Cyber threat – this year's top IT risks (part 1)

Is your computer really safe from cyber crime? Bernard Collin, CEO of SafeComs, has compiled this year's top ten major IT security and business risks and the best ways to prevent them. This month we offer the first three

■ IT'S the Year of the Ox and the astrologers tell us we can gain prosperity through fortitude and hard work. Given the global economic forecast for the coming year, it looks like we are all going to need ample quantities of both. Expect cybercrime to surge, expect Thai authorities to step up their crack down on copyright violations, hackers to create new and ingenious viruses, and your competitors to be looking for ways to control costs and retain customers. If that doesn't sound too promising, remember what Winston Churchill said: "A pessimist sees the difficulty in every opportunity, an optimist sees the opportunity in every difficulty."

With that thought firmly in mind, here are a few of the IT security and business risks for 2009 and the opportunities that come with them. Look out for part 2 in next month's BigChilli.

1. The Risk: Business Software Alliance crack down on unlicensed software

President Barack Obama is going to leave no stone unturned in his efforts to revive the American economy. Expect increased enforcement of copyright laws to be one of those stones. Thailand already has the enforcement mechanism Obama needs: the Business Software Alliance or BSA. This is not the typical 'window dressing' agency set up for the sake of appearances. The BSA has got the full support of the Thai authorities and they had an exceptional success rate in 2008.

For the BSA, 'success' is measured by the number of companies they bust and the amount of fines they collect. The reward to an individual reporting on a company using pirated software is now 500,000 Baht. In 2009, we are going to see a lot of layoffs and cutbacks, which

Bernard Collin, CEO of SafeComs

means a lot of very unhappy people who could use half a million Baht. I expect the BSA will be getting a lot more anonymous reports in 2009.

The problem with pirate software is that many managers are either unaware of the level of illegal software floating around on their systems or they underestimate the risk.

The Opportunity: Get legal, look at Open Source

A time of slow business activity is the perfect opportunity to do a software audit. This way you gain a full report on exactly what software is running on your systems, its legal status, and its productivity in terms of performing the tasks it is supposed to be doing. This is also a great time to explore the many benefits of Open Source software. You'll find details of SafeComs' audit service on our official website.

2. The Risk: Money and data theft through virus infection

Complacency is the big risk in 2009. It's been fairly quiet on the virus front over the past couple of years. Everyone is happily surfing the net and chatting with friends and feeling quite confident they are safe from infection.

Up until a few years ago, a hacker's main objective was fame and glory within the hacker community. Hacking is now organized crime controlled by big international syndicates and they are hiring talent.

The total value of cybercrime now exceeds the revenue from drugs and other traditional criminal activities. At SafeComs, we've seen a dramatic increase in the number of professionally designed threats like key-loggers and Trojans as well as an increased capability at remaining undetected.

The criminal hacker's objective is to silently infect a PC or network and use it to attack other systems or to steal identity and banking details. The most desirable targets: companies using illegal software. With unlicensed copies, you have no way to apply security patches or update your antivirus programs.

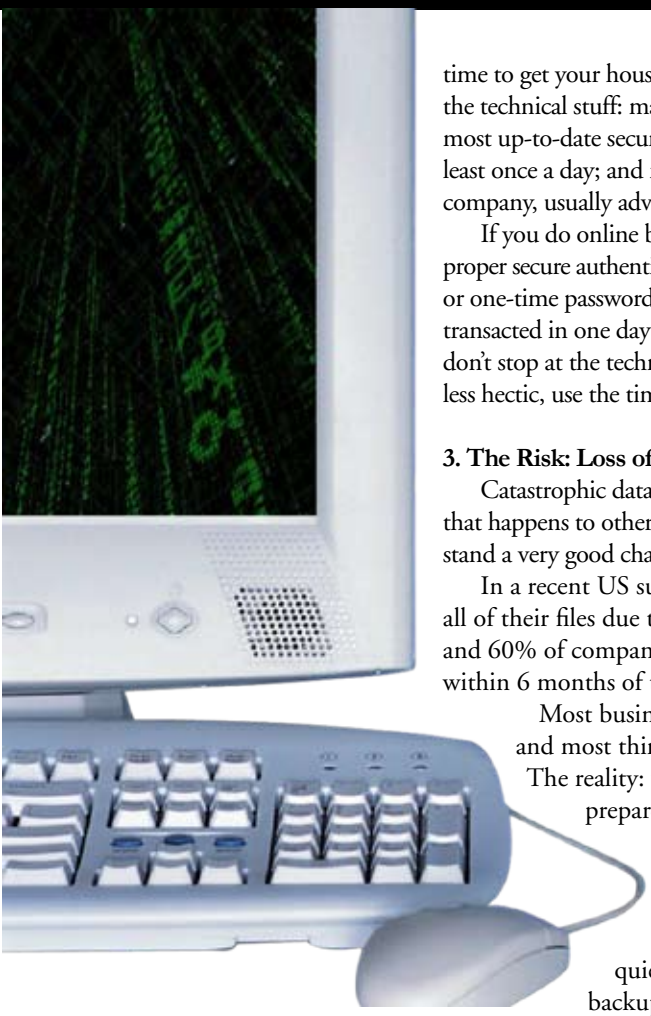
We did a quick and dirty survey once. We bought a few dozen pirate software packages at a well known location in Bangkok. One in three contained a virus, trojan or keylogger designed to infect whatever system it was installed on.

The Opportunity: Learn to protect your systems and put safety measures in place

Use this downtime to educate yourself and your staff so everyone understands the dangers and enforce strict penalties for staff who break the rules.

The steps required to protect your own PC or laptop or your company network are actually not that difficult. You can find lists of dos and don'ts on many websites and antivirus and firewall software is pretty cheap these days. People are the weak link. A very good rule of thumb is that if it sounds too good to be true, it is. That seems so obvious, but people are still falling for the Nigerian scam.

A slow business cycle is the perfect



time to get your house in order in terms of security. Do all the technical stuff: make sure your computers have all the most up-to-date security patches; update your antivirus at least once a day; and run a virus check from an outside AV company, usually advertised as a free online AV test.

If you do online banking, make sure your bank has proper secure authentication system (2-factor authentication or one-time password), or limit the amount that can be transacted in one day and check your balance daily. But don't stop at the technical fixes. Now that things are a bit less hectic, use the time to educate yourself and your staff.

3. The Risk: Loss of personal or company data

Catastrophic data loss is generally seen as something that happens to other people. Statistics indicate that you stand a very good chance of being the next 'other person'.

In a recent US survey, 30% of PC users had lost all of their files due to events beyond their control, and 60% of companies that lost their data shut down within 6 months of the loss event.

Most business owners are aware of the risk and most think they have backup under control. The reality: very few companies are adequately prepared for even minor data loss events.

The Opportunity: Upgrade your backup system

Use this period of relative quiet to review and revamp your data backup system. I recommend first sitting down with your management team and identifying essential company data. What data could you not afford to be without for even a day? Most of that will be financial and customer data, but it depends on the nature of your business.

The most appropriate choice of hardware and software will depend on the volume of data your company generates. For a small business that could mean something as simple as an external hard drive. If your business uses 25 to 100 computers, you are probably looking at more sophisticated tape drive or real-time systems that can cost hundreds of thousands of Baht to install and maintain.

The ongoing maintenance costs, including dedicated personnel, can be substantial. Also look into outsourcing your data backup.

Useful links:

SafeComs: www.safecoms.com

SafeComs is a Bangkok based company specializing in network security for computer systems and for unique security solutions delivered over the Internet. SafeComs can provide Internet security audits, license legalization audits, critical backup solutions and anti-spam services.