www.pipelinepub.com
Volume 17, Issue 2

Why Cybersecurity Is Key to Business Resiliency

By: Kerry Singleton

Soon after the World Health Organization (WHO) declared Covid-19 a pandemic, consumers and businesses realized that digital is the key to the future. Today people shop online, pay via mobile devices and—because they work remotely—access many apps that enable them to collaborate, innovate, and remain productive.

According to a recent study, global Internet disruptions saw an unprecedented, dramatic rise in March, coinciding with pandemic-related shelter-in-place orders. These remained elevated through the first half of 2020 compared to pre-pandemic levels. Obviously, this impacted the user experience of customers and employees—not just from a network and infrastructure perspective but also from a security perspective.

A new Cisco-commissioned survey of 3,196 IT decision-makers across small, medium, and large organizations in 21 markets, for example, revealed that 61 percent of organizations globally experienced a jump of 25 percent or more in cyber threats or alerts since the start of the pandemic. This was experienced by 55 percent of small businesses, 70 percent of medium organizations, and 60 percent of large enterprises.

More than six months in, as we strive for normalcy and aim to return to work, it is clearer than ever before that we need to transform our organizations into resilient enterprises and ensure that cybersecurity underpins all our efforts. To be honest, my interactions with customers and the survey Cisco conducted both suggest that investment in cybersecurity is set to rise, making it a critical part of the concerted, enterprise-wide effort to become resilient.

Resilience, however, doesn't come easily. From experience, here's a blueprint (illustrated in Figure 1) that emphasizes the principles and building blocks of the approach we are using at Cisco to help customers morph into the resilient enterprises they aspire to be. The resilient enterprise is designed to be future-ready.

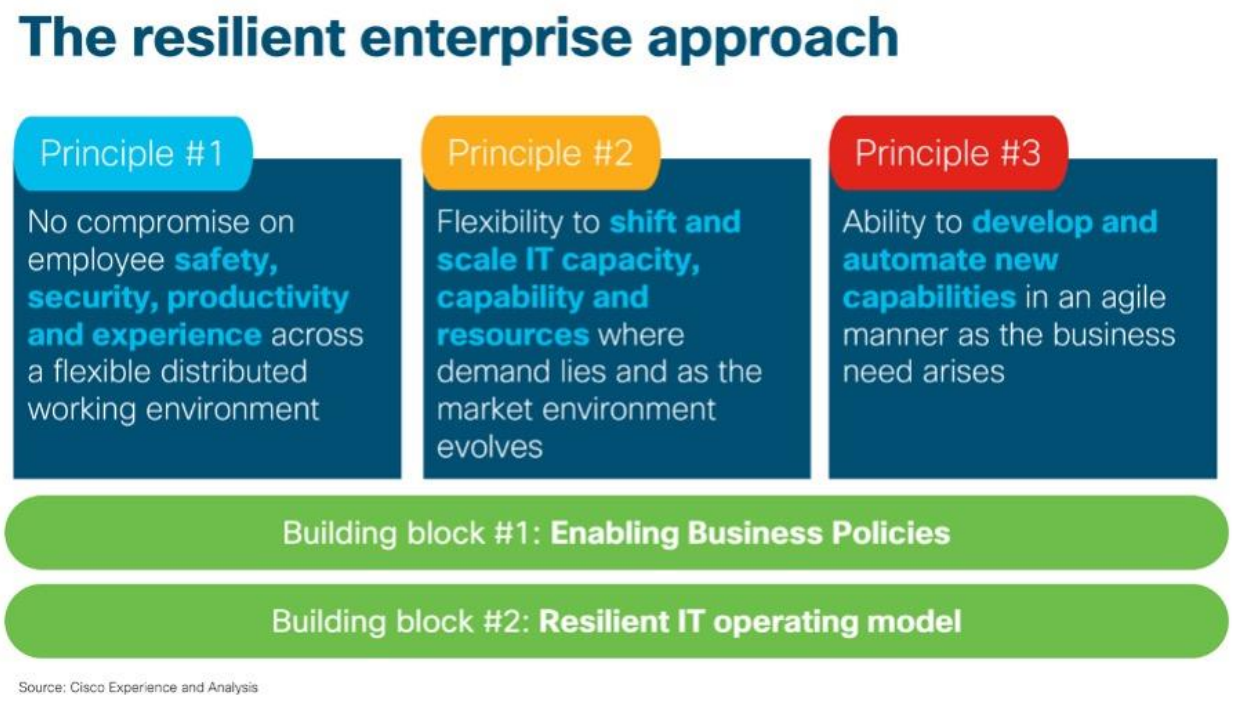

Figure 1: The Future-Ready Blueprint

The emphasis in the first principle is on ensuring that employees have the best experience regardless of where they choose to work (in the office, at a café, or at home); what device they use, personal or corporate; and which network they pick to log into the organization's network, apps and services.

From an implementation perspective, this means leveraging a variety of intelligent tools, such as digital collaboration solutions that bridge the gap between virtual and physical collaborations to health and safety solutions that make offices safer despite the pandemic.

The second principle addresses the need to support customers and employees as demand for digital services and solutions rise, along with a need to transact digitally.

Tactically speaking, for any organization that has been neglecting to move as much of its workloads to the cloud as possible, now is the time to change that. Moving to the cloud provides the flexibility, agility, and the scalability that today's organizations looking to become resilient need. Of course, that does mean having to reexamine an organization's cybersecurity posture as well, to ensure that businesses are protecting their workloads in the cloud. With our recent survey indicating that organizations are looking to increase their future investments in cybersecurity as a result of Covid-19, this is a good time for businesses to ensure that their investments are allocated accordingly as they move to the cloud.

The third and final principle highlights the need for resilient organizations to develop and automate new capabilities. This is important to ensure that businesses have the flexibility built in to adapt to the needs of the future hybrid work environment, which will continue to emerge and evolve. Doing so can help businesses ensure that they have a smooth, secure and seamless user experience no matter where their employees are working from.

To adopt these three principles on the journey to resiliency, enterprises need to consider two key building blocks. First, they need to revisit their business policies to enable executives as well as IT teams to make the decisions that can really facilitate the shift to the modern enterprise structure they're aspiring toward. Next, organizations need to upgrade their IT operating model to ensure that capabilities such as scalability and automation are acquired to serve as catalysts to resiliency.

Our blueprint has been tested rigorously over the past few months. Looking holistically, it is easy to see why most organizations seeking to thrive in the new normal and prepare for the systemic shock seem to find it resonant. It helps them focus their IT and digitalization efforts on immediate priorities while keeping them climbing the digital maturity curve that has been adjusted for the market's response to the pandemic.

All-around cybersecurity is foundational

Cisco has always had a strong emphasis on cybersecurity. It has been baked into products we've created from the beginning. In this accelerated digital era, however, securing a client's network to thrive in the new normal requires planning and foresight.

For example, organizations now need to find ways to validate incoming network traffic and provide strong user authentication using tools and technologies that offer a seamless experience while also amplifying security layers when required. The key is to strike a fine balance, because a strong cybersecurity posture will fail if the experience lacks simplicity.

Organizations also need to find ways to secure traffic regardless of the medium and device used. During the sudden need to work from home, this capability has proven critical, especially when staff had to use personal, unmanaged devices or connect their corporate devices to the office network via their home Wi-Fi connection.

In the coming months, as we aim to restore normalcy to our offices, ensuring that the right device and right user have access to the right apps, data, and services at all times is going to be critical to productivity, security, and the user experience. From an IT operations standpoint, this means deploying suitable policies, governance, and auditing systems. More importantly, security, networking and collaboration can no longer be seen in silos; they must work hand in hand. Alongside these functions, companies must put in place additional enforcement protocols and enhanced cybersecurity policies. Solid employee education programs around cybersecurity are also critical to building a healthy security culture.

Given the various cybersecurity elements involved in transforming into a resilient enterprise, businesses tend to value partners who have the right experience and flexibility to scale with them.

At the end of the day, whether organizations are looking to optimize the various segments of their architecture or starting from a reactive position and looking to quickly deploy, scale, and be agile in this new normal, they need to seek the support of established partners with solutions that work together.

After all, deploying a flexible, multi-domain architecture using a zero-trust approach and covering the workplace, workloads, and the workforce is critical to those looking to preserve business continuity and build resilience. There's no better way to future-proof.