ASSESSING AND MANAGING CYBER RISK

As organizations evolve and their reliance on technology increases, securing the enterprise becomes more complex. ***Robert J. Carey,*** *vice president and general manager of global public sector solutions at RSA, explains how a business-driven approach helps state and local agencies manage risk.*

How have security and risk management become more complex with the rise of mobile, edge, cloud and other innovations?
As the pace of innovation accelerates, government organizations may embrace new technologies faster than they are ready to secure them. The network carries the organization's mission "on its back," so as new technologies are introduced, digital risk management is critical. This means looking at how the technology provides a fundamental underpinning for a component of the business and understanding whether it introduces or reduces risk. Performing digital risk management is an ongoing journey as organizations continue to transform and their networks evolve.

What is a business-driven security approach and how does it help address growing complexity?
Business-driven security means understanding that the technology used to deliver on your mission and your business outcomes — servers, databases, mobile platforms, office productivity software and cloud — is wholly reliant on the network. It also involves identifying which technologies support your most mission-critical business functions and protecting them first. In the Department of Defense, we called it Mission Assurance, which means, can I perform my mission and how does the network support that mission. That analysis is really important because you might have to do something from a security point of view to give yourself the risk mitigation that allows the mission to succeed.

What tools or approaches can help organizations address workforce staffing and skills gaps?
One approach within the cybersecurity domain is to leverage AI, machine learning and quantum computing tools that help lighten the load on people in the security operations center. These blossoming tools can offload certain functions to machines so analysts can focus on higher-priority events. But we're not operating purely at machine speed today. Staffing and skills gaps must still be addressed outside of new technologies. The second part is strengthening the ability to hire, train and retain a workforce. To be competitive, people often look at the compensation only, but it also comes down to the "soft" aspects, such as making work meaningful for people, providing a path to grow and being a fun place to work.

How can organizations more accurately assess their cybersecurity maturity and begin moving toward a stronger defense?
Start by understanding the business or mission outcomes the network supports and taking an inventory of all the technology connecting to the network. Then benchmark your organization against an established framework — NIST and ISO have some — to assess your cybersecurity maturity. The assessment will help your organization develop a maturation path, prioritize where to invest and identify the controls needed to reduce or manage business risk. You must also understand your compliance requirements, but keep in mind that compliance does not equal security. It simply means sufficient controls are in place to comply with a specific regulation. Finally, devise a multiyear plan to move the business forward as new technologies emerge and additional funding becomes available.

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 by watching the RSA Threat Hunting webinar here: **carah.io/RSAWebinar**

RSA®