ACCENTURE FEDERAL SERVICES

ACHIEVING FEDERAL CYBER RESILIENCE

EXECUTIVE SUMMARY

Cybersecurity is improving globally, and cyber resilience is on the rise. Accenture's Third Annual State of Cyber Resilience Report - Federal Edition 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.

Federal agencies face additional challenges, such as inflexible procurement processes and a systemic focus on compliance, that can further hinder their cyber response. Despite these challenges, Accenture's research demonstrates 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.

Detailed modeling of cybersecurity performance across all industries identified this elite group of leaders — 17% —that achieve significantly higher levels of performance compared to the rest. Federal agencies outperformed the global sample, with 28% of respondents qualifying as leaders.

LEADERS ARE:

- **4x better at stopping attacks**
- **4x better at finding breaches faster**
- **3x better at fixing breaches faster**
- **2x better at reducing breach impact**

Federal agencies can seek to replicate the behaviors of cybersecurity leaders to lower costs and minimize the number and impact of cyberattacks.

Given the frequency of cyberattacks, this study assessed cyber resilience, which is an organization's integrated ability to successfully defend itself, respond quickly to breaches to minimize impact, and maintain overall continuity of operations. Furthermore, we focused on targeted cyberattacks as they have the highest potential to both penetrate network defenses, cause damage, and extract high-value assets from within the organization. Our survey included 4,644 security executives globally, spanning 24 industries. One hundred federal leaders participated in the research.

THE STATE OF FEDERAL CYBER RESILIENCE

Cyberattacks continue to escalate across the federal government with indirect attacks via third parties representing a growing threat. Fortunately, agencies are improving their ability to defend their environment, but many wonder how much longer they can continue to invest at their current pace.

Federal cyberattacks on the rise

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.

For federal agencies, though, the number of year- over-year attacks increased 53%, from 211 to 320, while security breaches decreased 43%, from 30 to 17 per year. Federal agencies outperform their global counterparts in successfully stopping breaches.

Despite this progress, there are hidden threats. Nearly half (45%) of federal agencies' security breaches are now indirect, as threat actors target the weak links in their extended operation. This shift to indirect attacks blurs the true scale of cyberthreats.

With the growth in indirect attacks, organizations should look beyond their four walls to protect their operational ecosystems and supply chains. Fully 85% of federal respondents agreed their organizations need to think beyond securing their enterprises and take steps to secure their ecosystems to be effective.

Investment grows – but costs may be unsustainable

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.

86% of federal respondents said that cybersecurity tools have advanced significantly over the past few years and are noticeably improving their organization's cyber resilience. However, this comes at a cost, with three-quarters of federal agencies reporting year-over-year cost increases for cybersecurity. 20% of federal agencies say their costs increased over 25% and 60% say that these cost increases are unsustainable.

Leaders realize greater ROI

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

PERFORMANCE ACROSS FOUR SECURITY METRICS

METRIC	LEADERS	NON-LEADERS	FEDERAL AGENCIES
Enterprise Coverage	**85 percent** of organization is actively protected	**55 percent** of organization is actively protected	**79 percent** of organization is actively protected
Detection Rates	**83 percent** of breaches found by security teams	**54 percent** of breaches found by security teams	**70 percent** of breaches found by security teams
Breach Remediation	**55 percent** say all breaches had an impact lasting more than 24 hours	**97 percent** say all breaches had an impact lasting more than 24 hours	**72 percent** say all breaches had an operational impact of more than 24 hours
Customer/ Citizen Data Exposed	**15 percent** had more than 500k records exposed in the last year	**44 percent** had more than 500k records exposed in the last year	**39 percent** had more than 500k records exposed in the last year

Federal agencies can reduce costs by modeling their behavior after that of leaders. The average cost globally of a cyber breach for non-leaders was $380,000 compared to $107,000 for leaders.

HOW CYBER LEADERS SUCCEED

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**

CYBERSECURITY PERFORMANCE CHARACTERISTICS

CHARACTERISTICS	LEADERS	NON-LEADERS	FEDERAL AGENCIES
Stop more attacks	**1 in 27** attacks breach security	**1 in 8** attacks breach security	**1 in 18** attacks breach security
Find breaches faster	**88%** detect breaches in less than one day	**22%** detect breaches in less than one day	**45%** detect breaches in less than one day
Fix breaches faster	**96%** fix breaches in 15 days or less	**36%** fix breaches in 15 days or less	**58%** fix breaches in 15 days or less
Reduce breach impact	**58%** of breaches have no impact	**24%** of breaches have no impact	**35%** of breaches have no impact

Cybersecurity leaders succeed by:

1. **Investing for operational speed:** Leaders prioritize moving fast and choose turbo-charging technologies to help them get there. The top three measures of cybersecurity success for leaders emphasize speed.
2. **Driving value from new investments:** Leaders scale more, train more, and collaborate more to increase the value from innovative technology. They perform four times better than their counterparts at scaling technologies—defined as 50% or more of tools moving from pilot to full-scale deployment.
3. **Sustaining what they already have:** Leaders place more emphasis on maintaining existing investments and perform better at the basics of cybersecurity. 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.

Key enabling technologies for leaders include next-generation firewall (NGF), secure orchestration, automation, and response (SOAR), and artificial intelligence (AI).

MASTERING FEDERAL CYBERSECURITY EXECUTION

Federal agencies share many of the same cybersecurity challenges as commercial entities (e.g., deficit of cybersecurity professionals and overabundance of segregated security technologies), but they also face unique compliance requirements and acquisition challenges that complicate their approach to cyber resilience.

A cyber managed service can address federal agencies' gaps in talent and functional capabilities, as well as simplify complex security stacks.

Furthermore, cyber managed services combat the inefficiencies and weaknesses that can result from slow government procurement processes. Flexible contracting models, with an emphasis on managed service solutions based on delivery outcomes via contractual service level agreements and key performance indicators, help federal agencies' cyber resilience evolve as threats do.

The benefits of cyber managed services include:

- **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.
- **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.

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.

GO MORE IN-DEPTH

Read the full report with key research findings, charts and analysis from our experts.
www.accenture.com/us-en/insights/us-federal-government/achieving-cyber-resilience

AUTHORS

AARON FAULKNER
Managing Director & Cybersecurity Practice Lead
Accenture Federal Services
linkedin.com/in/aaron-faulkner-abbb441

MAJOR GENERAL GEORGE FRANZ (RET.)
Managing Director & Defense Cybersecurity Lead
Accenture Federal Services
linkedin.com/in/george-franz-3a32533a

GUS HUNT
Managing Director & Cyber Strategy Lead
Accenture Federal Services
linkedin.com/in/gus-hunt-55b57

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.

accenture