August 2010, Issue No. 31

SOCIETY OF ACTUARIES Entrepreneurial Actuaries Section

THE INDEPENDENT CONSULTANT

CONTENTS

Information Technology—A Double-Edged Sword

by Andrew Chan

Technology has transformed the way we do business. We can make timely, informed decisions by extracting meaningful business information from a multitude of recorded data, literally in seconds. We can improve our customer satisfaction by automating the order processes and letting our customers check their online status. We can also discuss marketing plans with our global business partners through Web conferencing and other collaboration software.

However, information technology is a two-edged sword. It can seriously damage your business if you don't handle it properly.

IT Security

IT security awareness has been significantly improved over the last five years. However, most IT security strategies are still very primitive and only include installing anti-virus software and a firewall. Let me share a few stories with you to illustrate my point.

Too Many User Rights

A client asked me to investigate why the computers in his office were getting slower and slower. During my investigation, I noticed that the security software on some of the machines was disabled because the users wanted to speed up the machine. The question is, "How can security software protect the PC if you've turned it off"?

Data Encryption

Some employees work from a home office from time to time and need to access data with their office computer. They use laptops and USB drives. Unfortunately, most of these methods are not protected against accidental loss or computer theft. What would happen if your employees

ENTREPRENEURIAL ACTUARIES SECTION

SOA Staff

OTHER SITES OF INTEREST

lost their laptops or USB drives? Some clients told me that all their laptops were password-protected and no one could access the data without a password. I proved otherwise in just a few minutes!

Remote Connection

If you allow your staff to access data in your office via remote desktop or other file sharing software, you open a door of uncertainty. Do you know what computers they are going to use? Are their home computers secured? Is your staff only using home computers? They may work on computers in a public library while they take their kids to swimming lessons. The bottom line is someone else may already have their user IDs and passwords if you allow them to remotely log in to office computers.

Security Patch

If you read the Symantec Global Internet Security Report, you would be surprised to see how many software security vulnerabilities exist. The good news is that software vendors are usually able to fix problems with a patch. Installation, however, is your responsibility. When was the last time you installed any security patch? How about your security software? How old is your virus and spyware definition file? There are new viruses and spyware programs being introduced every day. How can the security software protect your computers if you are still using a two-year old virus and spyware definition file?

Online Presence

Most marketing professionals suggest you should use social media sites to increase your visibility — LinkedIn, Facebook and Twitter among them. Certainly, social media sites can reach out to your client, improve your branding and collect market intelligence. Another positive result is you can expand your client data base. Before you relax and enjoy the rewards, please read David Airey's story. David is a brand designer and his website got hijacked. I heard similar stories about other social networks. If you don't keep your user ID and password safe, someone may take control of your account. The damage can be huge.

Servers

If you are hosting your own file server, Web server or e-mail server, the security issue can get much more complicated because all your critical business data is stored in the servers. Imagine if someone hacked into your e-mail server and sent inappropriate literature to your entire database? Smartphone

Do you know that your smartphone is actually a very powerful computer and it also contains some sensitive business information? How do you safeguard it? I did an informal survey at a networking event; over 70 percent of individuals in the group had smartphones, but less than 20 percent had them password protected or locked. I hope they never lose

their phones!

A proper security strategy is not just about technology; it should include processes and people. You are naïve if you believe that only installing current security hardware and software is sufficient. I sincerely hope you change your mind after reading my article. And if I fail to convince you of the need for a properly planned and implemented security strategy, you may want to read about the recent cyber-attack on Google. Google has invested a lot of resources on IT security but all the hacker need is one single unpatched computer.

Business Continuity Planning (BCP)

I am an IT consultant, not an insurance broker, but if your office is hit by a natural disaster (e.g., fire, flood or tornadoes), would you not be happy that you were covered by insurance? However, insurance companies do not guarantee the continual operation of certain critical business processes. You have to have your own business continuity planning to cover the risks. Since most offices are heavily reliant on computers, IT should be a critical component in your business continuity planning.

What is Business Continuity Planning?
BCP is not disaster recovery planning (DRP). DRP recovers Information Technology (IT) assets after a disastrous interruption; it does not prohibit a stoppage in critical operations. BCP proactively ensures critical services to be continually delivered to clients.

BCP includes:

- Identification and prioritization of necessary resources to support continuity of critical business processes.
- Plans, implementations, control and tests to ensure the continuous delivery of critical services.

Why Do We Need Business Continuity Planning?
Every organization is at risk from potential disasters that are high impact but low probability. BCP can lower the cost of disruption and enhances an organization's image with your clients by demonstrating a proactive attitude. During the course of conducting BCP, we normally find additional benefits including a better understanding of business operations, improvement in overall organizational efficiency and identifying the key personnel, business partners and financial resources to critical services and deliverables.

How to Create a Business Continuity Planning
Every BCP is unique, but generally development involves six steps:

- Get management buy-in. You would be surprised how difficult

this can be. Management understands the impact can be high, but most of them argue the probability is extremely low. Good luck to them!

- Build a BCP Committee which is comprised of the sponsor, BCP coordinator, and key personnel from IT, operations, security, and finance.
- Identify risks, critical services and their dependencies; prioritize them; and identify internal and external impacts of disruptions.
- After the analysis, it is time to prepare detailed procedures and arrangements to ensure continuity. The pros and cons of each possible option for the plan should be considered, keeping cost, flexibility, minimum level of critical services and the probability of risks in mind. For each critical service, choose the most realistic and effective options when creating the overall plan.
- A lot of companies stop after planning. BCP is not just about planning; you have to implement it, train your staff what to do in the event of a disaster, and have frequent trainingsessions to achieve and maintain high levels of competence and readiness. How often do you have fire drills in your office?
- BCP is a living process and it will evolve with your business and its external environments; for example, a lot of companies in Toronto downtown are reviewing their BCP to prepare for the G20 meeting. Continuous appraisal of the BCP is essential to maintaining its effectiveness.

BCP is not free! However if critical services cannot be delivered, then consequences can be severe and the potential damage can be huge. We are all at risk and face potential disaster. A Business Continuity Plan is an insurance to make sure your business can continuously deliver critical services despite disruption.

IT Management

Management 101 – you either manage it or it would manage you. A lot of small business owners do not have any IT management so they let their IT take control; here are a few example of what the problems could be:

- *Desktop environment is not standardized*. I have noticed a lot of small business offices have machines from Acer, Asus, Dell, HP; and have a full spectrum of Microsoft Office, e.g. 2000, XP, 2003, 2007 and soon 2010. They purchased PCs from local computer store and the decision is normally driven by the price. It is just chaos and costly to support such IT infrastructure! By standardizing desktop hardware and software, organizations can

ultimately save money and advance toward a more flexible, agile and optimized infrastructure.

- *They don't manage the users*. Their users can install anything they want, configure whatever they feel fit (including disabling antivirus software), or even download illegal movies/ music. I did a software inventory audit for one of my clients and I found over 500 software titles installed on three different machines that I randomly selected. You may also want to find out how much Internet usage is used for downloading music or watching YouTube.

- *No training is provided*. Most users are still using very basic functions; e.g., they have all their e-mail in their inboxex because they don't know how to create new folders or use a macro to automatically filter the e-mail. Proper training can definitely increase the productivity in your office; however, it is very difficult to train your employees if they are using different versions of Excel.

Conclusion

What I described here in this article is only the tip of iceberg! If you ask an IT consultant to do an audit on your IT infrastructure, processes and usage, you may find out how lucky you are that you don't have any major issues. IT is a very powerful tool and you may be enjoying the benefits that it offers but if you don't manage it carefully and professionally, then it can bite you badly soon or later. Use IT wisely!

Andrew Chan, ASA, is an IT solutions consultant for ALG, Inc. He may be reached at chan_a@algconsultings.com.