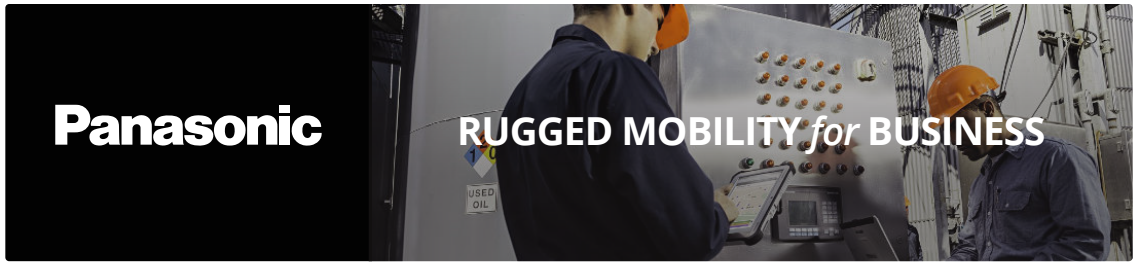
Security Considerations for Mobile Devices



It's no wonder that security is always cited as IT's number one concern. Security threats and pitfalls abound – data loss, viruses, and ransomware can bring a company to ruin. Mobile devices are vulnerable, in part due to their portable nature and because as an endpoint they can be used as an entryway to a company's network. So it's no surprise that one in five breaches involves lost or stolen mobile devices or storage media[1]. How do compromised devices lead to data loss? Unencrypted drives may have lists of passwords and logins as well as sensitive PCI, HIPAA or other sensitive data. A purloined device without proper access security can lead prying eyes to corporate resources with just a few clicks. But far beyond the cost of the lost device itself, the soft costs of insecure devices can lead to a loss of confidence in a company's brand or service. How does IT balance security and mobility?

Securing Mobile Devices: Multi-dimensional Approach

Physical security for mobile devices is important and physical damage to a device can expose device data to new risks[2]. However, other aspects of security also play a big role. For example, device access should be limited to authorized users to protect critical data, the hardware itself, and access to additional corporate resources. Data security features, such as encryption at rest and in motion help to prevent data loss by scrambling data, and network security is important, particularly when remote workers use vulnerable public Wi-Fi. For devices that are lost or stolen, enterprise IT should be able to perform a remote lock-down or drive wipe to eliminate loss.

Best Practices for Secure Devices

A security plan for mobile devices should consider people first and limit what users can bring into or take out of the environment. For example, a removable hard drive or stray USB key can lead to data loss even if used innocently. IT should ensure that updated security polices are in place and enforced to enhance overall device and data security. And finally, because IT has less control over consumer-grade, employee-provided devices, businesses should avoid BYOD for maximum security.

[1] Businesswire, 2016 – "Almost One Third of US Business Had a Data Breach"
[2] IDG/Panasonic Quick Pulse "Multiple Layers of Security Needed to Protect Mobile Devices"

Consider these five security-related factors when sourcing mobile technology:

1. What physical features protect the device from theft, such as removable hard drives, cables and locks?
2. What security features are built-in at the hardware level to secure access to devices (and by extension to corporate business systems) or lock it down in the event of theft or loss? Does the vendor have specific tools for your market sector (private, public safety, government, utility, medical, etc.)?
3. How do the device's physical and logical security features work within your organization's overall security program?
4. Does the device offer configurable, built-in security features like fingerprint and smart card readers, or other methods that matter to your business today?
5. What software, services, and support such as disaster planning does the vendor offer?

The Panasonic TOUGHBOOK Security Difference

Panasonic TOUGHBOOK mobile devices have a 20+ year history of delivering secure, rugged, mobile devices for a broad range of industries, and their ruggedized design largely eliminates the threat of data loss due to device damage. The devices also include various enterprise-level security features enabling IT to address data security, access privileges, connectivity security, and device security needs.

Hardware-level security certifications include Trusted Platform Module 1.2 or 2.0 and FIPS 140-2 compliant encryption. TOUGHBOOK laptops are also NIST BIOS compliant to protect against unauthorized modification. Panasonic TOUGHBOOK devices offer removable hard drives, cable locks, and a broad range of accessories such as fingerprint and smart card readers to authenticate user access.

You can find out more about Panasonic TOUGHBOOK device security by reading the **Rugged Mobility for Business** blog.