A **TrendLabs**Security in Context Paper

TREND MICRO™

Implementing BYOD Plans:

What are the Risks to Your Corporate Data?

Employee-Liable Mobile Devices: Challenging 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 work is forcing security to compete with other equally important activities.

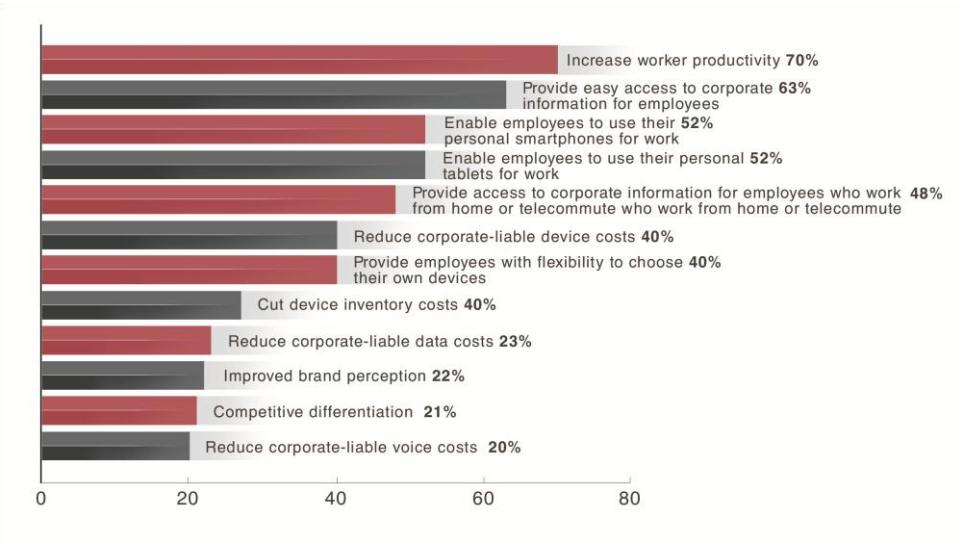

Figure 1. Factors driving bring-your-own-device (BYOD) in organizations and enterprises

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 that are 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 the BYOD trend 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 emerged both from the enterprises and employees' end. In a study, the top challenge in consumerization of IT that enterprises cited is mobile device security.

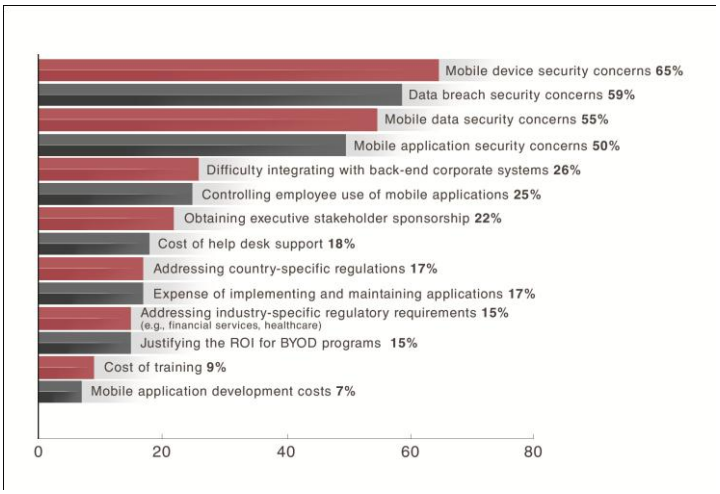

Figure 2. Top challenges in implementing BYOD

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

Data Breach

In a Trend Micro study[1], 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.

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 campaign[2], our threat researchers found 2 APKs in one of its C&C servers, suggesting that threat actors may launch attacks using this platform. In our 2014 Security Predictions[3], we cited that attackers will likely target mobile devices as its 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-risks 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 is expected to reach 3 million by end of 2014. Data stealers rank as third in the list of mobile threat types. While majority of these applications are found in malicious domains, we also spotted it on legitimate third party app stores.

---

[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

[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

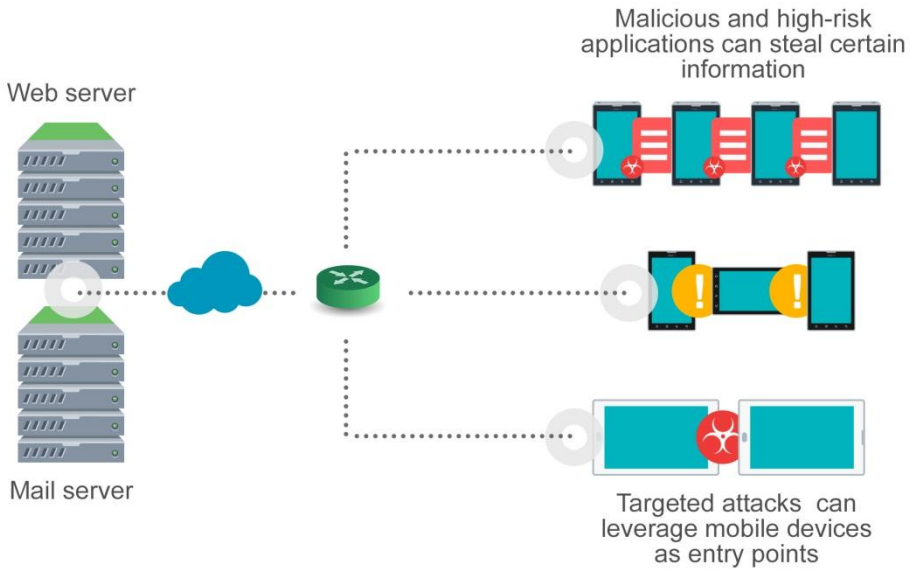

Figure 3. Risks to corporate data

Maximizing BYOD with Security in Mind

The availability and accessibility of corporate data is crucial for both enterprises and employees to increase work productivity. However, it also poses security risks to their confidential data. With the use of employee-liable devices, IT faces the challenge of visibility and control of what types of devices are accessing the network and in differentiating corporate from personal data stored on these devices.

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

Security solutions with mobile device management provide control in a centralized, scalable, single console and allow 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 and prioritizing this is crucial.

Enterprises can efficiently manage employee-liable devices and prevent data leakage or loss via these devices by complementing their MDM solutions with virtualized mobile infrastructure like Trend Micro Safe Mobile Workforce. This endpoint solution for mobile users provides clear infrastructure separating corporate and personal data. Through this solution, users can safely access corporate information with the same mobile environment in any mobile device they use, since the mobile operating system is hosted on centralized servers. In addition, the data and apps are also accessible from any location over a network using an efficient remote display protocol. For IT administrators this means that they can easily

manage and maintain workspaces centrally from a web console, giving them visibility and control.

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 not directly stored on the device. Furthermore, this mobile 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 Trend Micro Mobile Security 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 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

TREND MICRO™

Securing Your Journey to the Cloud