SOPHOS

Four Data Threats in a Post-PC World

Managing BYOD, mobile devices, cloud storage and social networks

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

PCs dominated our desktops for the last 40 years, but our need for on-demand information is rapidly changing the types of devices we use and the way we work. As we enter a post-PC world, four threats have emerged to challenge data security—BYOD (Bring Your Own Device), mobile devices, cloud storage and social networks. In this whitepaper we'll describe each of these threats and give you best practices to successfully manage them.

What is the post-PC world?

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]

Industry analysts agree. According to research from JP Morgan and the Gartner Group, smartphone sales in 2012 will surpass PC sales by almost 300 million (657 million to 368 million).[2] Tablet sales will reach 106 million in 2012, according to IDC. And Forrester Research predicts the tablet will become most users' main computing device by 2016.[3]

We have entered a new stage of technology that offers end users far greater independence and convenience for accessing data than the PC alone. This trend has introduced four major threats to protecting your data and intellectual property. In the following four sections, we describe these technologies and related threats. And we explain how to manage them successfully.

1. **Bring Your Own Device (BYOD)**
2. **Mobile devices**
3. **Cloud storage**
4. **Social networks**

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/
2. "Smartphone, tablet sales outpace PC growth," Thomson Reuters, http://graphics.thomsonreuters.com/12/02/GLB_TECHMKTB0212_SC.html
3. "Tablets will be preferred devices by 2016," Computerworld, http://www.computerworld.com/s/article/9226890/Tablets_Will_Be_Preferred_Devices_by_2016

Threat 1: BYOD

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.[4]

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.

4 "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 protection 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 you 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 hot spot 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 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 (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

Threat 2: Mobile devices

Whether they are company-owned or employee-owned, mobile devices introduce a threat to your data security. These devices act like portable computers, and that means you should think about protecting them as much as you would your PCs. You need a plan for locking down data stored on the devices and keeping the devices secure.

According to the Ponemon Institute's 2012 Annual U.S. Cost of a Data Breach study, the average cost of a data breach is $194 per lost or stolen record with an average cost of a data breach of US$5.5 million.[5] Data breaches caused by malicious attacks increased from 31% in 2010 to 37% in 2011, and mobile device theft was responsible for 28% of malicious breaches.[6]

National and global compliance rules and the bodies that oversee them have the ability to levy fines against businesses who lose customer data on unencrypted devices. Aside from paying for credit monitoring services and court-related judgments, the damage to a company's reputation can be costly.

Before introducing BYODs into the workplace, you need to consider several factors as part of a remote working policy. What additional applications need to be installed? How can the device be secured? How can network access be secured? What about the data on the device?

5. "Cost of data breaches falls for first time in seven years," PC World, http://www.pcworld.com/businesscenter/article/252195/cost_of_data_breaches_falls_for_first_time_in_seven_years.html

6. "Data breach costs drop," InformationWeek, http://www.informationweek.com/news/security/attacks/232602891

7 tips to secure mobile devices

Mobile BYOD is a balance between allowing employees to use their personal devices for work and the security of your business.

Employees are often the first, only and best defense against the theft of sensitive data. They need to understand the appropriate use of mobile devices and how to handle, maintain and protect sensitive data. Employees using their own mobile devices must follow policies that keep the business compliant with regulatory requirements.

To keep mobile devices and the data on them secure, follow these seven tips from Sophos and the Ponemon Institute.

Tip 1. Develop an enterprise strategy for mobile security. Your strategy should include classifying data on mobile devices, such as regulated data (credit cards, driver's license number), non-regulated customer data (purchase history, email addresses), non-regulated confidential business data (such as IP, business plans and financial records) and employee data.

Tip 2. Create a comprehensive policy and guidelines for all employees and contractors who use mobile devices in the workplace. Institute an accepted use policy (AUP) and security procedures to address the risks associated with each device. Guidelines can include what types of data should not be stored on these devices, how to determine if an application can be safely downloaded, and how to report a lost or stolen device.

Tip 3. Establish organizational accountability. Organizations have a responsibility to provide their employees with the policies, procedures and technologies they need to keep mobile devices secure. In turn, employees must be accountable and aware of the importance of using their mobile devices responsibly.

Tip 4. Launch awareness training for end users (to reduce employee mistakes). Beyond policies and monitoring of employee behaviors, organizations should implement a training program to help employees understand the new and emerging security threats present when they use their mobile device.

Tip 5. Use application control, mobile device management (MDM), patching and other controls to prevent hacking and malware infections. In our opinion, blacklisting methods aren't enough to control which applications can be downloaded by employees onto their mobile devices. With so many targeted attacks exploiting vulnerabilities, you need to be sure operating systems and applications on mobile devices such as browsers, PDF readers and Flash players are patched and up to date.

Tip 6. When possible, use remote wipe, mobile device encryption, and anti-theft technologies to reduce the risk of a data breach. A lost or stolen device that is encrypted is much less costly to the organization than an unencrypted one. In fact, the Ponemon Institute reported in May 2009 that the total economic impact of one lost laptop is $49,256. Encryption on average can reduce the cost of a lost laptop by more than $20,000.

Tip 7. Understand emerging privacy issues related to mobile devices. The exposure of customer or employee personal information can result in reputation damage and costly fines as a result of non-compliance. You need to understand how this information is being shared and what it means for compliance with data regulations.

Get more on these tips. Download 7 Tips for Securing Mobile Workers at Sophos.com

2012 Mobile Security Survey

- 62% percent of organizations allow employees to use personal mobile devices for work and 24% percent are developing a policy for personal mobile device use
- 84% of respondents identify lost or stolen devices as a key mobile security concern
- 31% cite mobile malware on applications from public app stores as a top concern
- 42% allow employees to install personal applications on personally owned mobile devices accessing corporate data with no restrictions
- 87% say securing data on mobile devices is somewhat or very important, but just 14% mandate hardware encryption for corporate data stored on mobile devices
- 48% have had a mobile device containing enterprise data come up missing within the past 12 months; 12% report that this data loss required public disclosure

Source: 2012 State of Mobile Security, a new report featuring results from InformationWeek's recent 2012 Mobile Security Survey. More than 300 business technology professionals responded to the survey. Courtesy of InformationWeek Reports (http://reports.informationweek.com), a service provider for peer-based IT research and analysis.

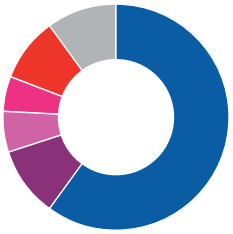
See how Sophos Mobile Control helps you protect data, manage applications and stay compliant

Policy on Personal Mobile Device Use

Does your mobility policy allow employees to use personal mobile devices for work?

- Yes **62%**
- No, but we're developing a policy **24%**
- No, and we have no plans to allow personal device use **14%**

Percentage of Mobile Devices Experiencing Security Incidents



What percentage of the mobile devices you manage, including laptops, experience security incidents in a given year?

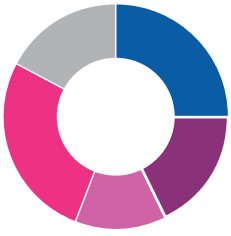
- Less than 10% **60%**
- 11% to 20% **10%**
- 21% to 30% **6%**
- More than 30% **5%**
- We don't collect mobile security incident metrics **9%**
- Don't know **10%**

Missing Mobile Devices

In the past 12 months, has any mobile device containing enterprise data, including laptops or netbooks, come up missing (including accidental loss and theft)?

- No **52%**
- Yes **48%**

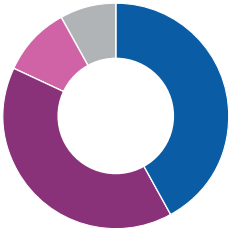
Mobile Device Management



Does your organization currently or plan to have a mobile device management system?

- Yes, we have an MDM system **25%**
- Yes, within the next 12 months **18%**
- Yes, within the next 24 months **13%**
- No **27%**
- Don't know **17%**

Personal Mobile Device Policy



Which of the following best describes what is or will be your policy on acceptable user-supplied devices?*

- Users can bring in any device and we'll let in on our network as long as the user agrees to certain policies **42%**
- Users can bring in a limited range of devices and must run our device management software **40%**
- We allow user-supplied devices with no restrictions **10%**
- Other **8%**

Data: Information Week 2012 Mobile Security Survery of 322 business technology professionals, March 2012

Copyrighted 2012. UBM TechWeb 89886:612JM

* Base: 278 respondents at organizations with, or developing, a policy for personal mobile device use.

Threat 3: Cloud Storage

The popularity of cloud storage is on the rise—today's most popular services have more than 50 million users combined. But all that perceived convenience often comes at a price. Attacks tend to follow technologies as they become popular.

For example, cloud storage providers have full access to your data and control where it is stored. You normally don't have much information about the infrastructure and the security mechanisms in place. And it might be that this storage isn't in your own country, which could raise legal challenges.

In spite of the risks, the demand for cloud services in the workplace is growing. In one survey, 66% of 4,000 employees in the U.S. and UK said they use free file-sharing platforms at work. Of those workers using free file-sharing apps, 55% do so without alerting their IT departments.[7]

At a recent Information Security conference, Sophos found that 45% of 214 conference attendees are using the services for work, and 64% reported that they thought this type of service is "scary."

Independent research supports these findings. In a 2011 Ernst & Young survey, 61% of organizations were either already using or planning to evaluate cloud storage. However, more than half of organizations (52%) had yet to put controls in place to mitigate data risk.

In fact, public cloud storage providers typically do not offer any kind of back-up guarantees, meaning that if your data is suddenly lost or the provider stops doing business altogether, you have no standing in recovering that data.

If you're storing data in the cloud, a single successful breach could put your whole business at risk.

To decide what's best for your organization and your users, ask yourself the following questions:

- Who administers your data?
- Do you remain in control of your data?
- What are the consequences of a data breach?
- What is the probability of data loss?
- Can you account for your data's security?

You may not get the best answers to these questions if your users are accessing cloud services without your knowledge, consent or encryption policies applied. And if you're not yet controlling user access to cloud-based storage services and applications or encrypting all your sensitive files, it's time to start.

7. "Workforce mobilization: What your IT department should know," SkyDox, http://www.skydox.com/workforce-mobilization-what-your-it-department-should-know

There are still three simple steps you can take to increase the responsible use of cloud services while maximizing data protection for your business.

1. Apply web-based policies using URL filtering

You can control access to public cloud storage websites with URL filtering, which prevents users from browsing to forbidden sites.

2. Apply application controls

Use application controls to set policies for the entire company or specific groups to block or allow particular applications.

3. Apply data encryption

Automatically encrypt files before they are uploaded to the cloud from any managed endpoint.

An encryption solution allows users to choose their preferred cloud storage services because the files are always encrypted and the keys are always your own. And because encryption takes place on the client before any data is synchronized, you have full control of the safety of your data. You won't have to worry if the security of your cloud storage provider is breached.

Central keys give authorized users or groups access to files and keep these files encrypted for everyone else. Should your web key go missing for some reason—maybe the user simply forgot the password—the security officer inside the enterprise would have access to the keys in order to make sure the correct people have access to that file.

Download our cloud storage whitepaper Fixing Your Dropbox Problem

Threat 4: Social networks

The explosive growth of social networks like Facebook (850 million users), Twitter (140 million users)[8] and LinkedIn (161 million users)[9] brings increased malware, spam and continuing erosions in privacy.

And then there's this amazing statistic: 50% of all smartphones are connected to Facebook every hour of the day.[10]

The extraordinary popularity of social networks has made them an attractive platform for malware authors, spammers, identity thieves and other cybercriminals. Social media networks encourage and reinforce an implied trust between users. Your new friend, or more likely a complete stranger, can then use and abuse this trust to take advantage of you, your social network accounts and maybe even your identity and bank accounts.

LinkedIn suffered a data breach in June 2012 that leaked password hashes online. After removing duplicate hashes, SophosLabs determined there were 5.8 million unique password hashes in the dump, 3.5 million that had been brute forced. That means over 60% of the stolen hashes were publicly known and could have ended up in the hands of criminals. Sophos recommended that all LinkedIn users change their passwords.[11]

The social sharing on these networks opens up other attack vectors including:

Clickjacking, an exploit in which malicious code is hidden beneath legitimate buttons or other clickable content on a website. SophosLabs has seen clickjacking links with headlines such as "Lady Gaga found dead in hotel room," "Japanese tsunami launches whale into building," and "Justin Bieber stabbed." You believe you're clicking one thing (e.g., watching a video), but you're actually clicking on an invisible button that contains a clickjacking worm.

8. AVG Community Powered Threat Report, http://aa-download.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf
9. http://press.linkedin.com/about
10. "50% of smartphones connect to Facebook every hour of the day," Forbes, http://www.forbes.com/sites/ericsavitz/2012/06/05/half-of-all-smartphones-connect-to-facebook-every-hour-of-the-day/
11. "LinkedIn confirms hack, over 60% of stolen passwords already cracked," Naked Security blog, http://nakedsecurity.sophos.com/2012/06/06/linkedin-confirms-hack-over-60-of-stolen-passwords-already-cracked/

Likejacking, a Facebook-enabled clickjacking attack that tricks users into clicking links that mark the clicked site as one of your Facebook Likes. These likes then show up on your profile and Facebook News Feed, where your friends can see the link and click it, spreading it to their contacts.

Facebook takes steps to reduce user risk

With nearly 900 million users Facebook has become a magnet for malware. To protect its users Facebook has partnered with five antivirus companies, including Sophos, to provide malicious URL data for Facebook's URL blacklist system. This partnership may benefit the growing number of companies creating a business presence on Facebook who want users to be confident they can click on their links without downloading malware or viruses to their computers.

How to secure users on social networks

Put in place a social media policy–and then make sure it's enforced. This policy should detail acceptable uses and explain the consequences of violating or failing to follow the corporate code of conduct around client confidentiality and intellectual property.

Explain social media threats and how to prevent them. Create a training or education program that explains the real day-to-day threats found on social networking sites. For example, offer examples of how to identify phishing and why you shouldn't click on a friend's link just because they think you should. Employees should understand how they might unknowingly download a virus onto a corporate PC or mobile device and how rapidly it can spread throughout the enterprise network.

Make sure users are aware of basic principles of privacy and password creation. Pick a strong, unique password and keep it secret; check privacy settings regularly and carefully choose a configuration; be wary of downloading applications; and only friend people you know.

Sophos Complete Security Suite

Our Sophos Complete Security Suite protects you everywhere, from your network to your servers, endpoints and mobile devices. And, because it's all from Sophos, it works better together. It's easier to use, saving you time and money, and it's backed by a vendor you trust.

- **Web protection** that combines the best of our endpoint, cloud and gateway to protect users everywhere
- **Encryption** deployed and managed from our antivirus console
- **Consistent DLP policies** across email and endpoint
- **Mobile security** for your iPhone, iPad, Android, Blackberry and Windows mobile devices
- **SophosLabs analysts** constantly monitor and fine-tune detection for you—keeping an eye on websites to avoid, threats, spam and more
- **One vendor to call** for 24/7 expert certified support

Contributors:

Barbara Hudson, Product Marketing Manager

Beth Jones, SophosLabs

Thomas Lippert, Senior Product Manager

Chris Pace, Product Marketing Manager

Sophos Complete Security Suite

Get a free trial

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
© Copyright 2012. Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.

A Sophos Whitepaper 06.12v1.dNA

SOPHOS