Supply Chain Risk

Technologies, framework can help agencies automate and manage the third party lifecycle

Organizations rely on third parties to provide essential products and services that support their mission; however, they must closely manage these relationships to reduce risk and protect the supply chain.

A supply chain involves anything and everything in the supplying of a product or a service to an end customer, including organizations, people, activities, information and resources.

Government agencies and commercial organizations rely on third parties because they add value, expertise, and extend their capabilities. "They allow us to create, to deploy, to support and to maintain operational capabilities and to provide services to the customers …we support," said Dan Carayiannis, Public Sector director, at RSA Archer.

However, there are challenges and risks associated with leveraging a third party supply chain, including new operational risk considerations that impact physical security, IT security, compliance issues, and introduce the potential for fraud.

"It's imperative to put capabilities, tools and processes in place to mitigate the risk by understanding that they are part of your ongoing ecosystem."

– DAN CARAYIANNIS, PUBLIC SECTOR DIRECTOR, RSA ARCHER

An organization's risk universe can be quite broad, Carayiannis said, and "it only takes one supplier to severely impact my operations and capabilities."

Third parties leverage fourth and fifth tier vendors to provide the products and services that they ultimately provide to the end user. Often agencies don't know everything about the third parties they do business with; however, "they are extending the risk footprint that we have to deal with on an ongoing basis."

Organizations should know what third parties support their operations, which ones pose the most risk, whether all third parties are performing as expected, what products are being sourced from third parties, and whether there are

Article Source: FCW Supply Chain Workshop | January 19, 2021

SPONSORED BY :
RSA

contingency plans in place around third party risks.

"All these challenges relate to organizational resiliency," Carayiannis said. "At the end of the day, organizations really need to understand how they optimize the third parties they are working with, but, at the same time, are reducing the risk to the operations."

About 59 percent of data breaches are due to third parties. For example, the Target breach in 2013 was due to a less secure HVAC network, and more recently the SolarWinds breach exploited the software supply chain.

It's not always IT-related either. The current COVID-19 pandemic has also disrupted supply chains including everything from food and clothing to the distribution of vaccines.

Third parties can impact critical mission and operational capabilities, he said. Around 87 percent of organizations have faced a disruptive incident as a result of third parties in the last two to three years, which is why they "need to really start to think about operational resiliency."

Operational resiliency builds resilience in from the start, focuses on third party external products and services, and understands the impacts they have on the operation and incorporates extensive risk management.

"Organizations really need to understand how they optimize the third parties they are working with, but at the same time are reducing the risk to the operations."

– DAN CARAYIANNIS, PUBLIC SECTOR DIRECTOR, RSA ARCHER

To achieve this, agencies need to first build a "culture of awareness," Carayiannis said, "recognizing that third parties are part of our extended ecosystem." They also should establish a risk management framework that takes into account their contractors, subcontractors, vendors and technologies. The framework "has to embrace and embody all those entities around you that you are leveraging."

Technologies can help them automate many of these processes and are key to managing the third party lifecycle from cradle to grave, he said. "If you're doing that in a highly manual way, that is a painful process, that is a highly reactive process, and I don't think it's going to get it done."

Tools for instance, can help catalog and assess the criticality of third parties and the products and services they deliver, and can help establish the business context around vendor relationships and dependencies on them. They can also help agencies evaluate third party controls, obtain on-demand independent verification of any organization's security practices, and monitor and manage vendor performance.

RSA Archer can provide agencies tools and capabilities that help them evolve and automate their supply chain program. Organizations leverage third parties on an ongoing basis "for just about everything," he said. "It's imperative to put capabilities, tools and processes in place to mitigate the risk by understanding that they are part of your ongoing ecosystem."

RSA

Thank you for downloading this RSA whitepaper! Carahsoft is the public sector distributor for RSA cybersecurity solutions available via GSA, SEWP, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring RSA's solutions, please check out the following resources and information:

For additional resources:
carah.io/RSAResources

For upcoming events:
carah.io/RSAEvents

For additional RSA solutions:
carah.io/RSASolutions

For additional cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
RSA@carahsoft.com
888-936-2246

To purchase, check out the contract vehicles available for procurement:
carah.io/RSAContracts