Business Resiliency: Making Risk and Recovery a Major Component of Business Strategy

Introduction

Business resiliency may be defined as all the measures that a company can take to make sure the business runs smoothly after a disaster or other disruptive event. Within a large enterprise, this can include both the crisis management and the business continuity functions. Business resiliency focuses primarily on maintaining the integrity of critical business operations at all of a company's sites and throughout its supply chain. But other considerations often find a place under the business resiliency "umbrella", including safeguarding employees and protecting the company's market, stakeholders, and reputation from harm.

Every manager faces the prospect of an operations breakdown. That is the risk of doing business in an uncertain world. But business resiliency implies more than successfully coping with disasters and disruptions when they occur. Managers need to give their employees the knowledge, means, and confidence to overcome, and even take advantage of, the potential risks that pervade the business environment. A successful business resiliency program involves anticipating and preparing for the major disruptive threat exposures that any company faces, while taking a risk-adjusted, capital-allocation-based approach to managing risks.

Managers planning for business resiliency must take into account how the various components of the company operate and communicate with each other, and employ a common methodology that measures and evaluates threats as accurately as possible. In large organizations, business resiliency professionals should be able to make good business cases to justify their activities to top management.

Managing risk effectively also entails informing employees about where and how potential disruptions originate, and teaching them how to respond. And it involves putting mechanisms in place to keep the lines of communication open inside and outside the organization during a potentially disruptive occurrence.

Business interruptions are inevitable. A company that can respond decisively and positively to misfortune is strategically positioned to survive, prosper, and gain an advantage over its less-prepared competition. With foresight and proper planning, organizations can develop a level of resilience that allows them to withstand any emergency that could put their people and business in jeopardy.

Surveying the Risk Spectrum

Businesses function on a daily basis despite a host of risks that they take more or less in stride. And managers know that business opportunities that initially appear promising may not be, when all eventualities are considered. Some risks are unavoidable, while others may be assumed intentionally as part of a prudent decision-making process. Often it is necessary to balance potential risks by assessing the alternatives, allowing risk takers to make informed choices based on sound metrics and risk-adjusted criteria. As a consequence, these risk takers are better able to allocate scarce resources to minimize risk and maximize shareholder value.

Every business should have a thorough understanding of the major uncertainties it faces. In general, the threats to a company's business can be divided into external and internal risks. Internal risks may be further divided into three subcategories: strategic, operational, and financial risks.

- **External risks** include events such as economic downturns, pandemics, natural and man-made catastrophes, acts of war and terrorism, political turmoil, and regulatory concerns.
- **Internal strategic risks** involve threats to the company's business model, product or service portfolio, brands, reputation, and standing in the marketplace.
- **Internal operational risks** are problems that can affect productivity, profit margin, the supply chain, and the physical plant, as well as employee relations and morale.
- **Internal financial risks** have to do with cash flow, equity, stock price, investments, mergers and acquisitions, foreign exchange, interest rates, and other fiscal matters.

Managers need to find ways to mitigate, transfer, prevent, or rationally assume all these types of risks. However, every risk should be addressed with a view toward mitigating the "fear factor" that can tend to make employees overly cautious and interfere with business growth and flexibility.

"You don't want to put your company at a business disadvantage by always saying 'no' to risk," says Gino Zucca, senior manager of Cisco's Business Resiliency Group. "The answer should always be 'yes', with qualifiers. The goal, after all, is to make the enterprise stronger and more agile, not throttle it down. You don't put brakes on a race car to make it slower. Brakes ultimately enable the driver to go faster."

Incorporating Risk Assessment

Risk assessment is the practice of predicting threats and determining their potential impact. It is an essential part of any business resiliency practice.

"We work with business groups across all the global business processes and functions to educate them on how to think about the risk of a major business interruption, and to build business resiliency into every level of their operations," Zucca says. "This requires a holistic view that includes physical assets like buildings and equipment and extends all the way to strategic assets such as the corporate brand. If we can get every decision maker to consider risks using a common methodology or framework, we've succeeded. Because then the risk management process has been 'operationalized' among all the employees. Instead of having just a few risk managers in the company, we end up having 50,000, which provides greater adaptability and resiliency during a disruptive event, and during business as usual."

Risk mitigation and prevention in a business resiliency context is different from the way an insurance company approaches risk. Insurance providers are in the business of assessing and taking on risk, but policy coverage must fit within a well-defined risk profile. The business resiliency process, on the other hand, involves not only assessing risks, but also identifying alternatives that incur less risk, decrease costs, or add productivity back into the process, while still accomplishing business objectives. In fact, a solid business resiliency program may decrease the need for business interruption insurance. But it is up to the risk owners within the company to make decisions based on accurate criteria.

Such decisions are rarely simple. "It's about trade-offs," points out Edward Erickson, senior manager of Cisco's supply chain risk management group. "The risk associated with business resiliency is multidimensional, so it's important to look at all the attributes. Any time we engage a new partner who is important to our business, we conduct an assessment that takes into account financial, technological, geographic, and political risks. We also determine site-specific risks to buildings and equipment. For example, one location may introduce a higher geopolitical risk, but present fewer natural-hazard risks. We try to get out in front of possible problems by making sound business resiliency decisions at the outset of our relationships."

Erickson notes that it is not just a matter of balancing risk against business advantage—for example, speeding up the supply chain at the expense of having to operate in a turbulent economic or political environment. "One of the best things a company can do to ensure continuity and reduce supply chain risk is to become a more effective, flexible, and adaptable manufacturer," Erickson says. "That not only allows you to avoid a lot of risk, it also lets you recover quickly from any adverse situation that does occur. A fast and adaptable supply chain in itself can reduce recovery time, helping to mitigate any risky links in the chain."

In any organization, there are people who move toward actions they perceive as potentially positive. And there are people who move away from actions that are potentially negative. Many employees possess both qualities and may exhibit either one, depending on the situation. Business resiliency programs can help people weigh the pros and cons of any situation that could have a significant impact on the part of the business where they are engaged.

Furthermore, a solid enterprise risk management approach can help balance risk among the business groups across an entire organization. Depending on the many variables involved, one business group may be willing to accept more uncertainty, thereby helping to equalize the burden on all the groups. And globalizing or internationalizing a firm's assets can diversify risks in the same way a diversified investment portfolio helps protect an investor's assets.

"The financial industry is a wonderful model for understanding what we do," says Erickson. "Good portfolio management means you diversify your investments and you understand the investments you're making. The financial industry is more mature in dealing with risks than are supply chains. Risk managers are in the process of learning best practices from them."

Preparing for a Crisis

When planning for a crisis, business resiliency experts often find that the organization has not taken all factors into account. For instance, a company may have a plan in place to make sure employee paychecks are processed if a hurricane disrupts the payroll process, but may not have a contingency plan for employees to follow if their office building loses power or they cannot get to work. Or the company may have a duplicate data center, but no plans for operators to keep it up and running in the event of a crisis.

Threats must be assessed according to the needs of the specific business. This is often measured in downtime or the impact to revenue. Some companies or government organizations can afford to have their enterprise data networks or phone systems disrupted for a matter of hours or even days, while other businesses are so dependent on communications that even a few hours of downtime would be financially catastrophic for them. But no matter the type of business, maintaining communications during the crisis is crucial in carrying out whatever business resiliency plans have been formulated. All key enterprise communications systems must remain operational, and the enterprise must be able to tap into emergency communications systems such as radio networks set up by public safety agencies. Because these systems often use disparate technologies, enterprises need to consider deploying equipment that can facilitate interoperability among the various networks.

The EBCCS strategy for business resiliency is a method for determining the order in which actions are taken and information is disseminated during a crisis. EBCCS stands for employees, business capabilities, customers, community, and shareholders (with “shareholders” interpreted in the broadest sense as anyone outside the company with a stake in its success). It is generally agreed that the welfare of employees should always be a company’s first concern during an emergency. Next in importance is ensuring the continuity of business capabilities and support for customers, followed by measures aimed at helping the community and supporting shareholders at large.

Cisco has integrated the EBCCS approach into a comprehensive plan for responding to any kind of adverse event—ranging from a local site emergency to a large-scale community disaster to a pandemic. The company conducts regular drills so that response teams can test existing and proposed processes and tools. This multilevel response structure is designed to make certain that employees are instructed and practiced in crisis procedures so these activities will come naturally if and when a crisis does arise.

Communicating No Matter What

A critical aspect of disaster preparedness is making sure that everyone can communicate. The “best” business resiliency plans can quickly go awry if the communications chain is broken. Everyone needs to know what is going on. Managers must be able to talk to each other and to staff members. Security personnel have to be able to contact public safety agencies if necessary. Moreover, most businesses today are so reliant on voice and data communications that any significant breakdown would immediately compromise operations and lead to additional business risk.

For these reasons, organizations must assess their networking technology in terms of how well it will function in the event of an emergency, and how it can be used to ensure business resiliency during the emergency. A natural disaster or other catastrophe can cause havoc in the workplace, damaging buildings, ruining equipment, and displacing employees. But even a washed-out bridge, an ice storm, or a labor strike can prevent people from getting to work. All of which means that “communications resiliency” is of paramount importance to keeping the business operational and viable.

Redundancy is crucial for ensuring continuing communications. But redundancy needs to be extended to network access as well as business-critical applications and data. When employees need to work from a remote location such as their homes, there should be communications measures in place to bring their offices to them. A fully functional virtual workplace includes full access to the data applications, telephony, and collaborative technologies that can make the difference between a major business interruption and “business as usual” during a disruption.

If employees’ home offices have been equipped with company-configured computers, broadband links, and resilient VPN connections, they have much of what they need to operate outside the office during a crisis. Since networks face the same threats from worms, viruses, and intrusions during a crisis that they would face in normal circumstances, the communications plan should be structured to keep network security measures in force. The plan should also take into account the fact that some displaced employees may have to use public Internet devices or mobile phones to access the network, both of which can be accommodated with go-anywhere VPN-based technologies.

Today’s low-touch, high-flexibility networks are capable of provisioning and managing devices wherever they may reside. The first step in ensuring seamless crisis communications is to categorize job roles according to their communications requirements. Network access can be granted based on the person's duties, access device, location, and other criteria. An engineer or accountant might require certain bandwidth-intensive applications, while a sales person or line manager may be at a distinct disadvantage without access to the company's IP telephony resources. If employees can get everything they need by accessing the network remotely, they can be absent from the workplace without being absent from their jobs.

To minimize the equipment necessary to connect employees remotely, the enterprise can use existing network infrastructure and IT processes to deploy and manage the services. For example, employees with telephony installed on their laptops do not require a phone in order to take advantage of capabilities such as sophisticated conferencing. And site-to-site VPN technology can fully replicate office functions and even meet quality of service requirements without requiring extensive equipment and setup at the remote site.

Another critical step in keeping communications lines open is to survey the existing IT infrastructure to make sure it has the capability to serve the company during an emergency. The network must be resilient enough handle the unusual access demands and disproportionate traffic loads associated with crisis communications. Enterprises have traditionally developed contingency plans for specific geographic areas where they do business—they might prepare for an earthquake in California and a monsoon flood in India, for example. However, with globalization has come the need for global preparedness. Companies are now concerned about incidents such as pandemics that could affect communication infrastructures worldwide.

In addition, business resiliency planning should address the communications implications of maintaining physical security during an incident. Surveillance cameras and building access control may be even more critical in a regional emergency, when the resources of civil authorities are often stretched to their limits. Implementing an advanced, comprehensive, fault-tolerant security system that can be monitored from a central location could benefit the company's security personnel greatly if a breakdown in law enforcement should occur and the company has to take on more responsibility for protecting people and premises.

The final step in the communications resiliency process is to make sure all the emergency procedures have been deployed and tested before a crisis occurs. By conducting a test or drill, managers may be able to identify simple problems, such as home PCs that lack the jacks necessary for plugging in company-issued IP phones. Simulating a crisis all the way up to the top management level can uncover weaknesses or omissions in the business resiliency plans that would not be revealed otherwise.

As demonstrated in these examples, communication is as reliant on the process as on the technology. And a resilient enterprise needs both to be successful in good and bad times.

"Operationalizing" the Process

A good business resiliency strategy strives to integrate resilience into the business model itself. According to Zucca, "We're constantly looking at the business, the information technology, and all our processes to make sure we're building an architecture that we can rely on—from a productivity and efficiency standpoint, as well as in terms of the many types of hazards that could disrupt operations."

"You want to build in both a reactive and a proactive capability," says Erickson. "In terms of reactivity, when something goes wrong, how should you deal with it? In terms of being proactive, how do you make decisions about weighing, mitigating, and accepting risk? And how do you embed risk management processes into the company's 'DNA,' so you think about risk management with every decision you make?"

Operationalizing business resiliency means applying a common methodology across the company. An organization may start by putting together risk maps that measure the likelihood and severity of an adverse event based on interviews with the risk owners within the company. The risk map identifies the portfolio of assets that are at risk, the criticality of the risks, what considerations need to be built into the business model to handle the risks, and how the risks can be made part of the group's decision-making process.

The risk map compiler needs to work closely with the risk owners in each business unit to understand what factors motivate them, and how they prefer risk-oriented information to be delivered. A gap analysis can measure where the business unit rates in its ability to monitor and deal with the various risks. When risk management effectiveness is rated low, it generally indicates that risks have not been adequately assessed within the group, risk mitigation is not in place, and reporting or monitoring is lacking. Based on the analysis, a manager can assign actions to the risk owners to raise their risk-management effectiveness.

Operationalizing business resiliency must involve the entire supply chain. For example, Cisco works with partners to help minimize their risks—a mutually beneficial arrangement. Some members of the supply chain risk management organization specialize in putting analytics in place to assess and predict risk scenarios, while others work directly with the manufacturing entities to help identify, assess, and avoid risks. The group either sends out teams to perform the site assessments directly, or employs a third-party to do the inspection. Risk assessors use actuarial data to look at factors such as the potential for a natural disaster at the site.

"We meet regularly with the contract manufacturers that build or add value to our products to discuss what risks we face and what we should do about them," says Erickson. "With regard to key component suppliers, we'll either meet with them or work through a relationship manager. Further down the supply chain we tend to rely more heavily on secondary interactions, unless the supplier is a big part of our business. Then we'll make sure we establish a direct connection."

Preparing for Pandemics

One example of a major threat to business resiliency is a pandemic: a widespread sickness that may occur if a disease such as avian influenza ever reaches a high virulence level and manages to infect a substantial percentage of the population in a region or regions around the world. Many companies have designed an extensive response plan for a pandemic, which may include an impact matrix, a preparedness working model, and a Website that gives information about the plan and can serve as a clearinghouse if a pandemic does occur.

An impact matrix identifies the risks a threat represents to the various aspects of the business. A pandemic would have a strong impact on human capital, the supply chain, and customer demand, but a negligible effect on the physical and IT infrastructure (unless the pandemic becomes so serious that physical plant and IT infrastructures cannot be adequately maintained). By contrast, a terrorist act or a regional war could affect all these sectors of the business to some degree. In addition, the matrix considers factors such as the possible duration of the threat, whether or not it is likely to be repeated, and any geographic limitations.

At Cisco, the Business Resiliency Group is responsible for dealing with a pandemic threat. The group began by collaborating across Cisco to form a pandemic planning committee to assess situations and develop and implement responses. This committee has evaluated the company's preparedness for a pandemic, assessing awareness within the company and finding out if employees felt they were ready for such an event. Because the potential impact of a pandemic is so broad, the committee has considered the scope and duration of business resiliency scenarios across several critical business functions. For example, mitigation strategies for the workforce include management succession planning, employee segregation policies, and mass-scale telecommuting through remote network access. Strategies for maintaining customer contact include expanding online transaction capabilities to deal with travel restrictions and limitations on physical access to customer locations.

Rob Rolfsen, director of safety and security at Cisco, leads a team that is responsible for physical security at Cisco sites, in addition to being a key contributor to the Global Pandemic Planning Committee. This includes everything from guards and building access systems to environmental health and safety and workplace ergonomics. His team conducts regular exercises to check on Cisco's crisis management plans, making improvements where necessary.

"The most recent pandemic exercise was spaced out over two weeks," says Rolfsen. "We sent out e-mail notifications that set up a fictional scenario about local flu infections that may be related to an avian flu. To respond, we set up an in-person meeting with people from various organizations—human resources, manufacturing, public relations, legal, and so on—and we handed out cue cards that gave scenarios and asked for responses. In these exercises, cards may be intentionally misdirected; for example, a corporate legal representative might receive something that should actually be handled by human resources. Everyone needs to know what their responsibilities are beforehand."

Such an exercise should be as realistic as possible, while at the same time challenging the team to test the limits of the business resiliency framework. Example scenarios include the following:

- What is the course of action if an employee has the flu and customers are afraid to have company representatives come to their sites?
- What happens if travel restrictions have stranded the company's executives?
- If social distancing measures need to be taken, how can essential employees still get food in the workplace?
- What if a manufacturing site has been quarantined or a child-care facility has been infected?

Because it is difficult to think of all possible scenarios, a company should consider employing an outside auditor to examine the plan and help spot gaps and omissions.

Making the Business Case

Business resiliency experts agree that it can be difficult to convince executives of the benefits of an effective program. Employee safety and obvious disruptive events are always concerns, but some of the more subtle aspects of resiliency may not be apparent to executives whose backgrounds do not include this discipline.

"You need to look at how you accomplish continuous value creation so it's not just a matter of putting measures in place that will be dormant until a crisis," says Zucca. "You need to build a resilience capability into the organization that can be used today for greater stability across the board, as well as for productivity gains in the future."

But Zucca admits that it is difficult to quantify the productivity loss that could come with a major disruption, especially if business groups, apart from those directly responsible for revenue generation, do not measure their productivity to begin with. That is where sophisticated analytics come into play. Cisco holds two patents in the area of quantifying business process risk, making it easier to integrate analytics into the decision-making framework and talk to business managers about risk in a language they understand.

“You can show value in various ways,” says Erickson. “You can talk to managers about reducing time to recovery when business is disrupted, or you can point out the impact that a certain situation will have on the revenue stream and how to reduce that impact. You can also help managers weigh their options, such as comparing a potential reduction in per-unit cost to an increase in the time it will take for the product to reach the customer.”

Managers can also make a good case that a sound business resiliency program creates competitive advantage. If something negative occurs in the marketplace, the company with a good business resiliency program will likely recover more quickly than the competition. And at the front end, a safer supply chain and a better-prepared organization can be presented to customers as a compelling advantage for them.

An effective business resiliency and enterprise risk management program makes a company more competitive by maximizing the risk/return equation. “It’s not just about minimizing risk,” says Erickson. “It’s about achieving an acceptable level of risk. You need to align business processes with the organization’s appetite for risk. If all you do is attempt to reduce and minimize the chances you take, you could very easily go broke.”

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-429223-00 9/07