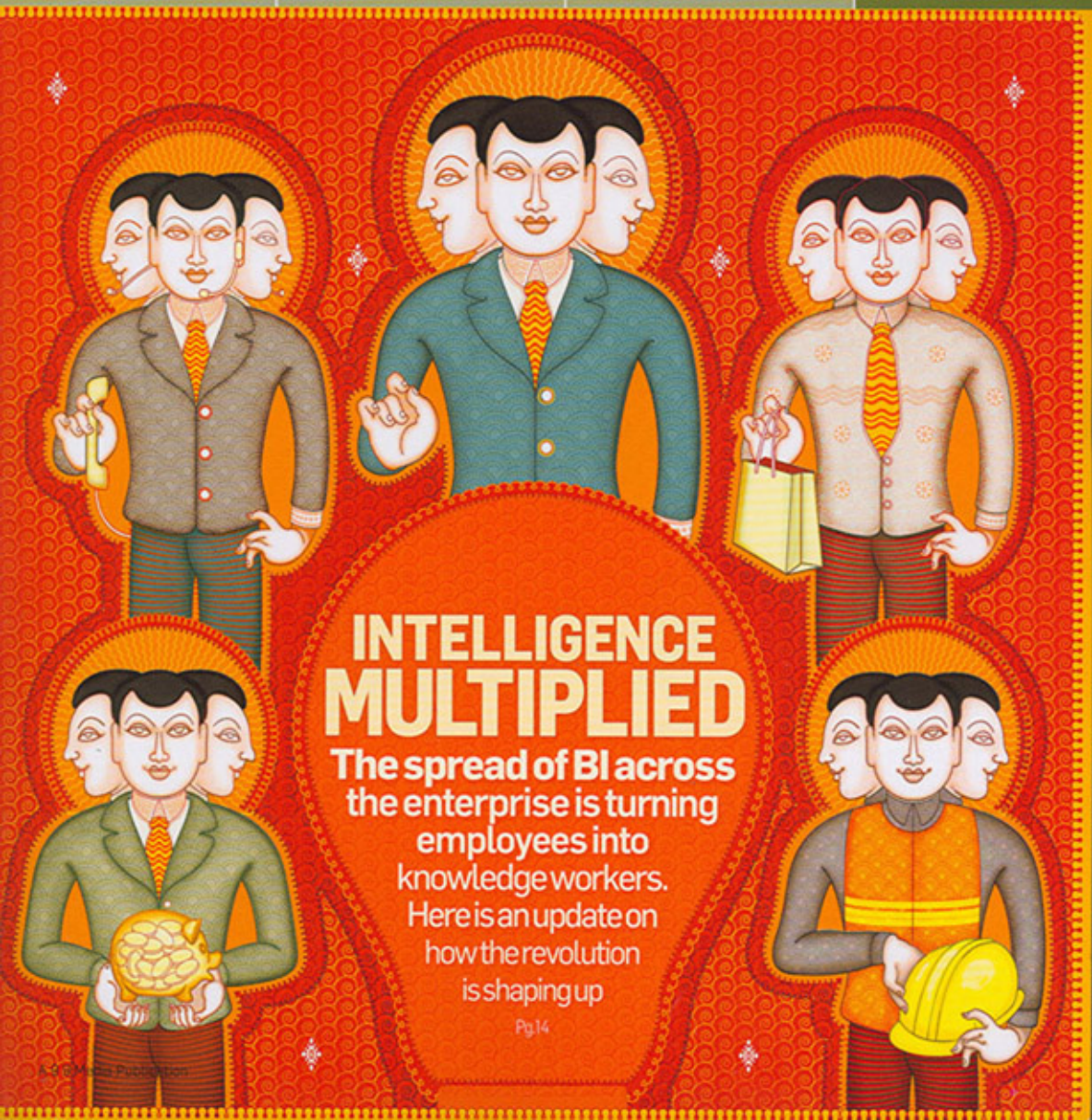
AUGUST 2010 / RS. 100
VOLUME 01 / ISSUE 08

IT NEXT

MEDIA FOR THE NEXT GENERATION OF CIOs



INTELLIGENCE MULTIPLIED

The spread of BI across the enterprise is turning employees into knowledge workers. Here is an update on how the revolution is shaping up

Pg 14

SECURING the AIRWAVES

A Wi-Fi plan should be robust enough to address **security concerns** and clean enough to **keep legal risks** at bay

BY BERJES ERIC SHROFF

Aren't we all at some stage disgusted to see the mesh of those wires connected to our computers? Don't we wish we could make it clutter-free by getting rid of at least some of the wires? Don't we wish we could connect to the Internet or access the printer without those wires, securely?

Well, Wi-Fi lets users access the Internet and other network resources, without the hassles of plugging in the Ethernet cable. It offers them convenience of moving their machines around the office, without losing connection to the Internet or other network resources.

Installing a Wi-Fi LAN in the office initially helps you set up the network for a fraction of the cost, especially if your office does not have structured cabling. Wireless access to the Internet at airports, restaurants and coffee shops is all courtesy Wi-Fi.

However, like most good things in life, Wi-Fi comes with its share of drawbacks. These negatives appear in the form of security risks, which can be of various types. These could compromise your confidential data, lead to theft of bandwidth resources, amount to a legal action against your organisation and in some extreme cases even land you behind bars!

Considering all these risks, is the convenience of Wi-Fi worth it? Alternatively, can we protect ourselves and the organisation against these risks, and at the same time take advantage of the benefits Wi-Fi has to offer?

While there cannot be complete security, there are ways to mitigate, and to an extent, circumvent some of these risks. So how should an organisation go about taking advantage of the technology and at the same time, protect itself from the risks identified above?

It all starts with planning

Planning the strategic location to install the access points, the strength of these strategically placed access points, who in the organisation can and cannot use the Wi-Fi technology (including visitors), and the security levels of Wi-Fi such as authentication or encryption are all very important prior to even procuring the infrastructure.

Aspects such as thickness and material of the outer walls and ceilings, and those of the different cabins inside also play an important part in the planning process.

Why is all this so important?

Well, let's say that you have installed an access point near a window, or maybe close by, which causes the signal to leak outside the office. A person with a laptop in the opposite building or maybe even a floor above or below your office is able to access the Internet using your facility. He is now going to 'steal' your bandwidth resource to access the Internet.

Not much harm done here, but what if this person now uses your Internet facility through Wi-Fi, to hack into another organisation? How would you ever be able to trace this person? Like it or not, legally, it's your organisation that is going to get penalised. Of course, this intruder can also hack into your own network, thus compromising your organisation's confidential data. And once again, how are you ever going to be able to trace him or her?

STRONG PASSWORDS RESIST BEING COMPROMISED THROUGH BRUTE FORCE ATTACKS. DISABLING SSID BROADCAST FURTHER MITIGATES RISKS.

Securing the installation

Let us address some technical aspects of securing a Wi-Fi installation in your organisation. Start by using strong passwords, to prevent the likelihood of this being compromised through brute force attacks. Also, it's strongly advisable to rename the default administrator user name. Disabling the SSID broadcast i.e. your network's 'name' is a good idea and mitigates the risk of an attack.

Restricting access through MAC address filtering will not deter a hard-core hacker, as MAC address spoofing is not that great a deal, but a combination of disabling the SSID broadcast and restricting access through MAC address filtering, will deter most novice hackers or script kiddies from compromising your Wi-Fi facility. Although it's not always possible to do so, especially in large organisations, it's a good idea to switch off a Wi-Fi network when not in use.

Personally, I am very uncomfortable with DHCP and prefer using static IP addresses, as this definitely helps as an added layer of security, in spite of its slight inconvenience. Ensure that your router's firewall is not disabled while on the other hand, firewall on all desktops and laptops is enabled.

Encryption scrambles messages sent over the air. Deploying encryption technologies such as WPA2 with EAP authentication, TKIP/RC4 or AES-CCMP encryption technology, is a must for large organisations and depending on the nature of the business, this is applicable to SMBs too. WEP encryption is outdated and should be avoided at all costs, as it can be compromised in a matter of minutes. Also, there is nothing stopping you from deploying a second layer of encryption, for added security.

Deploying a Remote Authentication Dial In User Service (RADIUS) server for authentication, authorisation and accountability should definitely not be overlooked by medium and large

1. Prepare a detailed plan for Wi-Fi installation
2. Ensure strong passwords are used and the default administrator user-name is changed
3. Deploy encryption technologies such as WPA2 with EAP authentication, TKIP/RC4 or AES-CCMP, but avoid WEP which is outdated
4. Disable SSID broadcast and restrict access through MAC filtering
5. Ensure firewalls are enabled on all devices, including laptops
6. Educate your users for safe usage of Wi-Fi
7. Conduct periodic IT audits

EDUCATING USERS ON SAFE USAGE OF WI-FI WILL HELP CONTROL COSTS FOR DEPLOYMENT OF EXPENSIVE TECHNOLOGIES SUCH AS JAMMERS

organisations. This will ensure that the user is authenticated before being authorised to access the network and at the same time, a track is kept of usage in terms of time and data transferred.

The IT manager of an organisation must be aware that there exists a plethora of free downloadable software on the Internet for detecting presence of Wi-Fi devices and hacking Wi-Fi facilities or capturing and deciphering packets. The IT manager must also be aware of the laws relating to Wi-Fi and the consequences of a Wi-Fi system being compromised.

Education is key

Educating users is a very important aspect, which sadly gets neglected by the best of organisations. Even in the absence of a Wi-Fi facility in your organisation, educating laptop users regarding Wi-Fi security is absolutely essential.

There are multiple dimension of educating them. It is important that they know about the risks involved when using Wi-Fi in public places like coffee shops and airports and how these risks can be mitigated, but it is more important that they are aware of the risks when they are in office, even when your organisation has decided against deploying Wi-Fi technology and your LAN is a wired network.

How? Well, your laptop users may access Wi-Fi at home or at airports and when they return to office, most of the time, Wi-Fi on their laptops is still enabled. As a result of this, they will be prompted of the presence of any external Wi-Fi signals leaking into your building / office. Either intentionally or unintentionally, a user may clicks 'yes,' to connect to this external network, which could very well be from a rogue access point. In this case, without the user's knowledge, the hacker can compromise not only the user's laptop, but your entire LAN security with firewalls and IDS and IPS. All your security precautions could go for a toss.

If you are able to detect, or an audit reveals presence of rogue signals in your office building, then a solution might be to install jammers to prevent those signals from entering your organisation's premise. However, this could be an expensive proposition, and educating users on a regular basis is the cheapest and best alternative. Also, software to ensure that at any given point in time, only one network connection can be present on a laptop is available. This solution too, can address the risk.

The IT manager should, even in the absence of Wi-Fi deployment in the organisation, have the network audited for rogue signals, for reasons mentioned above. If Wi-Fi is deployed, then apart from the security measures such as encryption and authentication methods used, the audit must also include rogue signals leaking into the office. At the same time, audit for signals leaking outside the organisation from your own network should also be carried out.

There are even phones under development that would help organisations to switch seamlessly from cellular networks to wifi networks without a call drop.

Be it a wireless or a wired network, educating users and scheduling periodic audits is extremely important. Educating users on safe usage of Wi-Fi could help you control costs for deployment of expensive technologies such as jammers, while periodic audits will enable you to identify the loopholes and plug those. Many organisations ignore these two activities and as a result, end up spending more on technologies while also increasing the risk of their organisation's data being compromised. ITNEXT

The author is Manager-Information Technology, Tata Services Limited