LinkResQ
A LEADER IN ENTERPRISE RISK MANAGEMENT

Technology Risk is Everywhere

A Risk Management White Paper by

Paul O'Brien and Gerard Joyce

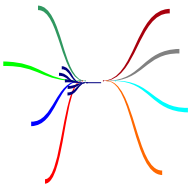
LinkResQ Limited

Things Just Got Complex

My granny learned about things when they were complicated, there were twelve pennies in a shilling, thirteen loaves in a bakers dozen and twenty one bob in a guinea. Young folk today have it easy, since we went metric, there are four bits in a nibble, two nibbles in a byte, a thousand bytes in a Kilobyte, one thousand, thousand bytes to a Megabyte and a Petabyte is something with more noughts than you can shake a stick at! Everybody knows technology has made things so easy for us……..

No matter what the business is today, Information Technology has infiltrated all aspects of every transaction. Nothing is conceived, designed, developed, manufactured, sold, bought or paid for, without the involvement of some of those bits and bytes. In any comprehensive enterprise risk framework most areas of risk have IT involvement. Failures in Information Technology, whether in its **confidentiality**, **integrity** or **availability** represent risks of significant consequence to most enterprises. The dependence on information technology and its proper management is mission critical, yet many enterprises have limited awareness of their exposure to the risks.

The LinkResQ full information technology risk framework looks like this:



Recent Irish examples of exposure to some of these risks include:

- The allegation in the high court that when five senior **People** of a waste management company left the company on the same day, much sensitive commercial information about its business was downloaded to portable hard drives by its former head of information technology and removed from the premises.
- The Blood Transfusion Service and the theft of a laptop, with thousands of customer records. The data was encrypted but the incident still sparked off an outcry in the press as to why the information was on the laptop in the first place, putting an already fragile **Reputation** at further risk.
- The Dublin based data centre outage. One of seven air-conditioning units failed and caused the other six to trip. In their response to the rising temperatures one of the engineers mistakenly powered down the DNS servers, which exacerbated the problem and prolonged the recovery. What started as an **Environment** risk was compounded by **People** risk turned into a **Reputation** risk with **Economic** risk consequence.
- 26,000 Eircom customers were left without a service on Feb 1st (Power outage) Many of these customers lost business because of their dependence on a single sourced **Supply** for a key service; telecommunications.

Technology enables traditional risks to become major disasters because of the ability to amplify the error, act or omission at the speed of light. The associated risk management has to be as swift.

Mitigating the Risks

John Ruskin put it eloquently over 100 years ago: *"It's unwise to pay too much, but it's unwise to pay too little. When you pay too much you lose a little money, that is all. When you pay too little, you sometimes lose everything, because the thing you bought was incapable of doing the thing you bought it to do. The common law of business balance prohibits paying a little and getting a lot. It can't be done. If you deal with the lowest bidder, it's well to add something for the risk you run. And if you do that, you will have enough to pay for something better"*

Reliability, Resilience, Redundancy and Recovery are words that populate the IT landscape and all have cost beyond the original benefit the "solution" offered. Defining the Minimum Essential Service and being compelled to plan around a Maximum Tolerable Outage and to agree a Recovery Point Objective is a challenge for many enterprise managers. All too often they look at *the price to mitigate risk rather than at the cost of failing to*.

43% of small to medium sized enterprises who experience a disaster go out of business within 18 months of the event. Some are killed by the disaster but most are squeezed out of business as a result of two outcomes. Firstly, the disaster makes the customers of the enterprise aware of their dependence on the enterprise as a supplier. Wise customers make alternative arrangements "just in case", often splitting their

business between two suppliers, reducing dependence on either, and by extension, revenue to the original enterprise. Secondly the suppliers, banks and funding sources take a different view of an enterprise that has had a disaster; credit gets tighter at the wrong time. Cash flow issues following the original disaster can do irreparable damage and slowly choke an enterprise out of existence.

In my granny's time reliability meant buying quality at the outset, resilience meant it could take a bit of rough treatment, redundancy meant having two of a few things and recovery was a state of mind.

So how dependant is your enterprise on the IT monster that has crept into every aspect of your business life? Have you identified the risk? Have you a business continuity plan?

Responsible IT

Information Technology Departments are no longer optional functions in an organisation. The influence of IT has permeated all aspects of business and its impact goes way beyond an IT manager's area of control. There are no longer IT projects, there are "business change projects" with IT elements. But more critically, businesses are dependent on their IT more than ever and consequently the need to ensure that the risks associated with each dependency are identified, understood and appropriately mitigated, is greater than ever. BE Risk Aware! Be very Aware!

Glossary

Maximum Tolerable Outage (MTO) is the maximum time you can be away from your customers.

Minimum Essential Service (MES) is the lowest level of service that is acceptable to keep customers loyal.

Recovery Time Objective (RTO) is the time within which systems or services must be restored to ensure minimal impact.

Recovery Point Objective (RPO) is determined by how out-of-date you can afford your data to be once the system is up and running again.

Who needs to hear this message? By training, the IT people in an organisation are cautious, they protect systems, know the dangers and the risks and generally manage the technology risks and most of the supply risks well. Information and the technology to keep the business operational, is the responsibly of everybody. Business managers need to understand the capabilities and the vulnerabilities of the technology.

The technology will determine its own limitations; the business must determine its requirement and clearly state the consequence of technology failure to the business. The business determines the MES and the MTO. It is reasonable for technical managers to challenge the assumptions made when arriving at these figures, but once they have been agreed and set as objectives in a business continuity plan, the organisation has to accept the collective responsibility to make sure they are attainable.

Many businesses fall into the trap of mitigating the likelihood of a loss event occurring and fail to look closely enough at mitigating some of the consequences of an event once it has occurred. Bad stuff happens, planning for survival is not an IT project it is a business process. As my granny used to say "you won't always get what you want but you always get what you deserve"

Know where and what your risks are and plan to, Terminate, Tolerate, Treat or Transfer them before they damage you.

.linkresq.ie
LinkResQ has a process tool called CalQrisk, that leads enterprise management teams through a comprehensive risk alignment and assessment exercise that provides a platform for mature risk management.

LinkResQ Ltd., 4200 Atlantic Avenue, Westpark, Shannon, Co Clare, Ireland
Tel: +353-61-477 888, email: @linkresq.ie, web: .linkresq.ie

