



DEAL MAKER:

T. Boone Pickens talks about qualities of good leaders

P10

CHARLOTTE BUSINESS JOURNAL

DONE DEAL:

How CB deal for Trammell Crow has impacted offices here

P13



VOLUME 22 NUMBER 1 • MARCH 30, 2007

www.charlottebusinessjournal.com • \$1.50

HOW TO: KEEP YOUR COMPUTER NETWORK SECURE

Develop and implement clear policies for your company's computers and network to create effective IT security

BEA QUIRK
CONTRIBUTING WRITER

The most important thing to keep in mind when securing your company's computer network is that while technology is important, security is first and foremost a state of mind and a way of doing business.

"It's not so much about what you install, but rather the process of making sure it stays tight going forward," says John Garrett, a partner in CNP Technologies, a Charlotte-based data, voice and security-services firm.

That means developing policies and procedures regarding the use of company computers and its network and then making sure employees understand and follow them. "Security is a practice," says Jeff Glass, network engineer for the Charlotte School of Law. "It's a matter of being diligent and mindful."

For help in setting up a security policy, visit www.sans.org, a leading resource for information security training, says Bill Chu, chairman of UNC Charlotte's College of Computing and Informatics department of software and information systems.

But security is more than installing firewalls and spam filters. It also means looking at your physical surroundings.

"Physical security is often ignored," Chu says. "If your computers aren't secured, people can walk right up to them and steal them. Keep computers with sensitive information in a locked room, and control who has keys."

Glass recommends locking your keyboard so that it requires a password before it can be used and "shred-



photo CLARK G. CURTIS

You may want to consider an outside network-hosting operation, says Bill Chu, chairman of the department of software and information systems at UNC Charlotte.

ding anything you don't want walking out the door."

Don't forget about laptops. "The main problem with laptops is that they're mobile and so are more exposed," Glass says. Don't use them in WiFi areas because those networks are unsecured. He also suggests encrypting sensitive information on the hard drive or storing data on a USB flash drive. "But you still have the mobility problem."

However, you may not have much flexibility regarding the security measures you take, depending on the kind of business you are in and whether you conduct e-commerce on your Web site. Federal regulations

TOPTIPS

- **Computer security** is not a one-time effort, but an ongoing activity.
- **Don't forget** the physical security of your computers, including laptops.
- **Research** what regulations affect your company's security requirements.
- **Consider** using outside companies for hosting network operations.

require companies in the financial services, insurance and health-care industries, as well as all publicly-traded firms, to follow a variety of security measures when conducting business online. Credit-card companies also have security requirements.

Glass recommends researching any governmental requirements because "enforcement starts from the get-go."

For companies with just a few computers, setting up firewalls, spam filters and virus protection can be handled by non-techies. Glass suggests turning to Windows Small Business Server for help.

But setting up wireless networks and making sure they are secure "is not user-friendly," Glass says, and you may want to turn to an IT professional or an IT student at a local college to do it for you.

Consider a hosted operation, Chu suggests. Before choosing a host, check its references, ask whether it uses dedicated or shared systems and what security policies and procedures it has in place. "The more sophisticated information you have, the more trust you must place in the hosting company."

Regardless of the type of network you use, Garrett recommends you have an outside contractor conduct an internal and external security assessment at least annually — although he says quarterly is even better. "The consultants will try to penetrate your network to figure out where the holes are so you can make adjustments."

Bea Quirk is a Charlotte-based free-lance writer who can be reached at beawrites@aol.com.