January 21, 2002

Mobile and Wireless Security: Worst and Best Practices

This research paper has been provided by Gartner. Gartner is a leading authority on information technology research.

How can enterprises most effectively manage networks?

1. Upgrade legacy security policies to support mobile and wireless device issues.
2. Treat unmanaged or loosely managed mobile/wireless devices as intruders. Shield the devices and the enterprise from accessing sensitive resources.
3. Enforce standards on personal devices by providing security tools to employees, and requiring that those tools are installed and operating.

The proliferation in mobile devices for immediate information access and work styles is quickly dismantling the enterprise security plan. Consumer toys have invaded the enterprise - and users expect to perform their jobs with these toys. A few years ago, enterprises could ignore these devices because their entry cost was high. Now, however, the entry cost is dropping to less than $150. These devices seem to be impossible to manage in a business environment, but their expanding access, processing and storage capabilities create serious threats to security that must be addressed.

Mobile and Wireless Security's 'Worst' Practices

The most effective way to develop new mobile/wireless access security best practices is to talk about some of the worst practices causing problems in many enterprises. Worst practices expose some of the fundamental problems with typical assumptions and perceptions about remote access security that need to change with the rise of mobile and wireless solutions.

Worst Practice No. 1: Users will maintain their own security and synchronization settings. At a certain point, users must be trusted to do the right things. However, any security parameter that is not auditable and documented should not be under user control. Under no circumstances should users be able to install synchronization and security software that has not been preconfigured and locked down by the security manager, or make personal decisions about turning off portions of the security.

Worst Practice No. 2: Passwords are good enough for access control. Password changing is a good example, as it is an illusion of security. If the password system is strong or quickly aged, users will write the passwords down and tape them to their computers or use the "Save My Password" option. Tokens remain the best near-term login protection solution. Enterprises will have to get over the shock of the token possibly

costing more than the PDA.

Worst Practice No. 3: Personal devices will be informally accepted in the enterprise. Users can buy PDAs on their own for less than $150, and the prices continue to fall. But allowing noncompany, unmanaged devices to access corporate data and networks creates a totally untraceable scenario. The enterprise might never know if information was lost or misused. If a problem was discovered, there would be no way to trace and close down the source of the leak.

Worst Practice No. 4: VPN eliminates piracy problems. VPN-encrypted sessions have the potential to introduce a manageable level of privacy to information sent through untrusted networks. However, VPNs must be strengthened with access controls, firewalling, etc. VPNs have been the focal point of many successful hacks, but the cause of the penetration was not the VPN, it was weak filtering and authentication associated with the VPN.

Worst Practice No. 5: Punishment will continue until security improves. When all else fails, the enterprise threatens the employees. This is the last line of management desperation in the traditional enterprise, and it never produces lasting, desirable results.

Mobile and Wireless Security's 'Best' Practices

Best practices that ensure success are designed to avoid unnecessary risks, clearly assign responsibilities and reward appropriate employee behavior.

Best Practice No. 1: Avoid security that hinges on user decisions and participation. Users want to access their workstations as quickly and transparently as possible. Good remote access security solutions do not waste users' time with distracting tasks and do not require the user to remember complex, secret information. Unfortunately, the systems that often have the highest theoretical level of security suffer from ease-of-usage problems that make them untenable and, if mismanaged, ultimately less safe. Attempts to improve low-quality authentication systems such as passwords often rely on support from the user base and introduce inevitable weakness.

Best Practice No. 2: Keep security policies short, succinct and enforceable. The subject of building and approving security policies leaves many managers cringing - thinking about protracted meetings and arguments, and about long, convoluted draft policies that have at least two pages of concessions from each member of the task force. Any policy longer than 15 pages is a waste of valuable time and is doomed to failure.

Best Practice No. 3: Connect policy violations to specific threats. Employees at all levels of the enterprise must be taught to believe that security problems are a real threat. The popular press does not cover all the known crimes because not all the events meet its requirements for sensationalism. Security managers should monitor government reports, computer security agencies and privacy watchdog organizations. Security stories should

be placed in company newsletters. Highlight publicly known computer security breaches and vulnerabilities. Explain how the same event could affect your enterprise, and highlight where security practices can protect from a similar attack.

Best Practice No. 4: Give rewards for finding and reporting security weaknesses. Employees are creative and energetic about protecting the enterprise and its assets if they are given constructive encouragement. This process has to be managed carefully so that it does not turn into a tale-telling session.

Best Practice No. 5: Use Gartner TCO models to estimate the impact of new devices so that expenditures on management solutions may be justified. As smart phones and PDAs become "asset tagged" and supported within the enterprise, they demand support for those found on notebooks and other enterprise-owned devices. Thus, what may appear to be an inexpensive device adopts costs similar to other client computers due to the tasks required to support it. Through 2005, smart phones, PDAs and other mobile appliances may cost more than $2,500 per year to maintain at a standard comparable to a workstation. The cost to implement basic security will be but a fraction of the total cost to maintain mobile devices.

Best Practice No. 6: Purchase advanced smart phones and PDAs for employees, rather than wait for employees to purchase their own. Company ownership is a prerequisite for maintaining a strong security profile. Enterprises should purchase new mobile appliances for users to eliminate the uncertainty of who controls the device. In this way, enterprises can ensure that their policies regarding personal and corporate information are implemented, thereby improving security and information management. Users can then select from a list of supported IT products, up to an amount set by the company. The list should contain sufficient variety to satisfy individual taste, but should be limited to devices the enterprise has decided are feasible to support.

Best Practice No. 7: Set standards for synchronization products that support a wide variety of personal and consumer appliances. Enterprises should not permit users to install their own synchronization tools. There are many popular products for general-purpose synchronization, such as shareware, available as independent retail products and bundled at purchase time. All synchronization products are immature. Future products must manage referential integrity and authentication for all three common synchronization paths (personal device to server, server to workstation and personal device to workstation), and must provide for an administrative console. Gartner recommends that synchronization standards be set immediately to ensure that the line between the controlled enterprise and the uncontrolled personal world of the employee remains intact. More practices related to synchronization include: 1) synchronize regularly; 2) expect the unexpected; 3) discard all bundled software; 4) protect the data, and encrypt it; 5) synchronize multiple devices in parallel; 6) control, test and approve access methods; 7) control, test and approve introduction of new device types and their OSs; and 8) formalize the process - make it a user habit - but make it easy for the user to be successful.

Best Practice No. 8 Set standards for power-on and network security. The first, best defense on phones and PDAs is the power-on password. Unfortunately, most mobile devices power on by default with no security. Security settings for power-on passwords and hidden files have been mostly optional, and can be turned off by the user. Default encryption may involve simple keys that are known to hackers. When placed on networks, the user's device may be vulnerable to DOS and spoofing attacks. To reduce these risks, enterprises must specify not only which brands of devices will be supported, but also what OS versions will be supported, because over time, OS vendors gradually fix the holes in their software. For example, ancient PDAs drawn from users' closets or handed down from friends are not suitable to withstand today's sophisticated hackers and thieves. On PDAs, products such as Communication Intelligence's Sign-On leverage the pen pad to enable users to sign on with their signature, or even a "secret doodle." VPN, authentication tokens and PKI must be considered for sensitive applications, especially if they will be accessed over the Internet. More practices related to security include: 1) discard bundled security software; and 2) provide all users with approved security software and training on how to use it. As with synchronization, formalize the process - make it a user habit - but make it easy for the user to be successful.

Best Practice No. 9: When designing wireless online applications, minimize the need for critical local data by using thin-client interfaces. Mobile devices are capable of supporting open environments such as SSL-based Web screens, Java and XML, as well as proprietary thin clients such as Citrix Systems' ICA and Symantec's PC Anywhere. Whenever a user's application requirement dictates online access to services, thin-client displays should be given priority to reduce the amount of local application and data that will need to be developed for the device, thereby reducing the exposure of that data.

Bottom Line: Through adoption of multiple mobile-computing appliances, users are creating the age of the "personal area network." But as every IS organization manager knows, user problems will eventually become IS problems, and the increase in complexity will be significant.

Acronym Key
DOS Denial of service
PDA Personal digital assistant
PKI Public-key infrastructure
SSL Secure Socket Layer
TCO Total cost of ownership
VPN Virtual private network