ACCIDENTS and disasters often strike when you least expect them, that's why it's wise to take precautions to minimise risks of facing either occurrence.

Drive extra careful on a rainy day, take all necessary shots before you visit a foreign country, and don't place that cookie jar on your lap when you're watching Hari Raya programmes on television. Attacks on information systems, like accidents and disasters, can happen anytime to any organisation. While enterprises are largely aware of threats such as virus, worms and malicious codes to their information systems, and taking relevant measures to address them, similar enthusiasm tend to be lacking among small and medium-sized businesses (SMBs).

The situation can turn more serious as threats to information systems get more sophisticated. When prior attacks mainly occur at the network layer, today's attacks increasingly happen at the application layer. Malicious codes, for example, are more content-based and carefully hidden at the application layer.

Cost is often quoted yet it is not the only reason why SMBs do not properly protect their information systems. There are other reasons SMBs overlook information security, and the more recurring one has got to do with perception.

"I am such a small company, why would anyone attack my business." Thinking along this line, an SMB would thus not place information security as a priority business concern that merits investment. Even among SMBs that view information security as important, many are lacking the basic anti-virus software.

Another misleading perception is that security solutions are difficult to install and maintain, and thus would drain the already limited information technology resources of an SMB, according to Sonicwall, which provides integrated network security solutions catered to SMBs.

These are the facts - attacks on information systems are on the rise and can happen to any organisation - big or small, and protecting one's information systems can easily be done by state-of-the-art security solutions available today. Apart from putting aside bonus allocation for their employees to celebrate the coming festivities, maybe it's time SMBs seriously shop for security solutions for their information systems.
A4.1 From the reading and lessons in our class, in general what are the main security issues and different modes of security breaches on information systems (IS)?

ANSWER

The main security issues for information systems in general comprise:

(1) **Information Theft**

Information theft can happen through many ways ranging from improper protection during unattended use of the computer (e.g. leaving the computer display on), password theft, weak passwords, critical business software applications not properly configured for specific personnel access, software application design weaknesses, poorly designed network infrastructure, network packet ‘sniffing’ activities, ‘spoofing’ i.e. by establishing external fraud sites that appear like legitimate sites (i.e. appearing as internal) to the network of the organization, unencrypted messages and information on the network, to many more. The sources of information theft and the breaches can be both internal and external to the organization.

(2) **Internal/External Intrusions and Malicious Attacks**

The types and modes of security breaches and attacks range from viruses (or malicious executable code that can cause havoc immediately, doing all kinds of destruction), Trojans (attached, disguised and hidden behind normal applications or files for future intruder entry), logic or time bombs (malicious codes that are set to execute at a specific date and time, or a specific event), worms (virus type codes that copies itself from machine to machine) and DOS (Denial-Of-Service attacks or simultaneous invasion of many accesses sent repeatedly to the servers and bringing down the network to a crawl or sometimes complete stop) to the many more names (with disastrous and undesirable effects) that we may not know.

A4.2 What would be your strategy in advising small and medium businesses (SMB) to change their perceptions regarding security issues of their IS/IT?

ANSWER

The strategy in advising SMB with regards to the importance of securing their information systems (IS/IT) involves educating and convincing them on protecting “information” as assets of high value and critical to the sustenance of their businesses.

An SMB must be convinced in spending its money’s worth (up to a reasonable and affordable amount) balancing the risks against the loss of “information assets”, and that may go further to possibly crippling or halting its business operations altogether.

(1) **Protection strategy**

There is no known foolproof or 100% protection for intrusions and malicious attacks on computer networks and information systems. Attackers will always find new ways to go around security flaws, holes or gaps. However, there are reasonable protection
methods for common types of attacks, using for example, a firewall mechanism (hardware or software types). You can choose a single layer or multiple layer firewalls or a combination of hardware and software firewalls.

(2) **Prevention strategy**  
Install anti-virus software and regularly update virus definition files, install operating system updates and application patches and fixes regularly, close certain well known service ports for software applications, using specialized software conduct content screening and filtering, spam filtering, spyware filtering, cookie blocking, removal and many more. Whether, being attacked or being hit by a virus or not, there is also the issue of regular backup of important business information and its on-site and off-site storage that has to be acted upon.

(3) **Monitoring and control strategy**  
Introduce a policy like “Computer and Network Usage” policy for the business, teach employees in the techniques of selection and protection of passwords, educate users on how to treat suspicious mails especially those with attachments, mails from unknown senders, monitor network packets on incoming and outgoing patterns – sites, frequency and bandwidth usage, monitor suspicious usage patterns, limit and control the types of applications your employees can have on the computers that is connected to the business network, and many more.

**At the first level**, the advice to an SMB organization on basic security is to implement the simplest of the things that can be done first at no cost, i.e. introduce a policy, inculcate good user habits, passwords security, local anti-virus scanning regularly, update security patches and fixes for the operating systems and applications regularly, make sure applications are configured at the correct security levels, implement the right security protections that come built-in with most application programs, monitor user habits, etc.

**At the second level**, install adequate anti-virus protection software for both the network and scanning of viruses of incoming and outgoing e-mail attachments. Ensure that the protection software is updated with the latest virus definition files. Turn on the automatic updates where available.

**At the third level**, hire a consultant or security expert to conduct a security audit of the business and provide advice on the appropriate protection strategies. Usually, a study will be conducted on the network and its applications, sometimes including executing a mock-up intrusion and penetration test into the network, before a recommendation is made on the best way execute the security implementation.

At what level an SMB should spend its money for its information security depends on how much the SMB values its own “information assets”, costs on the damages, loss of time, loss of information and its seriousness, if it happens, and the impact on the disaster recovery and likelihood of being able to go back to conducting its normal business at the usual level again. Some protection is certainly better than no protection. Most of all money for security like any other investments in business can be increased gradually.