VIPRE® AntivirusBusiness

It's Time Businesses Wake up to Mobile Security Reality

Ready or Not, You Need an MDM Solution.

The role personal smartphones and tablets are playing in the workforce is a phenomenon that has quickly impacted all businesses. As a result, the tall task of protecting company data accessible with a variety of devices has become top priority for network administrators.

Workforce mobility is undoubtedly a terrific luxury. But it leaves businesses susceptible to security breaches and other tech-specific headaches. IT administrators in medical practices, banks, law firms and schools alike need to recognize the days of solely monitoring employee activity on desktop computers are long gone.

IT administrators instead face a new reality: Pressure to account for, manage and secure an array of new endpoints. It's a giant task given the influx of smartphones and tablets on the market, and the corresponding employee expectation, if not outright demand, that connection to the office at all times be possible.

Technology analyst house Canalys this year reported that smartphone vendors in 2011 for the first time shipped more units globally than their client PC counterparts (488 million versus 415 million).[1]

International Data Corporation (IDC) adjusted its 2012 forecast for worldwide tablet shipments from 88 million to 106 million – reflecting a 54% increase – due to a late surge in sales a year ago.[2]

Tom Mainelli, IDC's research director for mobile devices, told the Associated Press that most people and businesses are "just waiting for a compelling reason to upgrade (from PCs)."

For businesses pushing workforce mobility and productivity, these technologies create network security issues unfamiliar to many IT administrators.

"We want … businesses to understand they cannot completely remain safe from cyber-threats if they do not take the necessary

Bring Your Own Device (BYOD) isn't just a faze, nor are the associated risks.

IT administrators instead face a new reality: Pressure to account for, manage and secure an array of new endpoints. It's a giant task given the influx of smartphones and tablets on the market, and the corresponding employee expectation, if not outright demand, that connection to the office at all times be possible.

precautions. A data breach or hacking incident can really harm [them] and unfortunately lead to a lack of trust from consumers, partners and suppliers," National Cyber Security Alliance Executive Director Michael Kaiser said in a statement.[3]

Many businesses are woefully unprepared to meet the challenges associated with Bring Your Own Device (BYOD) initiatives. They lack the time, manpower and budgets to fend off mobile threats. They also see most solutions applying to the needs of others, not necessarily themselves.

Clearing those hurdles is possible. Businesses can adopt a cost-effective and easy-to-manage network solution that offers system, email, web and mobile security with a small footprint.

While workforce mobility is a luxury, it also leaves businesses susceptible to security breaches.

Mobile Device Management

With all signs pointing to a growing number of personal devices affecting business operations, Mobile Device Management (MDM) needs to be every business' top priority.

"[Chief intelligence officers] and [chief technology officers] all over the world are struggling to accept that Bring Your Own Device is a trend that is here to stay," technology reporter Dan Woods wrote for Forbes Magazine.[4]

According to the "2012 IT Risk/Reward Barometer: U.S. Consumer Edition"[5] furnished by global IT association ISACA, among the 74% of consumers who have a work-supplied or personal device, 33% use it for work purposes.

But the survey also calls attention to the slippery slope that is BYOD. While allowing use of personal devices in the workplace has the potential to increase productivity, that isn't always the case.

The Risk/Reward Barometer found that consumers using smartphones, tablets and PCs for work purposes plan to spend, on average, 12 hours shopping online for the holidays using a BYOD device. And in that time, they could be placing network security at risk.

Of course, many companies aren't helping themselves, either. The consumer study revealed that 44% of respondents do not know if their company has a BYOD policy.

Knowing employees plan to access their company network with portable devices, IT administrators better have a solution capable of protecting against data loss and various internal issues.

'Corporate Equivalent of Privacy'

When IT administrators contemplate the best course of action for fighting various threats to the company's network, the first worry is typically ensuring sensitive material remains safe. They have the company's mobile device users to thank. Many of them don't know or don't care about taking steps to enhance mobile safety. Their online habits, in turn, expand the risk posed to the network.

"The real battle for mobile devices is ... on privacy and the corporate equivalent of privacy, which is data leakage," Andrew Jaquith, a former analyst for global advisory firm Forrester Research, told InformationWeek.[6]

Fear of failing to protect sensitive company data is founded. The Pew Research Center's Internet & American Life Project conducted a national survey[7] that revealed:

- Nearly 1 in 3 mobile phone owners (31%) have lost their phone or had it stolen
- 58% of mobile phone owners and 39% of smartphone owners do not back up the files, photos and other data on their devices
- 33% of smartphone owners – more than 4 times as many owners of "other cell phones" – disable location tracking on their devices
- 12% of mobile phone owners said their phones were accessed in a way that made them feel their privacy was invaded

Couple those statistics with the following findings from ISACA's research. They drive home the message that IT administrators must get a handle on MDM:

- 11% of employees have used a cloud service to store work documents, unbeknownst to the company

- 12% stored work passwords on their personal device
- 19% stored work documents on their personal device
- 28% assume their IT department is ensuring their work-supplied device's security
- One-third would still use their personal device for work purposes if the company could remove data (31%), track online activities (33%) or restrict online activities (35%)

ThreatTrack Security also commissioned a study on mobile security. Only 7.7% of respondents would rate losing work-related information stored on their phone as the biggest concern, if the device was lost or stolen. Furthermore, 46% would not pay anything to retrieve their smartphone, if lost or stolen.

Risky employee behavior is commonplace, even if it is unintentional. Nonetheless, it is clear that IT administrators need a network solution that can quickly and easily lock, locate and do a remote wipe of devices from a central hub.

Take the physician making hospital rounds, for example. Say his or her tablet carries patient health records or is enabled to access them. What if the device goes missing? It places the patient and practice at great risk. It isn't hard to imagine bankers, lawyers, teachers or government workers experiencing similar stress-raising situations.

Businesses are Easy Targets

Forty percent of cyber-attacks are directed at small- and medium-sized businesses (SMBs), according to a 2011 study discussed during a Congressional hearing titled "Cyber Security: Protecting Your Small Business."[8] To that end, the Government Accountability Office (GAO) in September submitted to Congress a report on mobile device security. The report noted that mobile-targeted malicious software – between viruses, spam and phishing attacks – has nearly tripled in the past year. It skyrocketed from 14,000 to 40,000.[9]

It isn't a coincidence that businesses are considered easy targets. Malicious software writers have adjusted their tactics to make mobile devices do their dirty work.

Cybercriminals are well aware that the widespread dual use of unencrypted devices invites viruses and other malware that adversely affect workflow. Businesses lacking a solution that detects vulnerabilities leave the network open to an attack that slows operating speeds or worse, brings it to a grinding halt.

Many businesses remain unprepared for the challenges associated with Bring Your Own Device (BYOD).

Which mobile subscribers pose the greatest threat to IT security? Nielsen Mobile Insights found that, as of February 2012, 48% of smartphone owners had a device that ran the Android operating system.[10] Hardly surprising, there are more than 10,000 known Android viruses.

IT managers have control over company-issued desktops, laptops and devices. But policing a company's employees whose personal gadgets connect to the network presents a new test entirely.

"When you get that brand new Droid, load it up with apps and then plug it into your work PC in order to update or sync necessary files, your company's IT guy has to worry about whether that last app you downloaded might infect the entire network," personal security expert Robert Siciliano wrote for InfoSecIsland.com.[11]

Your IP environment is changing. Your network solution needs to change, too. Your company's security is too important to jeopardize.

About VIPRE® Business Premium

VIPRE Business Premium is the antivirus software that provides the hassle-free protection your mobile workforce requires with integrated Mobile Device Management, which includes:

- Android antivirus, remote alarm, remote locate and remote wipe
- iPhone and iPad password enforcement, Wi-Fi configuration, remote lock and remote wipe

Additionally, VIPRE Business Premium includes many other features that allow you to easily manage security

on all your endpoint devices from a single console:

- Small-footprint anti-malware agent that uses minimal CPU and memory
- Patch management to eliminate the number one cause of PC infections
- Integrated Mac agent for centrally-managed Mac antivirus security
- Automatic threat scanning of USB flash drives and other removable media
- Unprotected endpoint detection to ensure all network PCs are protected
- Infected computer identification to quickly locate the source of an infection

Protect your business against BYOD threats now.
Download your free 30-day trial of VIPRE Business Premium at **www.ThreatTrackSecurity.com/VIPRE**

[1]Canalys.com, Smartphones Overtake Client PCs in 2011, February 2012 http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011

[2]TheNewsTribune.com, 2012 Tablet Sales Now Expected To Rise 54 Percent Over 2011's, November 2012 http://www.thenewstribune.com/2012/03/14/2065975/2012-tablet-sales-now-expected.html

[3]Eweek.com, Cyber-Threats Unaddressed By Small Businesses: Symantec, October 2012 http://www.eweek.com/security/cyber-security-threats-unaddressed-by-small-businesses-symantec/

[4]Forbes.com, Don't Let BYOD Distract From The True Potential Of Mobile Apps, November 2012 http://www.forbes.com/sites/danwoods/2012/11/08/dont-let-byod-to-distract-from-the-true-potential-of-mobile-apps/

[5]ISACA, 2012 IT Risk/Reward Barometer: U.S. Consumer Edition, November 2012 http://www.isaca.org/SiteCollectionDocuments/2012-Risk-Reward-Barometer-US-Consumer.pdf

[6]InformationWeek.com, 5 Mobile Security Issues to Watch, September 2011 http://www.informationweek.com/security/mobile/5-mobile-security-issues-to-watch/231602222

[7]PewInternet.org, Privacy And Data Management On Mobile Devices, September 2012 http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

[8]Smallbusiness.house.gov, Cyber Security: Protecting Your Small Business, December 2011 http://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=270278

[9]NetworkWorld.com, The 10 Most Common Mobile Security Problems And How You Can Fight Them http://www.networkworld.com/news/2012/091912-mobile-security-262581.html

[10]Nielsen.com, Smartphones Account For Half Of All Mobile Phones, Dominate New Phone Purchases In The US, March 2012 http://blog.nielsen.com/nielsenwire/online_mobile/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us/

[11]InfoSecIsland.com, BYOD: Mobile Security Tips For Small Businesses, September 2012 http://www.infosecisland.com/blogview/22010-BYOD-Mobile-Security-Tips-for-Small-Businesses.html