Commvault

KEY TAKEAWAYS

Expert Insights on Strategic Cyber Resilience: A Cloud-First Approach

Expert insights on achieving cyber resilience through a cloud-first strategy, featuring Sanjay Mirchandani of Commvault and Roland Cloutier of The Business Protection Group.

Executive Summary

This document explores the critical aspects of achieving cyber resilience through a cloud-first strategy, focusing on continuous security, readiness, and recovery. It draws on expert insights from the discussion between Sanjay Mirchandani, CEO of Commvault, and Roland Cloutier, principal at The Business Protection Group and former chief security officer, providing actionable strategies for CIOs and CISOs.

The cloud is a group of different types of environments, including AWS, Azure, and OCI. Even a business's own data centers or managed service providers (MSPs) can be considered a cloud. This expansive definition reflects the modern reality where "the business is the cloud and the cloud is the business." The integration of these diverse environments into a cohesive cloud strategy is pivotal. It empowers CISOs and CIOs by enabling them to manage security, resilience, and recovery across heterogeneous environments effectively and securely. The cloud's capacity to leverage advanced technologies for detection, management, and automation plays a crucial role in maintaining business continuity and resilience. The cloud also helps create a smooth and integrated working environment that supports business activities without interruption. This allows security, readiness, resilience, and recovery capabilities to be continuously implemented across different platforms. This strategic approach not only protects but also empowers businesses, making the cloud an invaluable asset in the digital age.

The following are key takeaways from a discussion between cyber resilience experts Sanjay Mirchandani, CEO of Commvault, and Roland Cloutier, principal at The Business Protection Group and former chief security officer.

> Security should be a quality of the product, not an afterthought."
>
> **Roland Cloutier**
> The Business Protection Group

CONTINUOUS SECURITY

Understanding the Digital Ecosystem

In today's interconnected world, understanding the digital ecosystem is paramount. Sanjay Mirchandani stresses the importance of recognizing the flow of data across various platforms and services. "Data doesn't just sit in one place; it moves across different environments, from on-premises to the cloud," he notes. This fluidity necessitates a comprehensive approach to security that transcends traditional perimeters.

Integrating Security in Development

Roland Cloutier advocates for embedding security into the development process from the outset. "Security should be a quality of the product, not an afterthought," he says. This involves integrating security measures at every stage of the product lifecycle, from design and development to deployment and maintenance. By doing so, organizations can ensure that their products are secure by design, reducing the risk of vulnerabilities.

Asset Management in the Cloud

Effective asset management is crucial in the cloud. Sanjay highlights the use of discovery tools to identify and manage cloud assets. "You can't protect what you don't know you have," he warns. Keeping track of assets and using tools to find them can help organizations maintain a complete view of their cloud environments. This will make sure that all resources are in the right place and protected.

CONTINUOUS READINESS

Building Muscle Memory

Achieving continuous readiness requires more than just having a plan – it necessitates regular practice. Roland emphasizes the importance of building "muscle memory" through frequent training and simulations. "The more you practice, the more instinctive your response becomes," he explains. Regular security drills and exercises can help organizations fine-tune their response strategies and ensure that everyone knows their role in the event of an incident.

Pre-mortem Simulations

Pre-mortem simulations involve envisioning potential security incidents before they occur. Sanjay advocates for this approach, stating, "By imagining the worst-case scenarios, you can better prepare for them." These simulations can help organizations identify gaps in their security posture and implement proactive measures to mitigate risks.

Clarity of Roles and Responsibilities

Clearly defined roles and responsibilities are essential for effective incident response. Roland stresses the importance of ensuring that everyone in the organization understands their duties. "When an incident occurs, there's no time for confusion," he says. Establishing clear lines of communication and responsibility can help organizations respond swiftly and efficiently to security threats.

CONTINUOUS RECOVERY

Preparation and Planning

Preparation and planning are the cornerstones of continuous recovery. Sanjay emphasizes the need for detailed recovery playbooks and scripts tailored to various incident types, noting that "Having a plan in place ensures that you can act quickly and decisively when an incident occurs." These plans should be regularly reviewed and updated to reflect changes in the organization's environment and threat landscape.

Leveraging Technology for Rapid Response

Technology plays a critical role in enabling rapid response to security incidents. Roland highlights the use of advanced technologies for monitoring and responding to threats. "Automation and AI can significantly reduce response times and minimize the impact of incidents," he explains. Investing in these technologies can help organizations detect and mitigate threats more effectively, ensuring business continuity.

Post-incident Learning

Every incident presents an opportunity for learning and improvement. Sanjay advocates for a continuous improvement cycle through post-incident reviews: "After each incident, it's important to analyze what went well and what could be improved." These reviews can help organizations refine their response strategies and enhance their overall resilience.

A CLOUD-FIRST APPROACH TO CYBER RESILIENCE EMPOWERS CONTINUOUS BUSINESS

When adopting a cloud-first approach to cyber resilience, the key is to focus on the three core pillars: security, readiness, and recovery. Commvault has built a platform and an ecosystem of partners and services designed to deliver across each core pillar and enable continuous business. It starts with securing your data with technology like Threatwise™, testing your ability to recover in a clean cloud-based environment with Cleanroom™ Recovery, and then fully recovering and restoring your apps and workloads to the moment before disruption – across any cloud, with true portability —, viah Cloud Rewind. It's time to take control and integrate these strategies into their organizational fabric to not only protect but also empower your business in a cloud-first world.

To learn more about adopting a cloud-first approach to cyber resilience, visit **commvault.com.**