SOPHOS

BYOD Risks and Rewards

How to keep employee smartphones, laptops and tablets secure

By **Gerhard Eschelbeck**, Chief Technology Officer
and **David Schwartzberg**, Senior Security Engineer

Whether you're an end user or an IT administrator, Bring Your Own Device (BYOD) is becoming the rule rather than the exception in today's workplace. Although BYOD may be a convenience to your employees, you need to think about its impact on corporate security models. This whitepaper explains the risks and rewards of BYOD, and shows you how you can adopt BYOD in your workplace while protecting your data.

What BYOD means for business

Today's IT leaders face many security challenges and rapid changes, all while having to do more with less. They must provide end users with the latest, most advanced technologies to remain competitive. And they have to protect company, customer and employee data while thwarting attacks from cybercriminals.

New technology brings more ways to access data, new types of devices and alternatives to the traditional PC platform. Apple CEO Tim Cook appropriately called this the "post-PC era."[1]

These dynamics have created a shift toward BYOD, a trend in the workplace that's rapidly becoming the rule rather than the exception.

BYOD encompasses more than personal computers. It means employees using smartphones, tablets, Blackberrys, ultralight books and more for their work. The concept of BYOD broadens to include software and services, as employees use cloud services and other tools on the web.

The shortcomings of technology which made BYOD unrealistic a few years ago have given way to broad popularity and use of these tools.

These include:

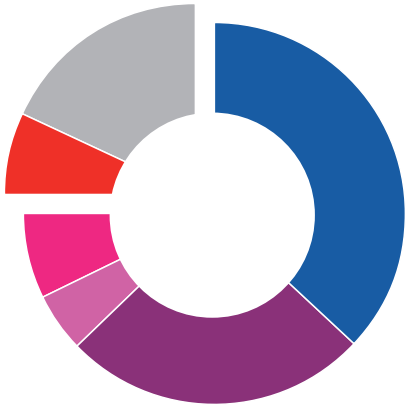
1. Web: Today's web is the singular way to access any application—business, financial, customer support, sales or technology.

2. Wireless: No matter where you are or what device you're using, you have access to the back office infrastructure through extensive Wi-Fi networks.

3. Mobile devices: Device form factors have become more sophisticated, cheaper and more portable, with more robust memory and battery life.

1. "The post-PC world is real and it's here," *The Globe and Mail*, http://www.theglobeandmail.com/technology/gadgets-and-gear/the-post-pc-world-is-real-and-its-here/article4098023/

One in four devices used for work are either smartphones or tablets.



- Desktop **37%**
- Laptop **26%**
- Ultraportable **5%**
- Netbook **7%**
- Tablet **7%**
- Smartphone **18%**

Source: Forrester's Forrsights Workforce Employee Survey, Q4 2011

What BYOD means for security

It's risky to assume that prohibiting personal devices solves the problem, because employees end up using their own devices anyway, unmonitored and undeterred by your security policies.

Whatever you think of BYOD and however you choose to implement it, IT managers should treat it the same way as any introduction of new technology: with a controlled and predictable deployment.

Ask yourself:

1. Who owns the device? That's a question that has changed over time. In the past, the company owned the devices. With BYOD the devices are owned by the user.

2. Who manages the device? Previously this was an easy question to answer. Today it could be either the company or the end user.

3. Who secures the device? Accountability is not something that goes away for a user just because they personally own the device. After all, the data carried on it is company owned.

Answering these questions is fundamental to both understanding the risks and taking advantage of the rewards of BYOD.

All organizations have the flexibility, based on their corporate culture and regulatory requirements, to embrace BYOD as much as they deem reasonable. For example, there are companies who have decided the risk is too great and choose not to implement a BYOD program.

In May 2012, IBM banned its 400,000 employees from using two popular consumer applications over concerns about data security. The company banned cloud storage service Dropbox, as well as Apple's personal assistant for the iPhone, Siri. Siri listens to spoken requests and sends the queries to Apple's servers where they are deciphered into text. Siri can also create text messages and emails on voice command, but some of these messages could contain sensitive, proprietary information.[2]

Ultimately, the success of your BYOD program is measured by your employees' willingness to use their personal devices within the rules you set for them. Your organization's security procedures and policies should determine whether and how you adopt BYOD.

You need to have the ability to enforce security policies on a device level and protect your intellectual property if that device is ever lost or stolen.

BYOS: Bring Your Own Software

The same technologies driving the turn to BYOD also allow users to access non-company software. This effect is known as Bring Your Own Software (BYOS).

End users may be using free public cloud storage providers as a way to collaborate on and transfer large documents. Those documents, however, could contain data that falls into scope of regulatory guidelines, which could place your data at risk.

You should evaluate how cloud storage providers transport and store your company's files. Consider these questions:

- How are they encrypting the data?
- Are they using a single key for all of their customers?
- Who has access to the key to decrypt the data?
- Will they surrender the data to authorities if it is subpoenaed?
- In which countries are the servers located that are housing the data?
- Does your organization have an agreement with customers that their data won't be stored in certain countries?

Download Fixing Your Dropbox Problem at Sophos.com

2. "IBM: Sorry, Siri. You're Not Welcome Here," InformationWeek, http://www.informationweek.com/news/security/mobile/240000882

How to secure BYODs

The first and best defense in securing BYODs begins with the same requirements you apply to devices that are already on your network. These security measures include:

- Enforcing strong passcodes on all devices
- Antivirus protection and data loss prevention (DLP)
- Full-disk encryption for disk, removable media and cloud storage
- Mobile device management (MDM) to wipe sensitive data when devices are lost or stolen
- Application control

You should always extend encryption to both data in transit and data at rest. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data. But if somehow your device-level password is compromised, encrypting the data stored on the device provides a second level of security a hacker must get through in order to steal your data.

You should encourage users to think of the extra layers of security as helpful tools that give them the ability to use their own devices within the workplace. By password protecting devices, a user acknowledges accountability and responsibility for protecting their data.

In addition to applying passcodes and antivirus prevention to your devices, you should apply a custom level of application control to BYODs. If applications are available to employees on the internal network, they should be able to access them offsite through a VPN or email software.

A successful BYOD program allows your users to be productive outside of their scheduled work hours while also giving them the flexibility to do the things they like to do when they're not working—like update their status or enjoy playing an interactive game.

Whatever decision you make for your BYOD policy, be sure that it's enforceable and enables IT to deploy software remotely.

Setting policy and compliance standards

You need to formalize policies specifically around BYOD. For example, will your policy include any and all devices currently available? Or will you limit use of personal devices to specific hardware and software platforms? What about devices that aren't yet available but could reach consumer markets in the next few years?

The handheld mobile device market is evolving rapidly with new versions and new manufacturers. Keeping that in mind, your BYOD policy should be adaptable. You should maintain written strategic policies based on what yoA few times we use the acronym as an adjective u know today and what you think will generally be available tomorrow. And you must apply technology that enforces your written policies to provide management, audit proof modeling, control and security.

Implementing a solution designed to verify that devices can be remotely managed can help you in the ongoing battle to keep security policies relevant and reliable, especially if you're in an industry with strict compliance and auditing standards.

Additionally, being aware of the service plans your employees have can help you offer the best services while reducing cost. Using a data plan's hotspot or tethered options can result in an overall better experience for end users. Consider data-only plans for personal Wi-Fi devices in place of maintaining a home office long-distance and ISP service plans.

7 steps to a BYOD security plan

Your company's security and BYOD can co-exist. And it starts with planning. Here's how:

1. Identify the risk elements that BYOD introduces

- Measure how the risk can impact your business
- Map the risk elements to regulations, where applicable

2. Form a committee to embrace BYOD and understand the risks, including:

- Business stakeholders
- IT stakeholders
- Information security stakeholders

3. Decide how to enforce policies for devices connecting to your network

- Mobile devices (smartphones)
- Tablets (e.g., iPad)
- Portable computers (laptops, netbooks, ultrabooks)

4. Build a project plan to include these capabilities:

- Remote device management
- Application control
- Policy compliance and audit reports
- Data and device encryption
- Augmenting cloud storage security
- Wiping devices when retired
- Revoking access to devices when end-user relationship changes from employee to guest
- Revoking access to devices when employees are terminated by the company

5. Evaluate solutions

- Consider the impact on your existing network
- Consider how to enhance existing technologies prior to next step

6. Implement solutions

- Begin with a pilot group from each of the stakeholders' departments
- Expand pilot to departments based on your organizational criteria
- Open BYOD program to all employees

7. Periodically reassess solutions

- Include vendors and trusted advisors
- Look at roadmaps entering your next assessment period
- Consider cost-saving group plans if practical

Implemented properly, a BYOD program can reduce cost while increasing productivity and revenue. As BYOD goes mainstream in IT departments, security should be front and center for users and IT administrators alike.

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

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

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

Boston, USA | Oxford, UK

A Sophos Whitepaper 06.12v1.dNA

SOPHOS