Keeping up with cybersecurity threats across government systems

How agencies continue to evolve to address threats

Dale Posont, a national client executive and cybersecurity expert at CSG Government Solutions, has more than 30 years of IT experience focused on state government system modernization projects. In this Q&A, he discusses flexible and proactive approaches for agencies adapting to an ever-changing cybersecurity threat environment.

Are state government agencies experiencing a significant increase in attempted cybersecurity attacks?

Government agencies are a constant target for bad actors and ransomware attacks due to the large amounts of valuable and sensitive data processed through their systems. As states deploy new technologies — including web-based, modular, or interoperable solutions — the number of system boundaries, coordination touchpoints, and attackable systems have expanded leading to increased attacks.

What advice do you have for agencies looking to establish a strong cybersecurity posture to prevent attacks?

My advice is to first establish a dedicated cybersecurity manager and team responsible for incorporating industry best practices and lessons learned from other states related to threat identification, analysis, and remediation activities and continue to assess their effectiveness. Even when remediation approaches appear to work well as designed, continue to analyze the speed of identification and mitigation to improve efficiencies.

Another key is to build inclusive security governance, a risk management framework, and team to coordinate the incident response approach across all systems, system owners, and vendors in the enterprise. This includes planning and executing a continuous monitoring program to provide visibility into security controls, varying trends surfaced by threat detection utilities, and confirmation of their effectiveness.

What security recommendations do you have for state agencies as they launch new IT projects?

Before launching a new IT project, agencies should assess whether their in-house cybersecurity team has the bandwidth to take on the influx of responsibility, risk, and threats related to the effort. Agencies should consider engaging an independent, experienced planning and project management vendor to support development of a project roadmap, procurement plan, risk management plan, privacy and security assessments, and penetration testing.

During procurement of the system, agencies should also ensure strict cybersecurity requirements are established in the RFP and that the resulting contract includes enforceable, performance-driven service-level agreements, key performance indicators, and metrics that align with the organization's cybersecurity strategy and goals. Agencies should work with their project vendors to periodically revisit metrics and measures to ensure they are continuously improving their posture and the contract terms are being met.

How can states safeguard against vulnerabilities during systems development??

Try to avoid simply reacting to threats as they occur on individual system development projects. That will result in disparate solutions that increase vulnerabilities, downstream costs, and deployment timelines. Implementing an enterprise-wide, proactive approach to security and privacy will streamline solutions that help safeguard an agency's entire enterprise. My top three recommendations to stay a step ahead of threats include:

- **Put cybersecurity at the forefront of planning** for your system enhancement and modernization projects. Engage business, technical, and security stakeholders to ensure cybersecurity is well planned and executed. Make sure security requirements are documented in RFPs and that contracts integrate enterprise security frameworks, guidelines, and standards into the software development life cycle.

- **Develop data management and protection strategies** that include who has access to data, where it is stored and transmitted, and whether vendors have multi-factor authentication and other safety measures in place to safeguard against unwarranted intruders.

- **Prioritize accurate documentation of your systems.** Implement standard change control processes and templates for security documentation with the level of detail required in system security plans, privacy impact assessments, and business continuity and disaster recovery plans.

CSG Government Solutions

CSG is a leading public sector consulting firm focused on helping government agencies modernize critical program enterprises. Founded in 1997, CSG has established itself as a trusted advisor to more than 200 government agencies, providing high-value services, including security assessments that help manage privacy and security risks associated with implementing IT systems. Named one of America's Best Management Consulting Firms five years in a row by Forbes, we deliver for our clients to help achieve their goals. Call or email Dale to discuss how CSG can help with your next system implementation at (815) 546-5677 or dposont@csgdelivers.com. For more information, **visit www.csgdelivers.com**.