget allocation

<table>
<thead>
<tr>
<th></th>
<th>Leaders</th>
<th>Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Scanning, piloting, trialing new capabilities (in a lab or pilot)</td>
<td>29%</td>
<td>30%</td>
</tr>
<tr>
<td>% Scaling new capabilities</td>
<td>32%</td>
<td>33%</td>
</tr>
<tr>
<td>% Sustaining what they already have</td>
<td>39%</td>
<td>37%</td>
</tr>
</tbody>
</table>
## Sustain what they have

### PERFORM BETTER AT THE BASICS

Security breaches most often happen when organizations fail at fundamental aspects of their protection practices. This is a challenge when the highest proportion of cyberattacks against leaders—35%—target customer records (citizen records for federal agencies).

### Protect the crown jewels

With only 15% of leaders report having more than 500,000 records exposed in the last year—compared to 44% of non-leaders and 39% of federal agencies—it is clear they are significantly better at the basics of cybersecurity protection.

Now, more than ever, it is vital for federal agencies to make sure the basics of data-centric security are in place. Bad actors in the form of individuals, organizations, and nation states are trying to undermine the credibility of American institutions. Accessing citizen data through cyberattacks is one of their key strategies, which necessitates an effective federal response for protecting key citizen data.

### The primary target of cybersecurity attacks

#### Customer/citizen records

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Leaders</th>
<th>Non-Leaders</th>
<th>Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>35%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Infrastructure (e.g., industrial control systems (ICS) attacks)

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Leaders</th>
<th>Non-Leaders</th>
<th>Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>28%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Stealing/extracting valuable IP or espionage-related

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Leaders</th>
<th>Non-Leaders</th>
<th>Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>24%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key: **Leaders**  [Non-Leaders]  [Federal Agencies]
Follow the leaders
A core group of leaders (which includes 28% of federal respondents) has shown that cyber resilience is achievable and can be reproduced. By investing for operational speed, driving value from these investments, and sustaining what they have, they are well on the way to mastering cybersecurity execution.

Leaders often take a more considered approach to their use of advanced technologies by choosing those which help deliver the speed of detection and response they need to reduce the impact of cyberattacks. The number of leaders spending more than one-fifth of their budget on advanced technologies has doubled in the last three years, and once they do invest in technology, they scale fast. The combined result is a new level of confidence from leaders in their ability to extract more value from these investments— and by doing so, exceed the performance levels of the non-leaders.

The state of federal cyber resilience
Federal agencies face a disproportionately large number of cyberattacks versus their commercial counterparts. Agencies are under a constant barrage of attempted breaches from organizations and individuals all over the world, and many of the cyberattacks (almost one-half) are now indirect, targeting federal partners and federal contractors.

Yet despite the growing and evolving threats agencies face, they are still able to outperform most organizations surveyed, though they lag behind the performance of leaders, on average.

As your agency continues its journey to improve against all key metrics – stopping more attacks, finding and fixing breaches faster, and reducing breach impact – Accenture can help you assess your current processes and technologies. We can help you define a strategy, architecture, and roadmap for strengthening your cyber posture in a sustainable, scalable, and agile manner.

Test your agency’s cybersecurity leadership
Ask your Accenture Federal Services contact if you would like to undertake the Accenture Security “Level-Up” Assessment to benchmark your organization’s cybersecurity program capabilities against those of your peers in a personalized report. The Accenture Cyber Fusion Center in Arlington, VA showcases a number of next-generation technologies for taking your cybersecurity to the next level.
THE CASE FOR CYBER MANAGED SERVICES

An answer to antiquated contracting models

Federal agencies are in a challenging position. They’re under cyberattack every minute of every day from individuals, organizations, and nation states. They must constantly evolve their technologies and processes for cybersecurity to stay ahead of evolving threats, yet their ability to innovate is directly hindered by government contracting practices.

How can an agency choose technologies (often down to the SKUs) that will protect it from threats two years from now – let alone five years? They can’t make that decision effectively without knowing the unknowable, namely, what attacks will look like in the future, and what new technologies will be available to aid in defense. This is especially true given the diverse and ever-changing set of tools needed to secure and monitor the end-to-end enterprise.

Choosing specific technology solutions in multi-year increments runs counter to the government’s interests. Flexible contracting models, with an emphasis on managed service solutions based on delivery outcomes via contractual service level agreements and key performance indicators, show great promise in addressing this issue.

A managed security service is the only contracting model that defeats legacy acquisition strategies of procuring point-in-time tools, manpower, and infrastructure. It delivers continuous innovations and protections for agencies.

Accenture’s Third Annual State of Cyber Resilience Report - Federal Edition survey results illustrate that strong cyber resilience is not achieved by throwing money at the problem or simply buying the latest technologies. Cyber resilience is achieved through a combination of good planning, a nimble approach to technology use and procurement, collaboration among organizations, and well-trained staff.
THE CASE FOR CYBER MANAGED SERVICES

Survey results support case for cybersecurity managed services

Drivers for managed service:
Extraordinary disparities exist between high and low performing security. Disparities take three primary forms:

1. **Talent gap**: There is a massive deficit in available resources in the security industry. Finding qualified staff to manage an in-house security team is challenging.

2. **Technology complexity**: There are more than 3,000 distinct cybersecurity vendors. Each organization’s security stack is different with varying levels of effectiveness. And each unique technology requires staffing.

3. **Functional capability gap**: Some organizations are better equipped to manage and analyze security data to aid in better organizational decision making.

A cyber managed service directly addresses each of the disparities to quickly place agencies into a stronger cyber resilient position while removing complexity and a false sense of security.

Benefits of managed service:
Cyber managed services yield particularly high results for organizations, largely due to the complexity of the cyber market.

- **Shared threat intelligence**: Agencies share information about threats, attacks, and effective response strategies.
- **Ongoing system updates**: Update one agency’s security solutions, it gets rolled out to other agencies.
- **Reduced costs**: Lower cost to agencies because each agency won’t have to build and man its own tech stack.
- **Capability leap**: Transitioning to a managed security service provides automation, orchestration, enrichment, intelligence, attacker emulation, and hunting at a scope and scale that most agencies would require 3-5 years to implement and operate.
- **Improved defense and performance**: Achieve service level agreements and key performance indicators (e.g., mean time to detect, respond, and resolution; true positive rate; alert coverage; percent of automated response; and more) well beyond what most individual organizations can achieve.
- **More rapid technology evolution**: Vendor responsible for tracking new technology and evolving threats, ensuring continuous introduction of new capabilities and features at the same fixed rate.
About the authors

Aaron Faulkner
Managing Director & Cybersecurity Practice Lead
ACCENTURE FEDERAL SERVICES
linkedin.com/in/aaron-faulkner-abb441

Major General George Franz (Ret.)
Managing Director & Defense Cybersecurity Lead
ACCENTURE FEDERAL SERVICES
linkedin.com/in/george-franz-3a32533a

Jason Layman
Managing Director and Technology Strategy & Advisory Practice Lead
ACCENTURE FEDERAL SERVICES
linkedin.com/in/jalayman/

David Dalling
XDR Capability Lead
ACCENTURE FEDERAL SERVICES
linkedin.com/in/daviddallingjr
About Accenture Federal Services

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Visit us at www.accenturefederal.com.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries — powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com.

About Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization’s valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

About Accenture Research

Accenture Research shapes trends and creates data driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients’ industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year.

Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. For more information, visit www.accenture.com/research.

Copyright © 2020 Accenture All rights reserved.