TECH TALK

PRASHANT MALI
Advocate and President, Cyber Law Consulting

The security driven enterprise

Cyber crime generally refers to criminal activity conducted via the internet. The attacks can include stealing an organisation's plain data or intellectual property, illegal online bank transfers, creating and distributing viruses or worms on other computers, posting confidential business information on the internet and disrupting a corporate or country's critical national-international infrastructure.

Every corporate, whether it is a bank or IT company, is vulnerable to thousands of cyber attacks that occur daily across all industries, causing information theft, disruption to business operations, loss of brand credibility and serious financial loss. Through actions such as the appointment of a Chief Information Security Officer (CISO), the rollout of an enterprise security strategy, and investments in technologies capable of addressing sophisticated threats and managing complex security events, companies are able to reduce the financial impact ofcyber crime

The most costly cyber crimes are those caused by web attacks, malicious code and malicious insiders which account for more than 90% of all cyber crime costs per organisation on an annual basis. Cyber attacks can be costly if not resolved quickly. Detection and recovery are the most costly internal activities. On an annualised basis, detection and recovery combined account for 46% of the total internal activity cost, with labour representing the majority of these costs.

"Every corporate, whether it is a bank or IT company, is vulnerable to thousands of cyber attacks"

Detection and recovery costs from cyber attacks can be mitigated by continuous employee training, following global best security practices. Now, under Section(85) of Information Technology (Amendment) Act, 2008, India's cyber law also makes corporate responsible for security leaks.

Some cyber crimes faced internally by enterprises are:

- Data theft (clients, employees, ex) by employee
- Theft of technology, designs, formats, processes, source code etc.
- Applying email forwarding rules to sensitive accounts.
- Data diddling (changing data beforeit is enteredinto a system).
- Industrial espionage, i.e. spying for competitors bygetting employed.
- Relaying video footages of sensitive places and technologies.
- Implanting trojans.
- Allowing corporate computers to act as zombies.
- Deleting or destroying live information or backups etc.

Even though India has a cyber law of its own, every organisation should be concerned about cyber crime happening and how much it will cost to manage and contain them.

You know how the police protects civilians inspite ofhaving various laws and procedures in place - they take help of civilians, groups and informers. So, having a global standard IT security policy is not enough. An ideal CISO should guard IT infrastructure with a law and enforcement mindset. If we equate Infosec Policy to a law within an organisation, then 'laws are meant to be broken' is a general philosophy with people. Policy can be enforced only with physical will of people and CISO.

There are standard "best practices" and the IT Act 2008 envisaged "Security Practices" that we should be performing to protect our IT infrastructure and networks, and any of these could also help against advanced attacks. But the issue always comes down to security versus productivity and functionality. The sad truth is that users almost always end up having more privileges and access than they need, making them an easier target. Fewer threats would affect your users' systems if they had to prove the importance of a particular business need before they wereallowed to access the web. ITNEXT

The author is an advocate and President at Cyber Law Consulting