In most of the large corporates, PSUs and government organisations, a dedicated information and data security department acts under the IT department or separately. This becomes an integral part of the respected business operations as secure computing has been recognised as a most important aspect of business processes.

There are several security tools that are available for safeguarding the day to day business computing. But with the growth of threats and maturity of threats, it becomes very important to evaluate newer security tools in order to utilise their strength for the business operations. But who does all this hunting for the small and midsized businesses.

Unfortunately, many small and midsized businesses fail to take advantage of security tools that are available and become vulnerable.

On such technology is -- encryption technology. Most of the business owners especially with less expertise on information security used to stay away from this technology, fearing that it's too complex and difficult to use on a routine basis. In reality, encrypting vital data isn't much more difficult than running a virus scanner or a data-backup program.

Knowing Encryption

However, from the technological perspective, encryption technologies include very simple backend process. There are few things that needed to be kept in mind while installing the encryption.

There are two basic ways to encrypt data. One approach is to use asymmetric PKI (public-key

infrastructure) encryption. PKI cryptography is based on a pair of cryptographic keys: One is private and known only to the user, while the other is public and known to the opposite party in any exchange.

PKI technology provides privacy and confidentiality, access control, proof of document transmission, and document archiving and retrieval support. While most security vendors currently incorporate some type of PKI technology into their software, differences in design and implementation prevent interoperability between products.

The other method of encrypting data is symmetric key protection, also known as "secret-key" encryption. Generally speedier yet less secure than PKI, symmetric encryption uses the same key to both encrypt and decrypt messages. Symmetric technology works best when key distribution is restricted to a limited number of trusted individuals. Since symmetric encryption can be fairly easy to break, it's primarily used for safeguarding relatively unimportant information or material that only has to be protected for a short period of time.

Applying Encryption

The easiest way to use encryption is to purchase a business application or a hardware product that incorporates some form of encryption technology. Microsoft's Outlook Express email client, for example, provides built-in encryption support. Meanwhile, vendors such as Seagate Technology LLC and Hitachi Ltd. have started incorporating encryption technology into their hard drives.

Since most software applications and hardware products don't include any type of internal encryption technology, business owners and managers need to look for stand-alone encryption products. This can be a confusing process, one that's best approached by first determining the business's precise security requirements, then finding an encryption product that fits each need.

Microsoft Vista Enterprise and Ultimate users can take advantage of BitLocker Drive Encryption, a full disk tool that offers powerful 1024-bit encryption. Another Windows offering is EFS (Encrypting File System), which uses symmetrical PKI technology to provide file encryption. Beyond Microsoft, leading encryption vendors and products include PGP, open-source TrueCrypt, DESlock+, Namo FileLock and T3 Basic Security.

Setting Encryption Policy

From how do you know to what to encrypt? to start with here are some vulnerable computing interfaces that needs to be encrypted..

Laptops/Handheld devices: Unlike office systems, laptops are easy to lose and are prone to casual theft. By ensuring that the system's data content is unreadable, a business can limit its loss to the cost of the laptop. An industry report mentioned that one out of ten laptops either got stolen or loss. In either ways, threat of losing the data becomes the top reason to worry. However, a growing number of government regulators and insurance companies are demanding that businesses encrypt any data that leaves their premises.

Hard Drives: Data theft is a big issue. Any business may choose to encrypt the hard drives as a way to reduce or eliminate data theft. Encrypting the complete hard drive can make the life easier but it also holds some limitation.

Removable drives/external drives/ USBs: Memory sticks, thumb drives and similar portable storage technologies provide portability, convenience, and an opportunity for data loss and theft. As with laptops, encryption limits a business's loss to the cost of the device itself. A growing number of removable-media devices come with built-in encryption support.

Individual Files and Folders: In cases where full disk encryption is overkill, file-by-file encryption provides added security on an "as-needed" basis. Many available encryption products offer drag-and-drop encryption capabilities.

Email: Encrypted email is kept secure during the transmission process and while sitting in its recipient's mailbox.

Encryption's Limitations

Like any technology, encryption software isn't perfect, it also has some limitation. Even the best products consume both processor speed and storage space. But even the bigger problem is the fact that users can also lose or forget passwords, thereby potentially locking systems forever.

However, it is also advised that before purchasing any encryption tool, one has to carefully research the product. Make sure that the offering addresses your company's needs, is compatible with your systems and has a good track record concerning reliability and support. If possible, check with your friends and colleagues for their opinions on various encryption tools.

However, the way we expanded our computing horizon, the threats of losing computing data has also gone far advanced. Level of threat have gone up, so as the need to prepare ourselves in order to safe guard the data.