

# e-Management Digest

A collection of management articles for the aspiring managers

October 2005

*This Management Digest is prepared for the aspiring managers as an update to what they already know. This newsletter is sent monthly to members of the Hong Kong Institute of Marketing and delegates following courses provided through Consort Management Consultants Ltd.*

BUSINESS SKILLS TRAINING

## Entrepreneurial Training

Entrepreneurial training is badly needed in Hong Kong to develop business skills and in-born creativity of young people.

It is amazing how innovative are the privileged few that enjoyed the fruits of such training. In one case, a doctorate candidate came up with an idea of selling a personalised novel. For a price of \$298, a customer can become the 'hero' of his own love story. Stories will be written around certain aspects of his fond memories and the show-off will bring him lots of pride among his friends and beloved. The 'producer' has been selling this concept since 2003 to more than 1000 customers around the world.

LiveWIRE is a non-profit making youth enterprise project aimed at providing entrepreneur training to young people like the doctoral candidate. It was founded by the Shell Group in 1982 and is now operating in 15 countries. Hong Kong LiveWire provides opportunities for participants to learn, conceptualise business ideas, acquire the necessary business skills for actually operating a business. Each stage of business



set-up is mentored by private enterprises through consultation, information sharing, training and counselling. Modern concepts of learning attach much importance to practice. The mission is: "Learn by Doing". It is in this area that LiveWIRE has succeeded.

LiveWIRE aims to promote business awareness to those between 18 and 35. Candidates have to be assessed before being accepted into the programme and for those successful, they will be supported by training, mentoring and counselling.

The value of this project is in providing valuable real life training to those interested to start a business. This training is practice based, but supplemented by four seminars and workshops a year on the basic skills and sharing of experience with others who had done this before.

There are a few other similar programmes in Hong Kong. The Trade & Industry Department operates a mentorship program to help SMEs, but this is for people who are already in a real business.



The HSBC Young Entrepreneur Awards aims to motivate young people to be entrepreneurial. It is an annual business plan writing competition for post-secondary students in Asia to display their creativity and business acumen. A one day training on

business operating and presentation skills is provided.

The Chartered Management Institute offers a formal course for non-business graduates. The Executive Diploma in Management offered at the Chinese University School of Continuing Studies is 9 months course which includes, at the end of it, a management simulation game in which students would form fictitious companies and run a business in competition.



More information from [www.shell-livewire.com.hk/home\\_eng.html](http://www.shell-livewire.com.hk/home_eng.html), [www.asiayea.com](http://www.asiayea.com), [www.scs.cuhk.edu.hk](http://www.scs.cuhk.edu.hk).

*K.M. Yim, Chairman, HKIM*

MANAGING TECHNOLOGY

## Data Security

How can businesses protect themselves from security flaws and weekly attacks of virus?

The first step is to understand why IT security must be constantly enhanced and up-graded to keep in line with the latest threats. Technology allows us greater access to data, information and technical tools allow us to increase our productivity, but they also increase our exposure to security threats. Virus infection, spoofing, spam and phishing are now commonplace so it is critical to have procedures to minimise such risks.

### *Security Audits and Reviews*

Security management is about finding the weakest link in the business. No matter how strong you think your security is today, unless you keep it updated against new risks, your protection level will diminish over time. Regular refresher security audits and reviews will keep you in pace with the ever changing

security issues, and enable additional and perhaps new concepts to be incorporated into your security protection and planning.

IT security audits alert both managers within companies to regularly assess whether current security plans needs improving to counter new threats. Such audits should also include a physical inspection of computer and associated equipment and also the software. This review can lead to updating the asset register.

The benefit of having reviews conducted by an outsider should not be underestimated. No matter how good are your internal IT security staff resources, unbiased assessments of systems are beneficial because an external review is independent and can often bring in valuable experience that comes from working with other companies' security practices. No matter how good you are, you cannot check your own work.

### *What to Look For?*

Every company's security audit will be different depending on the nature of the business and how IT is used within the organisation. The following areas are often the general items that are included in security audits, but your audit should not be limited to these.

- *Vulnerability Assessment*

This involves direct simulation of attacks and hacking attempts on your IT environment, normally your Internet communications, and allows weaknesses to be highlighted. Procedures to follow when you are being attacked should also be reviewed, as these will formulate planning against incursions.



▪ *Data Access*

Data access is less about security risk and more about constructing your data in a manner that will restrict access by unauthorised users. Part of this review should also look at the benefits of a centralised data storage system over local (normally on the user's PC or laptop) storage, and the associated risk of both loss of data and security 'break-in'. As a business you will often have to balance strong security procedures with usability.

▪ *Internet Access and Policies*

Most corporate Internet services are managed through firewall systems which 'filter' both incoming and outgoing communications. An audit should ensure your firewall systems are updated, the configuration is tuned to your corporate needs and there are easy alerts and logs available to your IT support team.

Policies regarding use of the Internet should be publicised to the staff. It is now becoming a standard in many companies to log all Internet activity and back up emails in a secure location.

▪ *Data Transmission*

When important data is transferred between two or more parties, methods to protect the communication, such as Secure Socket Layers (SSL) and data encryption should be used. Again, making sure users understand the company's policy for transmitting confidential data and how it is actually implemented, as well as reviewing the technical methods, should be part of any review.

▪ *Data Storage*

Managing the physical location of data, as well as who has access, is essential to data protection. Managing capacity planning, that is, assessing whether there is enough storage

space for data growth, as well as performance analysis of the disks and how the data are protected from disk failures, needs to be understood, tailored to your needs, documented and reviewed periodically.

▪ *Virus Management*

Virus management is a reactionary process. Make sure the corporate virus database is updated regularly, perhaps automatically. Ensuring that regular scans of your business systems are run, together with an easy alarm system to report problems will allow your IT staff to react to infections quickly and hopefully reduce any disruption or data loss.

Users should be educated about keeping good e-mail management skills, and how to detect a possible virus infection.

▪ *Backups*

Backup systems are normally the last line of defence when dealing with lost, corrupted or deleted data. Unfortunately, they are often seen as a one-off set up which can be left to run itself. This unfortunately is not the case - when backup data has to be called for, the value of good backup maintenance quickly comes to light.

**OFFICE EMBARRASMENTS**

In a survey by Post-it®, the following incidents make office workers blush – whether they are sitting in an office or using software by the same name.

Forwarding an e-mail to the wrong person	78%
Getting a colleague's or client's name wrong in a meeting	66%
Spell-check resulting in the wrong word	64%
Accidentally deleting a document	57%
Being caught e-gossiping about a colleague	46%
Not attaching a document to an e-mail	39%
Being drunk at an office party or night out	28%
Replying to 'Reply All' rather than just 'Reply' in an e-mail	27%
An inappropriate crush on a colleague	25%
Tripping over or stumbling while making a presentation	18%

(Adapted from *Professional Manager*, July 2005)



Backup systems need to be reviewed constantly to maximise their reliability. Data recovery procedures need to be practised regularly and the management authorisation method to confirm what data needs to be restored should be clearly documented.

It is also important to test your data restoration systems regularly to make sure the procedures and the data verification process work well. Location where backup media are stored should be known – always remembering that live data should be kept off-site in a secure fireproof location and with restricted access.

- *Disposal of Sensitive Data*  
Leaving confidential payroll documents on an old computer that is re-allocated to a new task is unfortunate, having business details left on a thrown away scrapped computer is disastrous. Easy-to-understand policies on the destruction of data, re-allocation of computers and the disposal of old computer equipment should be implemented.

#### *Compliance with Data Protection Regulations*

Jurisdictions around the world differ in the strictness of their data protection legislation, but enabling your security reporting procedures to conform to local legislation will ensure your business is operating within the confines of the law.

Businesses should actually look beyond the law. Business associations and professional bodies publish best practice guides and these guides will often assist businesses in setting up data security guidelines and hints as to the areas where you may be most susceptible to a security incursion.

#### *Ongoing Reviews*

Once a security plan has been implemented, it is important to maintain a calendar for regular reviews and emergency procedures should a new threat occur. There should also be a task force (usually one member of management and one member of IT) to keep the organisation up to date with industry security changes and emerging technologies to be on the look out for new risks that come to light as well as new solutions to old problems.

Making sure that security is a priority issue at the management level is the real task. Understanding corporate risk and making informed decisions on what level of security your business needs, and how often you need to review your plans is the tough job. However, managers should realise that trying to fix a system once it is broken is not a place you want to be; the goal is preventative security maintenance.

*(Adapted from Company Secretary, June 2005)*

ENGLISH

## Words Worth

WRONG	RIGHT
<p>× I took <b>a course of</b> computer last year</p>	<p>✓ I took a computer course last year. ✓ I took <b>a course in</b> computers last year.</p>
<p><i>When 'course' refers to a process, time or direction, we use 'a course of', e.g. in the course of study, When we <u>describe</u> a programme of study, we say 'a course in'.</i></p>	
<p>× After considering a number of factors, <b>at last</b> I decided to .....</p> <p>× After doing a lot of research, <b>at last</b> we wrote the report.</p>	<p>✓ After considering a number of factors, <b>finally</b>, I decided to .....</p> <p>✓ After doing a lot of research, <b>finally</b> we wrote the report</p>
<p>'At last' refers to time only, 'Finally' refers to time or sequence. When you chose something out of many, you refer to sequence, so 'finally' is the word to use. The following sentence refers to 'after a long time' so 'At last' or 'finally' can be used. 'She took a long time to find the job. <b>At last</b> she found one ....'</p>	

