PDA Security

The Personal Digital Assistant has brought freedom and mobility to the corporate work force. What was once a rather ineffective and underpowered digital diary has now become a business tool, which provides the power of a notebook computer in a form factor that fits in a shirt pocket!
Since those early days of the Palm Pilot, Apple Newton and Psion's the PDA has evolved from a digital address book to a hand-held computer often running a fully fledged operation system with Desktop PC connectivity and data exchange as its primary function.

The PDA is a tool which has 'circumvented' the traditional route into the corporate enterprise. It has not been implemented by IT dept but by users and this has lead to the problems faced by IT and Security departments.

Earlier PDA's had very limited connectivity to the desktop, normally a serial cable or Infrared which facilitated the transfer of the Personal Information Manager (PIM) data only.

Today's PDA's can transfer office automation data, Word and Excel formats being the most common, picture, sound files and Movie clips being among the other popular ones. This can allow data to 'leak' from the enterprise onto PDA's which are generally very insecure, having both weak or non-existent encryption and by there very size and nature being easily lost or stolen.
A second area of risk is the increased connectivity that the PDA's now have, by default many modern units have Wireless LAN (Wi-Fi) capabilities as standard or which can be 'bolted on' with inexpensive Compact Flash (CF) or Secure Digital (SD) form factor Wi-Fi cards.

From a security point of view, the two types of PDA which present the greatest risk are those running either the Windows Pocket OS or the Linux OS, with the Compaq IPAQ and Sharp Zaurus being the most common in these respective categories. Both can be easily connected via Ethernet LAN or Wi-Fi, can store large amounts of data and can support and run many of the well-known 'hacking' and security tools available on the Internet.
The Sharp Zaurus device runs the Linux Operating System and so programs can be 'added' to it or written especially for a certain task. The IPAQ runs the Microsoft PocketPC OS, which has a number of 'hacking' tools, ported to it. The IPAQ can also be 'converted' to run Linux OS which in some ways makes the IPAQ more dangerous than the Zaurus as the IPAQ (with PocketPC OS) may be legitimately allowed network connectivity, but it would not be obvious if it was running Linux – thus allowing covert ingress to the enterprise.

Both these PDA's can also run packet-sniffing software that will allow them to capture login and password information over the network. They can also load and run password cracking software. In many cases, the attacker (for example commercial espionage) would connect the PDA to the network by un-plugging there desktop system and connecting the PDA in its place – allowing the PDA to masquerade as the desktop workstation. It would then be used to connect to a network share on a file server and download all the sensitive or saleable company data. One further trick in the Zaurus's arsenal is its ability to run 'pure' TCP/IP over its USB PC connectivity cradle, this then allows the Zaurus to communicate in the same fashion that its PC host can.

Companies should consider the ramifications of PDA's in the work place and ensure suitable policies; usage guidelines and 'control' software is employed to avoid data leakage and the loss of corporate information.