Accenture
HIGH PERFORMANCE SECURITY
REPORT 2016: PUBLIC SERVICE

CONFIDENCE + CAPABILITY:

"REBOOTING" PUBLIC SECTOR CYBERSECURITY

US federal, state and local government agencies are confident in their overall cybersecurity strategies, but do their operational capabilities ensure positive outcomes?

As a target for security threats, the public sector is unique, experiencing more cyber incidents than any other industry.

The United States must step up to this national threat, and the Cybersecurity National Action Plan, which seeks to enhance cybersecurity awareness and protection, protect privacy, maintain national security, and empower Americans to take better control of their digital security,[1] will be core to that mission.

As the velocity and aggressiveness of cyberattacks continue to escalate, it is important for government agencies to adopt new strategies to identify and respond to rapidly evolving security threats.

New Accenture research shows that the majority of government executives are confident their cybersecurity strategies are achieving desired outcomes in three key areas:
- protect organizational information (88 percent),
- protect citizen and customer data (82 percent), and
- protect employee privacy (61 percent).

However, confidence levels begin to drop when it comes to the ability to monitor, identify and measure breaches, with approximately one third expressing satisfaction with their organization's abilities. Similarly, less than 50 percent of the commercial sector is confident in these areas.

And while nearly 70 percent of federal respondents (and around 40 percent state and local respondents) consider cybersecurity a top priority that they have completely embedded in their culture, most also admit that attacks are often unpredictable. For example, almost 90 percent of respondents agree with the statement, *"cyberattacks are a bit of a black box; we don't quite know how or when they will affect our organization."*

TODAY'S OPERATIONAL REALITY

These findings emerged from a survey of 150 federal, state and local government executives in the United States. A customized version of Accenture's global survey of 2,000 executives representing large enterprises, this report seeks to understand how public sector agencies prioritize security, the comprehensiveness of their plans, their organizational resilience in terms of security, and their levels of investment in this area.

Reacting to cyber breaches is an operational necessity for most organizations today; one that's even more critical for government agencies. When a breach occurs, over two-thirds (67 percent) of respondents say their agencies turn to "communication channels to law enforcement" as their most effective response, followed by their own internal cross-functional teams (66 percent) and standard operating procedures (50 percent). While bringing in a third party can be effective, it relies on the abilities of the agency's own security personnel to monitor and identify breaches in the first place, which requires strong cybersecurity capabilities. Many agencies are aware that the tools and technologies they use to safeguard digital assets do not provide the protection they require. In fact, fewer than 15 percent of government respondents say their "established technology and/or start-up technology" is effective when responding to breaches.

FEDERAL AND STATE/LOCAL PERCEPTIONS DON'T ALWAYS ADD UP TO A UNIFIED GOVERNMENT VIEW

The responses from federal agencies at times differ dramatically from state and local participants. Some of the differences clearly result from the often major scale contrasts between federal and state and local agencies, which can have a significant impact on complexity and the levels of resources available to address cybersecurity issues.

67%

67% of federal respondents say their organizations make cybersecurity a top priority that receives support from agency leaders.

In some cases, the differences also appear to reflect the maturity levels of cybersecurity capabilities. For example, nearly 45 percent of state and local respondents express confidence in their organization's ability to monitor for breaches, while far fewer federal survey-takers agree. Part of this difference could reflect the much greater scale of federal digital networks, but another element is likely a greater realization at the federal level that successfully monitoring for breaches can be an extremely difficult undertaking. Unlike a robber who breaks into a bank to steal cash (or digital bitcoins), digital data thieves often take nothing; they simply copy valuable information, leaving the original in place, seemingly undisturbed.

40%

only 40% of state and local peers agree.

Likewise, while 67 percent of federal respondents say their organizations make cybersecurity a top priority that receives support from agency leaders, only 40 percent of state and local peers agree. Another area that exposed significant differences between the federal and state and local responses involved the capabilities agencies say they most need to fill cyber security gaps. For example, roughly two-thirds of state and local respondents list end-point/network security and threat intelligence as most-needed abilities (similar to commercial respondents). In contrast, federal participants rank both 20 points lower, instead putting encryption (55 percent), vulnerability management (53 percent), security monitoring and cyber-threat analytics (both 52 percent) higher.

GOVERNMENT AND COMMERCIAL RESULTS AREN'T ALWAYS EQUAL, EITHER

While in many cases government survey responses align with those given in the commercial survey, some differences emerged. For example, 78 percent of combined federal and state/local agencies list protecting internal information as a top strategy, while only 56 percent of commercial organizations agree. At the same time, both groups express similarly high confidence levels regarding the things they are doing to protect internal and citizen/customer information. Both groups also have similarly low confidence levels as to their abilities to monitor for breaches, with 34 percent of government respondents expressing confidence compared with 37 percent of commercial respondents—likely recognition of the difficulty associated with this task.

78%

78% of commercial organization respondents are confident that its cybersecurity strategy will demonstrate valuable results.

The same proportions of government and commercial respondents (58 percent) identify end-point and network security as their most needed capability. On the other hand, over half of government agencies but only a quarter of businesses mention cyber-threat analytics as a key gap. Significantly more government managers than business executives agree that cyberattacks are a black box and are unsure how or when they will affect the organization: 87 percent government versus 66 percent commercial. And while three-quarters of businesses say their highest-level executives make cybersecurity a top priority and support it financially and culturally, just over half of government agency respondents agree. An even wider gap exists regarding whether the organization is confident that its cybersecurity strategy will demonstrate valuable results: government, 53 percent; commercial, 78 percent.

53%

only 53% of government agency respondents are confident that its cybersecurity strategy will demonstrate valuable results.

By "pressure-testing" their defenses, agencies can quickly determine whether they can withstand a targeted, focused attack.

ACHIEVING AGENCY-WIDE CYBERSECURITY CONFIDENCE

To replicate at the operational level the confidence that agencies have in their cybersecurity strategies, they may need to enhance their overall capabilities. For many, that will necessitate a cybersecurity "reboot;" one that recognizes success will require an end-to-end approach that considers threats across the spectrum of their service offerings and the agency´s ecosystem. They also need to identify and minimize their network exposure, and focus on protecting priority assets. The following steps can help government departments deal effectively with the high-impact cyber threats they face.

THE "REBOOT" CHALLENGE: DEFINE CYBERSECURITY SUCCESS AND "PRESSURE-TEST" CAPABILITIES

Organizations need to answer several critical questions in order to reframe their cybersecurity perceptions:

- Have we identified all priority agency data assets and their locations?
- Can we defend ourselves from a motivated adversary?
- Do we have the tools and techniques to react and respond to a targeted attack?
- Do we know what the adversary is really after?
- How often do we "practice" our plan to improve our responses?
- How do these attacks affect our agency?
- Do we have the right alignment, structure, team members, and other resources to execute our mission?

Agencies need to establish a realistic assessment of their capabilities to protect against high-impact threats. By "pressure-testing" their defenses, agencies can quickly determine whether they can withstand a targeted, focused attack. To that end, they can engage good-guy "white hat" external hackers in a real "sparring match" with their cybersecurity team to quickly determine whether it's ready for primetime.

SPEND WISELY ON INNOVATION

The survey indicates that, given greater security budgets, most federal and state/local agencies would spend the money on the same risks they currently fund--protecting internal and citizen data. However, to stay ahead of adversaries, agencies need to continually innovate. But where should they invest?

One reliable approach looks across seven key cybersecurity domains to identify potential opportunities for future investments in innovation. Currently, only about a quarter to a third of government agencies express confidence in their capabilities regarding any of the seven domains (the commercial survey generated similar results). Given their proven significance from a cybersecurity perspective, agencies should make these areas a priority focus for investment and greater leadership attention. The seven domains are:

- **Agency exposure** assesses cybersecurity incident scenarios to understand those that could materially affect the organization, and identifies key drivers, decision points, and barriers to the development of remediation and transformation strategies.
- **Governance and leadership** requires organizations to focus on cybersecurity accountability, nurture a security-minded culture, measure and report cybersecurity performance, develop attractive cybersecurity incentives for employees and create a clear-cut cybersecurity chain of command.
- **Strategic threat context** drives organizations to explore cybersecurity threats, including an analysis of geo-political risks, peer monitoring, and other areas to align the security program with the agency's overall strategy.
- **Cyber resilience** is the organization's ability to deliver operational excellence in the face of disruptive cyber adversaries. From technology and process foundations to cyber incident recovery performance, the organization seeks to understand the threat landscape, designs key asset protection approaches and uses "design for resilience" techniques to limit a cyberattack's impact.
- **Cyber response readiness** means having a robust response plan, strong cyber incident communications, tested plans for the protection and recovery of key assets, effective cyber incident escalation paths and the ability to ensure solid stakeholder involvement across all agency functions.
- **The extended ecosystem** should be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements, and focus on regulatory compliance.
- **Investment efficiency** strives to drive financial understanding concerning investments across cybersecurity domains and the allocation of funding and resources. It also compares organizational investments against benchmarks, organizational objectives, and cybersecurity trends.

The survey indicates that, given greater security budgets, most federal and state/local agencies would spend the money on the same risks they currently fund protecting internal and citizen data.

MAKE SECURITY EVERYONE'S JOB

Rank-and-file government employees can play a critical role in detecting and potentially preventing cyber-attacks. Nearly all of the federal and state/local survey respondents say that for breaches not detected by the security team, the agency learned about them most frequently from employees. Government employees represent the first line of defense, which is why agencies need to prioritize training and continually refresh cyber talent across the organization.

To build a culture of cybersecurity awareness, agencies should view state-of-the-art cybersecurity as an organizational mindset—one capable of continually evolving and adapting to counter changing threats. To foster this culture and move closer to a state of digital trust, organizations must emphasize an adaptive, evolutionary approach that addresses all aspects of holistic security on an ongoing basis. This approach reflects the belief that while achieving compliance with regulatory standards represents a significant achievement, that alone will not protect an agency's data from adversaries.

LEAD FROM THE TOP

Given recent developments, cybersecurity has a central position on many agency agendas. Even so, security leaders may need to step beyond traditional comfort zones (e.g., compliance audits, cyber technology) and materially engage with agency leadership on a day-to-day basis. Doing so will require them to make the case that the cybersecurity team represents a critical pillar in the battle to protect internal and citizen data.

DEFINE, INVEST, TRAIN AND LEAD

An incomplete cybersecurity strategy can result in catastrophic digital breaches for government agencies. While many organizations express confidence in their cybersecurity strategies, they also suggest that current efforts to monitor, identify and react to cyber breaches are insufficient. To align their high-level expectations more fully with ground-floor realities, agencies may need to reboot their cybersecurity strategies. That means redefining cybersecurity success as more than simply achieving compliance targets, investing in innovations, and prioritizing staff training; all of which require a rock-solid commitment from leaders to champion cybersecurity and dedicate the resources best-in-class performance requires.

To build a culture of cybersecurity awareness, agencies should view state-of-the-art cybersecurity as an organizational mindset—one capable of continually evolving and adapting to counter changing threats.

For more information:

Gus Hunt
Managing Director,
Cybersecurity Practice Lead,
Accenture Federal Services

gus.hunt@accenturefederal.com

Lalit Kumar Ahluwalia
Senior Manager,
North America Security Lead,
Public Sector/Higher Education

lalit.k.ahluwalia@accenture.com

Notes

[1] The White House, Office of the Press Secretary. (2016). Fact Sheet: Cybersecurity National Action Plan [Press release]. Retrieved from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

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.

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 approximately 384,000 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.