Network and Security Integration Tops IT Team Retooling Goals

Line-of-business objectives and modernization efforts drive IT leaders to recalibrate how to integrate networks and security and upskill teams.

Business imperatives are expanding expectations of how IT can support and secure line-of-business (LOB) initiatives outside of traditional security perimeters. That's causing a rethinking of roles and skills that IT teams must have to improve the security of network and business applications.

Over the past several years, the traditional concept of a security perimeter eroded as cloud and edge computing redefined the nature of distributed computing. The network has expanded far beyond the corporate headquarters and branch offices that were previously the main focus for IT security. The erosion quickened over the past two years as COVID-19 disrupted business operations and spurred a dramatic expansion of remote and hybrid work.

Integration with partners in lines of business and modernizing tools and technology are the overriding concerns for 2022.

Today the network edge can be in an employee's home running on a consumer-grade PC that may be accessed by various family members who lack security awareness and are relatively more susceptible to website malware and phishing attacks.

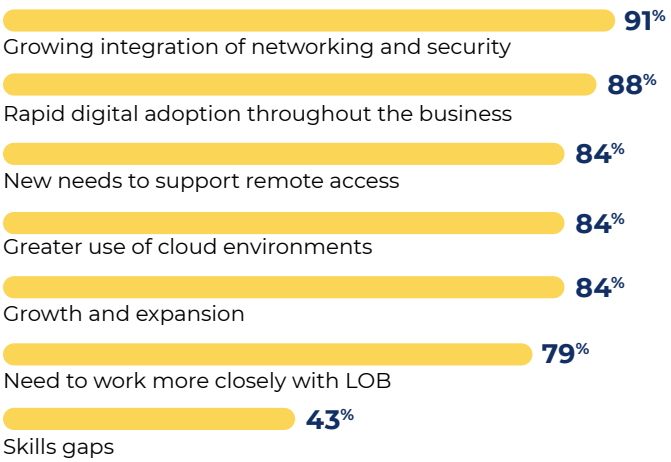
Many businesses are in a migration stage, often in uncertain or undefined territory between legacy networks and cloud-first network strategies. Instead of dealing with the hub-and-spoke nature of legacy networks, IT security must now account for multiple site-to-site and site-to-cloud interactions, especially as lines of business lobby for new initiatives and services aimed at transforming business and providing customers with new services.

IT security is on edge

A recent IDG and Comcast Business survey illustrates that integration of IT with LOB business partners is the leading issue causing IT leaders to rethink the role of their teams in supporting business initiatives.

The growing integration of networks and security barely tops rapid digital adoption throughout the business as the leading driver causing IT leaders to reevaluate the nature of their organizations. But several overlapping factors contribute to this strategic shift, including a new need to support remote access, growing use of cloud environments, and business growth and expansion.

FIGURE 1: **Factors driving rethinking for IT organizations**



Upskilling IT to meet new challenges

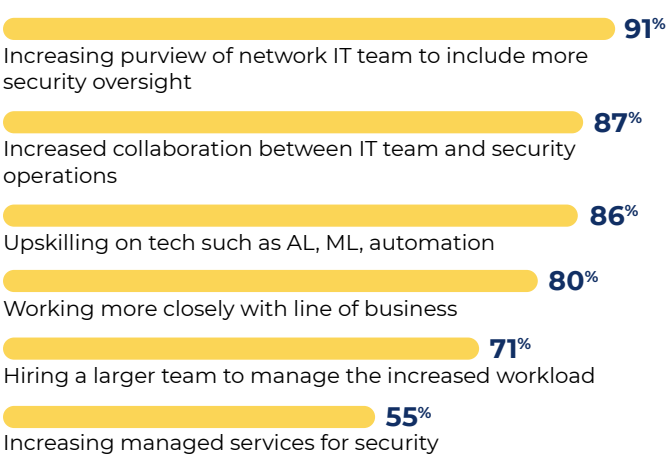
Network and security teams in many companies often work in separate silos. As a result, many organizations are struggling to reconcile highly skilled networking teams that have sparse security expertise and security teams with little insight into network architecture and operations.

That's changing. Surveyed IT leaders said that network teams will be given more leeway in security oversight. They also intend to encourage greater cooperation between IT teams and security operations.

Although many organizations have often relied on managed services providers (MSPs) to bolster infrastructure capabilities and fill skills gaps in recent years, IT leaders are increasingly focusing on the need to improve and realign the abilities of their IT teams.

They will continue to call upon MSPs to provide crucial security and networking services, but the survey indicates that IT leaders are now more highly focused on how to build up internal technologies and the skills needed to employ them.

FIGURE 2: **What IT teams are doing to improve security**



This likely reflects the growing complexity of networks and the need for more highly skilled IT members to oversee MSP services and integrate them further into the enterprise network architecture.

The survey may also indicate a growing awareness of the human factor in improving IT operations. Improving skills of existing teams and modernizing tools and technologies for doing the job are tied as the top strategies in recalibrating IT.

Those surveyed also indicated that they are focused on incentives, retention, and hiring. But they seem relatively unconcerned about attrition, even though the "great resignation" wave sweeping U.S. businesses is almost certain to further exacerbate IT talent shortages, especially given that the survey respondents indicated they are looking to upskill their teams with artificial intelligence, machine learning, and automation — talent that is difficult to hire and retain.

Revamping the IT toolbox

Today companies face a "volatile, competitive, and opportunity-laden" landscape, according to IDC. In response, digital technologies are driving future priorities for IT teams. The interplay of technology and the "human factor" is critical as IT teams strive to meet the ambitious digital transformation goals they're tasked with.

Traditional virtual private network (VPN) remote access solutions may not be enough to support the new demands of an enterprise that spans cloud, edge, and remote work. As IT teams look to invest in new security-conscious tools and technologies, they're bombarded by multiple solutions, ranging from zero trust to cloud access security brokers.

How much they build up internal capabilities versus increasing their reliance on MSPs remains to be seen, but clearly, integrated network security is becoming an essential pillar of IT strategy moving forward. IT leaders can't afford to stand still in pursuing new business initiatives, even as many struggle to accommodate a dramatic increase in the numbers of remote workers who are further stretching the capabilities of security perimeters.

IT leaders have long labored under the perception that security is too often an afterthought, from software development to systems architecture. The survey illustrates that the growing importance and rapid evolution of networks beyond traditional perimeters are driving them to rethink their teams and recalibrate how best to apply their resources for greater integration of networks and security.

IT executives must bring network and security teams together to tackle the challenge of protecting their business while meeting demands for easy but secure availability of information that will drive business unit decision-making.

Learn more about how enterprises are transforming their cybersecurity models.