Business Continuity and Capacity Building

April 10, 2015

Developing Institutional Business Continuity Plans and Implications for Capacity Development Plans

Business continuity

. . . is risk management + disaster recovery

"Being able to do business as usual"

What business are universities in ?

- Education

&

- Research

. . . and sometimes more: ISP/ASP, data center, IXP

Where's the bottom line ?

While a university will typically not go bankrupt, there are disasters that are hard to recover from, and can tarnish the reputation and funding of a university:

- disruption to a flagship research program
- loss of student acamedic records / work
- breach of systems and dissemination of confidential information
    - salaries, HR information

What is at risk (types of risk)

- Equipment damage/destruction/theft (loss of physical integrity)
  - Infrastructure (network, data center/storage, cabling)
  - Instruments (resarch labs/medical)
- Information (loss of data integrity)
  - Loss of data
  - Corruption of data

These cause various degrees of Service disruptions and non-availability (combination of physical + data loss of integrity)

Risk management: threat and risk analysis

Risk Management and Business Continuity assume the following elements are in place:

- Security policies and the tools to enforce them (adm & technical)
- Monitoring, logging (technical)
- Change management (technical & project management)
- Documentation of processes and systems, including their criticality
  - identify weak spots, "what if" scenarios
- Audit (all departments)
- Service Level Agreement (management & technical)

. . . how many of these do you implement ?

. . . who is in charge of these processes ?

Everyone is different

Like any business, universities have aspects that make them unique.

The people running your network have:

- a standard set of skills
- unique knowledge of your applications, systems, and data

Acquiring knowledge and experience of the systems, applications, and network is a time consuming process.

Staff retention should be a high priority!

Outsourcing vs in-house

2 scenarios that illustrate the need to have qualified staff with the right knowledge, regardless of whether some functions are handled by outside partners.

1. IT functions are in-house
   - but staff isn't skilled / knowledgeable enough to implement Risk Assessment, Recovery and Contingency plans
2. Some core IT functions are outsourced
   - in-house staff isn't qualified to assess the preparedness of the vendor that the functions are outsourced to

Beware of "trivial problems" (1/2)

Seemingly innocuous events such as a router failure or a hard disk crash, typically in a cascade of events, can lead to failures that can halt the functioning of a university for a long period of time.

1. Case

- a disk fails, containing the only copy of the university's accounting system - no one identified that a) the disk was not redundant anymore (was it ever ?) b) that no backup had been taken for 6+ months c) the knowledge on how to rebuild the data and/or restore from an older backup left with the employee who set the system up years ago

=> Mitigation: a criticality assessment would have likely noticed the risk. Also, in-house staff has better knowledge of the finance department than an external company would.

Beware of "trivial problems" (2/2)

2. Case

- a core equipment fails, and the backup equipment is not up to date configuration wise. The core equipment failed in a way that the configuration can't be recovered. Lots of time will be spent rebuilding the configuration manually, frantically trying to get hold of former employees who may remember the details.

=> Mitigation: change / configuration management processes, which can be automated, would have picked up the configuration from the equipment, thus saving lots of time. A properly qualified staff would have implemented the tools necessary to avoid such a failure.

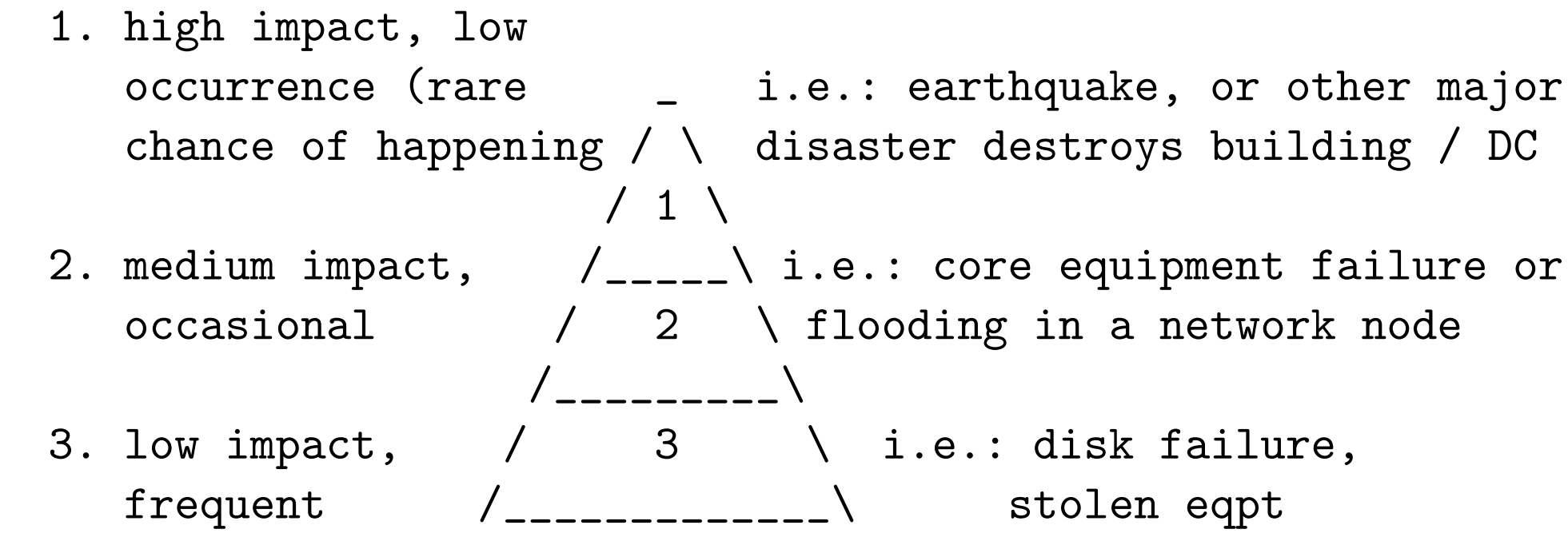
More serious issues

- Case 1: offsite backup hasn't worked for months, a fire breaks out, destroying local storage and backup
- Case 2: the ERP/CRM system is "in the cloud". The vendor goes bankrupt, and no provision was made to regularly back up and pull down data from the cloud vendor, back to the university.

=> Mitigation

- in case 1, in-house staff would have implemented automated, manually controlled reporting on backup processes, rather than rely on those of a the external vendor
- in case 2, in-house staff would have implemented a regularly scheduled backup process, and insisted that the vendor offer quarterly restore testing

Pyramid of risk



How high in the pyramid do you still expect to be “in business” ?

Key points

- staff retention of the critical staff should be high priority!
- external partners will never understand - or care about! - your environment as much as full time staff
- in-house staff needs to be trained and improve their skillsets so they can implement best practices, which go a long way to mitigating disasters, and also help them assess compliance in external vendors and services
- qualified staff, with a knowledge of your institution is more important than backup data centers, off site replication, etc.
- without them, even low impact events can severely disrupt business

Thank you!


OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
HELP! HELP!
SOMEDAY WE HOPE TO HAVE A BUDGET.
www.dilbert.com scottadams@aol.com
© 2000 United Feature Syndicate, Inc.