Deloitte.

Government & Higher Education 5x5 Cyber Change series:
A five-minute read to inspire new ways of thinking about cybersecurity

Creating the future of trust

As workplaces have become more virtual, there are three mutually reinforcing factors around how organizations can drive trust: Trust in information, identity, and automation. Along with technology innovation in general, these factors will continue to change the cybersecurity landscape. The role and value of trust to an organization will need to be defined to strengthen or re-build trust between the public and peer organizations. How can organizations be future-minded in thinking about cyber to implement the future of trust?

5 *insights you should know*

Digital identity is increasingly difficult. Increased telework and social distancing can create new considerations for proving a trusted digital identity.

Trust isn't just about your network, it includes citizens. Digital trust extends beyond networks into the trust citizens have in the services they receive over those networks.

Trust is also about the workers too. Trust in technology extends to the workforce who must trust the automation and tools they use.

Emerging tech needs trusted data. Emerging technologies such as artificial intelligence rely on the quality of training data for their accuracy, amplifying the need to trust the veracity of an organization's data.

It takes an ecosystem of trust. With the shift to online transactions and interactions, trust between the various systems, people, and data services will be required to maintain confidence from customers.

5 *actions you can take*

1. **Use data inventory**. Knowing what data you have and where it is stored is the first step to having trust and confidence in that data.
2. **Explore Zero Trust.** Executives highlighted Zero Trust networks as the top-ranked priority for transforming security capabilities.
3. **Explore advanced authentication.** Next-level IAM strategies can help improve user experience, both citizen and worker, and overall agency cyber posture.
4. **Build on COVID-19 transformations**. Build on the lessons learned from the shift to remote work during the pandemic to inform future considerations for digital trust.
5. **Communicate early and often.** Inform employees, citizens, and other stakeholders in the steps the agencies are taking to protect identities, transactions, and information.

Connect with us

Tim Li

Principal
Government & Public Services (GPS) Cyber & Strategic Risk Lead
Deloitte & Touche LLP
timli@deloitte.com

Mike Wyatt

Principal
Government & Public Services (GPS) Cyber
Deloitte & Touche LLP
miwyatt@deloitte.com