their home base, although it does happen sometimes. Many sites on the Internet do not have firewalls, and do not believe that they are at risk because they are public sites. The truth is that poorly protected sites are appealing targets for attackers seeking to launder their connections. Packets can be traced to their origin by their source address. In attacks other than denial-of-service, where no response is necessary, the attacker must either use the real source address or use source routing so responses will be directed back. You can discover source addresses by examining firewall logs, connection logs and via traffic logging systems. But do most sites attempt to trace all probes and intrusions? One expert describes several useful criteria for deciding how much energy to expend in tracking an attack back to its source. The severity of the incident, the damage done, or the persistence of the attacker are important criteria. What can you do? Besides strengthening you own defences, you can make it easier for other sites to find the person or persons who manage you site security. You should also practice reading logs, tracking down you own systems and using sniffers. *Network Magazine, February 1999, pp. 76-77.*

The need for host authentication, *Robert Moskowitz.* Internet addresses were created by researchers to provide a host identifier independent of the media interface name. Inevitably, Internet addresses also became the packet routing information, thus confounding these two key features in an Internet protocol. At best, IP addresses are weak assertions of identity. As long as an IP address performs routing functions, it can never really be reworked into a trustworthy identity. Today's business processes are exposing requirements for limited trust among untrustworthy systems. Protocol hacks, such as tunnelling and dynamic virtual address assignments, merely mask the demand for real, secure host identifiers. Careful reviews of the state of IP by Internet and security experts confirm the need for a host identity based on public key cryptography. Furthermore, we require a mechanism by which two hosts can actually work together with their cryptoidentities. IP addresses have never been unique host identifiers. With IP telephony, a new peer-to-peer process, the lack of a host identity for mapping to a 'phone number' generates the need for a rendezvous protocol. SNMPv3 uses a secret key as the host/user identity and establishes packet authentication via a hashed message authentication code. This packet authentication lets the receiving SNMP system truly know with which host/user it's communicating. Each host in the SNMP community is hardwired with the other host identity's secret key. The SNMP identifier that corresponds with the secret key is 'securityName' and is included in the authentication message. While this approach far outshines the use of IP addresses, it poses two problems: scaling and 'trust leakage'. With regard to scaling, shared access secrets must be kept secret, meaning each host must have a secure file of them; they must never exist in a public store. Next is the trust leakage problem. Every host that communicates with any other host must possess the secret key needed to prove the authentication of packets received from the host with which it is communicating. In this approach, the key can be stolen, enabling another host to impersonate the secret key's true owner. Thankfully, public key cryptography addresses both of these problems. The alternative is continued proliferation of host authentication techniques that will give attackers more ways to defeat authentication or to use host authentication as a denial-of-service attack. *Network Computing, February 22, 1999, pp. 109-110.*

Combating computer viruses, *Lenny Liebmann.* Computer virus infection rates jumped 48% during 1998. That's the sobering report of the 1998 Computer Virus Prevalence Survey from the International Computer Security Association. The biggest problem is caused by the macro viruses that users pick up from E-mail attachments or bring from their home computers. Hoaxes are yet another facet of the virus problem. Experts strongly recommend supplementing anti-virus software with other preventative measures, such as E-mail scanning solutions. Trend Micro's InterScan VirusWall, when it identifies an infected E-mail message, either cleans or quarantines the file, and then sends E-mails to the sender, the recipient and any designated administrators letting them know that the file had to be quarantined. Another way to strengthen virus protection is to tie anti-virus programs to systems management tools. In addition to choosing technologies to provide virus protection, IT managers must also manage employees

with training, policies and procedures. As the business value of data, applications and communications grows, the threat that viruses pose is growing as well. Managers need to look at the problem as an enterprise threat. Protecting corporate data is, after all, the ultimate goal. *Beyond Computing, January/February 1999, pp. 51-53.*

Securing Windows NT server, *Tom Yager.* In this article, the author discusses how to secure network assets using features embedded in Microsoft's operating systems. While outsiders are a threat to your information assets, internal users are a more likely source of trouble. One step to security is to install Windows NT Server 4.0 with Service Pack (SP) 4 which incorporates all the stability fixes released with SP 3, plus the many security patches that Microsoft released as hotfixes after SP 3. Windows NT's first and best defence against intruders is its authentication system. Windows 95, 98 and NT Workstation clients not only exchange encrypted user ID and password data, but also use a proprietary challenge/response protocol. This method ensures that authentication data is never expressed the same way twice. It also effectively foils internal hackers who capture network packets, hoping to decipher them or play them back to gain unauthorized access. With external access, you must strike a balance between convenience and data protection. To mitigate external security threats, you need to do more than install a firewall. For example, to secure your Internet and remote access servers from packet-sniffing bandits and other foes, run those servers on an isolated LAN. In the case of dial-up users, the best protection is to enable call-back security. The VPN approach is safer than ordinary Internet access because all traffic is encrypted. Even a packet-sniffing hacker will get nothing for his trouble. Securing Windows NT servers goes well beyond setting permissions on files. A holistic approach, which considers physical access, users roles, desktop policies and server restrictions is the only way to ensure your data is truly safe. After you've secured your servers, determine how each requested change to your network will affect security. *Network Magazine, February 1999, pp. 48-50.*

Mapping a network security strategy, *Bruce Middleton.* Computer networks are operating in an increasingly risk-prone environment. Hackers, competitors, dishonest data brokers and disgruntled employees have a seemingly endless menu of attacks to choose from. This article recommends a number of steps as a guide to securing company networks. The company should first develop an official IS security policy with guiding principals that communicate corporate security objectives. The policy should include a discussion of computer security responsibilities, penalties for non-compliance and classification of information. The security managers also needs to understand the topology of the network. He should examine the organizational infrastructure, noting the current configuration with an eye toward security holes and performance issues. The security manager should next talk with employees to assess how well they know the system and their roles and responsibilities in keeping it safe. The security plan should assign an individual or group in the company to be responsible for managing change. Each machine should have maximum security to the degree that it does not significantly impede required network performance. *Security Management, February 1999, pp. 79-85.*

More bark than bite, *Joanna Makris.* Managed firewall services are supposed to be the new weapon in the battle of the breach: providers take on all of the notoriously difficult firewall tasks, from policy planning, installation and configuration to software licensing, encryption and maintenance. Network managers who want to avoid trouble can get some firewall help from at least 12 providers now plying the trade including: AT&T Co., Infonet Service Corp. and Sprint Corp. Internet Service Providers and long-distance carriers tend to be the main suppliers of such services. They set up firewalls at their data centres or on the customer premises and, either way, they monitor customer security remotely through their NOCs. But even if a carrier can spot a vulnerability and come up with a way to plug the hole, it's not likely to guarantee stronger security. What they do guarantee are network connectivity and response time. *Data Communications, March 1999, pp. 37-50.*