avanade

Cybersecurity

Avanade is committed to being responsible in everything we do, from our purpose – to make a genuine human impact – to forward–looking leadership and sustainability. Please use the QR code below to receive your paperless copy of our point of view on cybersecurity in government and public service.

Flip the switch on Cybersecurity

Before investing in new security solutions, make sure you're using all the tools you have.

For many government and public service agencies, cyberattacks seem increasingly threatening and inevitable. Incidents are rising in frequency and severity. The risk of compromising data, losing time to recovery, and damaging trusted relationships is a powerful motivator to do what matters to keep an organization safe.

While there may be powerful motivation to invest in ramping up cybersecurity quickly, most agencies are constrained by a lack of funding and a lack of skilled people to meet the challenge. Even as the U.S. Infrastructure Investment & Jobs Act (IIJA) promises to infuse $1 billion into state and local governments to bolster cybersecurity, people with the skills to deliver on the promise of the grants are scarce and in high demand.

While Chief Information Security Officers (CISOs) make their case for increased budgets and staff – or wait for money or talent to become available – they have an opportunity to look around to make sure that all security tools are being used effectively. Doing what matters in cybersecurity for governments and public service means finding the best approach to maximize existing security assets before investing in new.

The public sector is an easy target

According to the Global Cybersecurity Outlook 2023 Insight Report developed by World Economic Forum and Accenture, "91% of all respondents believe that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years," and 43% of organizational leaders foresee a cyberattack within the next two years will "materially affect their own organization."[1] The public sector is already under siege, as the number of attacks targeting the public sector increased 95% for the last half of 2022 compared to 2021. The biggest targets were China, India, Indonesia and the United States, which, combined, experienced about 40% of total reported incidents.[2]

Agencies often leave security to small teams with limited tools. Many CISOs operate as teams of one. Most find themselves in positions of influence – not control – when it comes to investing in the platforms and solutions and implementing practices and policies. As a result, CISOs know their organizations are not prepared to fend off or recover from a cyberattack.What they may not realize is that they probably have tools they are not using that can add a powerful layer of protection.

The power of the Microsoft platform

Working with government and public service clients has demonstrated to Avanade's teams that agencies are not making the most of what they have on hand. Simply understanding the possibilities and deploying them to protect an organization would enhance security significantly and have a genuine human impact on government employees and the citizens they serve.

The mandate for action

The increasing levels of attack are bringing attention to the issue and identifying gaps that agencies need to close. The U.S. government is investing through IIJA in state and local security initiatives. The EU is creating a certification program for businesses and common rules for itself. And everyone who has a security solution is calling on governments and public service agencies to present their solution as the best option.

What to do

Assess and maximize existing security features. You can avoid buying what you already have (but may not be using), and you may even find obsolete technology and unused licenses that you are still paying for. For some agencies, security optimization will reveal the need for modernization. While requires a bigger investment, there will never be a better time to make security a priority.

Who can do it

The skills shortage in cybersecurity is real and unlikely to be solved soon. Governments and public service agencies can compete with the private sector for skills or collaborate with them. Working with a trusted partner that is committed to maintaining high standards of delivery makes more sense than trying to hire, train and retain specialized skills in house. When looking for a partner, consider these criteria:

- Does your partner have the capability to deliver end-to-end thinking and execution that covers IT, OT and IoT?
- Do the proposed security solutions work with existing systems, especially at the connection points to your larger technology ecosystem?
- What is the partner's approach to training the in-house team?

Governments and public service organizations need to step up the focus and investment on cybersecurity to do what matters for serving and protecting the citizens who rely on them. Doing what matters means responding instead of reacting. A measured response is far more effective than a quick reaction for governments and public service agencies focused on diligently and responsibly using the resources entrusted to them by their citizens and stakeholders.

1. World Economic Forum (weforum.org)
2. Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 (webflow.com)

Scan the QR Code to read our point of view.

Do what matters