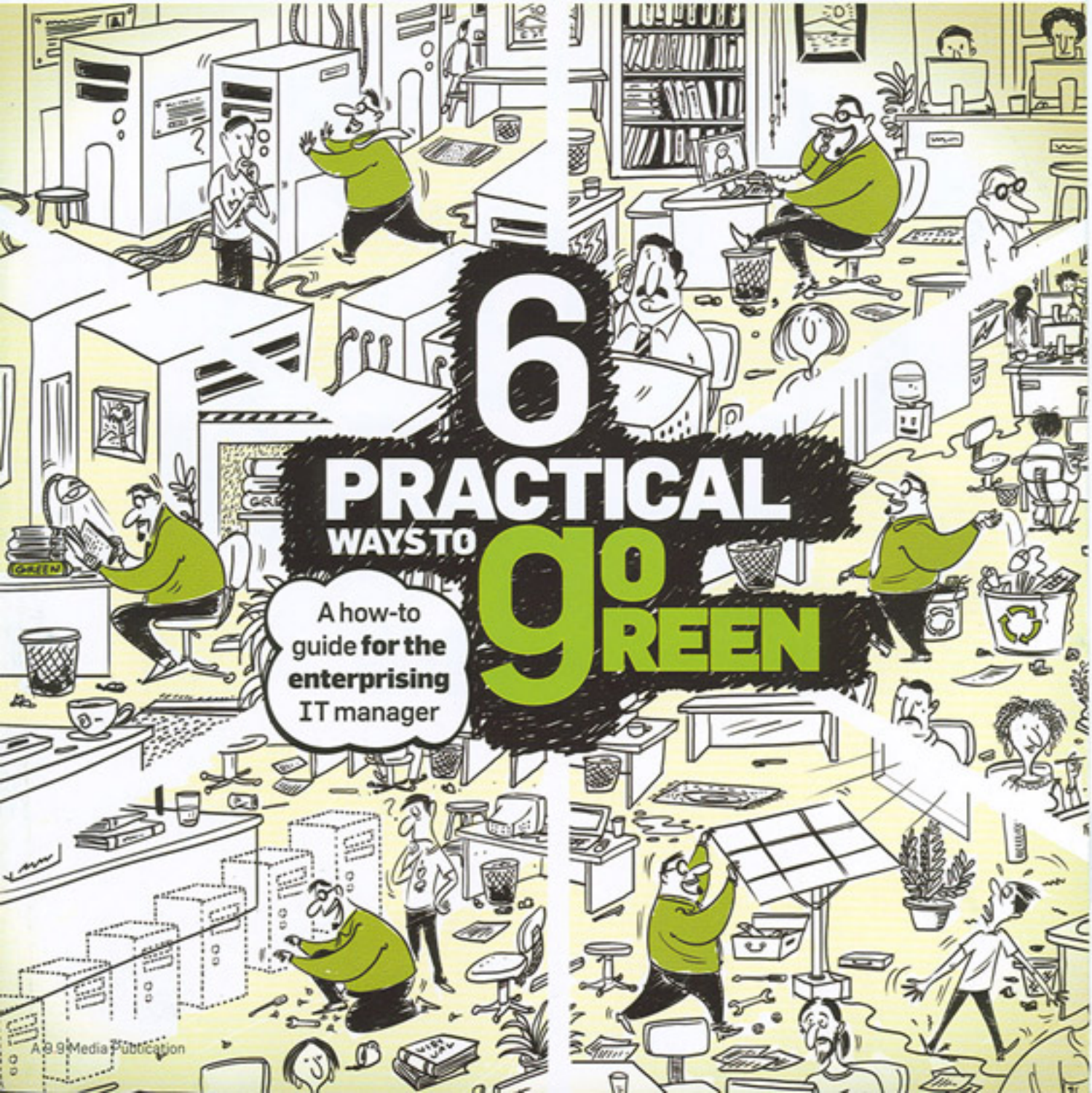
SEARCH IS ON
SEE PAGE 11

IT NEXT

JUNE 2010 / RS. 150
VOLUME 01 / ISSUE 06

MEDIA FOR THE NEXT GENERATION OF CIOs



6 PRACTICAL WAYS TO go GREEN

A how-to guide **for the enterprising** IT manager

A 9.9 Media Publication

THE FATAL FIFTY

Security solutions may tackle half the risks—the external ones- but employees can put corporate data at greater peril

BY BERJES ERIC SHROFF

70%
of data theft is carried out by internal employees

As an IT manager, you have deployed the best firewall; perhaps even dual firewalls from different vendors in series, intrusion prevention and detection systems, and have even got somebody to constantly monitor the audit logs.

Excellent! Your corporate data is safe, right?

Wrong!

Sorry to burst the bubble, but by deploying these technologies, you've merely secured your corporate data from 50% of the threat -- the external hackers, who would have to bypass the security systems to play havoc on your network. What about the remaining 50%?

But who exactly are this 50%? What threats do they pose?

This other 50% are none other than your own internal employees. They are the ones who have access to corporate data and thus are in a position to misuse it. They are the ones who have been provided the IT facilities by you, misuse of which could lead to a legal suit against your organisation. They are the ones you trust with the data and the IT facilities, or can you? Well, they are the weakest link!

So, can you protect your data from the ones who have been entrusted with the same? Can you protect your organisation from legal action as a result of employees' misuse of an IT facility?

No system in this world is 100% secure, but yes, you can take steps to mitigate the risk.

Latest trends show that over 70% of data theft is carried out by internal employees. He may be that disgruntled employee sitting in the corner, or the one wanting to leverage your corporate information to secure that job with the competition, or even someone who's secretly on

PHOTOGRAPHY: PHOTOS.COM

SALIENT POINTS TO REMEMBER

- Don't ignore the weakest link in the IT Security Chain – your employees!
- Policy document must be signed by the senior most management
- Involve HR & Legal departments when framing policies and penalties / punishment
- Create IT Security awareness through scheduled, periodic training
- Identify all technologies in the organization and the risks associated with it
- Ensure that employees sign a declaration that they have read and understood the IT Policy document. This document must be retained by the IT, Legal or HR departments

the payroll of your competitor and may be getting paid for siphoning your data and trade secrets.

The IT manager needs to be sceptical and at times even paranoid in identifying the risks to gauge the magnitude of possible damage. How can they misuse corporate email? Can they take confidential hard copies of the data outside the office? What about the Internet? Blackberry is available to them for accessing corporate emails and loss of this could also result in leakage of data. Also, USB is an excellent mode of siphoning off data.

So what can you do? How can you address the risks?

Implementation of technical controls such as web content filtering, email monitoring, and disabling of USB ports can be enforced as the first step.

Technical controls are very effective to an extent, but what happens when something beyond the control of technology takes place?

So, the answer to the conundrum lies not just in implementing technical controls, but augmenting technology with policies and training. Policies should be well planned, and as far as possible, address each security loophole, which at times may not be controllable through technology.

Revelation of a PC's network configuration as a result of a social engineering attack could pose a serious security threat. Access to external email such as Yahoo or Hotmail could be disastrous, since you would never be able to trace what data was leaked using this facility. An abusive or sexually-oriented email from the corporate email facility could result in legal action against the organisation. Use of the corporate network's Internet and Wi-Fi facility to illegally access another organisation's network can invite serious legal actions against the organisation.

As stated earlier, policies should as far as possible address each security loophole. Senior management support for the implementation of these policies is very crucial and cannot be stressed upon enough. The policy document itself should be signed by the top management.

Also, creation of policies is fine, but what about when these policies are violated, intentionally or unintentionally? IT managers are in no position to frame penalties or punishment as a result of violation of policies, nor are they in a position to decide as to what action can be taken against the employee who has violated the policy.

THE SOLUTION LIES NOT JUST IN IMPLEMENTING TECHNICAL CONTROLS, BUT AUGMENTING TECHNOLOGY WITH POLICIES AND TRAINING

Support and involvement of legal and HR departments is very essential when framing polices and determining the action to be taken in the event of a violation. Without the involvement and guidance of the HR and legal departments, penalties and punishments stated in the policy document may not hold ground, because they may not be implementable or enforceable.

Once you have the involvement of the legal and HR departments and the top management has signed the policy document for conveying it to the employees, does the buck stop there? There are two more very important and essential steps for the success of the policies and guarding the corporate data against any misuse.

One important step is scheduled, periodic training. All employees, irrespective of their designation, need to be trained in all aspects of security that form part of the policy. Failure to do so may result in an employee either forgetting what he has signed for, or not understanding what a particular point in the policy means.

So who conducts this training? If a senior executive volunteers or is convinced to conduct this training for the employees with the help of the IT manager, it will have a much greater impact. However, if the IT manager makes the presentation, then it is a good idea that a senior executive of the company at least introduces the IT manager and stresses upon the management's intent and seriousness on the topic.

Training should be carried out annually or biannually. There can be special training sessions for the senior-most management and directors.

The other important step is that each and every employee (including the senior-most management) signs the declaration stating they have read and understood the policy document and agrees to abide by all its provisions, both in letter and in spirit. This signed document needs to be retained by the IT, legal or HR departments. Else, in case of a violation, the employee may plead ignorance of knowledge about the IT policies of the organisation.

Policy must be accessible to an employee at all times, either as a hard copy document, or on the company's intranet. Also, a distinction should be drawn between a policy, a standard and a guideline and this must be explained to employees during the training. ITNEXT

The author is Manager – Information Technology, Tata Services

Find similar stories online on the website
www.itnext.in/Insight