Data Security– Few Aspects for the CA

Inadequate protection of both Information assets and Information System assets leaves any organisation vulnerable to computer crimes and can have catastrophic consequences, particularly when confidentiality is involved. This article discusses various aspects of data security from the professional perspective and also some of the measures that can reduce the risk of leakage of data.

The information asset is the organisational data while the Information System asset comprises the mediums and devices of storage, processing and communications. Inadequate protection of both these assets leaves any organisation vulnerable to computer crimes and can have catastrophic consequences, particularly when confidentiality is involved.

What is Data Security?

Webster's Dictionary for everyday use defines data as things known and from which inferences may be deduced. We all understand the importance of data. Whether it is the backup of accounts in Tally or other accounting software or that of important information relating to our clients in Excel and Word files, all are very important for us. But the problem is that generally we become complacent and do not even take periodic backups on CDs, tapes, etc. The result, at times is catastrophic. Loss of valuable data proves very costly in terms of money, effort and reputation. That is why all big corporates, banks, etc., have set up or are in the process of setting up Disaster Recovery and Business Continuity Sites.

Data Privacy and Data Protection

Many advanced nations have enacted legislations concerning "Data Privacy". These often take the form of prohibiting release of medical or other information to third parties without a court order. Regulatory bodies also require restriction on dissemination of data collected by certain industries, notably banks and financial services. The Britain's Data Protection Act, 1988, for example, is not limited specifically to data held electronically: it applies to all personal information held in "relevant filing systems", which may be in any medium (paper, database, spreadsheet, word-processing folder, etc.). The criteria for whether something is a "filing system" in the terms of the Act relate to whether the information is held in a structured way and indexed by individual identifiers. In essence, any file held specifically by a particular individual should now be regarded as subject to the legislation. There is an emphasis on giving data subjects advance notification about the data being collected and what will be done with it (how it is to be 'processed'). In this context, data subjects must have the opportunity to consent to the collection and processing of their data. That consent should be informed, given freely, (wherever possible) be obtained explicitly and in advance. There are "Fair Processing" principles. The personal data that is collected and processed must be for specified, explicit and legal purposes, and the data held must be accurate and relevant. Personal data must be kept secure, up-to-date and not longer than actually necessary. There are strict controls on the processing of 'sensitive personal data' (i.e. race, ethnicity, gender, health), even where it is processed only for research purposes.

The Act also prescribes compliance audits. The objectives of data protection compliance audits go beyond the basic requirements of

— CA. Keyur N. Parmar

(The author is a member of the Institute. He can be reached at cakeyurparmar@gmail.com)

say Data Security and address wider aspects of data protection including the mechanisms for ensuring that information is obtained and processed fairly, lawfully and properly. Quality Assurance ensures that information is accurate, complete, up-to-date, adequate, relevant and not excessive.

Integrity, Availability and Confidentiality

In the area of information security, integrity is often defined more narrowly as having two facets: Data Integrity and System Integrity.

Data Integrity is the requirement that information and programmes are changed only in a specified and authorised manner.

System Integrity is the requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation.

Availability is the requirement intended to assure that systems work promptly and service is not denied to authorised users.

Confidentiality is the requirement that private or confidential information is not disclosed to unauthorised individuals.

Data Classification

Access Controls enable authorised users or processes (commonly referred to as the subjects) gain access to Information and Information System ("IS") assets or resources (commonly referred to as objects). Different kinds of IS assets may require different degrees of access controls. Further, within an asset (say, a database), different elements or components of the asset (individual fields or records meeting a certain criteria) may require more stringent controls. For example, a bank manager may have rights to modify the borrower's database with regard to credit limit of a borrower but not have access to modify cash transactions in the cash database. Hence information and computer processes, in an organisation, may have different degrees of criticality. Information system resources may require be classified or categorised according to their sensitivity. This would depend upon the risks affecting such resources and impact resulting from exposure. Such classification makes for administrative convenience of implementing and maintaining access control systems and importantly optimising the cost of security.

Some information is more critical to a business than others such as production process information, formulas, strategic plans and research information. In the financial services industry, for example, information assets are very close to being financial assets. The loss of such information can jeopardise the existence of the business or create loss of goodwill and trust among stakeholders besides the loss of brand equity. Compared to this, the organisation may also have information, which is of less consequence, such as a list of customers, details of employees' pay, etc. Thus, in order to ensure cost-effective controls, it is beneficial to classify the entire organisational information. This also enables fine-tuning of access control mechanisms and avoids the cost of over-protecting and under-protecting information. IS resource classification also helps in determining the degree of access to be authorised to a user with regard to various classes of resources rather than the tedious task of assessing the extent of access in respect of every IS resource. For example, access to production or live programmes and data should be restricted to a limited set of users. Similarly, access to test data and programmes in the development area, must be restricted to identified group of programmers and analysts. The scheme of classification may vary depending on the type of organisation. However, some standard or popular classifications are also available.

Assuming that we have taken necessary steps for keeping backup of data, the next step is security of data. This is basically a question of access control, i.e., who all are authorised to read, write or manipulate data in any manner. Is

all data of equal importance? Obviously not. The data of sales for a quarter for Coca Cola Co., till it is published is sensitive information and can be used by punters to play in the share market. However, once this data is published, it is public information and there is nothing to hide about it. What about the formula for preparation of Coke? It is highly confidential and is a supreme example of one of the best-kept business secrets. Different types of data require different levels of security. Data classification determines how data will be managed, retained, archived and disposed of. There can be no one type of classification. It differs from organisation to organisation or person to person.

A usually accepted type of classification of data on the basis of its importance is as under:

(a) Top Secret: This indicates the highest classification wherein the compromise of the confidentiality, integrity and availability can endanger the existence of the organisation. Access to such information may be restricted to either a few named individuals in the organisation or to a set of identified individuals. Information in this category is strategic to the survival of the organisation. Unauthorised disclosure could cause severe damage to the organisation and stakeholders.

(b) Confidential Data: This type of data is very critical for an organisation. If this data comes in public domain or even if people at large in the organisation come to know of it, the working of the business is seriously impacted. The information about the tussle between the Ambani brothers falls in this category. When this information was telecast by CNBC, there was a big furor and the share price of the company had dipped sharply. Such data, if leaked out, may also result in violation of laws. In the Reliance case, subsequently, the layers of onion were peeled one by one and it was reported that there was a web of benami investment companies controlling Reliance Industries. This alerted authorities like SEBI, Company Law Board, etc. and they became active to find out if there had been any violations. Security for this kind of data should be very high.

(c) Restricted Data: This data is sensitive and may adversely affect business if it falls in unsafe hands. It includes information, which should not be used due to existing laws or policies. The bank clerk does not let anyone without your authorisation know the balance in your account as it is restricted data. The e-mails sent by Anil Ambani to his brother regarding various issues after their tussle that became public may also fall under this category. Security should be high in this case.

(d) Operational Data: The data, which enable the employees to execute the actual work, fall in this category. Their loss or unauthorised disclosure does not usually result in any loss to the business enterprise. The project plans, designs and specifications of optic fibre cables to be used by Reliance Infocom would fall under this category. Security at this level is fairly high.

(e) Private Data: These data should not go out of an organisation due to concerns of privacy, reputation, etc., but their disclosure does not result in any loss to business or violation of law. The e-mails sent by the two brothers to the employees of Reliance, and the minutes of their board meetings fall under this category. Security is required but its level may not be high.

(f) Unclassified Data: This data does not fall into any of the above categories. This data may be made available even to the public at large without any adverse impact on the business. The recent press statements made by Anil Ambani and even the quarterly results declared by them fall under this category. Very low security is required at this level.

Computer Crime

Any organisation which fails to take information security seriously may end up becoming an unwilling accomplice to computer crimes. Computers have indeed been significant in enhancing the quality of business operations and human lives but they have also facilitated easier and faster means of perpetrating crimes. The Organisation of Economic Co-operation and Development defines Computer Crime as "any illegal, unethical or unauthorised behaviour relating to the automatic processing and transmission of data". This covers both the information asset and the information system asset.

Low costs, high speed, and extreme difficulty in tracing the perpetrators' identity make computer crimes very attractive to the new age criminals. Most cyber crimes require only logical access to the target computer and this can be done at negligible cost.

The impact of computer crime can be any of the following:

- **Financial Loss:** Even though slow, the growth of monetary transaction processing systems fuelled by electronic commerce has resulted in much of the financial operations such as shopping, banking and employee payments, and vendor payments. All these operations have been significantly automated and networked. Direct monetary losses to businesses occur due to financial frauds such as stealing of bank balances and credit card numbers. Besides, with every successful attack, significant sums are required to be spent to recover from damage, refurbish the dented image due to computer crime and legal penalties.
- **Legal Implications:** An organisation is governed by numerous laws and regulations. Electronic commerce, including automation of business processes presents newer risks, which directly or indirectly affect the organisation. While the perpetrator of crime is protected, organisations suffer from legal action from customers, vendors, employees and other stakeholders due to consequences of computer crime and resultant losses and damage therefrom. Medical and financial organisations are required by law to preserve the confidentiality of their constituents' information. Inability to do so might invite civil or disciplinary action by the concerned regulatory body. Access controls seek to mitigate these risks.
- **Loss of Credibility or Competitive Edge:** An organisation's success depends, to a large extent, on maintaining its competitive edge through quality of its service, customer relations, global reach and innovative practices. Banks and financial service companies require intensive care in ensuring customer confidence. One single computer crime incident could shatter the business image and customer confidence resulting in long-term adverse effects for the business. These risks increase significantly while business is conducted online via the Internet or via extranets.
- **Cyber Espionage and Blackmail:** Undesired disclosure of sensitive information can result in the perpetrator blackmailing the organisation. Competitors can access sensitive business information resulting in compromising the growth and prospects of the organisation.

Any organisation which fails to take information security seriously may end up becoming an unwilling accomplice to computer crimes. Computers have indeed been significant in enhancing the quality of business operations and human lives but they have also facilitated easier and faster means of perpetrating crimes.

- **Sabotage:** Perpetrators may not be interested in personal financial gain but may be interested in just spoiling the credibility and prospects of the organisation or simply disrupting the business.
- **Privacy and Confidentiality:** Computers hold various types of information about a range of stakeholders and sensitive information relating to the organisation. The undesired disclosure or access of such information can lead to embarrassment and legal repercussions, besides loss of image.

Indian Scenario

Information Technology Act, 2000: In Indian context, Section 43 of The Information Technology Act, 2000 prescribes penalty for damage to computer, computer system, etc. It reads as follows:

"If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

- Accesses or secures access to such computer, computer system or computer network;
- Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- disrupts or causes disruption of any computer, computer system or computer network;
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

The following explanations are appended to Section 43.

- "computer contaminant" means any set of computer instructions that are designed—

  to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

  by any means to usurp the normal operation of the computer, computer system, or computer network;
- "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio and video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is

executed or some other event takes place in that computer resource;

- "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

While the Information Technology Act is punitive in nature, access controls are intended to be preventive in nature. Commission of a computer crime implies circumvention of access controls. Since there is no such thing as foolproof security, access controls are intended to make computer crime unprofitable or uneconomic by making the cost or effort of circumventing the control greater than the potential reward.

Data Centre

A business enterprise has so many functions to perform: ensure timely production and supply of quality goods, generation of additional demand, compliance with laws, dealing with parties and so on. Management of data, though critical, is not the core activity of a business enterprise. It generally lacks the necessary skills and expertise to store, track, and manage an ever-increasing volume of data. This has resulted in the setting up of independent data centres. Outsourcing is the order of the day and even data management has not been left untouched by it. A data centre offers specialised services and skills to efficiently manage availability and security of data of its clients. It requires highly professional services and substantial resources. In the absence of the same, many data centres have already downed their shutters. VSNL has data centers at Delhi, Mumbai, Bangalore and Hyderabad and has a total capacity of 30,000 sq. ft. The capacity of 4 data centres of Reliance is almost seven times that of VSNL. Moreover, it has expanded the capacity to 5,00,000 sq. ft. by setting up additional data centres at major software development hubs at the end of 2005. Reliance has been able to rope in more than 250 clients to manage their data at its existing data centres. These centres provide disaster recovery facilities by data mirroring and through redundant links. This no doubt is a lucrative business. It also means better management and security of data at a lower cost for the clients. But when we compare the capacity of data centres in India with those abroad, we still have a long way to go. Sun Microsystems and Sybase have the largest data centre in the world. It is reported that it can store data equivalent to all the debit and credit card transactions that have taken place throughout the world in the last seven years!

How Important is Data Security?

Data Security ensures quality, integrity and availability of data. Access to confidential data can have catastrophic consequences. Take for instance the recent case of issue of fake PAN cards from a paan shop. It was reported that a person was kept for data entry work in IT Dept by an IT officer. During the process of data entry, he came to know of the user name and password of several IT officers. He used this information and subsequent access to PAN database to change the details of existing PAN card holders and sell the same at Rs. 500 per card through his accomplice running a paan shop nearby. Considering that PAN card is an important document for various transactions and is issued only on the basis of a laid down procedure, the following were the immediate consequences:

(a) This incident put a big question mark on the reliability of PAN card per se.

(b) The reputation of IT Dept took a beating.

(c) Though India is not USA and not many people file suits in such cases but what if someone relies on a fake PAN card, say for sanction of a loan of Rs.1 crore to a person. The IT Dept. may be taken to the court and may even suffer a financial loss.

The above example clearly brings out that not everyone can and should have access to all data. Access to data should be on the basis of the golden rule of 'Need to know, need to do basis'. In the above case, there was no problem as

long as the data entry operator did what he was authorised to do, i.e., key in the necessary data. But the problem arose when he was authorised to access the database as he misused it to alter the existing information. In fact, there was no need to give him the read and/modify rights.

Outsourcing is a win-win situation for both the parties. But the data security is still a major concern so far as outsourcing is concerned. The companies to whom various activities are outsourced get confidential personal information like credit card and bank account details of clients. 75% of companies surveyed in USA and India have expressed concern over Data Security. There has been a perceptible change in the mindset of companies. They now find it a fruitful investment and not a wasteful expenditure. As per Gartner, companies are increasingly adopting a proactive approach towards data security because security and privacy concerns are slowly replacing job losses as the main concern of the off-shoring countries.

Recently, an Asian call centre executive held her employer to ransom on the question of a pay hike by threatening to post confidential medical records of a client on the Internet. In another case, the source code of a software solution developed by Geometric Software Solutions Ltd. for its overseas client was actually stolen.

It is strange that there is no separate law on data protection even though it is so important. No doubt, the IT Act has various provisions, which to some extent help in data protection by prescribing penalties and punishment for related crimes. But the fact remains that these are not sufficient. Even the maximum penalty for a cyber crime has been pegged at Rs. 1 crore. Would this penalty deter an employee in an IT company from stealing the source code of a software worth Rs. 50 crore. Other laws like the Indian Contract Act, Indian Penal Code, Indian Copyright Act, etc., all do their bit but the fact remains that there is no 'holistic' legislation to deal effectively with this issue.

Other Measures taken for Data Security

Some Indian concerns use Global standards for data protection. They take various measures to ensure protection of data. Biometrics is used to prevent unauthorised people from entering the facilities. Even personnel cannot enter areas, which they are not required to access. Group 4 Securities, which provides security guards and other security services to corporates has a good access control system for its staff also. The staff members are provided with smart cards through which they can enter their respective departments. In the normal course, they cannot visit the other departments at their sweet will. Use of firewalls and anti-virus programmes also prevent unauthorised access to data. In many secure sites like www.irctc.nic.in, through which railway tickets can be booked online, confidential information like credit card number is not stored on the server. This information is merely for the payment gateway.

A data centre offers specialised services and skills to efficiently manage availability and security of data of its clients. It requires highly professional services and substantial resources. In the absence of the same, many data centres have already downed their shutters.

But clearly these are not sufficient. Fortunately, the government and the various authorities have realised the importance of this burning issue. Following steps have been taken in this regard:

1. Necessary changes are being proposed to the IT Act, 2000 to plug loopholes and to make punishment and penalties more stringent for loss, manipulation or misuse of data.

2. NASSCOM has set-up a National Advising Board (NAB) on Information Security. Its member are experts from industry, educational institutions, legal and regulatory bodies. The aim of NAB is to create general awareness about data security, suggest changes in laws and strive for global standards of data protection.
3. NASSCOM conducts audit of the security levels of its member companies.
4. The government is planning to come out with a separate comprehensive legislation for data protection.
5. Use of Digital Signature is being made mandatory in various fields like online filing of TDS and IT returns.

Data Protection for CA

Traditionally, CAs enjoy the confidence of their clients. They have access to sensitive, confidential and other important data of their clients. But rights and duties go hand in hand. If we have the right to ask for any relevant information from our client, we naturally have the duty to ensure the security of the same. We cannot later on plead that the data was leaked by a clerk. Therefore, we need to devise systems and access control mechanisms to ensure Data Security.

A few simple measures, which can be used for security of data in our offices or even elsewhere are as under:

1. We should have a well-defined security policy. The risks, threats, etc., should be identified beforehand and steps should be taken to protect our valuable assets including data.
2. Even the best security policy is futile without proper training. Therefore, formal and informal training programmes should be organised regularly to familiarise the staff with the various steps to be taken for security of data. Just as physical security of office is essential, so is the security of data. Therefore, even a peon should be trained to shut down computers, UPS, etc., to prevent loss of data due to overheating of systems, etc.
3. Important Excel, Word and other files should be protected by passwords. Very simple passwords like name, initials of company or staff should be avoided as they can be easily guessed.
4. Passwords are not like our names, which normally remain the same. They should be changed periodically. I visited my ex-employer few months back and found that my successor was logging in with my user name, which was created 5 years ago!!! Thankfully, the password was not the same as the company had changed the system of setting passwords from static to dynamic, where a new password is required at each login. This is possible with the use of a special device being used in banks abroad or even on the basis of change in time, as the present incumbent looked at his watch every time he entered his password. Even in banks the user name and passwords set once are rarely changed. This should be one of the basic checks of access control when we are entrusted with IS audit of an organisation.
5. We are very lax in the matter of password

Traditionally, CAs enjoy the confidence of their clients. They have access to sensitive, confidential and other important data of their clients. But rights and duties go hand in hand. If we have the right to ask for any relevant information from our client, we naturally have the duty to ensure the security of the same.

administration. Most software packages like Tally come with the option of different levels of passwords. The basic level gives rights of data entry and viewing selective reports. The next level gives right to modify entries up to a particular date and view more reports. These levels provide object privileges, i.e., the right to read, write or modify in certain specific areas only. The final level is the supervisor password which gives all rights, i.e., system privileges to the user. Either, the option for use of passwords is not exercised or the supervisor password is known to all and sundry which puts data at risk.

6. Data encryption is another method of data security. Encryption refers to coding of data so that it is not readable by naked eye. Various software packages are available for encryption. However, since encoding and decoding of data requires system resources, it is desirable that only confidential data should be encrypted.

7. Data archival is different from data backup just as 'cut and paste option' is different from 'copy and paste' which we so frequently use while working in Word, Excel and other office applications. We need to keep duplicate copies of data so that the same can be used in case of loss of original data. But as the volume of data grows, their management becomes more and more time consuming and expensive. Data archival means removing non-current data from actual database so that the same does not become very cumbersome to handle. Even Tally offers this facility to separate and remove accounting years. Just as we put only our valuables in bank lockers, we should be more concerned about the security of important data. For this data classification and data archival is necessary.

8. Fire proof vaults can be used to store important physical files and backup of data.

9. Cost benefit analysis which we so frequently do for our clients is also required for Data Security. We do not need to install expensive biometric devices like retina scanners or fingerprint readers to prevent unauthorised access to data. Simple measures outlined above would generally be sufficient.

Data is the blood of business and any loss or damage to it can result in sickness or may even prove fatal. After human resources, data is the most important asset of a business. Inadequate protection to either information asset or the information system assets may result in computer crime.

10. Since Internet is so widely used in offices now, firewalls like Norton firewall should be used to prevent intruders from accessing our secure systems to manipulate, steal or copy our important data.

Conclusion

Data is the blood of business and any loss or damage to it can result in sickness or may even prove fatal. After human resources, data is the most important asset of a business. Inadequate protection to either information asset or the information system assets may result in computer crime. Therefore, we all must take very good care of our important data through backups and ensure Data Security through access controls. Loss or corruption of data may cause irreparable damage to business and at times, no amount of effort and money can recover it. ❐