Defining Information Security Policy

Information or **data** is anything that reveals facts about an object or subject that enables the receiver to react positively or negatively towards it. **Information security** is the collective processes put in place to ensure the safety, integrity, and privacy of a piece of information and data.

Chris works with Best Stocks (a stock brokerage firm) on Wall Street as one of its stock traders. He's frequently connected to the firm's network monitoring the stock market's indices for each day as well as closing up more deals on behalf of the company.

During his break period, Chris logs on to his social network profiles to chat with friends, he checks his personal emails and other websites of interest all on the company's assigned computer system.

On one of these occasions, Chris got an email supposedly from a close friend. The email with a catchy subject 'you Just Won $1 Million' contained an attachment **zipped** requesting him to download and fill out the details.

Unsuspectingly, Chris opened the zipped file and his computer screen went blank for a moment but came back on. Unknown to Chris, several of his colleagues in the office connected to the company's network at the same time and experienced the same issue. Consequently, Best Stocks lost a considerable number of clients to their firms that week.

Information Security Framework (ISF)

When Chris opened that file, there was a **breach** on Best Stock's network targeting the firm's information base. The file contained a specialized **worm** or **virus** which was programmed to steal passwords of users logged on to the network the same time as it was released.

Best Stocks could have protected itself from these issues if it had implemented some form of information security using a certified **information security frameworks** (ISF).

Information security frameworks are a collection of standardized policies, procedures and guides, meant to direct a firm or any organization, which adopts its use, on how to protect its hardware, software, data, information, network, computing devices, users and clients from potential security breaches through their use of the firm's resources or services.

There are three main reasons for using the information security frameworks:

- Ensure legal compliance with the country of operation's Data Protection Act.
- Assure customers of their personal data safety and privacy.
- Protect the entire firm from network security breaches and invariably, company's data breach.

There are several frameworks available which help in addressing key information security concerns like the popular ones listed below:

- Control Objectives for Information and Related Technology (COBIT): A product of vendor-independent organization IT governance professionals. Its key point of focus is on reducing technical risks in an organization.
- ISO 27000 Series: This was developed by the International Standards Organization and offers a much wider coverage over a company or organization's processes. It can also be applied to all types and sizes of organizations.

An example of a security policy, driven by the ISF mentioned above, are made up of sections or domains which address the company's operational processes or infrastructure as follows:

Security Policy Scope : This addresses the coverage scope of the security policy document and defines the roles and responsibilities to drive the document organizational-wide.

Organizational Security : This addresses the organization's security needs covering its staff, customers or clients, suppliers and other vendors handling key processes on its behalf.

Risk Assessment and Treatment : This helps define potential risks and subsequent responses to reduce its effect on the organization.

Asset Classification : The value of an asset determines the level of sophistication its protection would be. In order to implement this, the company's assets irrespective of its size or use are classified and protected.

Human Resources Security : This deals with the processes involved with staff engagement, onboarding and termination processes.

Physical and Environmental Security : Protection of the firm's building and physical entry access, as well as protection of the environment from the dangers which could have an impact on the building itself.

Communications and Operations Management : This section addresses the communication and operational channels of the organization. Protecting each channel on a need to know and access basis.

System Access Controls : This addresses the requirements and standards for the granting and maintenance of access to staff on systems, applications, and network.

System Development and Maintenance : This deals with the development of new systems, maintenance of existing ones and evaluations of security controls in line with changes affected in the system.