SPONSORED CONTENT

RISK AND CYBER RESILIENCE: CLOSING SECURITY GAPS

The manner in which agencies integrate technologies into infrastructure creates gaps and security holes that must be addressed.

ROBERT POTTER
VICE PRESIDENT, AMERICAS SALES, SYMANTEC

As cyberthreats become more pervasive and harder to predict, organizations have to be prepared for any outcome. That's why the concept of cyber resilience is so important. Cyber resilience isn't about eliminating risk; but being able to detect and mitigate problems and maintain continuity in a reliable and trusted way to support citizens and the mission.

At its earliest stage, the concept of cyber resilience meant blocking and keeping bad guys out. Over time, we've learned it's the manner in which you integrate technologies into your infrastructure that actually creates gaps and security holes. Cyber resilience now means understanding those gaps.

Agencies can take steps to close those gaps, starting with identifying people with valid access credentials. Even today, with the myriad threats out there, the misuse of a valid identity creates havoc through phishing attacks, ransomware and other approaches.

Organizations must keep track of how they manage identities to ensure credentials grant appropriate access. They must monitor how network traffic is flowing and how devices are communicating with each other. And they must have intelligent data protection in the data center to recognize and protect information.

Organizations must also know how to scale that protection—not just to endpoints, the network and the data center, but also to social media and the cloud as data moves back and forth. Is the multi-tenancy in those environments being protected? Deploy the best solutions to automate some of that capability, and carefully consider how to integrate those pieces. If your solutions don't integrate, the gaps widen.

There are other critical aspects to enhancing cyber resilience as well. One is having the network intelligence to recognize anomalies. Full visibility into network communications is also essential. And most importantly, agencies need to establish policies and deploy technologies for data loss prevention and encryption. When someone infiltrates your network, make sure they can't get away with any valuable data.

Education is another critical factor. There is a lot of information about products, but not enough about solutions or how to integrate products into a platform. Many organizations acquire technology, but don't necessarily have the skills to deploy it correctly.

Vendors must do a better job informing customers how they integrate with other solutions, how they partner, and how they offer combined collaborative solutions. It's incumbent on the vendor to integrate their technologies with other technologies to make the security stack more collaborative, more holistic, and elevate an organization's security posture.

At Symantec, security as a service leverages the intelligence vendors and partners bring to the table. This means access to our consumer division, our enterprise division, our government division, and in the investments we make globally in our global threat intelligence system. Building a strong public/private relationship is important because it fosters a strong sense of community.

Not only is the infrastructure changing, but also the job responsibilities. As organizations build cyber resilience plans, it's important to understand their touch points are going to evolve and expand far beyond where they are today. An agile and adaptable infrastructure will become critical.

***Robert Potter** is Vice President, Americas Sales at Symantec.*

TRACK, PURSUE, AND NEUTRALIZE THREATS.

The longer threats remain undetected, the more damaging they become. Take control of your information and fight threats on your terms. It's time to start advancing security. Learn more at Carahsoft.com/innovation/Symantec-Cyber.

Symantec™

Copyright © 2016 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.