



Archway International

Archway International Limited
51 Midhurst Hill
Bexleyheath
Kent DA6 7NP
United Kingdom

Email: archway.international@btinternet.com

Registered in England No: 3831835

Published and Printed in Australia

A group of independent consultants specialising in cross cultural IT and Business projects

We're on the web

www.archway-international.com

E-Day. Getting Ready for the Euro

On 1st January 2002, seven new banknotes and 8 new coins will be introduced to the 12 member countries of the European Union. 50 billion of these coins and over 14 billion of these banknotes have been minted. We have even had the first "Euro Heist" of bullion!!

As the bulk of our readers will be from the Finance industry - it would be naive of us to even suggest that you are not fully prepared for the onslaught of this change - especially if you deal in the provision of "Legacy Currency Cash".

However - how about your customers? How successful have you been in convincing the die hards that their currencies will soon disappear - and have you been successful in converting all your wholesale customer's legacy currency accounts to Euros? Time is getting short - in addition (a common AIM theme) have you carried out the appropriate Operational Risk Assessments to ensure that this time of change is not going to open you up to fraud?

As a reminder - the key areas for focus will be:-

- Pricing Policies – conversion rules, rounding rules, adapting prices
- Financing – calculating and storing cash needs, withdrawal of national currencies, accounting requirements, reporting requirements, legal issues
- IT Requirements – reviewing your systems, point of sales equipment, vending hardware, auto tellers, the euro symbol
- Staff training.

The logistics of the changeover are huge with the billions of notes and coins to be distributed across the Eurozone nations - and in most countries, the national currencies will cease to be legal tender from February 2002. For more information visit www.ecb.com, the website of the European Central Bank.

(The participants : Belgium, Germany, Greece, Spain, France, Ireland, Italy, Luxembourg, The Netherlands, Austria, Portugal and Finland. Denmark, Sweden and the United Kingdom are members of the EU, but are not currently participating in the single currency.)

Liquid Assets

Here is a snippet to smile about sent to us by one of our Archway associates in South Africa.
If you had bought ZAR1000 worth of Dimension Data shares a year ago, the shares would be worth ZAR117 today.

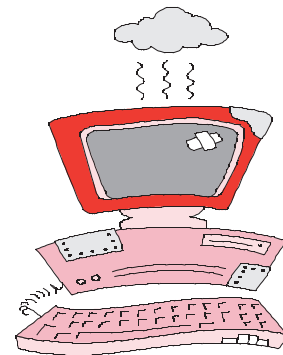
If, however, you had bought ZAR1000 worth of South African Brewery quarts of beer last year, drank them over the course of the year and kept the empties, the deposit on these bottles would be worth ZAR157 today. The moral of story is to remember the importance of liquid assets!



Archway International's mission is to raise the profile of process knowledge as core intellectual value in international organisations. Our objective is to advise and guide businesses through cross cultural process re-engineering and technology change.

Services include:

- * Managing the legacy systems trap and leveraging the power of internet technologies
- * Business process reengineering inception and management
- * IT and Operations Project Inception and Management
- * Operational Modelling
- * Designing and implementing Operational Risk and Control Processes
- * Applying technology to reengineer businesses *



"The e-mail is deadlier than the mail"



Archway International Magazine

Archway International

October 2001 Edition

As the dust settles

In the last edition of AIM, the issue of international terrorism was highlighted. What no-one realised was how prophetic this article was to be. Archway International extends its condolences to those who lost colleagues and loved ones in the American terrorist attacks. As the dust settles, literally, on the ruins of the World Trade Centre, it is becoming apparent that no-one is untouched by the tragedy. Stock markets have fallen, hotels are empty, and the effect on airlines is well reported. Even Hollywood has had to cancel movie releases.

Archway International clients and contractors will undoubtedly also be affected. Investment projects are likely to be cut as organisations spend money boosting public confidence. Perhaps management will direct investment to technologies such as video conferencing until the joint forces of collective forgetfulness and business demand drive people back to the skies. In the meantime, most companies will be dusting off their disaster recovery strategies (more about that later).

It is sad to reflect that, with the technological advancement mankind has made, evil cannot be eradicated. Previous editions of AIM have discussed the issue of security. As long as fanatics are prepared to die for their cause in suicide attacks, there is little that authorities can do to stop them. It is up to each of us to be diligent in both our corporate and personal security. Fire drills, baggage checks and identity checks may seem like a chore but are now, sadly, a necessary part of modern life.

No Longer Child's Play

Everyone, it seems, is getting into computer video games, and it's not just your nerdy high school kids. Recent USA polls conducted by the Interactive Digital Software Association (www.idsa.com) showed that 60% of Americans (145 million people) play video games with an average age of 28., 40% of the gamers are over 35.

The games industry is booming and apart from the popular traditional puzzle/board/card games such as online bridge or Scrabble, the games are becoming more & more complex and sophisticated – just as we increasingly imagine our lives as complex systems, with a lot of choices that can go in multiple directions.

As people spend more time at home, alone, chained to their computer screens they become detached from their traditional communities – but new cybercommunities are being created instead. Families and friends who live in different states or countries can play cribbage, golf, Pokemon or Quake together. And if you haven't got any friends, you can get some computer generated buddies by joining one of the adventure role playing games.

The games industry is also attracting the brightest and the best IT talent. The

DigiPen Institute of Technology in Washington State, offers a 4 year degree in Real Time Interactive Simulation. It's serious stuff. The curriculum includes Physics (to provide an understanding of the dynamics of moving bodies to achieve realism in simulation) and the Mathematics of Quaternions (the geometry of curves and hypersurfaces - apparently). The graduates are being headhunted by companies such as Nintendo, Dreamworks, Bioware and Microsoft before graduation. Where would you rather work if you were in the same position as these rising stars – maintaining accounting software isn't in the same league!

There is also a well publicised tussle on who will lead the way with the next-generation console system. Nintendo, Microsoft and Sony all have new product offerings. These systems will allow consumers to watch DVD movies, listen to CD's, connect to the Internet at high speeds and play games with feature film quality through one low-cost, easy-to-use system.

Video games on consoles alone is a \$15 billion industry and explosive growth is predicted over the next 5 years. No longer child's play.

Inside this issue:

**Project Management
AIM Crossword2**

**Business Continuity
and Disaster recovery
. 3**

E-Day 4



The Aftermath

IBM (www.ibm.com) got it's first recovery request 22 minutes after the first plane hit the World Trade Centre. It had about 1200 customers in the Ground Zero area and now has 3000 employees working on recovery efforts. Companies have set up temporary offices at their recovery centre and reports are that recovery plans (many set up for the millennium bug) work as expected.

Gartner (www.gartner.com) have prepared a special spotlight section on their website with comprehensive information to help enterprise decision makers manage Business Continuity Planning and Recovery.



Project Management

Risk and cost drive every IT and business reengineering decision. A recent, worrying trend finds Project Managers being dispensed with and their perceived activities assigned to other project staff in an attempt to reduce cost. Project Management is a recognised and respected profession. Practitioners are skilled communicators, negotiators, motivators and procurers. As mentioned previously in AIM, their job is to sell the benefits of a project and then deliver those benefits.

To do this they :

- Control scope, schedules and budget
- Manage stakeholders
- Procure resources
- Assure quality
- Mitigate risk and solve issues
- Communicate



But, buyers beware. When assigning a Project Manager make sure they are trained and experienced. The risks to the project of having an untrained/inexperienced Project Manager are nearly as great as having no one at all.

Management Mistakes

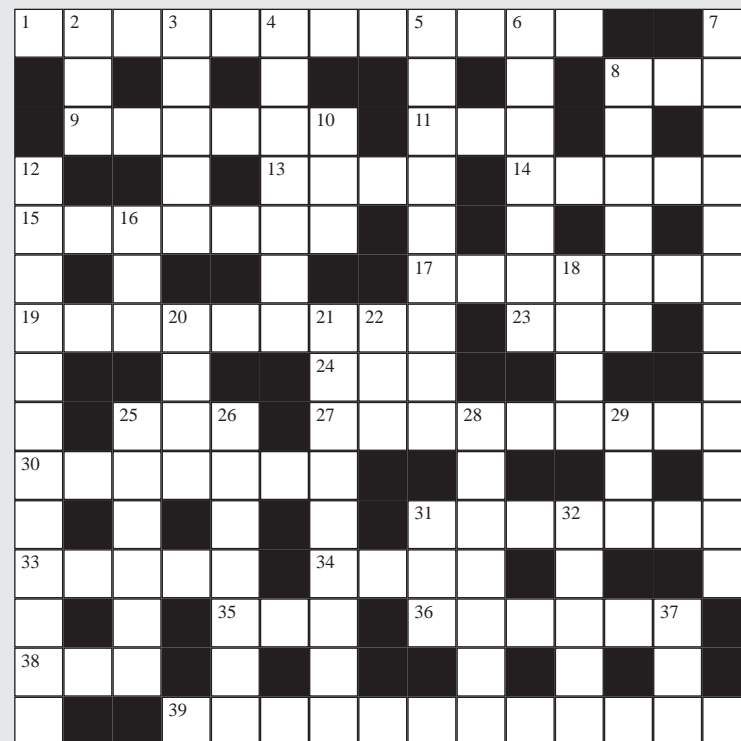
Found recently on a popular American website (www.msn.com), the 7 worst management mistakes.

- You flunk office Poli-Sci 101 (lack needed political skills)
- You want your employees to be carbon copies of yourself
- You fail to communicate
- You sprint out of the gate instead of pacing yourself
- You try to be Santa Claus to everyone
- You think getting there is good enough
- You're in a "glory daze" (missing that front line action)

ACROSS

1. Get going to tomb liaison (12)
8. 'ear about the time when (3)
9. Tell about being overdue (6)
11. Born in France (3)
13. What isn't odd (4)
14. The potato dish is in defrosting (5)
15. Gauge then sue mare (7)
17. A cut above any other doctor (7)
19. Lice sense they have been given authority (12)
23. Small mermaid in La Manche (3)
24. Want to know the answer to this one? Ask the National Register of Experts! (3)
25. A small-sized bit of pear (3)
27. Getting louder and louder (9)
30. Allows someone to get fitter (7)
31. Join bit of chain on cycle (7)
33. What a treasure kitty is! (5)
34. Look the same forwards and backwards (4)
35. Obtained reverse tog (3)
36. Saved by drapes (6)
38. Ten throw back haul (3)
39. Baton-waving activity (12)

The AIM Crossword



For answers visit our website www.archway-international.com

DOWN

2. Puts one in to row (3)
3. On islands I mix less (5)
4. Imprisons junior doctors (7)
5. State playwright (9)
6. Bowls too many weapons (7)
7. Cuts and airs toenails (12)
8. Get an egg if you're good on Friday (8)
10. First lady of the night (3)
12. Elf lamenting, we hear, when executing (12)
16. A bit of a curve (3)
18. He wears the trousers, we hear (4)
20. A gift from Eastern Energy and Electricity Board (4)
21. Secured in code (9)
22. Hesitate on the right side of caution (3)
25. Lose profit in remuneration (6)
26. Fast, or somehow legal (7)
28. Trim pooch a bit (7)
29. Ran around National Rivers Authority (3)
31. He has one letter less (3)
32. Of cherry liqueur, we hear in Russia (5)
37. Dorothy is short, period (3)



Disaster Recovery

As the term may suggest, it takes a disaster for anyone to place any importance on disaster recovery. Most of the time, DR plans remain at the bottom of the to-do list of managers with more profitable things on their mind. But when disaster strikes, all of a sudden budget and manpower are thrown at updating DR plans.

Therefore most readers will now probably have a DR plan awaiting review in their in-tray. This article aims to assist by giving an overview of disaster recovery strategy.

Before beginning work on a DR strategy, an organisation needs to carry out some sort of threat assessment. This is best done by considering the risk of something happening, along with the opportunity for it to happen. Risk can be assessed by asking questions like: is your business located in the centre of a major financial centre like London, Sydney or, needless to say, New York? Are you near an obvious terrorist target such as a government building? Is your business concerned with national security? Are you located in an area known for flooding? What is your building designed to withstand? Opportunity for disaster is concerned with the security measures surrounding your location. What would you do, for example, to deter a disgruntled employee from turning a gun on your staff, as happened in Switzerland recently with such tragic consequences?

It may be worth getting the local police to assist you with your threat assessment – what you deem to be high risk may not be in the grand scheme of things – or vice versa. They will also be able to advise you of the impact of any national threat – for example, at the moment general threat levels are higher with the likelihood of follow-up terrorist activity.

Conducting a threat assessment will enable you to direct appropriate resources to your DR strategy, which are always difficult to cost justify. Any DR strategy should cover four areas. Firstly, physical security. How will you ensure the safety of your staff in the event of fire/flood/bomb damage? Now is the time to practice fire drills – staff are likely to be very co-operative. After each practice drill, reviews should be carried out and lessons learned applied. For example, each floor/department should have fire wardens and first aiders, and someone should have responsibility for ensuring continuity should the fire wardens or first aiders move on. The local fire brigade will be able to help draw up robust evacuation procedures.

Secondly, technological security. Are your main computers housed in fire-proof locations? It is important to consider not only any mainframe computers, but network servers too, the smallest

of which may be home to a system that part of your organisation depends on. A multi-layered backup strategy for each key system, involving grandfather/father/son backups with at least one being stored off-site is necessary. A DR contract with a third party, who can recreate your systems at an alternative location, is a must for large organisations.

Thirdly, it is necessary for each business function to list its key processes, identifying which of those are essential for keeping the business running. It is those processes that will urgently need to be relocated to an alternative site in the event of a disaster. Any other processes can be suspended for a short period. Processes should be categorised according to when they need to be brought back on line – within 24 hours, 48 hours, a week, two weeks etc. (Any that can wait longer than that may not be necessary at all – opportunity for cost cutting?) Some thought will need to be given to the location of the alternative site. Suitable candidates include a nearby branch office or training centre. The site must be equipped with up to date systems so that it can be activated quickly – and such activation should be regularly tested. Perhaps some processes could be carried out by homeworkers, in which case staff's homes need to be equipped accordingly.

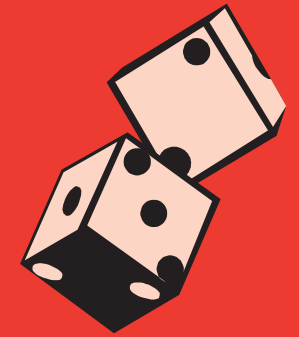
Fourthly, the logistics of managing the disaster need to be thought through in advance. A project team must be set up with responsibility for managing such tasks as evacuating the building, mobilising the alternative site, communicating with staff and, most importantly, handling the media.

Other matters to consider include the implementation of a clear desk policy so that sensitive documents do not end up on the pavement (as happened in the explosion at London's NatWest tower in 1993), and developing decision making hierarchies and contacts lists (one of our clients had to use the phone book to find their New York Managers so remember to keep this kind of information refreshed and readily available).

Having implemented your DR strategy, it is important to assign responsibility for keeping the plans up to date. This responsibility should include periodic walk-throughs, testing the plans against likely scenarios. This will highlight interdependencies and omissions that can then be included in the plans.

Finally, do remember to keep a copy of your DR plans off site. They will be important evidence of your diligence should any legal action be taken following a disaster. Also, it would be best embarrassing and at worst dangerous if they were one of the things destroyed in a disaster!

"Companies with comprehensive Business recovery and continuity plans, with input from both IT and business leaders are in the best position to survive"
Don deMarco - IBM



Take Action Now

Gartner (www.gartner.com) predict a significant increase in cyber attacks and have issued this checklist on what to do right now (in addition to jump-starting the Business Continuity Plan and mobilising the Crisis Management Team) :

- Increase the overall security posture
- Evaluate & test physical security
- Ensure that critical decision makers have multiple communication methods available to them
- Immediately update all systems with current security patches
- Update virus signatures more frequently
- Initiate vulnerability assessments
- Disable all inactive accounts
- Constantly monitor publicly accessible websites for security breaches
- Examine security practices for remote access
- Monitor security distribution lists
- Contact a managed security service provider if needed
- Educate users to be aware of an increase in cyberactivity
- Review external service providers security policies