"Data loss is a critical issue CIOs should look into"

by Sohini Bagchi Jul 24, 2012

With the IT security scenario becoming increasingly complex, enterprises are looking for reliable, scalable and efficient security system in place to achieve overall success in their business. In an exclusive interaction with CXOtoday, **Govind Rammurthy**, CEO & MD, eScan, speaks about how the role of CIO is getting shifted from technology manager to strategic business leader and also recommends IT decision makers on how to create a secured enterprise.

What are the key security threats faced by enterprises today?

Today, enterprises face a very complex and dynamic threat landscape. Security threats are becoming increasingly sophisticated and harder to detect. The major concern for these large networks is to protect confidentiality, integrity and availability of information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, or destruction. Data leakage and down-time due to network outrage can cost loss to business reputation, in addition to financial loss. Moreover, insider

attacks are increasing rapidly. Employees within the organisation may unknowingly introduce malware within the network either through endpoints, or via malicious emails.

Another growing concern to businesses is the rising trend towards BYOD (Bring Your Own Device), as this movement is blurring the lines between work and personal life. Implementing BYOD programs aren't a bed of roses for organisations as companies lose much of the control over hardware. There are major issues to look into as well. For instance, company issued devices come with predefined security policies that are actively managed and updated by the IT department – A more widely accepted policy that helps differentiate between what's acceptable and what's not.

BYOD isn't just about keeping tabs on a particular platform; it's about securing the perimeter irrespective of the OS. Take the example of bringing in a Smartphone. Here we aren't just talking about one particular platform but at least 5 various platforms - Android, iOS, Symbian, Windows for Mobile, Blackberry. The question here is one, will you be able to implement access policies on all given platforms? Secondly, is there be a need to block certain devices from accessing company resources when they enter the office perimeter?

Security breaches often take place through the LAN or Internet. So how do you advice CIOs to address this?

Ordinary firewall and network security solutions are not capable enough to secure data in motion. Moreover, companies have made attempts to address issues regarding data loss via corporate policies and various employee education programs, but without the appropriate controls, employee's can (through ignorance or malicious intent) still leak confidential company information. To tackle such situations and patrol various aspects for data loss, companies need to monitor and control all outgoing communications. This would include monitoring communications going outside of the organisation, securing email containing confidential content, enabling compliance with global privacy and data security mandates, securing outsourcing and partner communications, protecting intellectual property, preventing malware-related data harvesting and enforcing acceptable user policies. Besides, it is important to block of all known endpoints and communication ports and also block malicious users along with the possibility of being caught.

As the security landscape is becoming complex, how do you see the role of CIOs getting shifted from technology manager to strategic business leader?

Security in fact is a business enabler. Take the instance of a breach – not only do businesses incur significant losses but the overall hit is so significant that it could literally shutdown large enterprises. CIOs might not come in as core decision makers for the companies' profit and loss agenda but they do play a significant role in strategising and deploying various security protocols across the network. In terms of their profile CIOs are involved with driving the analysis and re-engineering of existing business processes, identifying and developing the capability to use new tools, reshaping the enterprise's physical infrastructure and network access.

Do you think it is necessary to have a Chief Security Officers (CSO) in an enterprise to address the security concerns?

Certainly yes. Addressing and nullifying security issues should come in as a prime concern for businesses. Networks have always been considered the backbone of both small and large businesses, and it would be foolhardy to ignore this aspect of their network. Big or small, the need to protect businesses against information theft, virus outbreaks, and application abuse should be on the list of all Chief Security Officers. When implementing BYOD companies should outline the key aspects which basically state the way devices are or need to be deployed. In addition companies should make it mandatory to implement company-issued security tools as a rule towards allowing personal devices when connecting to company resources.

What are your recommendations to CIOs or CSOs for creating a more confident and secured enterprise? What should they prioritise?

If you look at large Enterprises and MNCs of today, you get to see that a great deal of attention is given in protecting the companies' electronic assets (mostly from) outside threats. From intrusion prevention systems to firewalls to vulnerability management – while the mentioned few are what most companies implement or follow – the problem of data loss mostly lies from the inside. Be it in the form of email, instant messaging, web mail, website surfing or even file transfers, electronic communications exiting the company apparently go largely uncontrolled and unmonitored – with the potential of confidential data falling into the wrong hands. However, should there be a breach in information, it could create havoc within the organisation through fines, bad publicity, loss of strategic customers, loss of competitive intelligence and legal action. Thereby, looking into the current scenario and competitive environment, data loss is one of the most critical issues that are being faced by CIOs, CSOs, and CISOs and this is something they should prioritize.