Deloitte.

Stepping into the Future of Cyber

Government & Public Services

Deloitte's 2023 Global Future of Cyber Survey reveals that cyber increasingly plays a foundational role in delivering business outcomes. For government and public services (GPS), the quality of those outcomes will depend on how well decision-makers understand today's environment and prepare for what comes next.

What does the future of cyber look like for the industry?

What does the future of cyber look like for the industry? These five highlights provide a glimpse into where government and public services organizations are now—and where they are going.

Modernizing

90%

of GPS respondents said cybersecurity impacts the success of digital transformation implementations from a moderate to large extent

Talent

79%

of GPS respondents cite lack of skilled cybersecurity professionals as a challenge

Governance

78%

of GPS respondents report lack of inadequate governance across organization as a challenge

Investing

58%

of GPS respondents plan to increase their cybersecurity investment in the next year

Planning

75%

of GPS respondents conduct incident response scenario planning at the organizational and/or board level

Becoming cyber-ready

How can government and public services prepare for an evolving cyber landscape? The following five insights and five corresponding actions, based on Deloitte's experience and our survey findings, can provide a starting point for navigating the future of cyber.

Insights to inspire	Actions to consider
1. **Organizations are on a never-ending digital transformation journey.** Modernizing and replacing legacy systems is a constant priority as governments adapt to an increasingly digital world and the expectations of stakeholders—while also seeking new efficiencies and speed. Cloud initiatives and upgrades for operational/industrial control systems are among the top digital priorities of GPS respondents surveyed.	**Embed cyber consistently across the board.** Cyber must not be an afterthought as you deploy new systems and upgrade old ones. Weave cyber tools and practices into your IT and business process landscapes. Make it foundational and ensure that your cyber capabilities can evolve in lockstep with your organization.
2. **The need to find and nurture cyber talent is becoming more critical.** Finding talent is a massive and growing challenge for government and public services. These organizations simply cannot win a traditional talent war, competing against higher-paying industries. Compounding the challenge: persistent workforce turnover and the loss of institutional cyber knowledge, along with evolving cyber needs.	**Address talent needs through an ecosystem approach.** In the near term, outsourcing offers a pressure release valve for talent challenges. But what comes next? What constraints will you face 10 or 20 years from now? Feed the talent pipeline by working across government, higher education, and the private sector to develop programs for the next generation of GPS cyber specialists.
3. **Governance needs more governance.** Among GPS leaders surveyed, governance was the top challenge in managing cyber. Continuous change in rules, regulations, budgets, and leadership can make governance difficult and often chaotic. And talent challenges and digital initiatives just exacerbate the challenge. It is no surprise that, in many cases, cyber incidents may be left to agencies to manage, rather than a central IT group.	**Consolidate and centralize responsibility where you can.** Advocate for a centralized model of cybersecurity governance, where the CISO's office leads the cybersecurity efforts across agencies, offices, and departments—collaborating with other levels of governments and nongovernmental organizations to help strengthen cybersecurity overall.
4. **Funding will shape the future of cyber.** Funding is the engine that drives all government programs—from citizen services to infrastructure to cyber. Traditional government programs continue to take the majority of the spotlight when it comes to funding. At the same time, budgets for cyber can be nebulous or ill-defined. As a result, organizations may not be able to make the cyber investments they need to keep up with a changing threat landscape and government priorities.	**Keep pushing for funding reliability and simplicity.** A more centralized budgeting process can help CISOs know where and how funds are allocated, while reducing duplicative expenditures and providing a constant, dependable source of funding that is immune to changing economic or political cycles. One example: Roughly half of US states have a dedicated budget line item for cyber —which establishes it as a governmental priority and gives CISOs a reliable spending base.
5. **Mission-focused cyber is big and getting bigger.** Before there was cybersecurity, there was national security. The two have steadily become intertwined in recent decades. Today, "mission cyber" is the new mode of cyber for defense and critical infrastructure—requiring an extra layer of cyber vigilance and coordinated capabilities that are focused tightly on defending information networks and assets.	**Make it somebody's mission to lead mission cyber.** Much like a military mission, mission cyber must incorporate command, control, and communications—with a well-defined leadership structure. Those leaders must do more than determine strategy and guide tactics. They must make it their job to continuously listen to what others elsewhere in the organization are experiencing and doing on the cyber front.

To get a broader view of the cyber landscape, explore additional insights from the *Deloitte 2023 Global Future of Cyber Survey*, which asked 1,110 leaders across industries and across the globe to share their views on cyber threats, enterprise activities, and the future.

www.deloitte.com/futureofcyber

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Government & Public Services