Protecting the Portable Computing Environment

Phillip Q. Maier

Payoff

The use of portable computing has become a standard tool in the business world today, yet its use can present a wide array of threats to the business it is intended to benefit. This article provides detailed analysis of the various threats and risks of allowing portable computing in a business environment, including direct and indirect data disclosure, theft and destruction of computer data. Each of the identified risks are addressed with various protection methodologies that can realistically be applied in today’s business environment in order to reduce the risks of portable computing.

Introduction

Today's portable computing environment can take on a variety of forms, from remote connectivity to the home office to remote computing on a standalone microcomputer with desktop capabilities and storage. Both of these portable computing methods have environment-specific threats as well as common threats that require specific protective measures. Remote connectivity can be as simple as standard dial-up access to a host mainframe or as sophisticated as remote node connectivity in which the remote user has all the functions of a workstation locally connected to the organization's local area network (LAN). Remote computing in a standalone mode also presents very specific security concerns, often not realized by most remote computing users.

Portable Computing Threats

Portable computing is inherently risky. Just the fact that company data or remote access is being used outside the normal physical protections of the office introduces the risk of exposure, loss, theft or data destruction more readily than if the data or access methods were always used in the office environment.

Data Disclosure

Such simple techniques as observing a user's remote access to the home office (referred to as shoulder surfing) can disclose a company's dial-up access phone number, user account, password or log-on procedures; this can create a significant threat to any organization that allows remote dial-up access to its networks or systems from off-site. Even if this data or access method isn't disclosed through shoulder surfing, there is still the intermediate threat of data disclosure over the vast amount of remote-site-to-central-site communication lines or methods (e.g., the public phone network). Dial-up access is becoming more vulnerable to data disclosure, because remote users can now use cellular communications to perform dial-up access from laptop computers.

Also emerging in the remote access arena is a growing number of private metropolitan wireless networks, which present a similar, if not greater, threat of data disclosure. Most private wireless networks don't use any method of encryption during the free-space transmission of a user's remote access to the host computer or transmission of company data. Wireless networks can range in size from a single office space serving a few users to multiple clusters of wireless user groups with wireless transmissions linking them to different buildings. The concern in a wireless data communication link is the threat of...
Unauthorized data interception, especially if the wireless connection is the user's sole method of communication to the organization's computing resources.

All of these remote connectivity methods introduce the threat of data exposure. An even greater concern is the threat of exposing a company's host access controls (i.e., a user's log-on account and static password), which when compromised may go undetected as the unauthorized user accesses a system under a valid user account and password.

**Data Loss and Destruction**

Security controls must also provide protection against the loss and destruction of data. Such loss can result from user error (e.g., laptop computers may be forgotten in a cab or restaurant) or other cause (e.g., lost baggage). This type of data loss can be devastating, given today's heavy reliance on the portable computer and the large amount of data a portable computer can contain. For this reason alone some security practitioners would prohibit use of portable computers, though increased popularity of portable computing makes this a losing proposition in most organizations.

Other forms of data loss include outright theft of disks, copying of hard disk data, or loss of the entire unit. In today's competitive business world, it is not uncommon to hear of rival businesses or governments using intelligence gathering techniques to gain an edge over their rivals. More surreptitious methods of theft can take the form of copying a user's diskette from a computer left in a hotel room or at a conference booth during a break. This method is less likely to be noticed, so the data owner or company would probably not take any measures to recover from the theft.

**Threats to Data Integrity**

Data integrity in a portable computing environment can be affected by direct or indirect threats, such as virus attacks. Direct attacks can occur from an unauthorized user changing data while it is outside the main facility on a portable user's system or disk. Data corruption or destruction due to a virus is far more likely in a portable environment because the user is operating outside of the physical protection of the office. Any security-conscious organization should already have some form of virus control for on-site computing; however, less control is usually exercised on user-owned computers and laptops. While at a vendor site, the mobile user may use his or her data disk on a customer's computer, which exposes it to the level of virus control implemented by this customer's security measures, which may not be consistent with the user's company's policy.

**Other Forms of Data Disclosure**

The sharing of computers introduces not only threats of contracting viruses from unprotected computers, but also the distinct possibility of unintended data disclosure. The first instance of shared computer threats is the sharing of a single company-owned portable computer. Most firms don't enjoy the financial luxury of purchasing a portable computer for every employee who needs one. In order to enable widespread use of minimal resources, many companies purchase a limited number of portable computers that can be checked out for use during prolonged stays outside of the company. In these cases, users most likely store their data on the hard disk while working on the portable and copy it to a diskette at the end of their use period. But they may not remove it from the hard disk, in which case the portable computer's hard disk becomes a potential source of proprietary information to the next user of the portable computer. And if this computer is lost or misplaced, such information may become public. Methods for protecting against this threat are not difficult to implement; they are discussed in more detail later in this article.
Shared company portables can be managed, but an employee's sharing of computers external to the company's control can lead to unauthorized data disclosure. Just as employees may share a single portable computer, an employee may personally own a portable that is also used by family members or it may be lent or even rented to other users. At a minimum, the organization should address these issues as a matter of policy by providing a best practices guideline to employees.

**Deciding to Support Portables**

As is the case in all security decisions, a risk analysis needs to be performed when making the decision to support portable computers. The primary consideration in the decision to allow portable computing is to determine the type of data to be used by the mobile computing user. A decision matrix can help in this evaluation, as shown in Exhibit 1. The vertical axis of the decision matrix could contain three data types the company uses: confidential, sensitive, and public. Confidential data is competition sensitive data which cannot be safely disclosed outside the company boundaries. Sensitive data is private but of less concern if it were disclosed. Public data can be freely disclosed.

### Decision Matrix for Supporting Portable Computers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Classification</td>
<td>Not permitted</td>
<td>with stringent Safeguards</td>
<td>with Minimal Safeguards</td>
<td>with Few Safeguards</td>
</tr>
<tr>
<td>Company Confidential</td>
<td>Recommended Action</td>
<td>Not Permitted</td>
<td>Not Permitted</td>
<td>Not Permitted</td>
</tr>
<tr>
<td>Company Sensitive</td>
<td>Recommended Action</td>
<td>Recommended Action</td>
<td>Not Permitted</td>
<td>-----</td>
</tr>
<tr>
<td>Public Data</td>
<td>Recommended Action</td>
<td>Recommended Action</td>
<td>Recommended Action</td>
<td>Action</td>
</tr>
</tbody>
</table>

The horizontal axis of the matrix could be used to represent decisions regarding whether the data can be used for portable computer use and the level of computing control mechanisms that should be put in place for the type of data involved. (The data classifications in Exhibit 1 are very broad; a given company's may be more granular.) The matrix can be used by users to describe their needs for portable computing, and it can be used to communicate to them what data categories are allowed in a portable computing environment. This type of decision matrix would indicate at least one data type that should never be allowed for use in a mobile computing environment (i.e., confidential data). This is done because it should be assumed that data used in a portable computing environment will eventually be compromised even with the most stringent controls. With respect to sensitive data, steps should be taken to guard against the potential loss of the data by implementing varying levels of protection mechanisms. There is little concern over use of public data. As noted, the matrix for a specific company may be more complex, specifying more data types unique to the company or possibly more levels of controls or decisions on which data types can and cannot be used.
Protection Strategies

After the decision has been made to allow portable computing with certain use restrictions, the challenge is to establish sound policies and protection strategies against the known threats of this computing environment. The policy and protection strategy may include all the ideas discussed in this article or only a subset, depending on the data type, budget or resource capabilities.

The basic implementation tool for all security strategies is user education. Implementing a portable computing security strategy is no different; the strategy should call for a sound user education and awareness program for all portable computing users. This program should highlight the threats and vulnerabilities of portable computing and the protection strategies that must be implemented. Exhibit 2 depicts the threats and the potential protection strategies that can be employed to combat them.

### Portable Computing Threats and Protection Measures

<table>
<thead>
<tr>
<th>Threat</th>
<th>Data Disclosure</th>
<th>Data Loss/Destruction</th>
<th>Data Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Transmission</td>
<td>Direct Theft</td>
<td>Virus Tampering</td>
</tr>
<tr>
<td>Disclosure</td>
<td>Disclosure Theft</td>
<td>Indirect Theft</td>
<td>Malicious</td>
</tr>
<tr>
<td>One Time Passwords</td>
<td>Encryption Software</td>
<td>Physical Controls Antivirus Software Access Controls</td>
<td></td>
</tr>
<tr>
<td>Protection Hardware Control</td>
<td>Encryption Color-Coded Physical Control Disks Procedures</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User Validation Protection

The protection strategy should reflect the types of portable computing to be supported. If remote access to the company’s host computers and networks is part of the portable computing capabilities, then strict attention should be paid to implementing a high-level remote access validation architecture. This may include use of random password generation devices, challenge/response authentication techniques, time-synchronized password generation, and biometric user identification methods. Challenge/response authentication relies on the user carrying some form of token that contains a simple encryption algorithm; the user would be required to enter a personal ID to activate it. Remote access users are registered with a specific device; when accessing the system, they are sent a random challenge number. Users must decrypt this challenge using the token’s algorithm and provide the proper response back to the host system to prove their identity. In this manner, each challenge is different and thus each response is unique. Although this type of validation is keystroke-intensive for users, it is generally more secure than one-time password methods; the PIN is entered only into the remote users’ device, and it is not transmitted across the remote link.
Another one-time password method is the time-synchronized password. Remote users are given a token device resembling a calculator that displays an eight-digit numeric password. This device is programmed with an algorithm that changes the password every 60 seconds, with a similar algorithm running at the host computer. Whenever remote users access the central host, they merely provide the current password followed by their personal ID and access is granted. This method minimizes the number of keystrokes that must be entered, but the personal ID is transmitted across the remote link to the host computer, which can create a security exposure.

A third type of high-level validation is biometric identification, such as thumb print scanning on a hardware device at the remote user site, voice verification, and keyboard dynamics, in which the keystroke timing is figured into the algorithm for unique identification.

The portable computer user validation from offsite should operate in conjunction with the network security firewall implementation. (A firewall is the logical separation between the company owned and managed computers and public systems.) Remote users accessing central computing systems are required to cross the firewall after authenticating themselves in the approved manner. Most first generation firewalls use router-based access control lists (ACLs) used as a protection mechanism, but new versions of firewalls may use gateway hosts to provide detailed packet filtering and even authentication.

### Data Disclosure Protection

If standalone computers are used in a portable or mobile mode outside of the company facility, consideration should be given to requiring some form of password user identification on the individual unit itself. Various software products can be used to provide workstation-level security. The minimum requirements should include unique user ID and one-way password encryption so that no cleartext passwords are stored on the unit itself. On company-owned portables, there should be an administrative ID on all systems for central administration as necessary when the units return onsite. This can help ensure that only authorized personnel are using the portable system. Although workstation-based user authentication isn't as strong as host-based user authentication, it does provide a reasonable level of security. At the least, use of a commercial ID and password software products on all portables requires that all users register for access to the portable and the data contained on it.

Other techniques for controlling access to portables include physical security devices on portable computers. Though somewhat cumbersome, these can be quite effective. Physical security locks for portables is a common option. One workstation security software product includes a physical disk lock that inserts into the diskette drive and locks to prevent disk boot-ups that might attempt to override hard-disk-resident software protections.

In addition to user validation issues (either to the host site or the portable system itself), the threat of unauthorized data disclosure must also be addressed. In the remote access arena, the threats are greater because of the various transmission methods used: dial-up over the Public Switched Telephone Network, remote network access over such mediums as the Internet, or even microwave transmission. In all of these cases, the potential for unauthorized interception of transmitted data is real. Documented cases of data capture on the Internet are becoming more common. In the dial-up world, there haven't been as many reported cases of unauthorized data capture, though the threat still exists (e.g., with the use of free space transmission of data signals over long-haul links).

In nearly all cases, the most comprehensive security mechanism to protect against data disclosure in these environments is full session transmission encryption or file-level encryption. Simple Data Encryption Standard (DES) encryption programs are available in software applications or as standalone software. Such other public domain encryption as Pretty Good Privacy (PGP) is available, as are stronger encryption methods using...
proprietary algorithms. The decision to use encryption depends on the amount of risk of data disclosure the company is willing to accept based on the data types allowed to be processed by portable computer users.

Implementing an encryption strategy doesn't need to be too costly or restrictive. If the primary objective is protection of data during remote transmission, then a strategy mandating encryption of the file before it is transmitted should be put in place. If the objective is to protect the file at all times when it is in a remote environment, file encryption may be considered, though its use may be seen as a burden by users, both because of processing overhead and potentially extra manual effort of performing the encryption and decryption for each access. (With some encryption schemes, users may have to decrypt the file before using it and encrypt it again before storing it on the portable computer. More sophisticated applications provide automatic file encryption and decryption, making this step nearly transparent to the user.) Portable computer hardware is also available that can provide complete encryption of all data and processes on a portable computer. The encryption technology is built into the system itself, though this adds to the expense of each unit.

A final word needs to be made on implementing encryption for portable users, and that is the issue of key management. Key management is the coordination of the encryption keys used by users. A site key management scheme must be established and followed to control the distribution and use of the encryption keys.

**Virus Protection in a Portable Environment**

All portable or offsite computers targeted to process company data must have some consistent form of virus protection. This is a very important consideration when negotiating a site license for virus software. What should be negotiated is not a site license per se, but rather a use license for company's users, wherever they may process company data. The license should include employees' home computers and as well as company-owned portables. If this concept isn't acceptable to a virus software vendor, then procedures must be established in which all data that has left the company and may have been processed on a nonvirus-protected computer must be scanned before it can reenter the company's internal computing environment. This can be facilitated by issuing special color-coded diskettes for storing data that is used on portables or users' home computers. By providing the portable computer users with these disks for storage and transfer of their data and mandating the scanning of these disks and data on a regular basis onsite, the threat of externally contracted computer viruses can be greatly reduced.

**Controlling Data Dissemination**

Accumulation of data on portable computers creates the potential for its disclosure. This is easily addressed by implementing a variety of procedures intended to provide checks against this accumulation of data on shared portable computers. A user procedure should be mandated to remove and delete all data files from the hard disk of the portable computer before returning it to the company loan pool. The hardware loaning organization should also be required to check disk contents for user files before reissuing the system.

**Theft Protection**

The threat of surreptitious theft can be in the form of illicit copying of files from a user's computer when unattended, such as checked baggage or when left in a hotel room. The simplest method is to never store data on the hard disk and to secure the data on physically secured diskettes. In the case of hotel room storage, it is common for hotels to provide in-
room safes, which can easily secure a supply of diskettes (though take care they aren’t forgotten when checking out).

Another method is to never leave the portable in an operational mode when unattended. The batteries and power supply can be removed and locked up separately so that the system itself is not functional and thus information stored on the hard disk is protected from theft. (The battery or power cord could also easily fit in the room safe.) These measures can help protect against the loss of data, which might go unnoticed. (In the event of outright physical theft, the owner can at least institute recovery procedures.) To protect against physical theft, something as simple as a cable ski lock on the unit can be an effective protection mechanism.

**User Education**

The selection of portable computing protection strategies must be clearly communicated to portable computer users by means of a thorough user education process. Education should be mandatory and recurring to assure the most current procedures, tools and information are provided to portable users. In the area of remote access to onsite company resources, such contact should be initiated when remote users register in the remote access authentication system. For the use of shared company portable computers, this should be incorporated with the computer check-out process; portable computer use procedures can be distributed when systems are checked out and agreed to by prospective users. With respect to the use of noncompany computers in a portable mode, the best method of accountability is a general user notice that security guidelines apply to this mode of computing. This notification could be referenced in an employee nondisclosure agreement, in which employees are notified of their responsibility to protect company data, onsite or offsite. In addition to registering all portable users, there should be a process to revalidate users in order to maintain their authorized use of portable computing resources on a regular basis. The registration process and procedures should be part of overall user education on the risks of portable computing, protection mechanisms, and user responsibilities for supporting these procedures.

Exhibit 3 provides a sample checklist that should be distributed to all registered users of portables. It should be attached to all of the company’s portable computers as a reminder to users of their responsibilities. This sample policy statement includes nearly all the protection mechanisms addressed here, though the company’s specific policy may not be as comprehensive depending on the nature of the data or access method used.

**Portable Computing Security Checklist**
- Remove all data from hard disk of company-owned portables before returning them to the loan pool office.
- Leave virus scanning software enabled on portable computers.
- If it is necessary to use company data on home computers, install and use virus scanning software.
- Use company-supplied color-coded ("red") disks to store all data used outside the company.
- If no virus scanning software is available on external computers, virus scan all red disks before using them on company internal computers.
- Physically protect all company computing resources and red disks outside of the facility. (Remember that the value of lost data could exceed that of lost hardware.)
- Be aware of persons watching your work or eavesdropping when you work at off site locations.
- Report any suspicious activity involving data used in an offsite location. (These might involve data discrepancies, disappearances, or unauthorized modifications.)

Remote Access (Dial-Up) Guidelines.
- If dial-up facilities are to be used, register with the information security office and obtain a random password token to be used for obtaining dial-up access.
- Encrypt all company-sensitive data files before transferring them over dial-up connections in or out of the central facility.
- Report when you no longer require dial-up access and return your password-generating token to the security office.

Conclusion
The use of portable computing presents very specific data security threats. For every potential threat, some countermeasure should be implemented to ensure the company's proprietary information is protected. This involves identifying the potential threats and implementing the level of protection needed to minimize these threats. By providing a reasonably secure portable computing environment, users can enjoy the benefits of portable computing and the organization can remain competitive in the commercial marketplace.

Author Biographies
Phillip Q. Maier
Phillip Q. Maier is a senior network security analyst with Lockheed Missiles & Space Company in Sunnyvale CA. He is responsible for designing and implementing secure remote access networks at the Lockheed facility.