U.S. smartphone use has surged as more and more American businesses and consumers opt to purchase these powerful, feature-rich devices. As of November 2010, 61.5 million people in the United States owned smartphones, up 10% from just three months prior.¹

By 2011, smartphone sales are expected to overtake PC sales in the United States.² As their computing power grows, smartphones perform increasingly useful and varied functions that bring increased productivity and efficiency and cut costs. At the same time, many of these new uses involve sensitive data, including intellectual property (IP) and personal data, making security of growing importance. Smartphone hardware, operating system, and applications vendors invest in a range of security measures to protect these data.

### Smartphone Benefits: Increasing Productivity and Efficiency in the United States

#### Merchant point-of-sale
Merchants use smartphones to take payments, such as by credit card. This provides mobility, faster service, and improved merchant efficiency through integration of and fast access to sales, accounts, and inventory. These transactions typically handle financial and credit card data.

#### Health-care productivity
Physicians and nurses use smartphones to access patient, drug, and billing information; to perform research; and to e-prescribe medications – both from hospitals and patients’ homes. Health care providers securely collect real-time health data on blood pressure, blood sugar, and more from patients wearing smartphones and wireless monitors. Patients use smartphones to track and manage their medical conditions and wellness/fitness. These uses all improve patient care and bring operational efficiencies, and typically handle protected health information (PHI).

#### Sales force automation
Mobile sales representatives use smartphones to connect with people and resources, exchange vital product and customer intelligence, share information with other mobile employees, and build customer relationships to close deals faster and respond more quickly to sales opportunities. This brings enhanced enterprise productivity and sales performance. These transactions often handle sensitive customer data.

### Consumer banking
Consumers use smartphones to conduct online banking, such as account management and bill payment. This provides improved convenience, accessibility, and efficiency related to how, when, and where individuals can monitor and manage their money. In fact, 19 of the top 30 largest financial institutions offer mobile banking.³ These transactions typically handle sensitive financial data.

### Government services and public safety
Federal, state, and local government agencies nationwide rely on smartphones to support law enforcement, emergency medical, and other city services; to ensure continuity of operations during emergencies; and to conduct legislative activity. Mobile police officers connect to national criminal databases via smartphones, and emergency first responders use them in the field to securely access hazardous materials databases, intelligent dispatch, and more. This enhanced communication and ready information access improves the efficiency and effectiveness of government services. It also helps to ensure that officers are more secure (e.g. when approaching suspect vehicles). These uses often handle sensitive criminal databases and personal information.

What steps do vendors take to secure these activities?
See reverse to learn more.
Smartphone Security: Vendors Undertake a Variety of Activities

Smartphone hardware, operating system, and applications vendors invest in a range of security measures that establish a layered approach to information security. These are continually updated by security experts around the globe, evolving as threats evolve. Some key examples follow.

Vendors implement and use global practices:

• Vendors build and employ a variety of smartphone-related encryption solutions to protect data at rest on the device or in motion across networks.
  • Data at rest, including any data on removable SD cards, is protected with advanced encryption, such as Advanced Encryption Standard (AES)-256.
  • Data in motion - across carrier wireless or WiFi networks - is protected with AES-256 or other industry-developed advanced encryption standards, such as the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard for wireless local area networks (WLANs).

• Vendors leverage robust password requirements or two-factor authentication technologies for smartphones that manage the risks from unauthorized device and data access.

• Vendors build applications that let users or administrators remotely delete data, disable their smartphones, or locate their devices via GPS when a device is lost or stolen.

• Vendors protect platforms against malware security risks with application control policies that restrict access to sensitive resources on a need-to-have-basis, or by traditional antivirus applications.

• Vendors certify the security of their smartphone platforms, such as to internationally recognized Common Criteria requirements.

Vendors contribute to standards development:

• Vendors participate in the Institute of Electrical and Electronics Engineers (IEEE), a non-profit global industry organization, to develop important wireless communications security standards used internationally in hundreds of millions of mobile devices.

• Vendors contribute to the development of relevant National Institute of Standards and Technology (NIST) federal security standards and guidelines, such as Special Publication (SP) 800-124, “Guidelines on Cell Phone and PDA Security” or cryptography standards under Federal Information Processing Standards (FIPS) 140-2 that protect data at rest and in transit.

End-users play an important role as well:

• Organizations that use smartphones implement best practices for managing related security risks by
  1) deploying centrally managed security policies that preclude end-users from making critical mistakes with security configurations; 2) deploying secure mobile operating systems that are resistant to tampering; and 3) using flexible security controls and settings that are easily adjustable depending upon specific risks and business requirements.

1 “comScore Reports November 2010 U.S. Mobile Subscriber Market Share,”

2 “Garner’s Top IT Predictions for 2010 and Beyond,” December 2009. On a unit volume basis.


For more information contact Danielle Kriz, Director, Global Cybersecurity Policy at 202-626-5731 or dkriz@itic.org

2011 ITI Member Companies

Accenture•Adobe•Agilent Technologies•Altera•AMD•AOL•APC•Apple Inc. •Applied Materials•Autodesk•CA Technologies•Canon•Cisco Systems•Cognizant•Corning•Dell•eBay•EMC2•Ericsson•Fujitsu•Google•HP Palm•IBM•Intel•Intuit•Kodak•Lenovo•Lexmark•Micron•Microsoft•Monster.com•Motorola Solutions•National Semiconductor•NCR•Nokia•Oracle•Panasonic•Qualcomm•Ricoh•RIM•Skype•Sony•Symantec•Synopsys•Teradata•Texas Instruments•VeriSign

1101 K Street, NW • Suite 610 • Washington, DC 20005 • t: 202.737.8888 • f: 202.683.4922 • www.itic.org • @ITI_techtweets