Q: What is resilience and how it is related to business continuity?

A: Simply put, "resilience" means the ability to withstand an adverse situation and return to normal. In business terms, it is a process to ensure that the business can sustain an adverse situation and be able to continue operations with minimal disruption. Another meaning can be the "ability to recover quickly from a difficult situation."[1]

When the COVID-19 pandemic emerged in 2020, we heard the words "immunity" and "hygiene" repeatedly. Because COVID-19 was a new virus, as scientist raced to find ways to mitigate the spread of the virus, hygiene helped keep the virus at bay and scientists endeavored to understand what might create immunity to the virus. Understanding both of these concepts helped humans worldwide become somewhat resilient in the face of a global crisis.

> "As emerging technologies become more complex, building resilient systems becomes more challenging, but being prepared helps organizations overcome the adverse impacts of risk."

Due to a high dependence on IT, for organizations to be resilient, they must be prepared—that is, organizations must adopt good cyberhygiene and build immunity against IT-related risk. In other words, a resilient organization must have a robust risk culture and risk management practices.

Resilience and business continuity go together. When risk materializes, it affects the business adversely and may cause interruptions to business as usual. Risk cannot be eliminated, however, risk can be assessed and organizations can be prepared in case risk materializes. Building resilience follows several steps:

1. Selecting and implementing appropriate risk response options is essential. A risk owner may select one or more risk response options to reduce the likelihood or the impact (or both) of risk scenarios. The risk monitoring process facilitates early detection of materializing risk, which, in turn, helps minimize the interruption of business operations.
2. When risk materializes, it can interrupt operations, however, there are typically some critical business processes that cannot be interrupted. In these cases, organizations may choose fault-tolerant systems or implement high-availability solutions by investing in redundant infrastructure. Since these options require additional investments, they are subject to cost-benefit analysis. Such systems help resist smaller interruptions such as technical fault in devices/servers and high volume of transactions.
3. When impact due to risk is very high or disastrous, business continuity plans need to be invoked. However, these plans must be developed in advance and cannot be prepared on the fly. For example, if the primary data center suffers damage in a disaster and no alternate processing facility is available nor a backup of data and applications, what will happen to business?

SUNIL BAKSHI | CISA, CRISC, CISM, CGEIT, CDPSE, AMIIB, MCA

Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

As emerging technologies become more complex, building resilient systems becomes more challenging, but being prepared helps organizations overcome the adverse impacts of risk. Consider these practices for building resilient infrastructures:

- Use service providers such as cloud. Maintain diversity in service providers or alternate operational infrastructure so that in case one option fails, another will be operational. This prevents a complete blackout of operations in case one service provider or one set of infrastructure experiences disruptions.
- Embed resilience in applications by considering emerging technologies such as microservices and containers. Developers should build scalable applications and determine resilience requirements while designing applications based on the interactions between components. Should a service or component fail, there may be an interruption, but not a complete outage, as would be experienced with a single embedded application performing all functions.
- Continuously monitor performance. This is a good way to identify capacity- and performance-related issues before they lead to outages. Enterprises should define key risk indicators (KRIs) and service levels for performance so that early warnings can be detected by performance monitoring.
- Define and implement real-time monitoring and traffic-routing policies. This helps minimize risk associated with latency and possible downtime due to fluctuations in traffic.
- Start with less critical functions for building resilience. This approach helps organizations learn what issues can be avoided while building resilience for core applications. Downtime for core business applications can be costly.
- Conduct cost-benefit analyses. Enterprises should select the approach that maximizes benefit realization. Applications and services do not need to be recovered simultaneously.

Endnotes

[1] Hurley, K.; "What Is Resilience? Your Guide to Facing Life's Challenges, Adversities, and Crises," *Everyday Health*, 11 December 2020, *https://www.everydayhealth.com/wellness/resilience/*