Deloitte.

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

Leveraging the power of your extended ecosystems

Rarely is data housed in one place. When it comes to citizen and student services, information may start in a federal agency; flow through to states, local and higher education; and then into the hands of citizens. In this digital age, broader information ecosystems have emerged. Establishing trust between various systems, people, and data services is critical to maintaining services and trust. How can you identify your ecosystem and utilize relationships differently?

5 *insights you should know*

Connected whether you like it or not. While traditional architectures could often be isolated from the outside world, current approaches often rely on distributed architectures with many different vendors and partners.

Everyone is at risk. In one survey, nearly all executives indicated that they used third-party vendors in cyber operations, and 14% used them for over half their budget. [1]

Can't go it alone. Surveys of CIOs and CISOs suggest the most organizations need a little bit of help in a lot of places to reach their cybersecurity goals.[2]

New architectures demand new tools. Traditional security tools and approaches do not extend well to ephemeral virtual environments.

It's not just tech, it's talent. Wider digital architectures with more systems and players also increases the knowledge and skills needed to work on those systems.

5 *actions you can take*

1. **Increase access to cutting edge tools.** Connecting with a wide array of partner—service providers, government agencies, academia, private industry—can help keep government at the cutting edge of cyber tools.
2. **Grow your pool of leading talent.** No single organization can be experts in everything, so tapping into an ecosystem can expand access to the right skills.
3. **Scale the sharing of threat information**. Coordinate with ecosystem partners to ensure access to the newest threat indicators and that leading practices are in place.
4. **Cultivate internal relationships.** Cybersecurity needs a seat at the table, whether that be in executive decisions on new investments or operations in the form of DevSecOps.
5. **Implement automated and continuous monitoring.** Consider implementing automated risk techniques to keep up with continuous integration and development models that are much faster than traditional models.

Connect with us

Tim Li

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

Colin Soutar

Managing Director
Government & Public Services (GPS)
Cyber Deloitte & Touche LLP
csoutar@deloitte.com

Sources:
1:. Deloitte, *2019 Future of Cyber Survey*, March 2019.
2. Ibid.