Contemporary Approaches to Business Continuity

Author: David Papuashvili

December, 2025

There has been considerable interest in business continuity management in recent times. Increased concern has been reinforced by events such as the coronavirus (COVID-19) epidemic, extreme weather events, cyber-attacks, civil emergencies and other operational risk events (both internal and external). Business continuity planning is how an organization prepares for future incidents that may jeopardize its existence. One example from the last few years is associated with the global epidemic caused by the coronavirus SARS-CoV-2. Organizations in various sectors of the economy ranging from hotels and restaurants to financial institutions struggled to cope with the impacts of the new coronavirus. This became apparent when restaurants were either forced to close due to a lack of customers, or when financial institutions were unable to procure critical equipment such as laptops for their employees for remote work.

Based on what has been mentioned above, it has become fairly clear that considerable attention needs to be paid to the development of an effective business continuity plan. For one, the business continuity plan must be practical and easily understood by staff and others who are involved in the execution of the plan (Hopkin, 2016). The BCP needs to be tested, maintained and practiced in order to be effective. Additionally, all employees of the organization need to be familiar with the intended operation of the plan and training will need to be provided. A very important aspect to consider is the development of relevant risk scenarios that take into account the risks that an organization may face. This includes the identification of specific risk events both from historical experience, as well as potential future events that may have a significant impact on the operations of the organization. Last, but not least, there should be a lessons learned process, where the organization learns from the outcomes of its business continuity tests.

Contemporary business continuity management (BCM) needs to focus on an enterprise-wide approach to business continuity. This should include, first and foremost, the employees of the organization. Furthermore, a proactive, tech-driven, and holistic resilience approach to business continuity must move beyond just IT recovery to integrate all relevant processes from a business perspective. If the requirements of the business are not met, it is highly unlikely that the IT recovery process alone will meet the operational and recovery objectives of the organization.

The rapid emergence of artificial intelligence has also brought about interesting opportunities for the integration of artificial intelligence and machine learning within the context of business continuity. For example, artificial intelligence may potentially be used for threat detection which can enable real-time risk analysis. In addition, artificial intelligence can also be used for automating business continuity plan updates.

Continuous, consistent testing of the business continuity plan and associated processes should also form an inseparable component of business continuity management. This can be achieved by testing the recovery of critical processes within the organization, including from alternate locations such as secondary data centers, or through exercises like tabletop simulations, or crisis simulation exercises (CSEs). The key is to have a living, integrated business continuity strategy with strong communication and flexible plans that meet the changing requirements of the organization and operational environment.

It also needs to be noted that if a business continuity process is to be effective, a comprehensive business impact analysis (BIA) needs to be carried out within the organization. The business impact analysis forms the first step of the business continuity process, where the aim is to gain a thorough understanding of the organization and its interactions, both internal and external. It is important to understand the critical functions within the organization and identify key resources.

The Role of the Business Impact Analysis (BIA)

The BIA will identify the critical nature of each business function by assessment of the impact of interruption to that activity. This information will be required in order to identify appropriate continuity strategies for each function. The BIA is similar to the risk assessment that is undertaken as part of the overall risk management process. A critical difference is that the emphasis of a BIA is the identification of the relative importance and criticality of each function, rather than identifying the events that could undermine that particular function.

Business impact analysis has three main functions. These include identifying mission-critical activities and the required recovery time in the event of disruption, establishing the impact potential and the resource requirements for recovery within the agreed timescale, and determining whether the likely impact is within the risk appetite of the organization which forms the basis for the business continuity strategy.

This identification process should determine the timeframe within which the critical functions of the organization must be resumed after the occurrence of a disruptive event. The business requirements for the recovery of each critical function must be established during the resource requirements phase. The technical requirements for the recovery of the critical functions that have been identified also need to be established.

Business Continuity and Cyber Resilience

Another contemporary aspect of business continuity is the concept of cyber resilience, which has become a significant topic of discussion and even regulation. Various legal acts and global guidelines have emerged recently specifically dealing with cyber resilience. These include the European Union's Digital Operational Resilience Act as well as the European Union's Cyber Resilience Oversight Expectations for Financial Market Infrastructures, among others. Regulations in various countries and geographic regions increasingly demand integrated approaches, recognizing that resilience against cyber threats is key to business continuity and compliance.

Business continuity management and cyber resilience are closely linked. While business continuity management deals with ensuring continuous operations during a disruptive event, cyber resilience is largely concerned with protecting digital assets, forming a holistic strategy where cybersecurity measures (such as backups, multi-factor authentication and encryption) become core components of the BCM plan, allowing for a swift return to normal operations after cyberattacks and preventing minor incidents from becoming large-scale operational failures. Cyber resilience focuses on proactive digital defense, while BCM provides the framework to keep the business running, ultimately achieving true organizational resilience.

Overall, cybersecurity and cyber resilience can be viewed as one of the main pillars of contemporary business continuity management. For example, cyber risk events such as ransomware or distributed denial-of service (DDoS) attacks can pose major disruption sources to organizations. As a result, effective cybersecurity should not be viewed separately from business continuity. Cyber resilience is a vital part of business continuity management, which details how to prevent, detect, and respond to digital attacks.

In addition, both business continuity management and cyber resilience have the shared goal of operational continuity. Both processes aim to achieve and maintain essential functions during crises or large-scale operational events, with cyber resilience defending and strengthening the digital infrastructure that business continuity management relies on to deliver vital organizational services.

There is also the notion of integrated planning which links business continuity and cyber resilience. Effective business continuity management incorporates specific cyber incident response plans (IRPs), data recovery strategies (secure backups), and supply chain security, that moves beyond traditional IT recovery to address digital risks. Cyber Resilience is usually proactive and often emphases prevention, threat modeling and testing, while business continuity can be viewed as being more of a reactive or corrective control, but both need to

work together since a strong defense-in-depth approach that incorporates cyber resilience minimizes the need for extensive recovery from the perspective of business continuity management.

In essence, cyber resilience protects the "what" (systems, data) from digital harm. Business continuity ensures the "how" (processes, functions) keeps working during and after that harm. Together, these two components build organizational resilience, which is the ability to anticipate, withstand, adapt to, and recover from disruptions.

Adaptability for Modern Work

One of the other important aspects of contemporary business continuity management includes hybrid/remote readiness. This has become especially apparent since the coronavirus global epidemic that began in late 2019. Building secure remote access, hardware provisioning, and off-site communication into business continuity plans has become a necessity for many organizations across different sectors of the economy. The need to be able to provide decentralized operations that includes planning for distributed workforces and critical functions outside traditional offices is a significant consideration that may need to be incorporated into existing business continuity plans, if it has not been included already.

Supply Chain Management and Business Continuity

Similar to cyber resilience, business continuity and supply chain risk management (SCRM) are also closely linked. This is largely due to the increased use of outsourcing as a critical component of organizations operations. There are many risks that may arise from the supply chain that can have direct implications both to the organization and its business continuity.

Supply chain risk management focuses on identifying and mitigating threats *across the entire supply chain* (suppliers, logistics, customers) while business continuity planning deals with how the *organization* maintains essential functions, using SCRM insights to build overall resilience against risks such as cyberattacks, natural and man-made disasters, or supplier failure, ultimately protecting revenue and reputation. Supply chain risk management should typically involvee proactive risk assessment, developing contingency plans (like alternative suppliers), enhancing visibility, and encouraging strong supplier collaboration for rapid response.

Conclusion

Business continuity management is a holistic process. Modern organizations should take into account the fact that involving all relevant people, processes and systems is essential for contemporary business continuity. This includes the aspect of both business impact

analysis and risk assessment. Without sufficient thought and analysis as to what constitutes a critical business process, it will be challenging to develop an effective business continuity plan. In addition, risk scenarios should incorporate realistic, plausible, but also extreme risk events against which a business continuity test should be tested.

References:

1. Hopkin, P. (2018). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. London: Kogan Page Publishers.
2. Alexiou, S. (May 1, 2022). Is Business Continuity Management Still Relevant? ISACA Journal. 2022. Volume 3. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/is-business-continuity-management-still-relevant
3. Link between Business Continuity and Cybersecurity. (n.d.). Retrieved from https://pecb.com/en/article/link-between-business-continuity-and-cybersecurity
4. Cyber Resilience Oversight Expectations for Financial Market Infrastructures. (December, 2018). European Central Bank. Retrieved from https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf