

Implementing BYOD

What are the Risks to Your Corporate Data?



Employee-Liable Devices Challenge IT Readiness

Enterprises cite security as their number one concern with regard to consumerization. During the actual execution of a consumerization strategy, however, IT groups find that the increasing demand to use employee-owned devices for important work is activities forces security out of the picture.

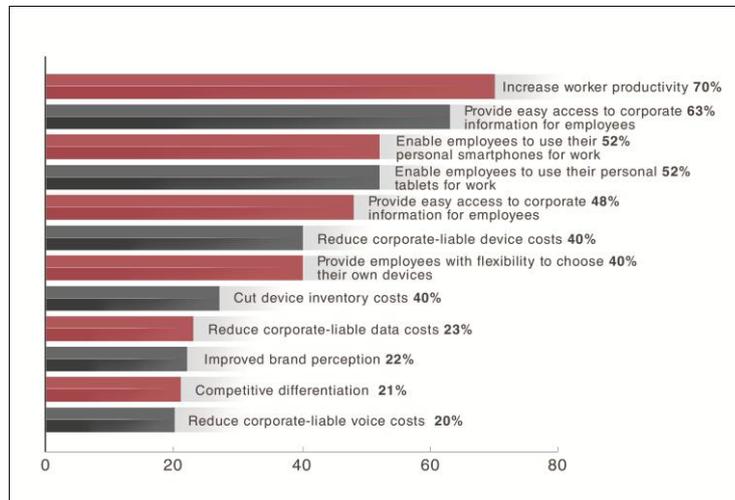


Figure 1. Factors driving bring-your-own-device (BYOD) in organizations and enterprises

A number of factors contribute to the diminished regard for security:

- **Lack of awareness:** IT groups may not be aware of the number of mobile devices connecting to their networks. A survey estimated that 69% of employees used smartphones for work while their respective IT groups said 34% did so.
- **Increased workload:** Unlike company-issued laptops, employees' smartphones require more from IT groups because IT administrators need to treat and configure each device and operating system version differently. As a result, IT groups may only enforce minimal security.
- **Technical support prioritization:** Device-carrying employees demand that IT groups make their devices work, forcing IT groups to deprioritize security in favor of providing technical support.
- **Mobile OS updating difficulty:** IT groups' jobs are not made easier by the open nature of the Android™ OS and mobile OS providers' weak vulnerability handling and remediation processes. Waiting for patches can take weeks; fully deploying those takes even longer.
- **Knee-jerk mobile device management (MDM) solution purchases:** IT groups may be tempted to buy an MDM solution that may be inappropriate to their specific environments and can negatively impact their security.

- **Informal adoption:** In some cases, enterprises may informally encourage BYOD to please their employees. They may, however, not have written usage guidelines or implemented best practices.

The introduction of employee-owned devices to workplaces has been acknowledged in order to increase employee productivity and satisfaction, business agility, and provable cost savings. Risks to security and data should, however, also be closely examined.

Security Threats Employee-Liable Devices Pose

While enterprises have embraced BYOD due to the benefits it offers, like increased productivity and flexibility, there are pain points that emerge both from the enterprises and employees' end. In a study, the top challenge in consumerization of IT that enterprises cited is mobile device security.

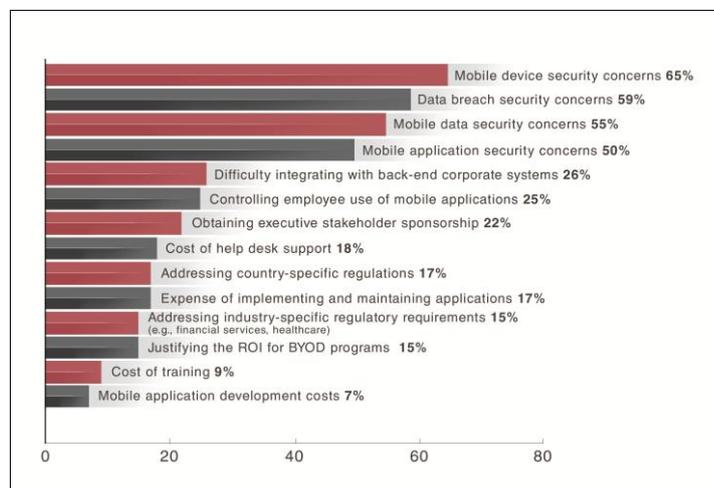


Figure 2. Top challenges in implementing BYOD

The risks of implementing BYOD are not just limited to device theft or loss but in securing the valuable enterprise data and apps contained in and accessed by multiple devices outside the network. Here are some security threats to mobile devices and data that enterprise should consider:

Data Breach

In a Trend Micro study¹, 46.5% of enterprises that allowed employee-owned devices to access their network have experienced data breach.

Similarly, device theft and loss is also one of the factors that caused large data breaches. Information stored on stolen devices may be used by threat actors for sabotage or espionage purposes.

¹ Trend Micro Incorporated. (2012). "Mobile Consumerization Trends & Perceptions IT Executive and CEO Survey." Last accessed February 12, 2014. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Targeted Attacks

Although email is one of the common entry vectors for targeted attacks, threat actors can also leverage mobile devices. Targeted attacks are high-risk threats with the aim of data exfiltration. In the Luckycat campaign², our threat researchers found two APKs in one of its C&C servers, suggesting that threat actors may launch attacks using this platform. In our 2014 Security Predictions³, we cited that attackers will likely target mobile devices, as a new threat vector, to penetrate the network.

Malicious and High-Risk Applications

One of the entry points in infecting mobile devices is via malicious and high-risk applications or applications that get device information and display unwanted ads without user's consent. In 2013, the number of Android malware and high-risk apps reached the 1 million mark, and by end of 2014, it had more than quadrupled to 4.2 million. Data stealers were the second most prevalent mobile threat in 2014. While majority of these applications can be found in malicious domains, some reside in legitimate third-party app stores.

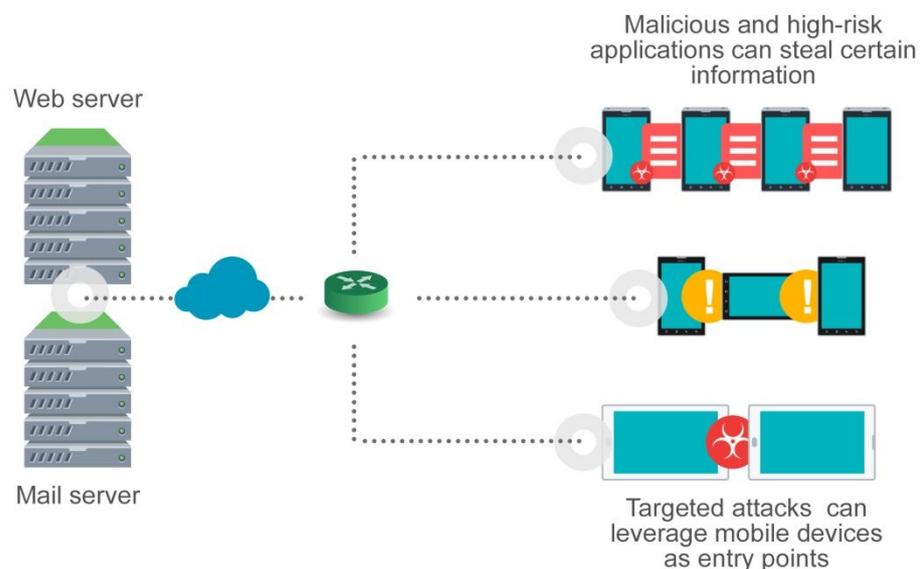


Figure 3. Risks to corporate data

² Genes, Raimund. (2012). *TrendLabs Security Intelligence Blog*. "DEFCON 2012: Android Malware in Luckycat Servers." Last accessed February 12, 2014. <http://blog.trendmicro.com/trendlabs-security-intelligence/defcon-2012-android-malware-in-luckycat-servers/>

³ Trend Micro Incorporated. (2013). "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed January 15, 2014, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf>

Maximizing BYOD with Security in Mind

In the end, businesses need to realize that consumerization is here and is not going away anytime soon. The sooner IT departments make adjustments to security protocol, the quicker organizations can participate in trends that can give them a competitive advantage over rival firms and increase opportunities for growth.

—Trend Micro

The availability and accessibility of corporate data is crucial to increase employee productivity. However, it also poses security risks to confidential data. With the use of employee-liable devices in the workplace, IT faces the challenge of ensuring the visibility and control of all employee-owned devices accessing the network, as well as differentiating corporate data from personal employee data stored on the said devices.

Security solutions with mobile device management (MDM) provide control in a centralized and scalable single console. This allows visibility with regard to devices and their respective statuses. The real objective of MDM is to enable an organization's security team to see and control each and every device that accesses the corporate network and uses corporate data. IT groups cannot hope to manage what they cannot see—prioritizing this is crucial.

Enterprises can more efficiently manage employee-liable devices and prevent data leaks or loss when they complement MDM solutions with virtualized mobile infrastructure (VMI). Solutions like *Trend Micro™ Safe Mobile Workforce™* provide a safe mobile infrastructure that separates corporate data from an employee's personal data. With this solution, users can safely access corporate information through a secure native mobile environment which can run on any mobile device regardless of its OS. Since the VMI is hosted on the company's centralized servers—accessed via a simple mobile app—company data never leaves the network or gets stored on employee devices. For IT administrators, this means they can easily and centrally manage and maintain workspaces from a single console. This gives them visibility and control over corporate data without encroaching on employee privacy.

In case of device loss or theft, IT administrators do not need to worry about securing data and remotely wiping it as in the case of MDM solutions, since with Safe Mobile Workforce, apps and data are no longer stored on the device. Furthermore, this solution does not require much administrative overhead since it has simplified management and deployment with its single sign-on for Exchange Server Access and active directory integration.

The scenarios that put security as less of a priority have dire implications. For instance, IT groups may have a bare-bones antivirus solution for mobile devices installed but neglected to orient employees about social engineering or corporate information sharing.

Taking a proactive stance in managing mobile devices in the corporate network ultimately reduces overall IT support costs. Solutions like *Enterprise Mobile Security and Management* and Trend Micro Safe Mobile Workforce enable consumerization while protecting corporate data accessed via mobile devices.



Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

©2015 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud