

www.benefitmag.com

BenefIT

A Business Minded Computer Magazine ■ January 2010 ■ Vol. 6 ■ Issue 4 ■ Pages 60 ■ ISSN 0974-1070



Is Your
**ERP System
Intelligent
Enough?**

ERP Special Series

Choosing The Right Laptop



For Your 'Team-On-The-Move'

More Buying Tips

- ▶ For Selecting The Right Projector
- ▶ 6 Projectors Below Rs 40,000



Now Pay Your Tax
At An ATM!

"Having a security system is
critical for businesses!"

—Sanjeev Sehgal, MD & founder, Samridhi Automations

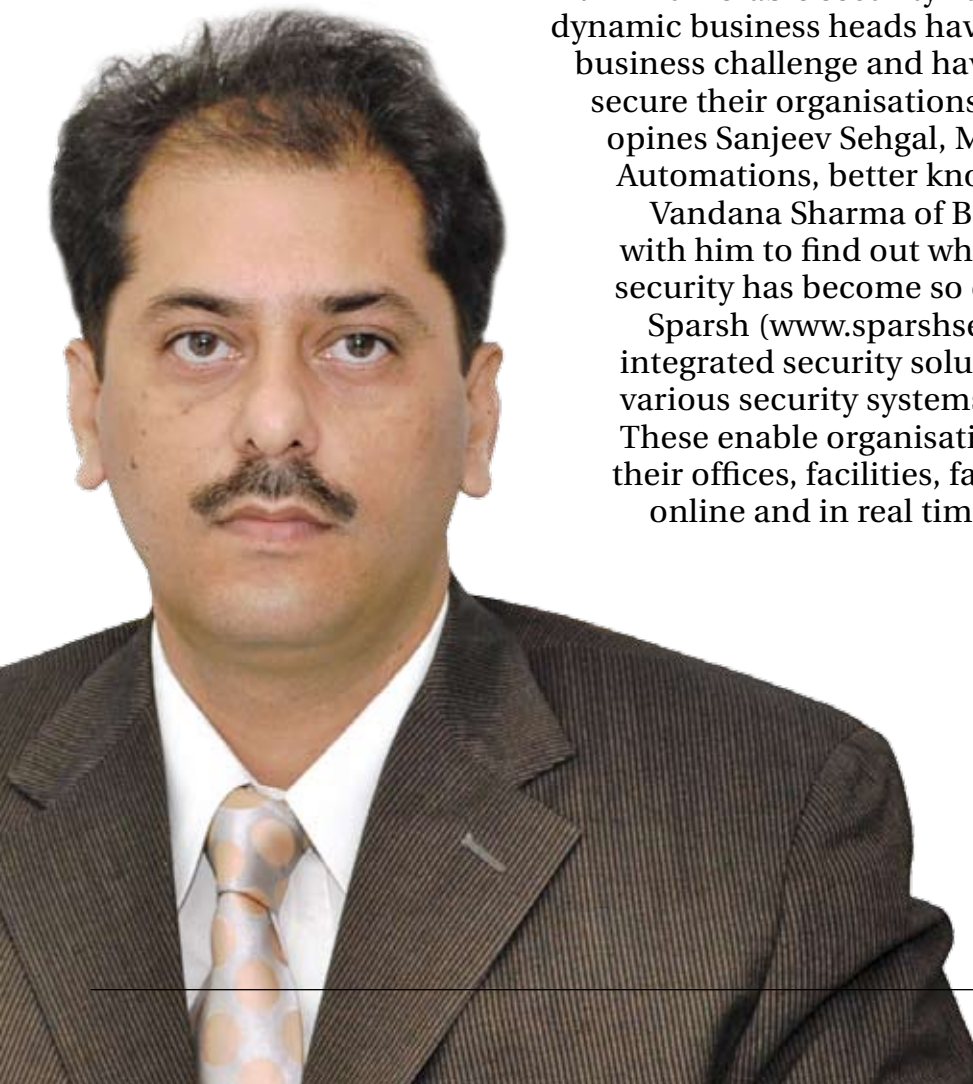


“Having a **comprehensive security system** is a critical requirement for businesses!”

Someone rightly said, "One of the tests of leadership is the ability to recognise a problem before it becomes an emergency." At a time when the online world is infested with innumerable security vulnerabilities and threats, dynamic business heads have realised the gravity of this business challenge and have initiated measures to secure their organisations' digital and physical assets, opines Sanjeev Sehgal, MD & founder, Samriddhi Automations, better known as Sparsh.

Vandana Sharma of Benefit Bureau caught up with him to find out why beefing up organisational security has become so critical.

Sparsh (www.sparshsecuritech.com) is an integrated security solutions provider that offers various security systems and software solutions. These enable organisations to monitor and control their offices, facilities, factories or auditoriums, online and in real time.



Sanjeev Sehgal

MD & founder, Samriddhi Automations

Q What are the type of security vulnerabilities that exist in any small or mid-sized company?

It's difficult to define and determine the exact type of security vulnerabilities in organisations. The extent and nature may vary, organisation to organisation.

Security threats can exist at both the physical and logical level. Theft, pilferage, sabotage and eve teasing are some of the other security concerns in most small and mid-sized organisations that demand management attention.

However, today, in the world of e-business, data security has emerged as a critical issue. This aspect needs special attention and care. Whether it is business rivalry, competition or ignorance of security issues with regard to information and data--all may lead to huge losses in terms of finance and reputation.

Q What best practices would you suggest to avert such threats in time?

As I mentioned earlier, from the operations standpoint, security can be divided into two sections: physical and logical security.

Physical security governs all the physical and tangible aspects of security from access control (which means setting up a system in the organisation where access to data or any other organisational asset can be restricted to a few authorised employees) to perimeter protection. The latter ranges from the verification of employees to identifying visitors and guests on the premises. Security guards and surveillance systems (like closed-circuit television cameras or CCTVs, etc) play a very important role in physical security management. Organisations can opt for a

combination of manned guarding, CCTVs, access control systems using various technologies like RFID active tagging*, smart cards*, biometric* identification systems, etc.

[Please refer to the glossary for an explanation of the terms highlighted with an asterix ().]*

Q How can organisations ensure logical security?

Logical security involves the maintenance and protection of information and data through various IT security solutions like firewalls* and antivirus software*. The network* of the organisation

“An ideal security system should integrate all types of security and telecom systems so that appropriate authorities can be contacted as soon as some security breach occurs.”

should be secure and no unauthorised user should be able to log in to it. Users' access rights on the organisation network should be defined at the outset by the IT manager. All incoming and outgoing data should be screened by the IT manager/administrator.

An ideal security system should integrate all types of security and telecom systems so that appropriate authorities can be contacted as soon as some security breach occurs.

Q Why is it that most small firms are oblivious to the challenges related to security? What would be the ideal budget to allocate for security?

It is important to understand that most accidents only happen due to ignorance. Thus, even in an organisation with a comprehensive security system in place, it is also important that everyone in the organisation is responsible for their own security. This implies the need to create an awareness about security. That's half the job done.

Apart from this, a security assessment of the premises and then the use and application of adequate measures may reduce vulnerabilities and threats.

As far as allocating funds for the security budget goes, it depends on the nature of an organisation's work. It has been often observed that cost cutting in security measures results in bigger losses, eventually.

Q What 'security solutions mix' (combination of antivirus software, firewalls, CCTVs, biometric devices, or any others) would you recommend to companies to safeguard different aspects of their business?

All establishments, organisations and industries have unique and different security requirements. For example, an automobile firm may have different requirements from an export house, or a law firm, in terms of security. So, the tools or mechanisms deployed by organisations may be similar, but the application and efficacy of these tools may depend on the infrastructural environment and usage pattern.

However, organisations may consider applying a mix of tools, like: access control systems and CCTVs to restrict access by unauthorised and unidentified people -- from within the organisation or outside; smartcards or biometrics-based authentication systems along with antivirus software and firewalls to

Glossary

- **Computer virus:** It is a computer program that can copy itself and infect a computer.
- **RFID tags:** This refers to small electronic devices that are made up of a small chip and an antenna. The device can carry approximately 2,000 bytes of data. And, just as information can be retrieved or read from bar codes or magnetic strips via a scanner or bar-code reader, RFID devices also require a scanner to retrieve the information stored in them.
- **Smart cards:** This is a plastic card with an electronic chip that can carry data related to an individual and can act as an identification device.
- **Biometrics:** Biometrics is a technique used to recognise humans based upon one or more physical or behavioural traits, like fingerprints, face recognition, DNA, hand and palm geometry, iris recognition, voice, etc.
- **Firewall:** It is a software tool that enables IT managers to block unauthorised access even while allowing authorised communications.
- **Antivirus software:** This can be used to make Internet access secure and prevent the computer network of the organisation from getting affected by viruses like malware, spyware, etc.
- **Organisation network:** An organisation network is the local area network comprising a group of computers within the organisation's premises or across its different branches connected to each other for the purpose of communication; the other type is a wide area network through which the organisation communicates with the world outside, over the Internet.

secure the organisation network; and restrictions on the use of external drives (such as pen drives, etc) on the network or computer systems.

Q Which of these suggestions would you rate as a 'must-have'?

Considering that ignorance is the only reason for an accident to occur, I don't think anything that we have evaluated so far can be ignored. At the same time, it would be difficult to declare that implementation of the above cited security tools guarantee a foolproof security set-up.

Q Are there some innovative, cost effective options also available?

There are various innovative solutions depending upon the

organisation's requirements. 'Cost effective' may not be the right term to use in this context. But yes, optimum solutions can be designed by doing a thorough study of the security requirements of a firm, under a detailed 'total loss prevention' programme.

Q What kind of integrated security solutions do you offer to businesses and at what price points? Are these solutions also relevant to small businesses?

Providing an integrated security solution cannot be taken as a product sale. It is more like providing a solution to a problem, and involves the integration of various products and commissioning skills, which

include hardware, software, solution designing, and so on.

There are various integrated solutions that can be designed for different businesses, depending upon their requirements. From surveillance systems and access control devices to intrusion detection and perimeter protection systems; from visitor management to employee identification tools—all these can be integrated using software interfaces or connects. The basic mechanism always remains the same but the design and size may vary between small/mid-sized firms and a large organisation's set-up. Since all solutions that we provide are tailor made, defining a price point is impossible.

Q Could you cite an example of a company that may have got affected because of security lapses of some kind?

There are many examples of companies that have suffered losses due to inadequate security systems. Inadequate systems, non functional equipment, unserviceable or obsolete technology, and prolonged negligence have resulted in disasters before, during or after the incidents.

Naming a company in this context would not be appropriate, but we all know that the CCTV systems at Sarojini Nagar Market and Gaffar Market were not functional when the serial blasts occurred a few years ago, causing so much devastation and irreparable losses! ■

Managing IT is **simpler**, and **more cost effective** using Open Source

Read LINUX For You: Asia's Leading Open Source Magazine

www.linuxforu.com

