



**TOLMAN & WIKER**  
**INSURANCE SERVICES, LLC**  
INNOVATIVE RISK ADVICE SINCE 1923™

BAKERSFIELD | SALINAS | SANTA MARIA | VENTURA

### **A Growing Corporate Risk: Work-Issued Mobile Devices**

April, 2013

Property Casualty 360

Corporate leaders issuing cell phones to employees to conduct business-related communication are realizing tablets are one of the evolving technologies that keep them walking the razor's edge of cyber exposure.

"Mobile device malware is growing exponentially, from 800 samples per month in 2011 to 6,300 new samples per month in 2012," said Nathan Steuer, business development director of PaRaBaL Inc., a mobile-device development company hired by the U.S. government to track the security flaws of smartphones. "Now is the time for companies to start looking at cell phones as miniature, flexible computers."

According to UBM Tech's website [Dark Reading](#), risk consultant RSA linked an attack that wiped data from hard drives at three media outlets and two banks in South Korea to an app downloaded on Android devices.

Meanwhile, Kaspersky labs identified that a targeted swipe against Uyghur activists in Asia in March 2013 involved Android malware used to steal private data—including contact lists and messages—from an infected phone, and send it to a remote server.

While there hasn't yet been a major reported breach of U.S. businesses via a smartphone, both Google's open-sourced and Apple's proprietary operating systems (OS) are vulnerable to phishing attacks that can cull data as personal as bank account passwords.

"Mobile phones operate like computers, and networked computers at that," said Scott Godes, counsel in the Insurance Coverage Practice at Dickstein Shapiro and leader of the firm's Intellectual Property Insurance Practice.

"Similar data and privacy risks apply in the perspective of overall risk to the company and for insurance coverage," he adds. "These considerations include a data breach and/or a lost device containing personally identifiable information, protected health information, and corporate or trade secrets—or confidential information that would be devastating if seen by the wrong party."

Whether email is passed through a PC at the office or during the morning bus commute, the enterprise must keep in mind state and federal laws, and contractual obligations to its business partners.

For example, under the Health Insurance Portability and Accountability Act (HIPAA), health practitioners are liable for information leaked while communicating with patients through unencrypted texts.

Moreover, not every mobile phone is created equally; there are unique vulnerabilities in both the popular Android and iPhone platforms.

Companies who provide phones to employees should set aside time to educate them in spotting malware, say the tech experts.

"Security isn't a product, it's a process of educating users before moving onto software solutions," says Steuer. Organizations like PaRaBaL provide training and white papers on the topic.

The Mobile Application Assurance Tool (MATS) created by PaRaBaL to analyze the legitimacy of Android apps is only available to the government, but the company is developing a service to conduct security scans for private customers.

Currently, companies can utilize a mobile Device Manager (MDM), which can wipe data remotely from a device if a phone is lost.

What risk managers should do is to comb through their insurance policies at renewal time for peace of mind.

Says Godes, "I would recommend a careful review of the Commercial General Liability (CGL) or Cyber policies, and how the terms 'computer' or 'computer network' are defined in terms of cyber fraud. Many are written broadly and may include mobile devices specifically."

© 2013 PropertyCasualty360, A Summit Business Media website

National Underwriter

[Return to Article Index](#)

**Forward this article to a colleague**

Address To	<input type="text"/>	Recipient Name	<input type="text"/>
Subject	<input type="text"/>		
Message	<input type="text"/>		
<input type="button" value="Send"/>		<input type="button" value="Reset"/>	