Fast Forward Investments, LLC™

FAST FORSIGHT

1 June 2013 FFIDN: 060113

In This Issue

Related Insights

Your Data is Backed Up... But Can You Get it Back?

Do You Know Where Your SPOF's Are?

The Worst Kind of Business Continuity Test

Where is the Plan?

Most People Will Only Accept What They Already...

Not If, But When

You Don't Know What They Haven't Told You

Related Help

www.ffinow.com/Predicting the Future.html
Can you predict the Future of Your Business?

www.ffinow.com/Services
The help you need to get the job done.

Contact Us

http://www.ffinow.com

info@ffinow.com

What is Enterprise Risk Management?

How can organizations identify and address every possible risk that could impact daily operations? A more realistic goal for most companies is to identify and attempt to mitigate the *most likely* risks to critical business processes. This should be the primary goal of what is often referred to as a Risk Assessment (RA). A Business Impact Analysis (BIA) should be performed in conjunction with the RA so that business executives can understand what is prudent, in terms of the cost to mitigate identified risks. The goal of the BIA should be to quantify the impacts that would be experienced by the business if the ***likely risk scenarios*** identified by the RA were to occur.

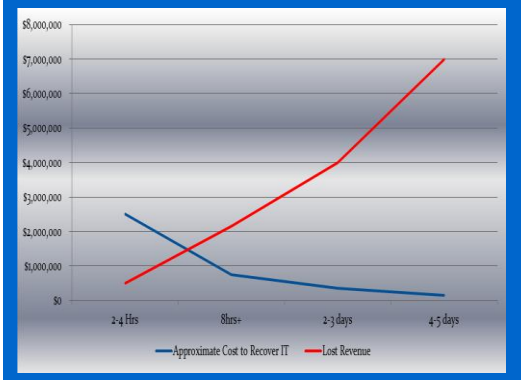
Typical options for mitigating risk as part of an Enterprise Risk Management (ERM) Strategy include:

- **Accept the Risk** – Executives weigh acceptable levels of risk vs. cost and practicality of options to completely mitigate the *likely* threats that have been identified. Once the threats and costs to mitigate those threats are known, management may decide to accept the level of risk or exposure that they believe they have.
- **Transfer the Risk** – Many companies either increase their Insurance coverage, or self-insure against identified risks. They may also contract for certain functions, in order to assign risk to external 3rd parties. In this case, a carefully crafted, contractual service level agreement with penalties for non-performance is a must.
- **Mitigate or otherwise Address the Risk Internally –** Organizations will often choose to make active investments that will reasonably minimize the level of threat or potential loss, in the event of a disaster. Such investments may include building out redundant infrastructure (or contracting for external capacity) to which employees could rapidly fail-over in the event of a prolonged disruption or outage.

What Should a Risk Assessment Include?

A proper Risk Assessment should focus on risk scenarios that are likely for the type and location of the business. For example, if all of the company's locations are in Southern California, it is ridiculous to spend any time looking at the likelihood of ice storms being a threat, unless the business is

How Much ~~In~~AS surance Do You Need?



Get a Business Continuity Strategy that really works. Contact us today: ***info.ffinow.com***

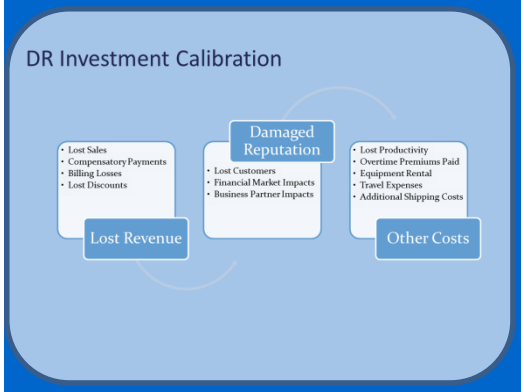
dependent upon shipments from suppliers that are located in parts of the world that could be impacted by severe weather. Instead of trying to quantify the various impacts of events such as fires, floods, tornadoes, lightning strikes, terrorist attacks and the like, focus on what would happen if your critical infrastructure became unavailable for a prolonged period of time. Explore what employees would do if their offices became inaccessible for days or even weeks.

If the business identifies its most critical processes as order taking, fulfillment and billing, the assessment should center around identifying the risks to those processes. An assessment that focuses on the company's ability to make payroll might be appropriate for a transportation company where there is risk of drivers walking off the job if they don't get paid for all of their hours in a given pay period, but many organizations are able to pay their employees off of the last period's payroll file in an emergency.

At a minimum, a proper RA should include the following components:

- **An Executive Summary** – A wise executive once said: "If it takes more than a page to explain a problem, your message is too complicated". At a summary level, management needs to know what the main issues are and how those issues could impact the organization. Save the rest for the detailed assessment section of the document.
- **Risk Scorecard and Assessment** – Organizations need to have a dashboard that identifies key risk areas, such as critical infrastructure components, vital processes and supply chains, potential single points of failure and how long critical systems or processes could be unavailable during likely disaster scenarios. The assessment should detail the rationale behind the scorecard ratings as well as provide justification for the way the risks were identified, prioritized and graded.
- **A list of Likely Risk Scenarios –** This list of likely scenarios should reflect what could realistically happen, based on reliable information obtained from: previous local disaster or outage experiences, USGS (earthquake, fire and flood information), surveys conducted by disaster recovery services providers and other recognized sources, as appropriate. If possible, the likelihood of occurrence for each scenario should also be estimated. Some common scenarios include: widespread outages of information technology or electrical power, local fire or flood in the data center, or building inaccessibility due to a HAZMAT spill or other toxic contamination.

*"It is not a question of **if**, but of **when** an unplanned outage will occur. Organizations must prepare for the likely event systems and the processes that they enable will be impacted in some way". –FFI*



Data Center Alternative Benefits

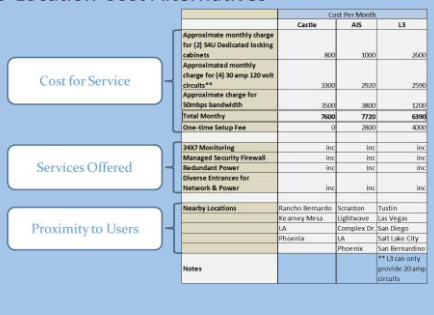
	Option		
Benefit/Attribute	**DC1**	**DC2**	**DC3**
Estimated 5 yr cost	$806,200	$1,123,000	$616,000
Meets Business RTO	Yes	Yes	Yes
Meets Business RPO	Yes	Yes	Yes
Flexibility	AA	A	AAA
Mitigates Local Risk	Yes	Yes	Yes

Data Center Alternative Estimated 5 YR Cost

Cost Component	**DC 1**	**DC 2**	**DC 3**
Build/Retrofit	415200	732000	
Server Hardware	50000	50000	50000
Storage Hardware	16000	16000	16000
Network Hardware	100000	100000	50000
Software	25000	25000	25000
Maintenance	125000	125000	125000
Hosting Charges	0	0	300000
Occupancy/Space	25000	25000	
Professional Svcs.	50000	50000	50000
Total 5 YR Cost	**$806,200**	**$1,123,000**	**$616,000**

Note: Estimate does not include staffing

Co-Location Cost Alternatives



	Cost Per Month		
	Castle	AIS	L3
Approximate monthly charge for (2) 54U Dedicated locking cabinets	800	1000	2600
Approximated monthly charge for (4) 30 amp 120 volt circuits**	3300	2920	2590
Approximate charge for 50mbps bandwidth	3500	3800	1200
Total Monthy	7600	7720	6390
One-time Setup Fee	0	2800	4000
24X7 Monitoring	inc	inc	inc
Managed Security Firewall	inc	inc	inc
Redundant Power	inc	inc	inc
Diverse Entrances for Network & Power	inc	inc	inc
Nearby Locations	Rancho Bernardo	Scranton	Tustin
	Kearney Mesa	Lightwave	Las Vegas
	LA	Complex Dr.	San Diego
	Phoenix	LA	Salt Lake City
		Phoenix	San Bernardino
Notes			** L3 can only provide 20 amp circuits

What to Look For in a Business Impact Analysis

When conducting a BIA, organizations should keep in mind that they are after rough order of magnitude (ROM) estimates, when attempting to quantify potential loss. The BIA itself is an estimate, based on the best information available at the time and mostly upon what the team *believes* would happen. Precise numbers are only possible when the organization has experienced an actual disaster that has been quantified for insurance or reporting purposes. If parts of the company would be unaffected by an outage of days or even weeks, but a critical few revenue generating processes would be impacted immediately, it is best to focus mostly on those processes that would have immediate and significant financial impact.

In some cases, those who may be tasked with quantifying impacts to the business will unintentionally over-complicate the process of estimating potential financial impacts to the business. In one example, an individual may get the idea that spending hours identifying the components that comprise the cost of goods sold (COGS) is somehow germane to the task of quantifying business impacts that would result from a disaster. In this case, they may attempt to argue that if they are not able to produce finished goods, all the daily costs of operation (DCO) that would normally be associated with the production of those goods must somehow be added to the other costs of managing through a disaster.

In actuality, the value of lost revenue has nothing to do with DCO. In fact, one could argue that DCO would actually *decrease* substantially during a disaster, because people would be unable to come to work, power may be shut off, etc. In many cases, the company would bear those same costs and more (including possible later overtime premiums to make up the resulting backlog of work) whether they are producing goods or not. If the company is unable to accept and fulfill customer orders (and realize the revenue that would normally be generated by them) the value of those lost orders would constitute the majority of lost revenue. Some percentage of customers may be lost permanently and impacts may also be felt due to damaged company reputation.

Not everyone needs to be interviewed when conducting a BIA. Make sure that you obtain buy-in from executives and key business leaders throughout the process, but be respectful of everyone's time. Remember, the ultimate goal of the BIA is to help determine a prudent strategy for mitigating the *likely* risks and potential impacts that will have been identified. You wouldn't buy a car and then disassemble it in order to determine how much auto insurance you might need. Set realistic goals and expectations for what you are trying to achieve with a BIA.