


A snowy owl is shown in flight, centered in the frame, with its wings fully extended. The owl is white with yellow eyes and a dark beak. The background is a vast, flat, snow-covered field under a pale, overcast sky. In the distance, a line of bare trees and utility poles is visible on the horizon.

THE NATURE OF EFFECTIVE DEFENSE:

Shifting from Cybersecurity
to **Cyber Resilience**



Nowhere is resilience on better display than in nature. Trees are designed to bend but not break under the weight of snow or high winds. Our bodies automatically clean our blood, renew our cells and formulate a response when unwelcome viruses and bacteria try to take hold.

Nature is inherently designed for resilience—and we believe it's time for federal organizations to take a similar approach to security. This requires a move from a posture of cybersecurity to one of Cyber Resilience.

Absolute security is absolutely impossible.

Nature was designed with the recognition that things can and inevitably will go wrong. That's equally true of security incidents. There's no question that they will occur.

When we erect virtual walls aimed at thwarting every invasion, we're working to achieve the unattainable goal of cyber certainty. The better approach? Architect systems and processes for Cyber Resilience. In other words, design the actual assets to be difficult to attack, to minimize impact and potential loss when an event happens, and to continuously deliver the intended capability—no matter what.

A brief history of resilience.

By no means is the idea of resilience new. It's been put to excellent use in a variety of fields.

Over-designed systems are a key tenet within both civil and mechanical engineering. In aeronautical engineering, self-contained redundant systems have been used to keep aircraft and space shuttles aloft. In the information technology realm, resilience has a mixed track record. The quest for "failure-proof" systems in the 1980s ultimately—and ironically—failed.

From there, technologists set their sights on failover, with automated switching to alternate sites when failures inevitably occurred. These sites provided readymade data centers with everything from backup generators to idle hardware waiting for the opportunity to be spun up. It may have worked, but it wasn't always easy, and it certainly wasn't cost-effective.

More recently, systems have been architected to be fault tolerant. We see this pattern not only in cloud computing but also in the electric power grid. The goal is systems that are highly automated, distributed, over-designed and redundant.

In other words, they're ready for anything.

**CYBER
RESILIENCE**
The ability to
continuously
deliver the intended
outcome despite
adverse cyber
events.

Stop reacting. Start anticipating.

Being ready for anything is at the heart of Cyber Resilience.

For too long, federal organizations have focused on building layers of protection for networks, systems, and data. These approaches are intended to enable detection and response. Although such techniques have value, they reflect a dangerous reality: that we've been letting the "bad guys" set the pace.

It's time to shift the balance of power away from adversaries and back in our favor. Some ideas to consider:

Know your adversary

Your adversaries want only two things: to steal, destroy, and/or modify your data and to implant a capability to take control of your systems or networks at the time of their choosing.

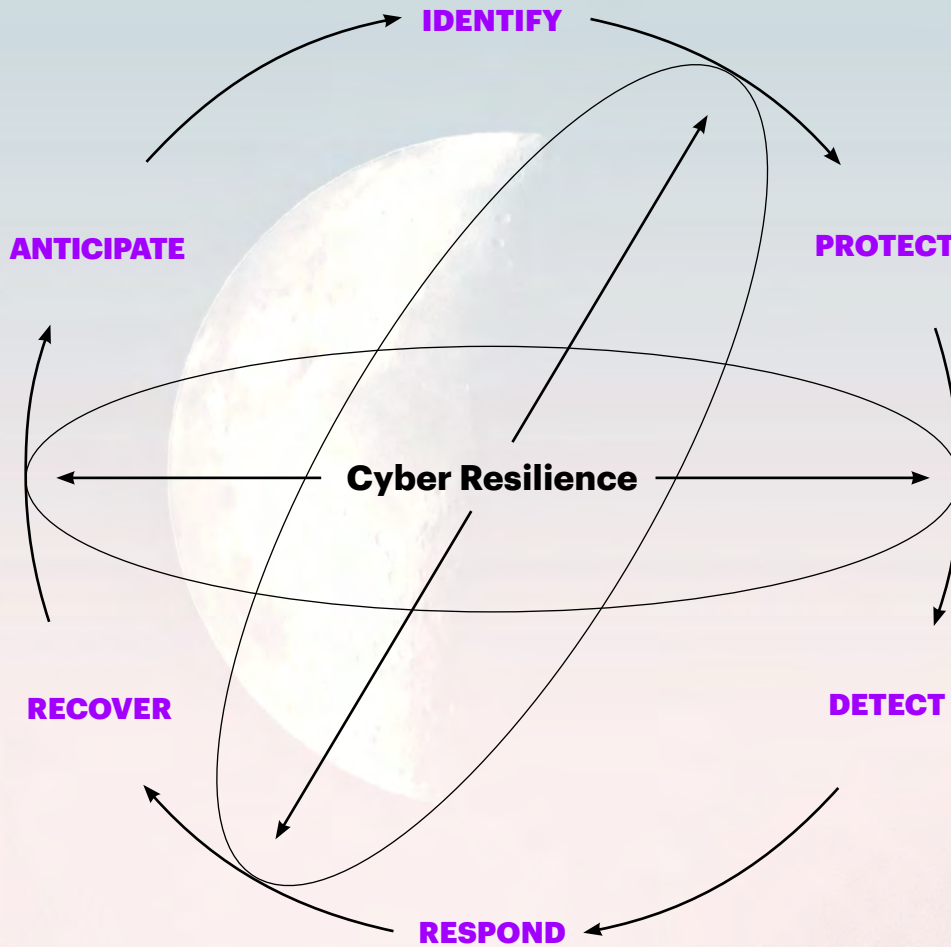
While you can never fully predict exactly when or how adversaries might initiate an attack, you can do something all the time. Become hard to find. Hard to attack. Hard to damage. In short, be resilient. Design systems so that even if adversaries succeed, you can minimize the damage of their "success" and ensure continued operations.

Cyber Resilience = IT Resilience = Mission Resilience

Combine the proven strengths of the NIST Framework (Identify, Protect, Detect, Respond, and Recover) with the Resilience Engineering Framework (Learn, Respond, Monitor and Anticipate) to create a new framework (see Figure 1). This framework supports not just cyber but ultimately IT and mission resilience, as well.



FIGURE 1: Cyber Resilience Framework



Cybersecurity is about reacting. Cyber Resilience is about anticipating. This framework highlights the critical and continual actions required to achieve Cyber Resilience.



Sowing the seeds of Cyber Resilience.

There are six ways federal organizations can plant strong roots for Cyber Resilience.

01

Be brilliant at the basics. That includes routine maintenance tasks, such as patches, updates, and access permissions. Though essential, these activities are wholly insufficient. They are reactions to previous events that reinforce the harsh reality that “good guys” are always behind.

02

Embrace the cloud for security. There are many reasons to migrate federal systems and data to the cloud. Security should be at the top of that list. That’s because the cloud can function as your “shell game.” When you become cloud native, you can take advantage of elastic workloads, multi-zone computing, and multi-cloud strategies that make it exponentially more difficult for adversaries to find and harm you. That, in turn, delivers assurance that your mission will continue to operate.

03

Implement data-centric security. Data-centric security goes far beyond traditional data security tactics. Among the possible techniques: encryption, tokenization, segmentation, throttle access, marking, tagging, strong identity and access management, and automated access decisions. With these techniques, data security is no longer an afterthought; it is embedded into the way you manage and use these critical assets. When you apply these techniques, you make it much harder for an adversary to steal, modify, or destroy data.

04

Demand application security by design. Again, this is about putting security top of mind. Make security integral to every stage of your development process. Adopt DevSecOps practices and use automated scanning and testing to continually identify potential vulnerabilities. Consider applying polymorphic coding techniques to constantly shape-shift your application attack surface—further frustrating and raising the cost to your adversaries.

A background image showing several thin, dark branches of a tree or shrub covered in a thick layer of white snow. The branches are out of focus, creating a soft, wintry atmosphere. The snow is piled up on the branches, and the overall scene is bright and clean.

05

Leverage software-defined networking. If adversaries can't find you, they can't attack you. This approach enables you to constantly shape-shift your network. You can literally change routes mid-session—sending adversaries on the proverbial wild goose chase.

06

Engage in proactive defense. Apply AI and security automation and orchestration tools to detect and act at machine speed. Constantly probe and pressure-test your environment to find vulnerabilities ahead of your adversaries. Fully leverage threat intelligence to better know the adversary and focus on the threats that matter most. These techniques empower you to become the hunter—not the hunted.



Create the right conditions.

In nature, there is a rhythm to growth and renewal. Living creatures take time to fully develop. So does Cyber Resilience.

Federal organizations have built their current infrastructures one system, one data set at a time, and Cyber Resilience will be achieved in the same way. That isn't a ticket to move slowly or indecisively; rather, it's an acknowledgement that this journey won't be completed overnight.

Throughout the process, nurture the right cultural conditions by fostering a mindset of resilience. Work actively to adapt people and processes—bringing together mission, IT, and security for a complete view of what's most valuable and how best to protect it.

In making the journey, take an agile and managed approach. Be open to growth and change as you set mission-driven priorities. Safeguard day-to-day mission continuity to avoid client impact or loss of confidence. Integrate IT Modernization and cyber security investments to achieve the biggest impact—and position yourself for true Cyber Resilience.

Heavy snow and rains will come. Prepare for the worst—and be the tree that bends but doesn't break.

APPENDIX

Measuring progress: 2018 state of Cyber Resilience

How well are federal organizations progressing in the journey to Cyber Resilience? Accenture's 2018 State of Cyber Resilience study sought to address that question by evaluating 33 cybersecurity capabilities across seven domains: Business Exposure, Cyber Response Readiness, Strategic Threat Content, Resilience Readiness, Investment Efficiency, Governance & Leadership, and Extended Ecosystem. We asked respondents to rate their own performance from "1" (no or very limited capability) to "7" (extremely competent).

Here's a look at the top five self-reported strengths and weaknesses. Strengths represent the five capabilities where the highest percentages of respondents rated themselves a "7." Weaknesses are capabilities with the lowest percentages of "extremely competent" ratings.

TOP 5

- #1 Investment Efficiency / Risk Analysis and Budgeting
- #2 Investment Efficiency / Cybersecurity Architecture Approach
- #3 Cyber Response Readiness / Cyber-Incident Escalation Paths
- #4 Strategic Threat Intelligence / Peer Monitoring
- #5 Resilience Readiness / Cyber-Incident Recovery

BOTTOM 5

- #1 Business Exposure / Identification of High-Value Assets & Business Processes
- #2 Resilience Readiness / Design for Protection of Key Assets
- #3 Business Exposure / Physical & Safety Risks
- #4 Investment Efficiency / Cybersecurity Investments for Key Assets
- #5 Extended Ecosystem / Third-Party Cybersecurity Clauses

Top 5 Cybersecurity Capabilities

STRENGTH #1: Investment Efficiency / Risk Analysis and Budgeting

By ranking themselves “extremely competent,” respondents are affirming that their budgets have provisions for protection of major assets and processes. Being “extremely competent” also means their budget design ensures defense and resilience, with security-budget accountability that covers cybersecurity.

STRENGTH #2: Investment Efficiency / Cybersecurity Architecture Approach

These respondents have affirmed that they have defined policies to ensure investment in future enterprise security architecture based on a cybersecurity foundational approach and overall risk structure. They have one team responsible for the design of future enterprise architecture, including cybersecurity and resilience. Each design architecture covers a full business unit, with senior management overseeing architecture design and the design processes being regularly reviewed.

STRENGTH #3: Cyber Response Readiness / Cyber-Incident Escalation Paths

These respondents’ organizations have defined escalation paths based on incident impact. They escalate cyber incidents to the most appropriate management level, with inclusion of local, national, and international agencies. Beyond that, they consider impact vs. time tradeoff and regularly review escalation paths.

STRENGTH #4: Strategic Threat Intelligence / Peer Monitoring

Capabilities in this domain are about anticipating future threats—including using and evaluating peer-monitoring feeds within and outside the security team. With an “extremely competent” ranking, respondents suggest their organizations are using the specific “business” context to enrich reporting in threat feeds. They regularly communicate peer-monitoring to the business and IT organizations, with the overall process continually reviewed and improved.

STRENGTH #5: Resilience Readiness / Cyber-Incident Recovery

Extreme competence in this capability means that an agency has integrated its cybersecurity recovery plan into Business Continuity and Disaster Recovery strategies, with the plan updated based on environmental changes. It also means the agency restores cybersecurity controls after a cyber incident and routinely tests cyber recovery capabilities using pre-defined test cases. There are formal plans for coordinating with internal and external partners.

Bottom 5 Cyber Security Capabilities

WEAKNESS #1: Business Exposure / Identification of High-Value Assets & Business Processes

Very few federal respondents indicated that their organization is identifying key assets and processes and then regularly reviewing cyber impact. Nor do they have policies enforcing key asset and process identification across business units. There's an opportunity to weave cybersecurity impact assessment into every new initiative and to strengthen organization-wide awareness about the importance of key assets and processes.

WEAKNESS #2: Resilience Readiness / Design for Protection of Key Assets

Less than one-fifth of respondents told us that their organization's design principles segregate operational, functional, and corporate risks—all while protecting cyber controls and their highest-value assets. Further, comparatively few organizations are considering their "crown jewels" at both a local and global level or balancing the tradeoff between cost and resilience for key asset protection.

WEAKNESS #3: Business Exposure / Physical & Safety Risks

This finding suggests that federal leaders have an opportunity to better identify key physical and safety risks and regularly review their cyber impact. Policy should also enforce physical and safety risk identification across units with the organization, and all new initiatives should assess potential impact on these risks. Senior management should demonstrate commitment to supporting awareness throughout the organization.

WEAKNESS #4: Investment Efficiency / Cybersecurity Investments for Key Assets

Only about one-fifth of federal respondents indicated that their organizations have identified and shared criteria for defining high-value assets or processes. Extremely competent organizations incorporate protection into their local and global investment process, and senior leadership oversees protection of these key assets and processes. They also continually review and improve performance through dashboards and/or reports.

WEAKNESS #5: Extended Ecosystem / Third-Party Cybersecurity Clauses

Any security program is only as strong as its weakest link—and that includes every part of an organization's supply chain. Only about 20 percent of federal respondents have policies to enforce active defense in provider and partner contracts. They have accountability for contracts, with contracts updated regularly based on new threats. Process review and improvement are ongoing.

These 10 capabilities represent relative strengths and weaknesses and should be interpreted accordingly. Across all 33 capabilities, survey responses from federal leaders suggested significant opportunities for further growth and improvement in Cyber Resilience.

FOLLOW US



@AccentureFed



Accenture Federal Services

[accenture.com/cyber](https://www.accenture.com/cyber)

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, 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.

Copyright © 2018 Accenture.
All rights reserved.

*Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.*