ASA

Risk Consultants

Research Note

BYOD: Organizational Impacts of Mobile Computing and Convergence

By: Rajesh Subramanian

Keywords: BYOD, devices, risk, threats, mobile security, mobile.

Abstract: BYOD or Bring Your Own Device policy allows employees to work from anywhere and at any time using their personal or preferred devices and has seen a meteoric rise across multiple industries. Although this working environment provides flexibility to the employees and value to an enterprise, it presents several threats that can affect an enterprise financially as well as in reputation. Big corporations have undergone a seamless transition to this program in recent times while laying down a structure for other growing companies to adopt. It is important for the Chief Information Security Officer to understand the risks and security measures to be taken in order for the BYOD program to be successful.

ASA

Risk Consultants

Introduction

BYOD or "Bring Your Own Device" refers to a business policy that allows employees the use of their preferred computing devices – like smartphones and laptops – for business purposes. This means employees are welcome to use personal devices (laptops, smartphones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smartphones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Research firm Gartner has predicted that by 2014, 90% of organizations will support corporate applications on personal devices.[1] This has not only led to an increase in employee satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.[2]

In the early 1990s, executing different tasks necessitated the use of different devices. For instance, an mp3 player was needed to listen to music; whereas chores, tasks and schedules were tracked by a PDA.

An addition to this list was a bulky laptop and a camera and it seemed a wait till eternity that we would ever have a single device to suit our different needs. However, remarkable advances in technology in the last decade have made it possible to perform all the above mentioned tasks using a single hi-tech device. Different technologies can work in synergy with each other which improves user productivity and convenience. The introductions of the Xbox 360 and Apple TV in 2006 are perfect examples of technology convergence as it allows users to play games, listen to music, watch movies and sports on a single "black box."

Emerging BYOD Threats

Every business decision is accompanied with a set of threats and a BYOD program is not immune from them. As outlined in the Gartner survey,[3] a BYOD program that allows access to corporate network, emails, client data etc. is a top security concern for enterprises. Overall, these risks can be classified into four areas as outlined below:

Network Risk

Example: Lack of device-visibility

When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of

the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smartphones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance,[4] this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

Device Risk

Example: Loss of Devices

A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threat as per the rankings released by Cloud Security Alliance.[5] With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

Application Risk

Example: Application Viruses and Malware

The Juniper "Mobile Security Strategies: Threats, Solutions & Market Forecasts 2012-2017" report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.[6] With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are in a Catch-22 situation in deciding who is responsible for device security – the organization or the user.

Implementation Risk

Example: Weak BYOD policy

The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

Industry BYOD Implementation

The BYOD program is becoming an exciting venture for most multinational firms, given its copious benefits. In spite of the threats identified above, its implementation of this burgeoning program needs to be strategic. The best practices outlined by Gartner for its efficacious execution entails a three-pronged approach – Secure the Device, Secure the Data and Protect the Network.[7] The manifestation of robust Mobile Device Management software optimizes functionality and security of the mobile communication network while reducing vulnerability.[8] VMware's Horizon Suite portrays that virtualization is a technique to secure data while following mobile users wherever they go.[9] IBM, on the other hand, ensures that BYOD users utilize the Lotus Traveler collaborative software that synchronizes email, contacts and tasks with the company's Lotus Domino server.[10] Likewise, Cognizant's BYOD directed market research puts forth a holistic strategy and a set of policy guidelines that would enable the effective and efficient application of this program.[2] This deployment comprises of the right combination of Mobile Device Management (MDM), Mobile Application Management (MAM) and a Mobile Application Development Platform (MADP).[11]

Steps to be taken by a CISO to Mitigate BYOD Threats

The Chief Information Security Officer (CISO) is a senior-level executive who is responsible for the protection of organization technological assets. They are in-charge of the organization's information security program that safeguards its information infrastructure and resources. The following action items are some of the steps that a CISO must take to assuage against these threats:

- Develop a robust Risk Management program to identify, assess and reduce risk exposure against these threats.
- Develop an Access Management hierarchy within the organization that resolves the access level granted to employees based on their roles and responsibilities.
- Identify and segregate critical and business sensitive data to a secure computing environment in order to avoid the problem of data loss or data corruption snowballing into a situation of massive chaos and humiliation for the organization.
- Ensure the existence of a disaster recovery program that enables business continuity.
- Finally, lead efforts in the development and review of a BYOD security policy, guidelines and practices.

Conclusion

While it has become typical for an organization to have separate devices for personal and professional use, Bring Your Own Device is a rising trend across multiple industries where this separation is converging. However, this new phenomenon continues to outpace security measures in place, presenting an organization with a plethora of security challenges. Although a change towards this program is tedious, it is the responsibility of the senior management within the organization to consider all variables involved to carve out a feasible plan for its implementation.

ASA

Risk Consultants

References:

[1] "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond?" *Gartner.com.* 24 Oct. 2012. Web. (Date) <http://www.gartner.com/it/page.jsp?id=2211115>

[2] "Making BYOD Work for Your Organization." *Cognizant.com.* June 2012. Web. (date) <http://www.cognizant.com/RecentHighlights/Making-BYOD-Work-for-Your-Organization.pdf>

[3] "Gartner Survey Shows BYOD Is Top Concern for Enterprise Mobile Security." *Gartner.com* 14 June Aug. 2012. Web. (Date) <http://www.gartner.com/it/page.jsp?id=2048617>

[4] Grajek, Garret. Five BYOD Threats you Must Solve Today - or Risk Losing Your Job." *SC Market Scope.com.* 22 June 2012. Web. (Date) <http://www.scmarketscope.com/five-byod-threats-you-must-solve-today--or-risk-losing-your-job/article/246926/>

[5] "Data Loss From Missing Mobile Devices Ranks as top Mobile Device Threat by Enterprises." *Cloud Security Alliance.* 4 Oct. 2012. Web. (Date) <https://cloudsecurityalliance.org/csa-news/data-loss-mobile-ranks-top-threat-enterprises/>

[6] "Malware Incidents Forecast to Increase as 95% of Smartphones & Tablets Remain Unprotected with Security Software." *Juniper Research.* 25 Sept. 2012. Web. (date) <http://juniperresearch.com/viewpressrelease.php?pr=339>

[7] "iPad and Beyond: Bring Your Own Device." *Gartner.com.* n. dat. Web. (date) <http://www.gartner.com/technology/research/ipad-media-tablet/bring-your-own-device.jsp>

[8] Finneran, Michael. "BYOD Requires Mobile Device Management. InformationWeek Mobility." *InformationWeek.com.* 7 May 2012. Web. (date) <http://www.informationweek.com/mobility/business/byod-requires-mobile-device-management/229402912>

[9] Babcock, Charles. "VMware Shows More Of BYOD, Virtual Desktop Tools." *InformationWeek Mobility.* 29 Aug. 2012. Web. (date) <http://www.informationweek.com/hardware/virtualization/vmware-shows-more-of-byod-virtual-deskto/240006422>

[10] Kanaracus, Chris. "IBM CIO Discusses Big Blue's BYOD Strategy." PCWorld. 26 Mar. 2012. Web. (date) <http://www.pcworld.com/article/252584/ibm_cio_discusses_big_blues_byod_strategy.html>