International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

IT Risk Register and Responses

Anshuman Awasthi

Director –IT Infrastructure Engineering, Restoration Hardware

Abstract: ***Business Continuity planning is the one of the core function for an organization Disaster Recovery and Incident Management plan. If an organization wants to save itself from heavy losses that may occur due to a disaster or a critical process failure it is essential to have a robust and working Business continuity plan (BCP). Risk Management is a critical function for an organization when it comes to BCP. Risk Management has two critical parts; the first one is creating a Risk Register and second is drafting the responses for the documented risk factors.***

Keywords: Business Continuity Planning, Risk Management, Risk Mitigation, IT Infrastructure Risk Factors

1. Discussion

This article explains how to create a Risk Register and draft Risk Responses for Business Continuity Planning for an organization.

2. Methods

Business Continuity Planning, Risk Management

3. Results/Conclusion

To formulate a BCP it is mandatory to start documenting risk factors that may affect the business directly or indirectly and prepare a risk response. It is better to assign severity to each risk factor to prioritize our work and channel our resources and efforts on the critical factors first followed by medium and low.

4. Article

In today's volatile market and variable business operating conditions, the essential task is to keep your business up and running in a healthy state. To run your company, a leader needs to prepare for the worse conditions so that he can continue to sail when the direction of the wind is not is his favor. To accomplish this task, he has to go through the Business Continuity planning. The BCP is a tedious task to accomplish, and when a leader starts to work on the plan, he would need to think what are all the risks that can affect his business operations and how he should respond to them. To do this, he starts documenting them in the form of a risk register. Let us try to understand the process by taking an example of a national retailer who is dependent on overseas for manufacturing and shipping commodities. The retailer relies on his strong supply chain to accomplish in his business goals and that functions can get affected in an adverse situation due to lack of proper planning. Please refer to the Risk Register that can be used as a starting point for the BCP.

a) Risk Register

Name of Risk	Description	Source (with explanation)	Likelihood of Occurrence* (with justification)	Severity of Impact* (with justification)	Controllability* (with justification)
Earthquake	Company's headquarters are located near San Andreas fault line and an earthquake can cause damage to corporate office and data center	External- Earthquake is one of the natural disaster	Medium-Company headquarters are not inside San Andrews fault line but near to the area	High-Earthquake can cause severe and disruption	Low-We cannot control earthquake but just prepare for business continuity
Internet Services	Internet services outage from a provider will cause service disruption as site operations depends heavily on internet connectivity	External-Internet connectivity is provided by internet service provider(ISP) on their own network	Medium-We have chosen a well-known (ISP) with reliable network infrastructure.	High-Internet outage at a critical site can cause severe impact to operations as important resources are available on network	High-It can be controlled by agreeing on aggressive SLAs with ISPs and installed network circuits from multiple vendors
Power Outages	At a facility or across a power grid	External-Power is provided by external companies	Low-Power outages are not common in area	High-We depend heavily on network and IT resources to run operations which will need power to function	Medium-It can be controlled by use of uninterruptible power supply(UPS) and generators
Hardware	Due to normal wear and	Internal-Hardware failures in	Low-We have	Medium-Impact can be	Medium-We have

Failures	tear, facility damage, or human error	network equipment's, servers and storage are common and can happen due to normal wear and tear	installed hardware supplied by a well-known vendor and they guarantee their performance	minimized by running servers in high availability environment	installed redundant servers for all critical applications
Fire/Heat Damage	Whether from equipment overheating, short-circuit, lightning, loss of environmental controls, or arson	External/Internal-Overheating of any network equipment or fire originated from an external source can cause damage.	Low-Company is taking precautionary measures to avoid overheating of equipment's and is performing regular fire-drills	High-Fire/overheating can cause significant damage to critical hardware equipment's and will directly impact operations	Low-Fire can be controlled by having fire extinguishers onsite and an immediate call to fire department
Water Damage	Whether from leaky pipes/roofs or severe weather	External/Internal-Water damage can happen from internal pipes or from external factors like severe weather	Medium-We carryout regular inspection of plumbing infrastructure and drainage system to avoid occurrence	High-Water damage can cause severe damage to company property disrupt company operations and can cause loss of revenue	Low-Water damage due to internal factors can be controlled but we have very limited control on water damage caused by external factors.
International tariff	Government policies to increase international tariff on imported goods will effect product prices and profits	External-Government policies to increase tariff on imported goods from one country or from multiple countries can adversely impact business.	Medium-Increase in tariff is not very common and takes a long time to implement as it needs several approvals from lawmakers	High-Increase in tariff can affect supply chain, profit on goods.	Low-Increase in tariff is a government decision and an organization has a limited control
Product Supply	Companies makes profit on sold products. If there is any impact to the product supply it directly affects companies business and reputation	External- Vendors located in different countries manufacture most of the products overseas. Vendor financial stability ,political unrest in their home country will affect product supply	Medium-Company had varies vendors located in different countries	High-Supply chain is a critical function of a retail organization and any disruption in product supply will have direct effect on revenues	Medium-Company has a very limited control on external factors effecting product suppliers in different countries

b) Risk Responses

Risk 1: Earthquake

To prepare for a disaster like Earthquake, an organization needs to work on a disaster recovery plan for its critical functions like the workspace, supply chain, e-commerce, and critical applications. The first step in BCP is to complete an external analysis of the business. Disaster recovery planning is a significant initiative and takes a lot of team effort. We need to have a natural disaster response plan that includes a communication plan, a temporary location, and a way to protect any unrecoverable assets.

Risk 2: Internet Services

The businesses are becoming increasingly dependent on information systems not only to conduct business but also to remain competitive; the stakes involved in the communication system outage have risen. Considering the network infrastructure requirement created by the convergence of voice, data, and video communications, the need for high-speed, reliable internet communications system/network recovery and restoration has taken on new significance.

Communication is essential for the company to remain in business; loss of contact could put the company out of business. To prepare for internet services outage, the company needs to plan for redundant network infrastructure and order circuit dual circuit from different service providers on a completely diverse media.

Risk 3: Power Outages

The organization's infrastructure requires power every day to run its operations. Unplanned downtime can occur when the power goes out, and that can cost an organization thousands or even millions of dollars. Unexpected outages can lead to situations from which it may be difficult to recover. Making sure that an organization has a plan to eliminate downtime in the event of a power outage will help the business mitigate the potential losses that can occur because of disruption. Power outages can affect the company's bottom line and ongoing business operations. Monetary damages due to downtime can vary based on the industry and other factors like length of the blackout, time of day, and the number of people.

Large companies cannot function long without the use of items such as computers, manufacturing equipment, and lights. Any business running today relies on web-based technologies and networks, and it may experience setbacks in the event of an outage. Power outages can affect the industry in a variety of ways. To prepare for any power outages, we need to improve on power redundancy by ordering power from two different feeds in all critical locations, install uninterruptible power supplies (UPS) with generator backup.

Risk 4: Hardware Failures

Hardware failures are among the most common problems that an organization has to face from an IT infrastructure perspective. These failures can cause an outage, which may temporarily stop access to an IT system, and that can cause loss of time, effort, and money. There are various reasons for the hardware failure to occur, like voltage spikes, power failures, overheating, hard disk failures, normal wear and tear, incompatibility, and human errors.

Loss of data is the primary impact of an organization due to a hardware failure. The issue can come up with the CPU, hard drive, motherboard, or any other output or input devices. To prevent permanent loss of data, we should schedule regular backups; also, the company should invest in the resources and workforce to perform, store, and retrieve these backups.

To minimize the risk of hardware failures, the organization should install a high availability infrastructure for all critical applications.

Risk 5: Fire/Heat Damage

Overheating is another common reason for hardware failures. The heat is generated as electronics components inside hardware operates. If we want to avoid hardware damages, excessive energy must be dissipated. Inadequate ventilation can become the most common contributor to the problem. In case we have a computer system under a desk or in a corner, it is a candidate for overheating because the heat has limited places to go.

Loss of data and property is the primary impact on an organization from the damage caused by fire/overheating, which results in loss of productivity. The time spent to retrieve the information or repair the physical hardware can cause loss of productivity. Replacement parts or systems may be a suitable solution to reduce productivity concerns, but the cost of maintaining these increases dramatically, especially when a standard configuration for hardware and software has not been established.

While insurance may cover an organization for the damages due to a fire. It is not straightforward to compensate for the cost of computer network downtime. If you lose data that cannot be retrieved, the bottom-line impact and the damage to your reputation may even be more significant.

Each office building is unique, so it is essential to conduct a proper risk assessment to establish the potential for the fire to break out. The company has worked with a third-party consultant who understands the nuances of a Server room fire safety. Fire extinguishers and sprinklers should be installed at the site as per recommended standards.

The company has also worked on business continuity planning to run its operations from a disaster recovery site in a worse case.

Risk 6: Water Damage

The water damage can come from a variety of sources, and not all of them may be applicable in every situation, the organization should nonetheless have some water detection as part of their business continuity plan.

Floods are one of the primary causes of disaster here in the United States, and statistics show that floods and extreme weather events profoundly affect the US, along with Japan, the Philippines, and China.

Many organizations that are at a distance from large bodies of water tend to ignore the damage a flood can cause. It is essential to remember that water damage from flooding is not just restricted to those near coastal areas. Water main breaks, overflowing rivers, extreme precipitation, internal plumbing failures, and heavy rains can all cause water damage from flooding.

If a leak is undetected, it can cause make as much damage as a storm or flood. Leaks can occur from different sources, including leaky and frozen pipes, leaky roofs, damaged windows, building foundation, malfunctioning sump pumps, and HVAC problems.

Over 90% of significant water damage can be easily avoided. The company has set up proactive water and leak detection that can help to notify if the water is detected anywhere in the organization's building or facility.

The company has also included water and leak detection in the business continuity plan. Helping to keep our facility and assets protected will help the organization to avoid costly repairs and downtime over the long run.

Risk 7: International Tariff

The risks of tariffs are significant in an organization, primarily supply chain, and the effects can be more widespread than they initially appear. The impact of tariffs is broader as companies have a complex supply chain to consider. "Most companies don't necessarily source 100% of what they make in the same country that they make it," Diaz said. "It's physically impossible in the global world we're in today. Typically, everybody imports something that goes into the final product."

Tariffs can disrupt these supply networks and create additional costs. "Tariffs are especially risky with very complex and deeply intertwined global value chains," Blanchard said. "When policy changes disrupt an industry's ability to import vital inputs, they can jeopardize the whole value proposition for local businesses. It's tough to predict all of the effects in advance, which makes it a risky game to slap tariffs on parts and other intermediate inputs."

To minimize risk for rising international tariffs company is working on developing vendors in countries that are free from increasing recent tariff changes.

Risk 8: Product Supply

Managing demand and supply uncertainties is critical for all manufacturers. Supply and supplier risk speaks to the potential disruption of raw material and component supplies. Manufacturers need to produce products of acceptable quality to customers and to deliver those products at a competitive cost with highly reliable delivery times. Achieving timeliness of deliveries, high-quality levels, and efficient processes along the supply chain cannot be achieved by relying on the organization itself but should be ensured through collaboration and coordination with trading partners.

Supply uncertainty may be manifested in the form of uncertainty regarding material availability/supply capacity, material price, alternative sourcing availability, and supply lead time. A higher level of flexibility is required, in case supply is uncertain, to achieve better customer service levels.

Working with a single supplier is risky. An organization should maintain multiple suppliers, which will guarantee the availability of products.

References

[1] The Definitive Handbook of Business Continuity Management
[2] Corporate Risk Management-By Tony Merna
[3] https://strategiccfo.com/
[4] https://www.fosterfuelsmissioncritical.com
[5] https://www.tandfonline.com/doi/pdf/10.1080/21693277.2014.882804
[6] https://disastersafety.org
[7] https://www.business.qld.gov.au
[8] https://www.aferm.org/erm_feed/the-business-impact-of-trump-tariffs/
[9] https://www.nyu.edu
[10] http://www.emergency-response-planning.com
[11] https://searchdisasterrecovery.techtarget.com

Author Profile

Anshuman Awasthi, Director, Infrastructure Engineering at Restoration Hardware, responsible for IT infrastructure management and new implementations. Member of Forbes Technology Council.