

# Security, Security, Security

Since the terrorist attacks on September 11, security has been foremost on the minds of both IT professionals and business executives. Despite the importance attributed to information security, however, recent surveys and security analyses of commercial and government organizations indicate that companies have not taken adequate steps to secure network resources. For example, on November 9, 2001, the U.S. House Government Reform Subcommittee on Government Efficiency held a public hearing to share the results of security analyses on 24 U.S. government executive branch departments and agencies. (See [www.house.gov/reform/gefmir/hearings/2001hearings/1109\\_computer\\_security/1109\\_witnesses.htm](http://www.house.gov/reform/gefmir/hearings/2001hearings/1109_computer_security/1109_witnesses.htm).) Two-thirds of the departments and agencies failed.

All 24 agencies showed significant weaknesses in two areas in particular: security program management, which refers to the overall controlled approach to managing information systems, and access controls. As a witness to the hearing, U.S. director of information security Robert F. Dacey succinctly explained why strong access controls are critical to the success of a security policy: "Weak access controls for sensitive data and systems," Dacey explains, enable "an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage." Dacey adds that "poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise." (See [www.house.gov/reform/gefmir/hearings/2001hearings/1109\\_computer\\_security/testimony\\_dacey.DOC](http://www.house.gov/reform/gefmir/hearings/2001hearings/1109_computer_security/testimony_dacey.DOC).)

## ROUNDING UP YOUR COMPANY'S NETWORK RESOURCES

As a network administrator, you know that enhancing security involves implementing layer upon layer of controls. On an existing network, however, how do ensure that you have closed all the gaps and adequately protected your company's data? Faced with daunting task of opening your company's doors to the Internet while simultaneously providing iron-clad protection for every resource on your company's network, you may feel much like the man in this month's cover illustration—as if those resources are almost beyond your reach and your tools for securing them are as flimsy as a rope. In this issue, Alan Mark helps you get back to basics and take the first steps to tightening security on your company's network and bringing those resources under your control. (See "Rethinking Security: Seven Steps to Tighten Network Security" on p. 6.)

Of course, ensuring that only authorized users can access your network resources is the bare minimum you can do to protect your information systems. This step is one that Novell can help you with. Novell access and security solutions enable organizations to securely manage access to

applications, databases, and platforms. (For a list of these solutions, see the "Novell Access and Security Solutions" sidebar on p. 12.) With these platform-independent solutions, users have only one set of credentials to access all network resources, regardless of the platform supporting these resources.

This issue features the stories of two organizations that have deployed Novell access and security solutions: Taipei County Government and Beneficial Life Insurance Company.

Taipei County Government uses Novell eDirectory 8.5.1, Novell Account Management 2.1, Novell Modular Authentication Service (NMAS) 1.0, and BorderManager Authentication Services (BMAS) 3.6. (See "Taipei County Government Secures Access to Its Assets" on p. 24.) This solution solved Taipei County Government's access-management problems and now enables 1,700 employees to access all of the resources to which they have rights by entering only one set of credentials. This solution also better protects Taipei County Government's network resources by requiring one-, two-, or three-factor authentication, depending on the level of importance or confidentiality of the information to which an employees seek access.

Beneficial Life uses eDirectory 8.5, BorderManager Firewall Services 3.5 and iChain 1.5. (See "Beneficial Opens Its Internet Doors to Customers, Agents, and Employees" on p.36.) Beneficial Life uses eDirectory alone to control access to the NetWare servers running on its LAN. In combination with iChain, eDirectory also controls web access to applications and information on Beneficial Life's intranet. iChain also provides users with single sign-on access to these web-based resources. In addition, iChain uses Secure Sockets Layer (SSL) encryption to secure Beneficial Life's confidential information as it traverses the Internet. BorderManager Firewall Services and iChain also accelerate web content—content coming into and leaving Beneficial Life's network.

## GOING FROM BAD TO WORSE

Implications of recent terrorist attacks aside, cyber attacks (whether driven by terrorists or bored teenagers) are on the rise. In 1999, the CERT Coordination Center received reports of 9,859 security-related incidents for the year. This number nearly quadrupled during only the first nine months of 2001: During this time, the CERT Coordination Center received reports of 34,754 security incidents. (See [www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).) Mind you, this number reflects only reported incidents. The CERT Coordination Center estimates that as many as 80 percent of attacks go unreported.

Clearly, protecting network resources must be a top priority—not necessarily because of what might happen but because of what has happened. With your priorities straight, you can begin to gain some measure of control over who accesses what on your company's network. ●