A reader from Singapore wrote,

"I would like to know what are your views on email forwarding; i.e., should staff be allowed to forward mails to their external accounts (Internet mail accounts)? I work in a hospital and I have request from Doctors who asked that the auto-forward feature of their Lotus Notes e-mail messages be enabled to forward their e-mail to their external Internet mail account so that they can read it while at home or overseas. There were some security concerns here that confidential mails would then end up circulating in the Internet."

This question forces us to confront the conflict between theory and practice. E-mail and other traffic on the Internet has no inherent confidentiality. In theory, anyone capable of intercepting TCP/IP packets anywhere during transmission can breach confidentiality. Thus, again in theory, anyone with access to the equipment of Internet Service Providers, Internet backbone transmission lines, and even to the public switched telephone network can intercept packets. With downlink footprints from satellite relays amounting to square miles, practically anything can in theory be intercepted from much of the traffic circulating on the Internet.

However, in practice, reported breaches of confidentiality have almost all resulted from data access at the end points, not in transit. Insider attacks and breaches of server security have been responsible for most of the data interceptions that have reached the press and the courts.

A practical impediment to effective interception of meaningful data in transit is the datagram routing that underlies the Internet: datagrams are packets of information with origin and destination information; store-and-forward transmission allows these datagrams to be sent through the Internet via different routes from other packets in a message stream. Routing tables can be updated in real time to reflect changes in traffic density or availability of specific links to other destinations on the Internet, so there is no guarantee that packets from the same message will travel the same route or arrive in the proper sequence (sequence numbers allow reassembly of the original message). Therefore seizing individual packets at random anywhere other than the origin and destination of packets is unlikely to result in very much result for the effort.

Nonetheless, best practices do recommend that encryption be used for communication of sensitive data; therefore, many organizations install Virtual Private Networks (VPN) for communication with established trading partners. VPN software is also available for "tunneling" through the Internet from a remote workstation over non-secure communications lines. A simple example of such a link-encryption function is the Web-based e-mail services that use SSL to establish a secure link to the e-mail server (i.e., they use HTTPS instead of just plain HTTP). The user can pick up e-mail from the corporate server without having it forwarded in the clear to an insecure external e-mail service. Some of the e-mail products include facilities for direct...
communication between a secure e-mail servers and the users' e-mail clients.

Using "VPN tunneling software" as a search string in the GOOGLE search engine brought up hundreds of hits, many of them for specific products and data sheets, so I am sure you will be able to find a solution that fits your needs.

In your specific case, the fact that some of the e-mail might include confidential patient data means that the relatively modest investment in VPN technology would make a lot of sense for you in complying with your local legal requirements for protecting such data. But once you have the VPN in place, please make sure that all your users have also implemented driver-level data encryption on their computers so that the received, decrypted data are not susceptible to discover if someone steals their laptop or home computer.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.