Automation Enables Governments to Address Growing Digital Risk

Dan Carayiannis, RSA Archer public sector director, discusses how government organizations can use automation and best practices to manage digital risk.

How is digital transformation magnifying the scope of risk?

Digital transformation introduces new risks as organizations transition from legacy environments to new digital platforms and capabilities. For one thing, organizations often bring in third-party technologies and outside vendors as part of these transformation projects, so their risk footprint broadens. While the benefits of digital transformation may be great, agencies must understand, account for and mitigate the potential new risk factors being introduced into the enterprise. In addition, as governments deploy new technologies and capabilities that give citizens and employees easier and more pervasive access to information and services, they need to put in place stronger control processes around data privacy and security.

How can automation help governments better manage and protect data?

As agencies accelerate their use of digital technologies and collect more data, it's no longer viable for human beings to understand and manage this risk manually given the sheer volume of information. Automation lets governments manage and protect data more efficiently and with greater visibility. We're seeing agencies move aggressively to platforms and technologies where they can automate, assess and continuously monitor security around the data they manage.

Please discuss integrated risk management and the role of data analytics, AI and automation in improving decision-making across IT and business groups.

Improving decision-making processes is a big part of mitigating digital risk. Integrating a risk management framework into an agency's culture strengthens its ability to understand and manage risk. Advanced technologies like AI and machine learning can help agencies quickly diagnose a situation or risk and then adjust as needed. In many cases, their decisions can be more immediate, thoughtful and deliberate because they have more complete information to draw on.

How can governments help their cybersecurity teams adjust to the use of AI, machine learning and other advanced tools?

AI and machine learning can and will offer a wide range of cybersecurity capabilities. Training and expertise development will be huge aspects of leveraging these technologies so cybersecurity teams can react to threats faster and reduce the overall agency risk. As an intermediate step, some government organizations are leveraging third-party contractors with expertise in these areas to work alongside employees with the ultimate goal of performing this work in house. Other organizations want to leverage these new technologies and capabilities through outsourcing. Both approaches let cybersecurity teams take advantage of these new technologies.

What else should governments consider in terms of managing digital risk?

They need to automate, update and maintain their resiliency plans, processes and controls to account for changes brought about by digital transformation. Existing plans may be built around legacy IT and analog technologies and processes. But today these plans need to cover possible risk factors introduced by new technologies and capabilities like third-party cloud services and contractors, for instance, that agencies may have adopted for data storage. Resiliency plans also should be updated frequently as agencies continue to modernize.

Where should agencies start on the road to a more data-driven, automated approach to cybersecurity?

We strongly encourage organizations to adopt a risk management framework, such as the National Institute of Standards and Technology (NIST) cybersecurity framework. A risk management framework helps establish a common vernacular across the enterprise, so government leaders, IT personnel, application users and others talk about and understand risk in a similar way. These frameworks also include processes and procedures to assess, detect and mitigate risk. By leveraging these best practices, organizations can ensure their controls and security measures are followed in a consistent way.

In addition, we recommend leveraging tools such as RSA Archer to support the documentation and automation of compliance, risk assessment and continuous monitoring processes. As organizations continue their digital risk transformation journey, they need a tool that can help them visualize and understand risk. By implementing and standardizing on a risk framework across the agency and having a tool that provides the metrics and analytic elements that come through automation and continuous monitoring, government leaders can make better risk-based decisions.

RSA

Resilient in Times of Disruption

Build a resilient foundation to keep your business running

Learn More