Keeping pace with complexity

The mission rides on the network, so agencies must be ready for the tectonic shifts happening in technology

Robert Carey
Vice President and General Manager,
Global Public Sector Solutions, RSA

THE GOVERNMENT'S MUCH-NEEDED commitment to modernizing and becoming more efficient and effective can add complexity to agency networks. That complexity, in turn, can make facets of the IT infrastructure vulnerable to attack, thus requiring a sound digital risk management strategy. Meanwhile, the threshold for hackers to have a big impact on an organization's network is low, which means more capable threats are on the horizon.

Once agencies understand that success is tied to the uptime of their networks, it becomes easier to address risk management and make appropriate investments in modernization.

Both government and industry need to closely examine the intersection between business processes and networks so they can make decisions that address today's reality while also accounting for the technology "tectonic plate" shifts of the next several years. Advances in cloud, mobile and 5G technology for ubiquitous wireless networking can be expensive to adopt but will have huge benefits.

These advances will also require a cybersecurity review.

Prioritizing mission outcomes and cybersecurity

A key obstacle to IT modernization is the appetite of the organization to invest in becoming more effective and efficient. It's a simple equation: How much am I willing to spend, and what's the business outcome I will derive from that investment?

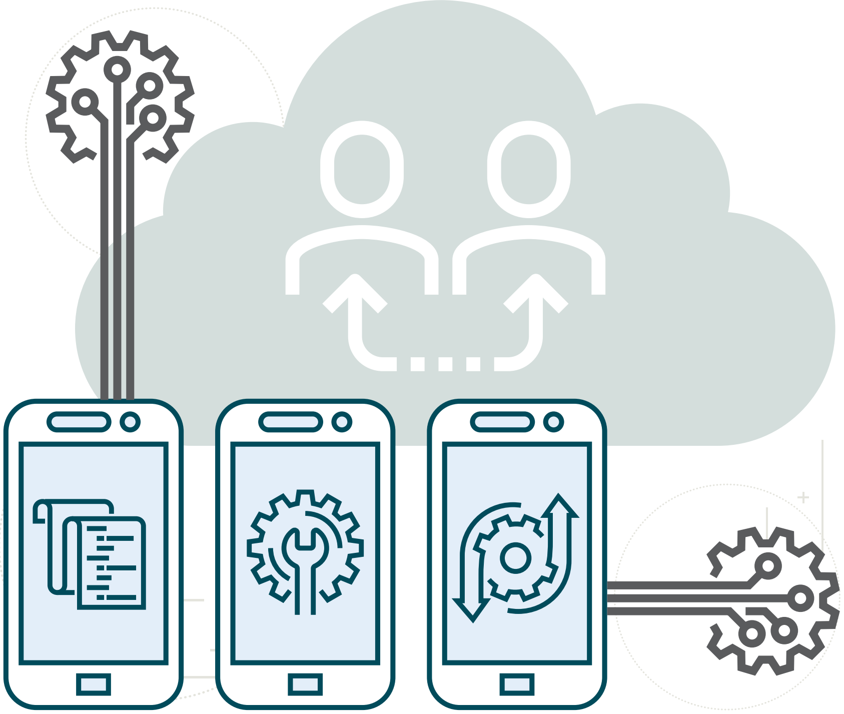
Modernizing legacy systems currently running in government is an expensive proposition. Therefore, agencies must prioritize the mission outcomes they're trying to achieve and the IT that supports those outcomes. Then they can more easily quantify what new technology – for instance, 5G or cloud – can do for them.

In addition, the IT team needs to determine how to invest in the right technologies to ensure the security and resiliency of the network so that it supports the agency's ability to conduct business. And the organization as a whole must invest in cyber hygiene and make identity management and other cybersecurity tools as transparent as possible. For example, the use of phishing exercises can help employees know what to look for and understand the consequences of clicking on a malicious link in an email message.

Building resilient networks

Most organizations use a complicated legacy set of tools to manage network security and perform digital risk management. However, the future requires a simplified, more coherent approach that incorporates automation and allows technology to perform certain activities.

Automating responses to security incidents, for example, is crucial. If an analyst in a security operations center is seeing something, more than likely it has already happened. State-of-the-art tools and appropriate cybersecurity metrics can help



davooda/Shutterstock/FCW Staff

> “Advances in cloud, mobile and 5G technology for ubiquitous wireless networking can be expensive to adopt but **will have huge benefits**.”

the IT team understand whether the network is resilient and performing appropriately. These metrics, if captured in near-real time, help organizations prevent successful attacks and ensure mission success.

Automation informed by artificial intelligence engines can help agencies modernize to operate in an increasingly complex world. AI, along with quantum computing and other evolving technologies, enhances the capabilities for both attackers and defenders. Dashboards support SOC decision agility, which is a key to defense.

The goal is for network defenders to stymie attackers and make them expend energy and resources to succeed. Developing and implementing a digital risk management strategy that links the network to mission success is crucial. Becoming a hardened target means that attackers spend time and resources to attempt to get in. When government networks are modern and resilient, attackers may move on and agencies can focus their energy on conducting their missions. ■

Robert Carey is vice president and general manager of Global Public Sector Solutions at RSA.

Mission-Driven Security
Achieving Successful Cyber Outcomes
RSA delivers Mission-Driven Security so organizations across the Public Sector can take command of their evolving security posture.
Learn more at Carahsoft.com/IIG-IT-Transformation/RSA
RSA