Protecting Laptops

Marshall D. Abrams, The MITRE Corporation
1820 Dolley Madison Blvd., McLean, VA 22102 <abrams@mitre.org>

Ann Marmor-Squires, TRW Integrated Engineering Division
One Federal Systems Park Drive, Fairfax, VA 22033 <ann.marmor@trw.com>

Bernard Ramsey, Federal Aviation Administration
800 Independence Avenue, SW, Washington, DC 20591 <Bernard.Ramsey@faa.dot.gov>

Jerry Trammel, Kaiser Permanente
393 E. Walnut, Pasadena, CA 91188 <Jerry.J.Trammel@kp.org>

This forum will address experience in protecting mobile computers such as laptops and smaller formats. In particular, we will address protecting the data on the laptops in case of loss, theft, exposure, Trojan horses, and corruption. The discussion will encompass perceptions of risk, threat, and vulnerability; countermeasures taken; how the procedures and products were selected, implemented, and received; and any other relevant information.

In this discussion, representatives from government and the business community will focus on strategies to protect laptop computers. The laptop is a highly proliferated form of information and communications technology—the "notepad" of the nineties. This panel will review the significance of laptop loss and the need for security.

The following key issues will be discussed:
- Significance of stored information on laptops
- Impact of loss:
  - Capitol loss (laptops cost $3,000 to $4,000)
  - Data loss/compromise. Potentially far greater than capital losses, data compromise can be disastrous. All data has value. Examples: Laptops of executives negotiating mergers, bank officials, or insurance adjusters. How do we know if a laptop was stolen for hardware resale or for its stored data? (Random or targeted theft?)
- Protection strategies:
  - Access
    - Passwords (common but usually easy to break)
    - Electronic keys
  - Physical security
  - Security policies

Our job is to provide secure access to quality data. We once protected data that resided on a single floor in a secure building. Now we must deal with data that is as mobile and in some cases only a few keystrokes away via Local Area Networks, Wide Area Networks, and the Internet, for example. As our focus changes, the customers and clients must now assume more responsibility.