SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

What is New (and What Isn't) in Business Continuity Planning Pt.2

July 2, 2019

Kevin Alvero and Wade Cassels

In the first half of this article, we established that well done business continuity (BC) planning already considers that The Big One could hit at any time, thus organizations do not need to continuously run to the drawing

board as threats rise and fall. However, in Part 2 of this article, we look at some newer approaches to BC planning that could help organizations maximize the value they receive from their BC planning efforts.

Reconsideration of Roles

According to the Disaster Recovery Institute (DRI), the actual scope of work of a BC or resilience professional hasn't really changed. Organizations still must have high-quality response and damage limitation plans formulated by skilled planners. The change in the resilience profession, however, is moving away from a technical specialization and into mainstream business risk management. DRI reports that consolidation of resilience disciplines has increased over the past year. The main result of this is that fewer organizations have independent business continuity departments, with BC professionals being incorporated into existing risk management or information security divisions.

This movement toward integration plays to the strength of BC professionals, who are accustomed to understanding the roles of people broadly across the organization. According to DRI, however, they may find senior management to be overemphasizing compliance compared to effectiveness when it comes to BC planning. It is easier, for example, to designate responsibility and demonstrate compliance in a traditional departmental structure than a highly integrated one.

In a survey of resiliency professionals conducted by DRI, 30 percent of them believe that senior management doesn't understand their resilience role, and over 20 percent do not believe they get adequate support from senior management. A significant concern among those surveyed is that many C-Level executives have no direct experience managing a major disruptive event. Most senior managers, BC practitioners believe, understand the importance of crisis communications with the media, but they don't have crisis management skills beyond that. There is concern within the profession that despite having risk and continuity programs in place, inappropriate decisions made during a crisis could put the entire enterprise at risk. With this concern in mind, and with natural disaster and IT-related threats on the rise, one potential implication is that crisis management background could increasingly become a required skillet among senior management.

Less Segregation Between Disaster Types

Another way in which traditional approaches to BC planning are evolving is in the way organizations regard IT-related disasters as opposed to natural disasters. To be sure, there is still a line of delineation between the two. DRI reports that in many organizations, key risks such as data breaches and cyberattacks are still largely outside the realm of BC practitioners and treated as security issues. At the same time, many organizations tend to underestimate the impact of an IT-related disaster as compared to a natural disaster that involves harm to "physical" resources.

According to a *Harvard Business Review* article by Prashanth Gangu, a partner in the insurance and digital practices at Oliver Wyman, "Many companies are exposed to intelligent device risks that could harm both their own operations as well as their customers. Yet few have formally quantified the size of their revenue at risk and potential liability. Nor have they set up safety and security protocols for potential Black Swan

AI events." Nevertheless, as reliance on technology continues to increase along with threats to that technology, some organizations are coming around the reality that IT-related disasters can threaten the very existence of the organization just as much as a storm, fire, or earthquake.

In fact, Gangu believes that the risks posed by intelligent devices will soon surpass the magnitude of those associated with natural disasters. "Tens of billions of connected sensors are being embedded in everything ranging from industrial robots and safety systems to self-driving cars and refrigerators," he writes. "At the same time, the capabilities of artificial intelligence (AI) algorithms are evolving rapidly. Our growing reliance on so many intelligent, connected devices is opening up the possibility of global-scale shutdowns."

The good news, Gangu believes, is that organizations can follow the template they have used for extreme weather disasters by beginning to establish international protocols and standards to govern AI not just internally, but also working with other companies, insurers, and policymakers. Just as sound recovery planning for a natural disaster involves coordination with local emergency services, insurers, and agencies such as the Red Cross and FEMA (in the US), plans for maintaining operations through an IT-related disaster such as a cyberattack should include coordination with law enforcement, agencies (in the US) such as the Department of Defense and FBI, insurers and, where possible, threat information sharing with other companies. If companies do not adopt this approach, Gangu believes, no company will be able to recover on its own from an IT disaster due to the growing interconnectivity of AI-enabled devices.

Early Detection

The traditional approach to risk assessment is to assess risks in terms of likelihood and impact. However, according to an MIT case study[i] some organizations are finding success in looking at the added dimension of lead time. Lead time, essentially, is the amount of warning time during which a company can prepare for the disruption and mitigate its effects. As the author of the case study, Yossi Sheffi, explained in an article for *Harvard Business Review*, some disruptions involve long-term trends that are widely discussed in the media or are prescheduled events, while others occur after a short warning of a few days and others occur without warning. For example, a hurricane about to make landfall has a likelihood of 100 percent, but so does a regulatory requirement that is set to take effect twelve months from now. Though these two likelihoods are both 100 percent, they are not really equal because of the amount of time (i.e. lead time) the organization has to prepare.

Sheffi identifies nine data sources that leading companies use to improve their ability to detect potential disruptions early:

1. Monitoring the weather
2. Tracking the news
3. Using data from sensors
4. Monitoring the supply base
5. Visiting suppliers

6. Being on the alert for deception
7. Developing traceability capabilities
8. Monitoring social media
9. Tracking regulatory developments

Sheffi observed that companies armed with this data are taking four key types of actions to improve their abilities to both detect and respond to disruptions:

1. Mapping the supply chain to determine the locations of their suppliers to assess supplier risks
2. Assessing global events to identify potential disruptions that could affect production or revenues
3. Creating supply chain control towers with technology, people, and processes that capture and use supply chain data to enable better short- and long-term decision making
4. Improving response time through data and analysis.

"Detection," Sheffi writes, "depends on creating visibility into the supply chain and understanding how the global moving parts connect to each other and impact each other. At its heart, detection is the conversion of the relevant unknowns into salient knowns in a timely fashion."

Conclusion

The fundamentals of sound BC planning have not changed, but the world of risks swirling around them is constantly changing as threats rise, fall, and evolve. Organizations that feel compelled to respond to predictions of mega-disasters do not need to reinvent the wheel, but trends such as BC integration, disaster approaches to IT threats, and early detection offer ways to enhance the company's chance for success and survival in the event of The Big One.

This article originally ran in *Today's Cybersecurity Leader*, a monthly cybersecurity-focused eNewsletter for security end users, brought to you by *Security* Magazine. Subscribe here.

Recent Articles By Kevin Alvero

What is New (and What Isn't) in Business Continuity Planning

Kevin Alvero, CISA, CFE, is senior vice president, Internal Audit, Compliance, and Governance at Nielsen.

Wade Cassels, CIA, CISA, CFE, CRMA, is a senior IT auditor at Nielsen.