avanade

Do what matters

Flip the switch on Cybersecurity

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

Imagine your neighborhood is seeing an uptick in burglaries. Not only are the home incursions becoming more frequent, thieves are becoming bolder about what and how much they take. When your sense of security is threatened, you'll do whatever it takes to keep your family safe.

Before you invest in a top-of-the-line home security system, take a minute to stop and look around. There are probably ways you can make your home safer just by using what you have to its full potential. Are all the windows closed and locked? Are the outside lights working or do you need to replace some lightbulbs? Did you turn off notifications on your video doorbell because they were too frequent – and too frequently nothing to worry about?

Now let's apply that thinking to the public sector. 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.

It's like calling the home security company after deciding to make the investment and learning you're on a long waitlist for installation.

While Chief Information Security Officers (CISOs) make their case for increased budgets and staff – or wait for money or talent to become available – there is 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.

We see potential for governments and public service agencies to make a genuine human impact for their constituents without creating massive disruption to budgets or operations.

What makes the public sector an easy target

In the mid-20th century, renowned crook Willie Sutton allegedly responded to the question, "Why do you rob banks?" with "Because that's where the money is."

If we could ask cybercriminals why they go after governments and public services agencies, we might get several responses that are just as logical:

- "Because that's where people's data are."
- "Because that's where I can create the most disruption or chaos." (Including hacktivism)
- "Because it's easy."

The first two reasons are integral to the function of public service. Agencies need data to serve citizens, patients, travelers. And the ability to live and work in local, national and international arenas depends on continuity of infrastructure that governments provide, coordinate or regulate. Everything is connected in a complex chain, and a chain is only as strong as its weakest link. The European Union is working to strengthen cybersecurity for its institutions as well as the companies that operate within the EU. Details of a set of common rules across all EU institutions, offices, bodies and agencies are being developed by the Council of the EU[1]. And the EU Cybersecurity Act is a certification framework to recognize and encourage private institutions to meet a baseline of protection requirements[2].

The idea that agencies are an easy target is the most frightening and the most solvable. First, the frightening part.

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."[3] 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 just one year to 2021. The biggest targets were China, India, Indonesia and the United States, which, combined, experienced about 40% of total reported incidents[4].

Agencies have not been able to prioritize security, leaving it to small teams with limited tools at their disposal. 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.

Ignoring or downplaying investment in security is common because governments and public service agencies are grappling with a lot of competing forces, including inflation, increased demand for services and citizens' expectations of safe and seamless experiences – both online and in person. And many are still reeling from the effects of the pandemic, which exposed vulnerabilities by pushing organizations into remote work and digital services without a chance to prepare.

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 utilizing that can add a powerful layer of protection.

1. Cybersecurity at the EU institutions, bodies, offices and agencies: Council adopts its position on common rules – Consilium (europa.eu)
2. The EU Cybersecurity Act | Shaping Europe's digital future (europa.eu)
3. World Economic Forum (weforum.org)
4. Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 (webflow.com)

The power of the Microsoft platform

The sheer volume of transactions completed by government agencies each day is mind-boggling, especially when you consider all the interdependencies among agencies, suppliers, employees and citizens. Consider regulatory requirements for financial services or keeping travelers safe within and between borders. Or the challenge of providing health care and social services in collaboration with individual citizens and countless partner agencies.

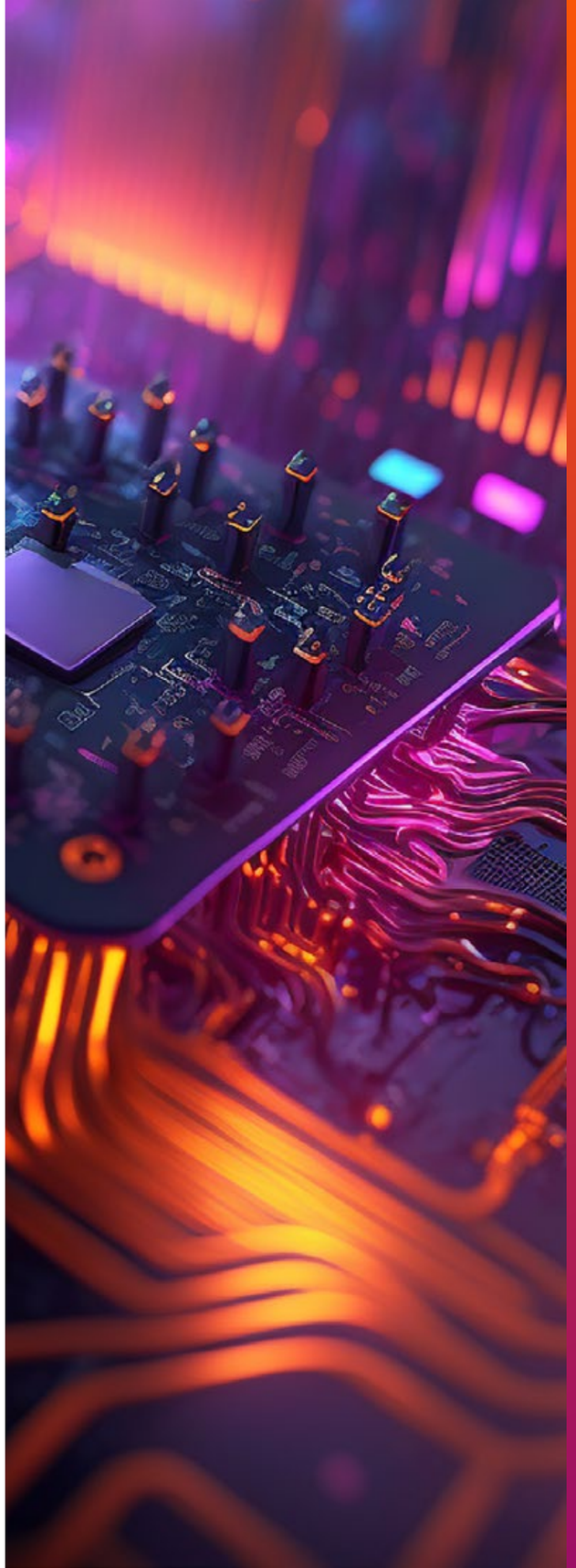
The complexity of operations among agencies requires major processing power and the ability to integrate systems across organizational boundaries. Microsoft has provided the power and the integration capabilities that keep agencies – and economies – running smoothly.

> And, since 2021, has committed **$20 billion** in investment to build cybersecurity into those solutions and platforms.

Working with our government and public service clients has demonstrated to Avanade's teams that agencies are not using the full range of security controls and features that are built into their existing Microsoft systems. They are not doing what matters with 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.

Think about a complex piece of technology, like a digital SLR camera, or even a smartphone. Most users leave the camera on "Auto" mode to take pictures. Or they figure out how to make their phones do what they need them to without exploring the full capabilities of technology. Why? Because we often don't have the time to sit down and figure things out, or we convince ourselves that the technology has more advanced features that we really don't need.

There are several factors at play: CIOs usually have more influence than control as agencies and business lines are always looking to do more with less. And skills are scarce to truly get all aspects of systems and solutions delivering to their potential. The result is that a lot of agencies have not fully benefited from their existing investments in Microsoft, especially when it comes to cybersecurity. In essence, they are leaving money – and cybersecurity options – on the table.



At Avanade, we help public sector clients to get the most out of their Microsoft investments. This can go from building an in-depth understanding of the inherent security controls available and baselining their current deployments to developing and executing a roadmap for secure integration.

We have the largest and deepest range of experience of Microsoft security capabilities available in the market today. We use that Microsoft expertise, combined with our knowledge of the public sector, to help our clients to achieve more with what they already own. We can also implement new capabilities such as Sentinel to help protect their digital assets.

Power to the people – with some built-in protections

To paraphrase U.S. President Abraham Lincoln, cybersecurity should be of the people, by the people, and for the people. No approach can be effective without buy-in from an entire organization – from top to bottom. Revisiting the home security comparison, a high-end security system will only benefit the home, its residents and visitors if everyone is committed to using it and knows how to use it properly.

Going from the top down, the first layer of human impact on cybersecurity lies in the organization's leadership. A commitment to security means giving the CISO budget, control and accountability over all the areas that are vulnerable to cyberattack. This stretches beyond IT to operating technology (OT) and the Internet of Things (IOT). It's time to move away from the model the CISO only gets attention when things go wrong.

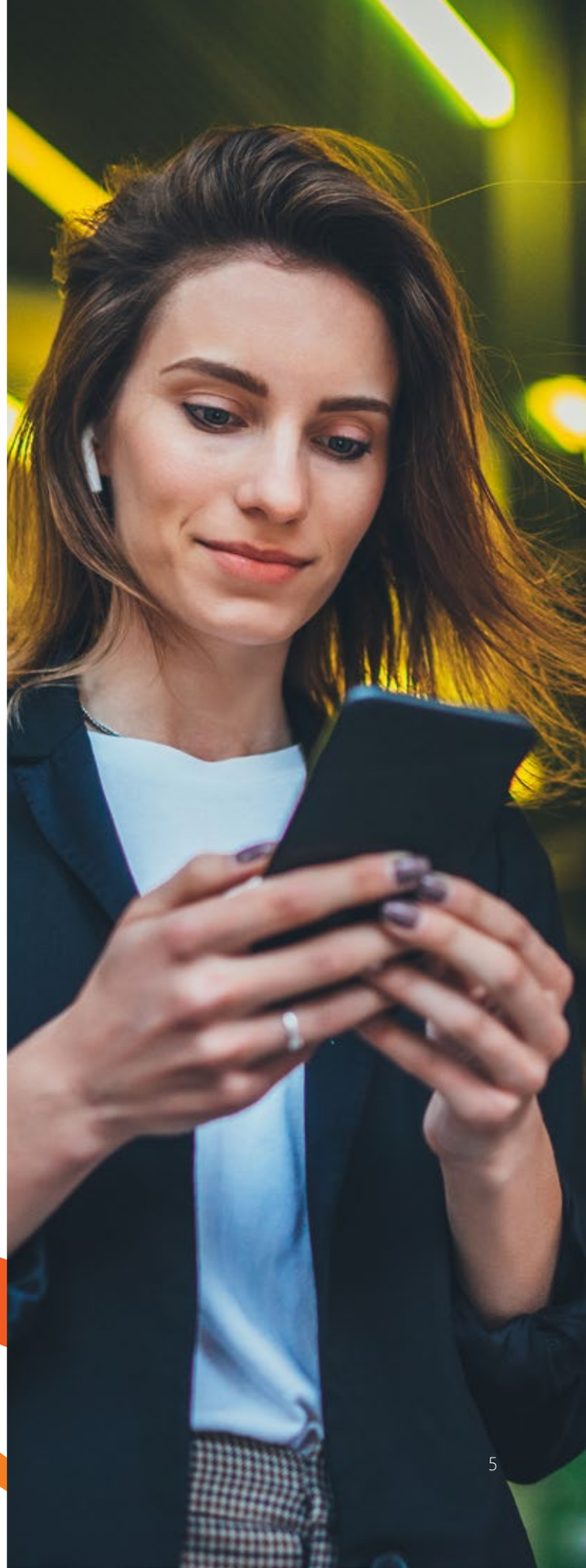
Integrating cybersecurity more fully into an organization's full operations also calls for a governance model. Once people understand what systems and capabilities their organizations have, then they can be collaborative and smart about deciding how to use them. Having buy-in from across the organization will help ensure that policies and practices feel "of the people" and not "at the people."

Ultimately, an organization's cybersecurity effectiveness lies in the hands of users. **According to the WEF 2022 Global Risks Report, 95% of cybersecurity incidents can be traced to human error[5].** Reduce that risk by creating a culture that emphasizes security and providing ongoing training to keep people from becoming complacent. When one human mistake can have an oversized impact,you'll want to sure everyone understands **How to do what matters and why it is so important.**

The paradox of good cybersecurity is that no one notices when everything is going well. Rarely do you hear someone say, "We haven't been hacked in more than two years – congratulations to us." It's when things go wrong that a chorus of voices fills the silence.

The same is largely true of how citizens interact with government. The goal is to be unobtrusive, easy and forgettable, so people can go about their daily lives. This isn't exactly a powerful motivator, but the idea of facing the negative consequences – disrupted services, loss of trust, public outcry – may spark a commitment to action. It pays to remember and ensure that the IT, OT and IoT truly are "for the people."

5. Chapter 3. Digital Dependencies and Cyber Vulnerabilities - Global Risks Report 2022 | World Economic Forum (weforum.org)



The mandate for action

The time is now to meet the opportunities and challenges of cybersecurity. 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.

The threat is real

The pace of cyberattacks, data breaches and ransomware is too fast to track regularly, and even a snapshot is a sobering reminder of the enormity of the issue.

Out of 10 known ransomware attacks in January 2023, as reported by Cyber Management Alliance, seven were public institutions, including SickKids Hospital in Toronto, the Royal Mail of the UK, Costa Rica's Ministry of Public Works and Transport, the Los Angeles Unified School District, and universities in Queensland, Australia and Duisburg-Essen, Germany.

While the report assigned no data breaches to the public sector in January 2023, five of the nine known cyberattacks targeted government and public service agencies, including German administrators and airports, an energy company, and the Ukrainian news service[6].

Being prepared to fend off or at least survive the ongoing onslaught of attempts to do harm means staying ahead of the miscreants. It also requires creating an approach that is strong, scalable and nimble enough to handle what bad actors are doing today and what they will attempt in the future. As part of your armory of defense, getting the most out of what you already own along with extending your capabilities through strategic partners like Avanade can make the difference between being tomorrow's headline and the safety of your operations.

6. Recent Cyber Attacks, Data Breaches & Ransomware Attacks January 2023 (cm-alliance.com)

What to do

Taking the time to assess and maximize existing security features can pay off in a couple of ways. First, you can avoid buying what you already have (but may not be using). Eliminating spending is always a welcome prospect. Beyond this is the opportunity to cut costs. A skilled team looking for security features to activate also find obsolete technology and unused licenses that you may still be paying for. It's the equivalent of a home security system installer unearthing some valuables you had in storage that you forgot about.

For some agencies, security optimization will quickly reveal the need for modernization. While this may require a bigger investment, the time is right to make the case as security is a universal priority.

Who can do it

The skills shortage in cybersecurity is real and unlikely to be solved soon. Microsoft is addressing a projected 3.5 million open cybersecurity jobs in 2025 by conducting a skilling campaign in Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Germany, India, Ireland, Israel, Italy, Japan, Korea, Mexico, New Zealand, Norway, Poland, Romania, South Africa, Sweden, Switzerland, the United Kingdom and the United States. Microsoft is looking at data for each market and developing a skills program in collaboration with local education institutions, nonprofits, governments and businesses.

The lack of resources presents governments and public service agencies with a choice. They 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 through ongoing training makes more sense than trying to hire, train and retain specialized skills in house.

When looking for a partner, consider these criteria:

- **Does your security partner from the private sector have the capability to deliver end-to-end thinking and execution that covers IT, OT and IoT?** Ideally, security is one piece of an overall technology strategy and a well-rounded partner will be able to help identify the big picture and deliver all the detailed work that the strategy requires.
- **Are the proposed security solutions able to work with existing systems, especially at the connection points to your larger technology ecosystem?** Agencies have complex interdependencies with external partners – utility companies, health care systems, tax collectors, financial institutions. There is an art to keeping these connections secure without being cumbersome. Building from within an existing ecosystem like Microsoft provides a good head start.
- **What is the private sector partner's approach to training the in-house team?** Too many IT service providers come in, do their thing and then leave without passing on the knowledge and skills needed to keep a system up and running at its best. It's time to move from staff augmentation to staff enhancement and evolution.

Beyond a doubt, governments and public service organizations need to step up the focus and investment on cybersecurity to maintain their ability to serve and protect the citizens who rely on them. The key to investing in an approach that is sustainable and scalable starts with distinguishing between reacting to a potential threat and responding to one.

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.

Our customers have told us that our ability to partner with them, being truly part of their team, supplementing their knowledge with our global experience has been critical in helping them to stay on top of the ever-changing security risks that they face. We partner with our customers in different ways to ensure they are protected. These arrangements can take the form of everything from short-term targeted skill supplementation and managed services all the way through to large scale complex enterprise transformation. All of it underpinned by our commitment to making a genuine human impact.

avanade

About Avanade

Avanade is the leading provider of innovative digital, cloud and advisory services, industry solutions and design-led experiences across the Microsoft ecosystem. Every day, our 60,000 professionals in 26 countries make a genuine human impact for our clients, their employees and their customers. Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation.
Learn more at www.avanade.com.

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

avanade

Do what matters