IT NEXT

FEBRUARY 2011 / ₹ 75
VOLUME 02 / ISSUE 01

MEDIA FOR THE NEXT GENERATION OF CIOs

airtel

our managed solutions bring you peace of mind...

15-MINUTE MANAGER

TRAINING
EDUCATION
WORKPLACE
COMPENSATION
WORKFORCE TRENDS
SKILLS DEVELOPMENT
PERSONAL DEVELOPMENT

LEADERSHIP

CYBER LAW AND ORDER

A thorough knowledge of cyber laws is essential for IT managers responsible for safeguarding enterprise assets

BY BERJES ERIC SHROFF

IT laws are often ignored by the best of IT managers. It does not matter whether you are heading IT for a large or small corporate house: in this day and age, an IT manager can ignore this area only at his or her peril. IT has evolved over time, and along with that there has been an increase in risks, threats and associated crimes. In such a scenario, while IT managers need not be lawyers, they must be aware of the multidisciplinary approach that cyber law has adopted over time.

Let us consider some common e-crimes that can be committed by employees (including IT personnel) and outsiders involving your organisation and how you could possibly tackle and deal with such instances. In SMEs, the IT manager is generally the custodian of data. In such organisations, the IT manager also has access, direct or indirect, to most of the organisation's confidential data, whether financials, marketing plans, business strategies, etc. As part of their daily routine, it is not unusual for IT managers in such organisations to devote more time to helping users and business heads with their daily IT-related problems. But, sadly, with all this routine work, security is generally put on the backburner and, as a result, an employee's handling of the

ILLUSTRATION: PHOTOS.COM

IT systems may lead to a breach of some IT law.

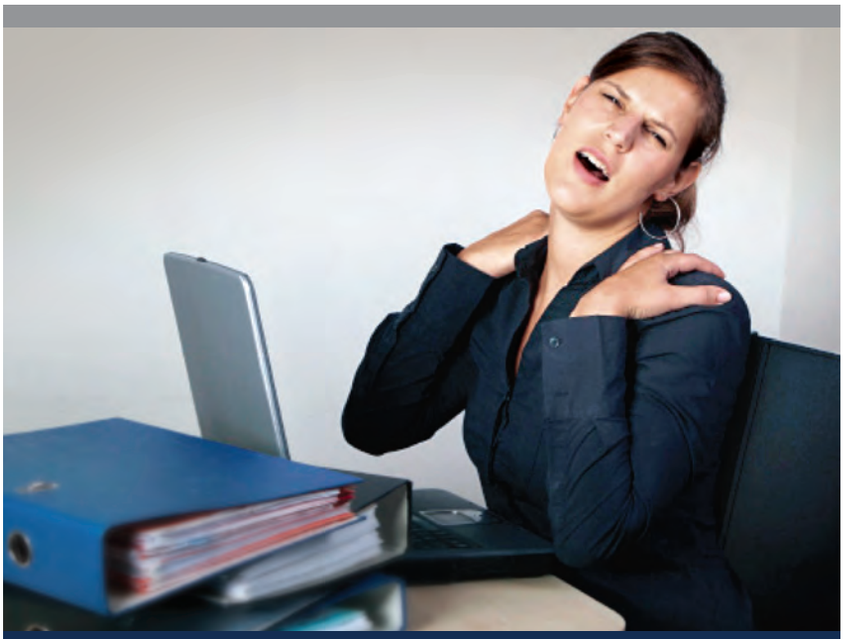
Above all, in such organisations, the IT manager's PC/laptop is usually never audited. He is often deemed omnipotent. To make matters worse, some SMEs rely totally on IT support through a vendor, and the vendor's engineer is based on the premises to administer the network and assist the users. It appears that his role requires him to have full access to all the company's data.

In such an instance, IT managers have the potential to damage or steal data. But do they always get away with it? As IT personnel we may perhaps not realise the 'value' of the data, or be unaware of the 'laws' related to deleting, gaining unlawful access or stealing data, nonetheless, damage and theft of company data for personal gains can definitely land us behind bars.

The latest well-known case is that of Edwin Vega Jr., an IT manager with the Consuegra Law Firm in Tampa–Florida, who deleted files from a computer that belonged to the human resources manager. Edwin Vega Jr. was sentenced to 18 months in prison for this act. An IT Manager of another law firm was recently caught using the confidential information of the law firm's clients, who were mainly major corporations, for insider trading.

While these are examples of actions taken by the US courts, one should not mistakenly think, that India is far behind. Nowadays, multinationals, larger Indian conglomerates and even SMEs are taking action against employees and IT managers who damage, steal or unlawfully gain access to data. My recent visits to the Cyber Cells in Mumbai and Pune were eye-openers—a number of small companies have lodged complaints against their employees and even IT personnel, for actions similar to the ones cited above. In most case, in order to protect the reputation of the company, these complaints are not made public by the organisations.

In my opinion, these organisations should do the opposite as this would have a two-fold effect. Firstly, the employees (non-IT personnel) and IT



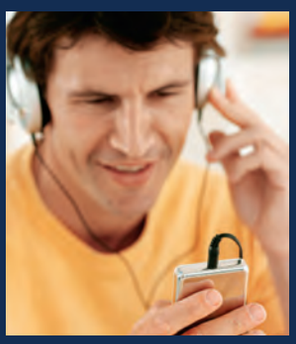
HEALTHY HABITS

EXERCISES IN THE OFFICE

FACTS

Women, aged 35 to 50, spend a lot of time on **social networking sites,** finds a poll conducted by a UK-based firm **Deep Pain.**

78 per cent are in agony because they spend too long **sitting at a desk or on the Net. Nearly one in five,** endures backache every day, **reports The Daily Express.**



Austrian researchers found that the group listening to relaxing music reported 40 percent less pain than those given the silent treatment.

Suffering from back-ache, stiff neck or sore shoulders. Here are some stretching and warm up exercises you can do at the office that hardly take much time but help you stay fit:

Upper Body Stretches: Sit firmly on the edge of your chair, gripping its back. Straighten your arms, and then, keeping your back straight, let your upper body pull you forward to stretch your shoulders, upper back and chest. Repeat a few times.

Shoulders and Back Stretch: Sit erect with your hands clasped behind your head. Now, gently pull your elbows as far back as you can, then hold them firmly in position. Repeat a few times.

Leg Stretches: Sit and grip the seat of your chair and raise one leg while you flex your foot. Slowly move the leg outward and then back toward the center and down. As you stretch, straighten your shoulders and relax your neck and hands. Hold each stretch for 15 seconds to a minute then repeat with the other leg. Raise the number of repetitions as you progress.

Spinal Stretches: Sit on your chair with your spine erect and both feet flat on the floor. Pretend there is a cord attached to the crown of your head gently tugging you up. Direct your gaze in front of your nose then bring your hand to your chin. Now gently press your chin in to your neck. Do 4 or more sets.

Ear to shoulder exercises: Sit on your chair with your spine erect and both feet flat on the floor. Now, inhale deeply. As you exhale, slowly roll your left ear towards your left shoulder.

PHOTOGRAPHY: PHOTOS.COM

"Wikileaks would force organisations to act better. Now they know that their own employees will expose them if there is corruption"

— Mikko H Hypponen, Chief Research Officer, F-Secure

"Mobile growth has opened new avenues for attacks, especially on new networked platforms with personal data attached."

— Jose Nazario, Sr. Manager, Security Research, Arbor Networks

TOP EXPLOITS OF THIS ERA

Top exploits representing different eras of cybercrime:

1) "I LOVE YOU" Worm's False Affection: Estimated damage $15 billion

This infamous worm cost companies and government agencies $15 billion to shut down their computers and remove the infection.

2) MyDoom's Mass Infection: Estimated damage $38 billion

This fast-moving worm first struck in 2004. Due to all the spam it sent, it slowed down global Internet access by 10% and reduced access to some websites by 50%, causing billions in dollars of lost productivity and online sales.

3) Conficker's Stealthy Destruction: Estimated damage $9.1 billion This 2007 worm infected millions of computers and was designed to download and install malware from sites controlled by the virus writers.

TO AID THE PROSECUTION PROCESS, THE IT MANAGERS SHOULD CAREFULLY RETAIN SECURITY AND AUDIT LOGS AND ANY OTHER EVIDENCE.

personnel would become aware that one cannot get away by committing acts of theft, damage and unlawful access to data. Secondly, the external stakeholders of an organisation, be it customers, business partners or shareholders, would realise and appreciate the fact that the organisation is serious and taking action against erring employees. From an IT personnel perspective, earlier such acts would be simply considered unethical and the matter might have been overlooked. But not anymore. The law is catching up and culprits are being booked.

To aid the prosecution process, the IT manager should carefully retain security and audit logs and any other evidence. The executive management of an organisation, irrespective of the size of the organisation, should ensure that the IT manager is maintaining and retaining the logs as required. If the executive management fails to evince interest in this area, the doors may be wide open for IT personnel to commit such transgressions.

Turning our attention to the threats posed by outsiders, how can the IT manager help his/her organisation book people who damage the reputation of the organisation through electronic means, be it through hacking, spreading defaming or false messages or through other electronic means such as SMS (text messages) using mobile phones. Phishing emails, received in the name of banks and other websites have become commonplace: these try to con people into revealing usernames, passwords and personal and credit card information. What about the numerous emails regarding false job offers? Sadly,

FASTER & STRONGER

5 BUSINESS APPS FOR THE IPAD

With the iPad gaining popularity in the enterprise, here are 5 must-have business applications for the iPad.

1 **BOX.NET:** This application helps break down all traditional barriers between you and the elusive content. You need not worry whether you are at work or not, behind a firewall or not, what OS are you on, one can access content anywhere, anytime as needed. The application helps you leverage the best of CCM (Cloud content management) whether you have the right desktop applications to view documents, spreadsheets, images and other types of content.

2 **GOTOMEETING:** The best of things in life are free. So is the application that can keep you virtually at work even if you are absent physically. With GoToMeeting all you need do is TAP to attend online meetings. Also, through the application you can view slide presentations, design mockups, spreadsheets, reports – whatever meeting presenters choose to share on-screen. Get started for free.

3 **DRAGON DICTATION:** We all have used umpteen voice recognition applications for Windows PCs. There's one for the iPad as well, powered by Dragon Naturally Speaking. It allows you to easily speak and instantly dictate small text or lengthy email messages.

4 **DESKTOP CONNECT:** A desktop viewer that allows you to view and control Windows, Mac OSX and Linux computers as if you were sitting in front of them, or observe others as if you were watching over their shoulder. Get started at Rs 675.

5 **KEYNOTE:** While this presentation application for the Mac needs to be redesigned to suit the iPad's requirements. The application has retained its basic feature to help you build an appealing presentation, complete with animated charts and transitions. One could use Apple-designed themes, custom graphic styles, and animations and effects to add glitter to the presentations. The application is also PowerPoint compatible. Get started at Rs. 450.

— Compiled by Anoop Chugh

very few organisations are taking any action against such violators. Most are turning a Nelson's eye to such acts.

The Cyber Cells set up in India are there to help in this regard. However, before approaching them, it is advisable that IT managers do some groundwork and investigation on their own. For example, in the case of emails luring the public with job offers that do not exist, the IT manager should first try and trace the origin of the email. Of course, one needs to be able to analyse the header of the emails to do this. This would speed up matters and make it easier to take the case to the Cyber Cell.

Approaching legal representatives, be they internal or external lawyers, and seeking their help to take such issues to the Cyber Cell would definitely be advantageous and beneficial. The IT Act 2000 depends on the IPC (Indian Penal Code) and this is where a lawyer or legal representative will add value in convincing the Cyber Cell to take action.

Of course, in such instances, the IT manager must think on his feet and ensure that the recipient of any defaming or false emails does not delete the original email. This would be disastrous, as invaluable evidence would be destroyed.

An IT manager must also be aware of the laws and cases cited under the IT Act 2000, including Cyber Squatting of domain names, intellectual property, copyright law, trademark law, data protection and privacy laws, among other things. Although most would be tackled by the legal representatives of the company, the IT manager can add value with his knowledge of such issues.

So where does the buck stop for the IT manager? It would be worthwhile to either take up a course on cyber laws or to educate yourself by reading books on cyber laws and the IT Act 2000. This will definitely add value both to the manager and the organisation. ITNEXT

The author is the head of IT for Tata Services and is responsible for IT security of the head office of the group.