Whitmann Price Consulting: Security, Privacy and Ethical Considerations

Security and privacy are two major concerns that Sandra and Josh addressed in the development of the Advanced Mobile Communications and Information (AMCI) system. Anytime that access to network resources are extended beyond the walls of a business, extensive measures must be taken to maintain control of the system, and secure it from attack.

The AMCI system must be locked down to keep confidential records, such as customer and employee information, from being accessed by outsiders, and to keep Whitmann Price Consulting (WPC) business strategies safe from snooping competitors. WPC systems need to be protected from attackers who might access the system through the AMCI BlackBerry devices and destroy, damage or steal corporate information and resources.

WPC runs standard security software such as firewalls and virus detection. It also employs more sophisticated security software that watches for suspicious activity within the system. Any sensitive data stored on the device is encrypted to protect it from being viewed without a password. The primary concern with the AMCI system is that a BlackBerry might be stolen or lost, providing someone outside the company with access to the private network. For this reason, Josh and Sandra employ virtual private network (VPN) software to restrict access to the network from the BlackBerry devices. The VPN software requires a username and password prior to connecting the corporate network. It also provides encryption to safeguard data travelling between the handset and the corporate network.

Another security concern at WPC is the danger of damage or theft from within the organization. To address this concern, the system allows access to confidential records only by those with a need to know. This is not an AMCI-specific concern, but a system-wide concern. The system group has established access policies that regulate data access according to employee status. Each username on the system is assigned a status and confined to accessing only information pertinent to that user's duties.

WPC also has well-defined and comprehensive network usage policies. New employees are provided with the policies when they are given a network account. Employees must provide a signature affirming that they read, understand, and will comply with the corporate network policies. These policies are updated periodically to include policies to secure the new AMCI system. For example, restrictions have been placed on personal use of the device. While incidental personal use was expected, users cannot use the device outside of standard business hours. The hope is that this policy will reduce the chance of the device being accessed by others outside the company.

Other policies include protecting passwords from access by others, not allowing the device to be accessed by others, and logging out of the VPN connection at the termination of each use. The company installed software on the devices that restricts the use of Bluetooth to the headset only. This was done to secure the device from attacks through Bluetooth connectivity. Also, users of the AMCI BlackBerries are only allowed to connect the device through USB to an approved PC. The company hopes to protect the device and the corporate network from infection by viruses on outside PCs.

As with most businesses, WPC has invested significant amounts of time and money in network security. Through a combination of software security tools and strictly enforced policies, the company is doing all that it can to keep its valuable and private information protected and its systems running smoothly. The extension of the network to mobile users requires a full review of network policies, and some stronger policies have been put in place. The new policies come at a cost of some convenience, but provide a most important benefit of information security.