

A secure network?

Information today is the most important asset in any organisation. And unlike other assets, the misuse of this is regarded to be the highest



PICS. USED FOR REPRESENTATIONAL PURPOSES ONLY

Business information asset is the collection of a company's intellectual property, client information, employee intellect and any hardware/software required for information storage and processing. It is, thus, one of the most critical business assets, and in today's extensively interconnected business environment, these assets get continually exposed to increased threats like theft, unauthorised access, data alteration, hacking, etc.

"Information security is highly applicable in areas, especially where data is lying in an electronic form and is shared across internal network," says Mahesh Shah, chief information security officer, Kale Consultants.

It is, therefore, essential for every company to have robust information security systems and processes to avert any intrusive or disruptive attempts internally as well as from public domain.

KPIT Cummins Infosystems, an IT, Engineering and BPO services firm, believes that businesses work on competitiveness and compatibility of the associates, as such complete confidentiality and reliability is an obvious expectation. "For us, information security is about building and maintaining trusted relationship between information resources and people, thus not only protecting our intellectual capital, but also protecting confidential client information," says Mandar Marulkar, chief information security officer and head, business continuity management, KPIT Cummins Infosystems.

Matters of the mind

So, at what stage are Indian organisations on this mindset? The density of organisations across the risk awareness spectrum is quite even. While on one end of the spectrum are organisations that are totally unaware of the risks, there are others that lay a lot of emphasis on risk management. Says Prakash Seernani, COO, Synlog, "There is a good density of organisations that are well aware of the risks and have their risk management plans in place. However, what is lacking in many cases is the regular validation of these risk management plans, at the desired frequency, keeping in mind the dynamic nature of the business. For e.g. banks today are getting into newer instruments and markets and diverse businesses like portfolio management, insurance, etc."

"New roles have also been introduced into the corporate fabric, which includes specialists for security policies development, security process execution and management, risk mitigation, regulatory compliances managers and internal information security auditors," notes Marulkar.

While most companies take different measures to secure their data, there are some who believe that personal freedom of employees should not be curbed to ensure data security.

However, Mohan Ram, MD, Lattice Bridge Infotech says, "I don't think personal freedom of employees should be curbed to ensure data security. This can lead to dissatisfaction. We do not restrict our employees from

accessing emails or using camera phones, etc. They are even allowed to carry their own USB cables."

Means to the method

Different organisations adopt different ways and means to secure their information. Synlog, which is in the business of payment solutions, ensure they keep abreast with the notifications issues by RBI from time to time about the various risks that banks face.

"We keep our banks informed, our solutions and services updated to help customers manage risks. The solutions designed for our clients have this as a basis and we try our best to ensure that the information stays as safe and secure as possible. We also ensure that all information communication has an acknowledgement such that the information is sent only to the intended recipient system," confirms Seernani.

KPIT Cummins Infosystems has built an Information Security Management System (ISMS) to protect vital corporate and customer information. "We have built a dedicated team of highly

conducted for creating ongoing awareness about company security policies and employees roles in creating vigilant culture in the organisation," says Marulkar.

"With ISMS, we have managed to balance between controls without compromising security risk and providing necessary flexibility in operations. We do not intend to make the system hack proof, but strive to devise a mechanism that can anticipate potential problems, pre-empt through proactive measures, ensure recovery and restoration and protect against considerable damage," he further adds.

Information security is the protection of information assets from a wide range of threats in order to ensure confidentiality, integrity and availability of critical business assets, in turn enhancing customer trust, people safety and business continuity.

"Awareness of the problematic nature of information security is approaching an all-time high. Organisations worldwide are realising the importance in securing the information and investing in infrastructure to

Information security is about building and maintaining a trusted relationship

qualified and experienced information security professionals, which actively drives policy implementation and monitors its effectiveness. E-learning modules, classroom sessions, posters, computer screen savers, sessions from external experts etc. are

mitigate the risk arising out of these threats," concludes Prince Thakur, AVP, I.T. GlobalLogic.

(So what kind of security system does your organisation have? Blog on www.timesascent.in/blogs)