Multiple Layers of Security Are Needed to Protect Mobile Devices

SPONSORED BY:

Panasonic

Mobile devices have become essential tools for companies reacting to today's breakneck rate of change. Just as customers and consumers expect to be able to do more with devices such as smartphones and tablets, so too do employees and the companies that hire them.

A new survey from Panasonic and IDG demonstrates the increasing importance of mobile devices from the perspective of business and IT managers who purchase and deploy mobile devices for business use, mainly outside of traditional office settings. In the survey, 84% of respondents report that their companies rely on data captured by mobile devices to benefit the business to a "large" or "very large extent."

Mobile devices empower customers, employees, and organizations to be more productive in a wide range of environments. But the benefits of these devices come with a caveat. As the dependence on mobile devices and data captured from the field increases, the challenges of securing those devices multiply.

Added to the challenges faced by desktop computers, servers, and other stationary platforms, mobile devices must also contend with the dangers of connecting to outside networks, the increased risk—due to theft or loss—of unauthorized use, and all the perils of life outside the office, with its potential for drops, spills, and other accidents.

As the devices proliferate, so too do threats such as hacking and malware. Securing mobile devices against these multiplying threats is more important than ever if companies are to realize the powerful benefits of data collection by mobile employees. Effectively addressing this concern is possible only with a multilayered approach to mobile security.

Top Security Risks Named for Mobile Devices

Mitigating the risks faced by mobile devices requires first accurately assessing those risks. IT managers responsible for the security of mobile devices used by corporate employees report an array of challenges:

More than half—52%—of respondents to the IDG/Panasonic survey report malware as a top concern.

Nearly half—47%—report data leakage as a top concern.

Rounding out the top three concerns reported by IT managers is data loss due to device damage, reported by 44% of respondents.

Lower down on the list of concerns—but still important—are the risks posed by misuse. These include downloading unauthorized applications that can potentially access sensitive data (reported by 37% of respondents), accessing unsecure networks (36%), losing or having devices stolen (27%), and connecting to unsecure Wi-Fi hotspots (21%).

Rising Concerns About Security Standards

In addition to the risks to devices themselves, IT managers are also concerned about the risks and requirements presented by the prevailing mobile security standards.

Nearly three quarters—72%—of IDG/Panasonic survey respondents cite both reporting requirements under HIPAA (for safeguarding medical data) and CJIS (for securing law enforcement data) for lost devices, as well as 4G's reliance on IP architecture and the resulting hacking vulnerabilities, as top concerns.

More than half of respondents—51%—cite the need to be FIPS 140-2 Level 2 compliant as a top concern. This U.S. government standard for the encryption of data is a must-meet requirement for organizations doing business with government bodies.

Only 5% of respondents report that they had no concerns about security standards that might affect

Top 3 Mobile Security Concerns

Source: IDG Research

the mobile devices used by their organizations.

Meeting the Mobile Security Challenge

Given the varied security concerns surrounding mobile devices, a multilayered approach is the only viable way to protect them. Data security as well as physical security must be taken into account equally. That's why countermeasures currently in use against threats to mobile devices take many forms, including:

- Strong/complex passwords (used by 84% of respondents)
- Auto-lock timeouts (79%)
- Virus and malware protection (79%)
- Two-factor authentication (71%)
- Hardware-level embedded security features (68%)

When asked specifically about the security features that their organizations have deployed for mobile devices used outside of the office in nontraditional settings, respondents named software encryption more than any other measure.

More than three quarters—76%—report currently relying on software encryption to secure mobile devices. Adding the 21% of respondents who plan to deploy software encryption in the next 12 months brings the total of those using or planning to use software encryption for mobile devices to 97%.

Software encryption may be seen as a fallback response for a host of risks, including theft and loss, exposure to compromised networks, and more, highlighting the value of a multilayered approach to security. In other words, if one or more security measures in place on a mobile device fail, another can prevent the data on the device from falling into the wrong hands.

Given the varied security concerns surrounding mobile devices, a multilayered approach is the only viable way to protect them. Data security as well as physical security must be taken into account equally.

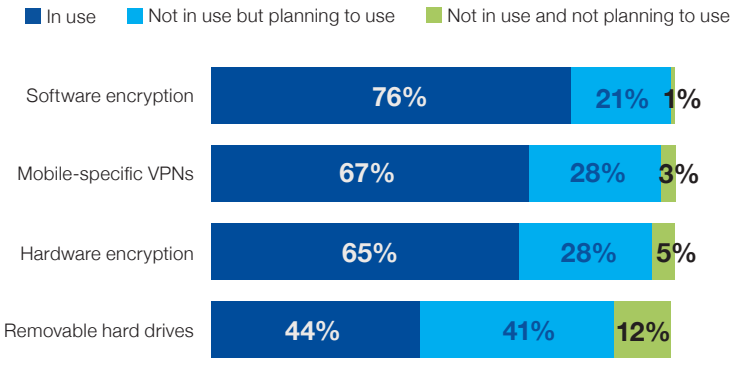
After software encryption, mobile-specific VPNs are the most-used security measure. Well over half—67%—say their organizations currently use VPNs on mobile devices. An additional 28% plan to use VPNs in the coming 12 months, bringing the total to 95%—very close to the number using or planning to use software encryption.

Hardware encryption is right behind VPNs as a top security measure for mobile devices. Factoring in both current (65%) and planned (28%) usage, hardware encryption is favored by 93% of respondents.

Also in the realm of hardware-based security, removable hard drives get high marks from 85% of survey respondents, 44% of whom use removable drives now, and 41% of whom plan to in the next 12 months.

Given the expanding use and importance of mobile devices for work, concern about protecting those devices as well as the data connected to them will only continue grow in the foreseeable future. A combination of countermeasures that accounts for all of the potential threats is the only way to keep sensitive data safe so companies can continue to enable the mobile workforce, and enjoy the benefits it brings.

Common methods used to protect mobile devices outside of a traditional office environment



Source: IDG Research

Visit **panasonic.com/toughbook** to learn how rugged mobile devices can help companies meet the challenges of capturing data in the field and securing the mobile workforce.