IDC ANALYST CONNECTION

Sponsored by: Aryaka

Digital transformation is a key strategy for navigating the complex business challenges imposed by economic uncertainties.

Embracing Business Transformation During Economic Uncertainty

September 2022

Questions posed by: Aryaka

Answers by: Christopher Rodriguez, Research Director, Security and Trust

Q. Rising interest rates and global economic uncertainty are throwing new challenges at CIOs and IT leaders. What considerations are bubbling to the top as they build plans for the future?

A. Growing uncertainty about the world economy is looming over business plans. According to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3* (April 2022), the top 3 concerns for business leaders in 2022 are inflation, supply chain disruptions, and geopolitical tensions. Businesses are adjusting their strategies accordingly, and many IT organizations are being asked to do more with less. For example, businesses that expect inflation to have the greatest impact on pricing for infrastructure costs are adapting their spending as follows:

- 28% are looking to delay projects to stay within budget.
- 13% are shifting from capital expenditure models to as-a-service consumption models.

However, 43% are increasing budgets to maintain plans (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3*, April 2022, n = 300). This was the top choice overall, ahead of delayed plans or cheaper alternatives, demonstrating that business leaders recognize the value of leveraging technology to adapt to challenging business conditions.

Overall, this strategy follows an ongoing trend of businesses leaning into digital transformation to drive innovation and overcome limitations. But real-world challenges such as lack of skilled personnel, rising energy and fuel costs, and protracted delivery times are forcing IT organizations to work smarter and more efficiently. Replacing wasteful legacy systems with more efficient, scalable, and flexible technologies is another key factor for future success.

Q. In light of the economic climate, how will themes like convergence, SASE, and the integration of traditionally siloed network and security functions play a role in enterprise road maps over the next five years?

A. The security industry goes through steady cycles of expansion and convergence as new technologies introduce new vulnerabilities and threat vectors that confound existing security architecture. However, this "whack a mole" approach has led to a patchwork of security point products and data silos. The network security market has been primed for further convergence and consolidation as IT buyers face a deluge of security tools, including intrusion prevention, firewalls, secure web gateways, cloud access security brokers, sandboxing, browser isolation, and data leakage prevention. This sprawling security toolset not only is too much to manage and too much to learn but also, ultimately, represents too many expenses.

As a result, consolidation has a business value proposition that is based on tangible, clear benefits: fewer vendors to manage, potential for bundled discounting, and fewer systems to deploy, train on, and maintain. However, convergence offers benefits beyond deeper discounting. According to IDC's February 2021 *Future of Trust Survey* (n = 507), 42% of businesses aimed to modernize their cybersecurity infrastructure in 2021 to improve organizational trust too. A further 38% of respondents said they planned to limit the number of infrastructure and security vendors to improve trust posture.

When asked "what are your organization's greatest challenges to establishing organizational trust," respondents listed the following answers as top challenges:

- Fragmented IT and security infrastructure (26%)
- Extended vendor ecosystems (20%)
- Infrastructure silos (17%)
- Legacy IT architecture (15%)

Ultimately, converged security solutions make business sense but also provide improved security outcomes.

Q. Combined with rapidly evolving threats, there continues to be a shortage of talent and security expertise, especially in network and security disciplines. How do, or should, managed services and as-a-service solutions play a role in enterprise planning?

A. IDC research confirms that business leaders are concerned about hiring challenges. This type of concern is not new in the security industry as multiple industry sources have documented a growing talent gap over the years. Business leaders have taken note as well as "lack of personnel" (28%) and "lack of in-house talent" (26%) were noted as key factors considered when choosing a security services provider (IDC's *Global Outsourced Cybersecurity Services Survey,* December 2021, n = 517). Outsourcing strategies, such as managed services, are gaining popularity as a force multiplier for embattled security staff. As a result, the percentage of companies that are "mostly outsourcing" infrastructure security will grow from 22% to 28% in the coming years.

Similarly, shifting from "capex" models to as-a-service consumption models is another popular option to combat rising IT costs in 2022. These as-a-service models require no investments in hardware, eliminate related costs such as installation or maintenance, and are considered easier to deploy, with flexible licensing that is based on utilization, user count, or other factors that allow the investments to grow as the company grows. According to IDC research, 13% of organizations are already planning to pivot to SaaS models in direct response to rising inflation and infrastructure costs.

In the security realm, "mostly cloud, hosted, and SaaS security" was cited as the most popular approach to IT security (37% of organizations), according to IDC's February 2021 *Future of Trust Survey* (n = 468). Security as a service is the future — only 16% of organizations expect their IT infrastructure security to be mostly or entirely on premises.

Q. Remote work was suddenly thrust upon a lot of enterprises during the pandemic. What "quick fix" solutions are IT teams now revisiting as the remote and hybrid workforce becomes more permanent?

A. While IDC tracked the digital transformation trend prior to 2020, the pandemic certainly did accelerate the process. When asked to describe their approach toward digital-first strategies, 26% of organizations indicated that they had already adopted a digital-first strategy, which helped them navigate pandemic-era challenges (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2021, n = 858).

However, the top response (34%) was "the pandemic forced us to quickly shift to a digital-first strategy." In March 2020, the sudden migration to work-from-home models was the first and top priority. Many organizations focused on extending existing infrastructure. The process was full of challenges, and many lessons were learned, including the limitations of legacy networking and security approaches, such as VPNs. Overall, these pandemic-related disruptions helped highlight the need for a digital-first strategy; as of 2021, 24% of organizations had started to execute on their strategies.

Furthermore, 45% cited "remote and hybrid work models will be an embedded part of accepted work practices" as the single most likely innovation to endure. Strategies are being adapted accordingly: 41% of organizations are planning to "improve network bandwidth and security for remote and in-office workers" to improve collaboration and communication. This involves security modernization, including adoption of emerging security frameworks. ZTNA is an example of a new security solution that is better suited to the needs of modern networks and business practices. However, IT organizations also require performance and value, as indicated by growing interest in SSE and SASE.

Q. With users anywhere and applications everywhere, how have application performance and the customer/employee experience reshaped how IT teams are building for the future?

A. Performance has long been recognized as a key competitive factor for drawing in customers with engaging, delightful experiences. Unfortunately, the experience of internal users has traditionally received less consideration. The need for convenience and efficiency has driven a "democratization of IT" trend among workers. This loss of centralized IT control

over data, applications, and usage has become untenable. The effort to regain control of the IT environment necessarily must account for performance and user experience.

Since 2020, business leaders have recognized the importance of supporting remote/hybrid workers with optimal network and application user experiences. When asked "which work practices and technology advanced emerging from the pandemic are the most likely to endure," 36% of respondents cited "employee experience as a driver of business growth and innovation will remain a top priority" (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2021, n = 858).

An obvious but often overlooked truism is evident: Workers require secure but uninhibited access to stay productive. However, the mainstream acceptance of this sentiment represents a seeming shift in perception compared with even a decade ago. Ubiquitous access improves productivity. Performant security also prevents workarounds and other risky behavior. As a result, 39% of businesses are planning investments in tooling to assess network performance problems and 37% of businesses are investing in network infrastructure (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3*, April 2022, n = 828). Overall, the pandemic era proved that people, whether workers or customers, require access, anywhere, anytime, and on any device, that is seamless and secure.

About the Analyst

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure.

MESSAGE FROM THE SPONSOR

About Aryaka

Applications are now anywhere. Users are everywhere. And threats are evolving faster than ever. The question is no longer if the silos of network and security converge to solve these challenges, but when and how. For every enterprise, the answer is unique. Legacy hardware, outdated architectures, contracts with carriers and data centers, and even the skillset of existing teams place each enterprise on its own path on this journey to convergence. It requires a new paradigm, one that not only meets enterprises where they are on this evolution, but also flexible enough to adapt to the inevitability of change. To learn more about how Aryaka is solving this challenge for global enterprises, visit https://www.aryaka.com/sase/.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com