How Do Agencies Feel About Their IT Security Posture?

Many federal tech leaders are somewhat confident their agency can fight off cyber threats.

Amanda Ziadeh
Mon, 02/05/2018 - 13:16

Most federal IT leaders aren’t very confident in their agency’s ability to prevent IT security threats, largely because of inadequate budgets and a reliance on legacy systems.

56
percent of respondents said the top IT security concern in the past 12 months is external threats

That’s according to Unisys’ recent Digital Trust Survey. The report includes responses from 200 U.S. federal government tech leaders, half from civil or independent agencies and half from the Defense Department and military branches.

70 percent said budget limitations were a significant or moderate challenge of migrating to an Identity-Based Security Management System

Though 22 percent of respondents are “very confident,” 66 percent are “somewhat confident” in their agency’s ability to prevent IT threats — and DOD respondents are three times as likely as civilian respondents to express a high confidence.

And while 64 percent of government IT leaders view identity management solutions as a very important way to address these growing cybersecurity threats, they still need to address challenges related to budget, staff and infrastructure. In fact, most haven’t even implemented the technology.

Below are additional facts from the report:

- **On Security Threats:** 56 percent of respondents said the top IT security concern in the past 12 months is external threats, followed by mobile device use, vulnerability patching and internet of things.

- **On Solutions:** More than half of respondents said the most used security products at their agencies are smart cards, endpoint security software and configuration management software.

- **On Identity Access Management:** The most cited major benefits of an identity access management system include increasing security, helping agencies meet missions, and complying with mandates.

- **On Identity Access Management Use:** Only 16 percent said those systems
were fully automated and integrated, 20 percent use biometrics to detect identity and 40 percent limit user access rights to the bare minimum needed for that job function.

- **On Challenges Implementing Those Systems:** 70 percent said budget limitations were a significant or moderate challenge, followed by a dearth of skilled staff and a lack of an adequate IT infrastructure able to support these systems.

- **On Security Challenges:** More than a third of respondents said adequate funding, managing the complexity of security and preventing data breaches by outside attackers are significant challenges to IT security.

- **On Security Posture:** In the past 12 months, 34 percent report their agency’s security posture is more secure, 25 percent said their posture is more vulnerable and 41 percent said their posture has not changed.

- **On Cyber Expectations:** 71 percent expect cybersecurity threats to spike this year.

- **On IT Security Outlook:** In terms of the most anticipated change in IT security threats in the next 12 months, 20 percent think it’ll significantly increase (and 37 percent of those respondents think their agency will become more vulnerable), and 51 percent say it’ll moderately increase.

- **On Vulnerability:** The most common reasons as to why federal IT leaders think their agency is more vulnerable is because of the increased sophistication of threats and the increased use of mobile devices.

--- Sign up for our weekly newsletter to receive the latest analysis and insights on emerging federal technologies and IT modernization.

View printer friendly version

Federal Cybersecurity
cyber