How I learned to stop worrying and love risk [1]

Sachin Melwani

Let's face it, the world is a more complicated and scary place nowadays. The very real possibility of terrorist attack – both physical and virtual – has increased, and with it comes different kinds of 'what if' questions that should be asked: For example what if a virus invades our computer system and corrupts the data held? A critical consideration in the analysis of the risks and their possible controls is the duration of the impact and how long could the interruption last or, *more appropriately*, how long can the company afford it to last?

Often IT Managers lack a framework to analyse a comprehensive business continuity plan which actually can work when required and actually adds value. The following seven-step contingency process can be used by a company to develop and maintain a viable contingency planning program for their IT systems:

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance.

Of course that all sound's very straight-forward but it is difficult to know how to start. An IT Manager can hold a workshop and create long list of risks and tackle these in an incoherent manner. A *risk management framework* should be developed in advance of this *risk identification*. The following types of impact/categories of damage can be used to identify the effects of disruption and loss exposure:

- Financial
- Customers and suppliers
- Public relations/credibility/reputation
- Legal
- Regulatory requirements/considerations

[1] How to cite this article: Melwani, S. (2020). How I learned to stop worrying and love risk, *PM World Journal*, Vol. IX, Issue II, February.

- Operations
- Competitive position
- Personnel

The *effects* of these disruptions could be felt in terms of:

- Loss of assets: key personnel, physical assets, information assets and intangible assets.
- Disruption to the continuity of the service and operations
- Violation of law/regulations
- Public perception

To measure the extent of the effect the loss exposure could be determined quantitatively or qualitatively as per Table 1.

Quantitative Measures	Qualitative Measures
• Loss of bank customers	• Human resources
• Fines	• Morale
• Cash flow	• Confidence
• Accounts receivable	• Legal
• Accounts payable	• Social and corporate image
• Legal liability	• Financial community credibility
• Human resources	• Human resources
• Additional expenses/increased cost	• Morale
• Loss of customers	
• Fines	
• Cash flow	

Table 1 Methods of measure for calculating Loss Exposure

So what could be the worst-case scenario? Let's look at what this means using a worked example. For companies with a strong internet presence this could be a loss of IT infrastructure, including all email and Internet facilities, the loss of databases, documents and records and all web sites. Such a scenario may occur through physical damage to a property, or through a problem with the Internet Service Provider or hosting facility.

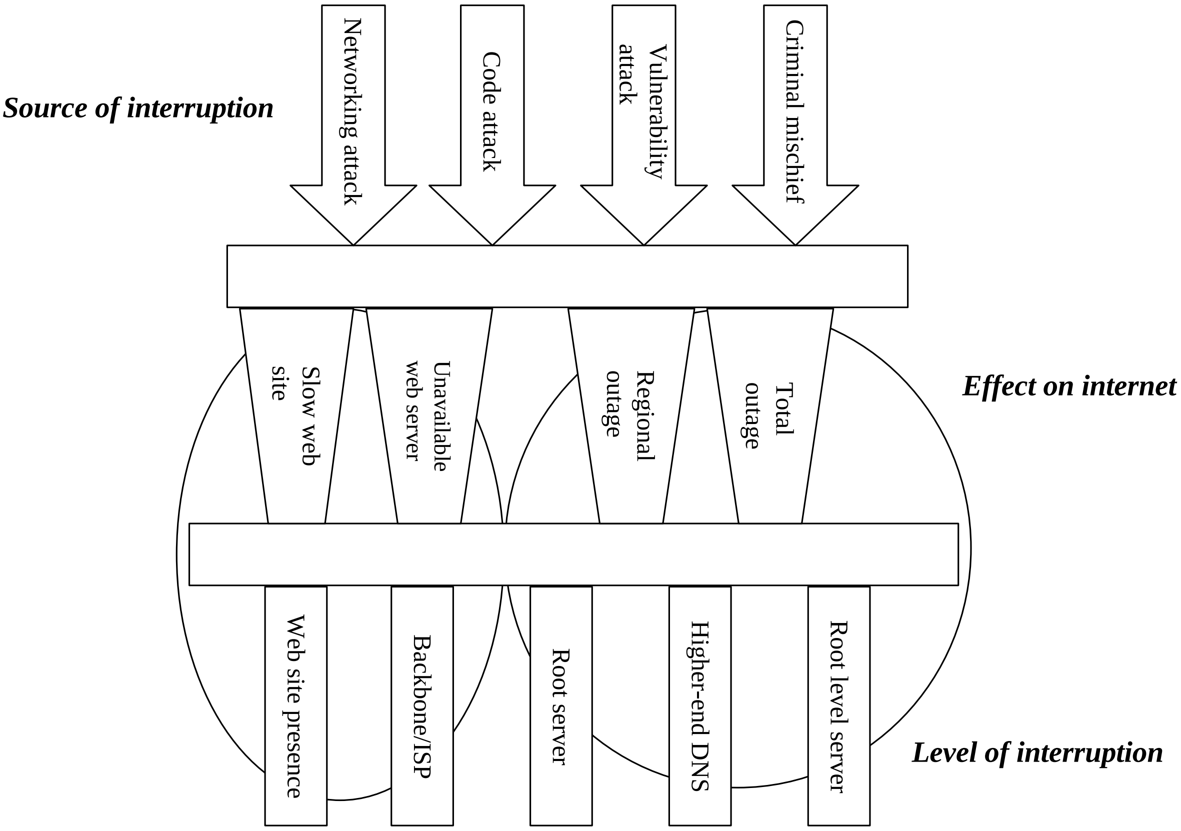


Figure 1 Sources of interruption for an Internet company

By this time you now would have identified a list of risks which categorised against a Risk Breakdown Structure (RBS) where the risk impact has been assessed. In establishing disaster scenarios it is useful to classify them according to relevant criteria, such as: risks under a company's control, risks beyond the company's control; exposures with prior warning (e.g. a tornado), and exposures with no prior warnings (e.g. earthquake). The matrix below provides a framework for classifying types of risks according to where the crisis is generated and *which* systems are the primary causes. This is a useful step before developing risk mitigation measures in order to concentrate effort on developing effective risk mitigation plans. Rather than having to develop contingency plans for every eventuality, the matrix provides the basis for clustering 'families' of crises together and preparing for these rather than for each individual incident.

	Internal	**External**
Technical/economic	Computer breakdown Computer virus Fire Loss/management of data Remote access via dial-up connection	Natural disasters Telecommunications failure System failure
Human/organization/social	Sabotage Fraud Loss of key staff Casual mistakes Disgruntled employees Email Unauthorised modems	Terrorism Third-party failure Poor public image

Table 2 Crisis typology

Against each risk there would be risk mitigation measures which be proactive preventative measures, reactive impact reduction measures and fall-back plans. Any disaster recovery plan or business continuity plan should enable the organisation to react to, recover and restore from the disaster within acceptable recovery point and recovery time objectives:

- **Recovery Point Objective –** The time at which the mission critical data must be recovered to resume business transactions
- **Recovery Time Objective –** The time at which the business functions must be recovered before the organisation is severely impacted

Key consideration to any disaster recovery plan or business continuity plan would be the following business continuity issues:

Timeframe

The use of 'hot sites' could be one form of reactive control to compensate for the immediate impact of exposure and keep the organisation's critical systems and connections, as well as for any critical business partner.

Location

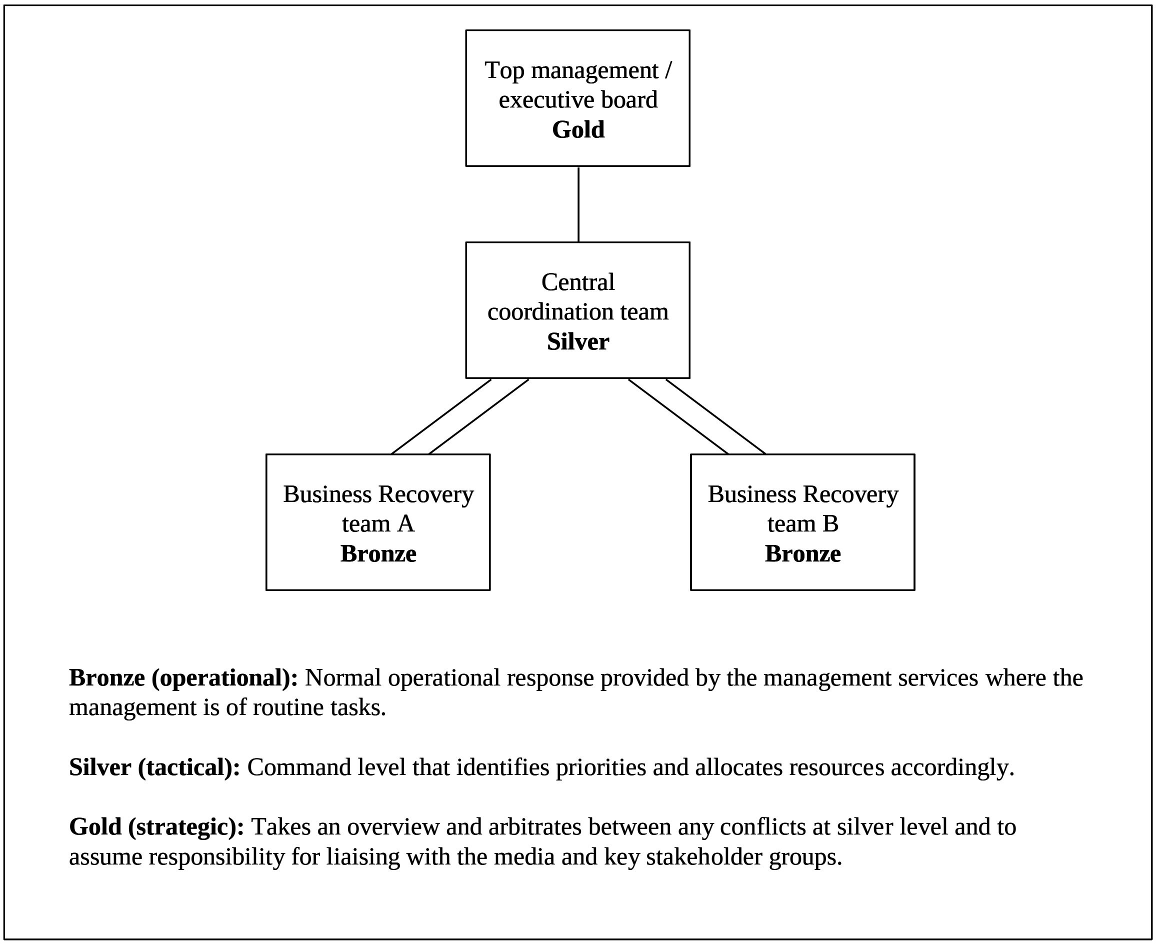
In planning the organisation's response, the bank must also appreciate that it finds itself in a 'brownfield' planning context. Outsourcing would be another way of ensuring the resilience of the bank, as it would assure 24/7 monitoring by technical experts, who would help to identify and eliminate problems before they occur.

Communication

The communication strategy would also entail a systematic way in which to call out employees in the event of a business interruption outside office hours and overlap with customer relations.

Personnel

Having identified appropriate system recovery strategies the organisation must also designate appropriate teams to implement the strategy. The specific types of teams required are based on the system affected. Each business recovery team would be trained and ready to deploy in the event of a disruptive situation. The company could also utilize the three-tier structure to ensure that the bank's response to an incident is effectively coordinated



Bronze (operational): Normal operational response provided by the management services where the management is of routine tasks.

Silver (tactical): Command level that identifies priorities and allocates resources accordingly.

Gold (strategic): Takes an overview and arbitrates between any conflicts at silver level and to assume responsibility for liaising with the media and key stakeholder groups.

Figure 2 Three-tier command and control system

These are just some of the techniques that can help you develop a disaster recovery plan or business continuity plan that provides an effective return in terms of investment which would actually add value on the ground when you actually needed it. Some that are used with great success by companies of all sizes are Virgin and London Metropolitan Police.

About the Author

Sachin Melwani

Based in United Kingdom

🇬🇧

Sachin Melwani gets problems solved through his 'disruptive creativity'. Leveraging his strong knowledge of ERP transformation from the Client, Prime Integrator and Tier Supplier perspectives, through DADA he now aims to bring genuine innovation to the traditional consultancy model by offering a unique "Consultancy as a Subscription" service.

He has over eighteen years' experience in multiple industry sectors across Europe, Africa and the Middle East, involving both management of projects and implementing enterprise-wide project control systems, that deliver authoritative and informed governance information to C-level management on P3M3, Earned Value Management & Project Planning methodologies.

As an AXELOS Consulting Partner, DADA helps companies on project controls setup, NEC4 contract administration, ERP systems integration (Ares PRISM, Deltek Cobra, Oracle, SAP), critical projects delivering to automating SharePoint business workflows.

DADA provides on-demand resourcing & flexible monthly plans to provides a unique, low-cost delivery model which combines both extra staffing and software tools. The advantage over a traditional consultancy is that DADA provides an economical and responsive way to support any project by offering a "Consulting Service at Contractor prices" through flexible monthly subscription packages.

Sachin can be contacted at sachin.melwani@big-dada.co.uk
Learn more about DADA at https://www.big-dada.co.uk/