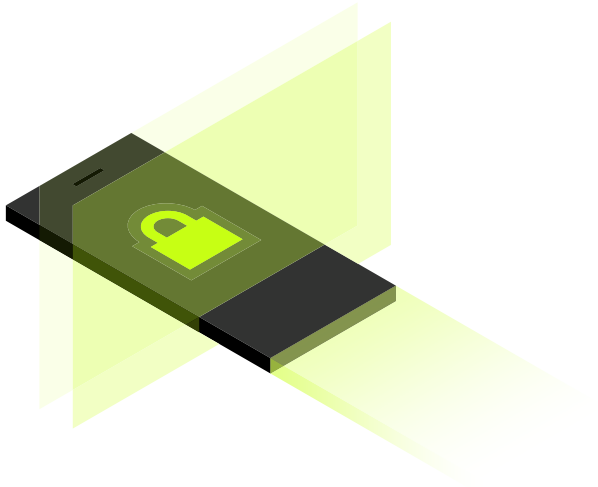
SOPHOS
Security made simple.



Your CEO Wants to Connect a New Device to the Corporate Network. Now What?

Key challenges and rewards of a comprehensive BYOD strategy

By **Simi Kamboj**, Senior Product Marketing Manager,
and **Alan Phillips**, Product Specialist

It used to be possible to reduce the risks of mobile devices by requiring employees to use a corporate device. Now, with the growing BYOD (Bring Your Own Device) trend in full effect, your CEO has a shiny new tablet and inaction is no longer an option. How do you balance the benefits of BYOD with the increased security risks? How do you keep that CEO from turning that little tablet into a gaping hole in your company's security? This paper examines the key challenges, risks, and rewards of BYOD. And it explains how to develop and implement the right strategy to protect your company today, and in the future.

The Changing Landscape: New Devices = New Threats

There was a time that businesses were like mighty fortresses, with all of their data and information stored safely behind locked doors. Then technology began opening those doors, bringing unprecedented availability and opportunities—for both employees and, unfortunately, cybercriminals as well.

If you think there are a lot of mobile devices out there now, brace yourself. According to some projections, mobile devices will outnumber humans by 2014.[1] In this rapidly proliferating environment, BYOD can quickly become BYOST—Bring Your Own Security Threats.

There is no doubt that BYOD increases productivity. But with the average businessperson now carrying three mobile devices[2] and working anywhere and everywhere, those once-mighty corporate walls can come crumbling down, unless you develop a comprehensive mobile device security strategy.

The following are some of the major threats and risks you need to consider.

Where is your company's data? Every mobile device should be viewed as an unlocked file cabinet of confidential company information sitting on the sidewalk. How do you determine and keep track of which employee has what data on which devices? Is that data stored on hard drives, flash drives, the cloud, or on some other form of mobile storage? If disgruntled employees leave the company, how much data are they bringing with them?

It's easy to lose a mobile device. Lost mobile devices end up in up cabs, restaurants and airports every day. And smartphone theft is a major problem. In the U.S. alone, statistics show that lost and stolen smartphones cost consumers an estimated $30 billion in 2012.[3] Of course, that simply takes into account the hardware costs, not the value of lost data, compromised networks, or possible fines.

Malware has gone mobile. Some mobile operating systems are less restrictive than others when it comes app development. This works for the greater good, but it also works for the bad guys. With employees often acting as system administrators with their own devices, unrestricted downloads of new apps can introduce new malware and unregulated access to your company's network and sensitive information—which can result in data loss and unexpected cost issues.

How many operating systems can you handle? Can you provide security for BlackBerry, Apple and Android? How about Windows Phone 8? Any comprehensive, effective mobile device security plan needs to work across existing and new operating systems. Each present their own shortcomings and challenges.

Public Wi-Fi hotspots are a hot target. Public Wi-Fi hotspots and other unsecured network access points are security breaches waiting to happen. How do you make sure that your CEO's cup of coffee at the cybercafé doesn't lead to an endless buffet for cybercriminals?

1. "World to have more cell phone accounts than people by 2014," Silicon India, January 2, 2013, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html
2. "Infographic: Users weighed down by multiple gadgets - survey reveals the most carried devices," Naked Security, March 14, 2013, http://nakedsecurity.sophos.com/2013/03/14/devices-wozniak-infographic/
3. "Theft of cell phones rise rapidly nationwide," USA Today, October 20, 2012, http://www.usatoday.com/story/tech/2012/10/20/thefts-of-cell-phones-rise-rapidly-nationwide/1646767/

Poor policies and unwritten rules. Written policies are vital to reinforce the steps tech teams have to take to integrate mobile devices into the corporate environment. Don't forget, an unwritten rule isn't a rule at all.

Benefits of a Secure BYOD Policy

There are many challenges to formulating and enacting a BYOD strategy. Although management may balk at the time and expense involved, it's important to focus on the benefits of a comprehensive strategy.

Reduced hardware costs and maintenance

When employees bring their own devices to work, it means they are paying for their own devices and data plans, saving thousands of dollars per employee. In addition, employees are responsible for their own device maintenance, freeing IT staff from endless help desk tickets. Once an effective BYOD policy is in place, IT will benefit from increased productivity.

More satisfied and productive employees

Employees want to use their own mobile devices. They are more comfortable with their personal devices. When it comes to attracting and retaining employees, a good BYOD policy can be a powerful incentive. A satisfied employee is a more productive employee.

240 more reasons

Mobile employees work 240 more hours per year than the workforce average.[4] That's the equivalent of six weeks of additional full-time work per employee. Multiply those numbers by the number of your mobile workers and it's easy to see how an effective BYOD policy greatly benefits your company.

How to Solve BYOD With a Mobile Device Management (MDM) Solution

Every company's needs are different, but there are basic policy requirements that you should look at when creating a BYOD plan, and it is not just about the devices. Who will the users be, what apps will they need or want, where will data be stored, and what IT infrastructure will be necessary to provide support and security?

From the outset, you need to set firm guidelines as to what mobile devices will be incorporated into the plan, what level of network access will be granted, what operating systems you will support, what data will be accessible, and what type of storage will maximize both security and productivity.

A mobile device management (MDM) solution with robust features can make BYOD compliance much simpler. An MDM controls device passwords and encryption, keep devices

4. The iPass Global Mobile Workforce Report, iPass Inc., May 24, 2011, http://www.ipass.com/wp-content/uploads/2011/05/iPass_MWR_Q2_2011.pdf

up to date with network and manufacturer patches, and secures devices with a device lock or wipe in case of loss, theft, or any breach of security or policy rules.

An ideal MDM solution should also ensure cloud storage and app downloads come from approved sources. A self-service portal offers customers complete visibility into their mobile devices, making it simple for small and mid-market organizations to secure, monitor, and control mobile devices.

Consider some of these aspects of a comprehensive BYOD strategy and how an MDM can offer the solution.

- You don't have to grant access to every mobile device under the sun. Find out what employees like and want, and create a list of approved devices.
- Determine the level of access needed by individual employees and departments. An MDM solution should enable varying levels of access.
- Establish a list of acceptable apps, and consider software that can identify and block the download of suspicious and high-risk apps.
- Cloud-based storage services must be carefully vetted for reliability and trustworthiness, as well as what types of data can be stored there.
- Be realistic about what your IT staff can handle in terms of managed services, and network security and support. Look for solutions that both IT staff and mobile workers can easily use. Remember that resources you can allocate for support today may not be sufficient next year.
- The average user has three mobile devices, so look for a solution that offers a license for each user, not each device.
- Consider compliance requirements, as well as legal and privacy issues. Be certain that employees realize that even though they own the mobile device, all of these issues are their responsibility, too.

How Sophos Meets the BYOD Challenge

Sophos Mobile Control

Imagine easily deployed and managed MDM software that covers all mobile devices with just the options and policies your company needs; a total solution that puts you in control. With Sophos Mobile Control you can stop dreaming and start enjoying the benefits of BYOD. This simple yet comprehensive solution offers:

- Software options of on-premise installation, or Software as a Service (SaaS) hosted by Sophos or a managed service provider of your choice. The intuitive web-based console allows you to monitor and manage all devices with ease.
- MDM that covers both company and employee-owned devices from the first day of use to the final decommissioning or device theft or loss. Whether it is iOS, Android, Samsung, or Windows Phone, you control security and device policies.

- The Self-Service Portal allows users to register their own devices and perform tasks such as a password reset, check their compliance status, and decommission a device. That makes it ideal for companies considering BYOD.
- One license per user, no matter how many devices. This allows users to have multiple devices without increasing the cost for their employer.
- Block all of those risky apps with Mobile App Management (MAM), while safely distributing secure apps from the Enterprise App Store.
- Set levels of access of individuals or groups based on your compliance requirements. Regularly check compliance status, as well as automating compliance violation responses so there are never any unpleasant, and costly, surprises.

SafeGuard Encryption

Even the best device security is useless if an employee loses a memory card full of client files, or a cloud storage service is breached and your company's most sensitive information is exposed.

Encrypted data is the backbone of your security defense, so Sophos offers SafeGuard Encryption. From a single SafeGuard Management Center run on Windows or Mac, you can encrypt and monitor all of your data from in-house, the road, or the cloud, ensuring compliance even in worst-case scenarios of loss, theft, or a system breach.

- Encrypt data on desktops, laptops, shared files, and removable media such as memory cards, USB sticks, and even CDs and DVDs.
- Cloud storage encryption is automatic when files are uploaded to services such as Dropbox, SkyDrive and Egnyte.
- Mobile devices (iOS and Android) can utilize the Mobile Encryption file readers.

Sophos Unified Threat Management (UTM)

You want a UTM solution with no weaknesses for your web and email gateways, and mobile devices. Setup times can be as little as 10 minutes, and Sophos UTM can be installed as hardware, software, a virtual appliance, or even in the cloud, and you choose only the services you need.

Other features include:

- Advanced threat protection, dynamic app control, and customizable web filtering.
- Eliminate those risky remote network access points with a secure site-to-site VPN.
- Comprehensive antivirus for desktops and mobile devices, plus a simple and powerful web application firewall.
- Fast, affordable, effective.

Conclusion

Ignoring your BYOD strategy is good news—for your competitors. There are many challenges to BYOD, but there are also many rewards in terms of increased productivity, reduced costs, and increased employee satisfaction. Sophos can show you how easy and affordable it is to manage and provide security for the CEO's shiny new tablet, and for the ever-growing number of mobile devices and mobile workers. So your organization is protected from data security and compliance issues while making IT's job easier.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

8.13.GH.wpna.simple

SOPHOS