Insights on governance, risk and compliance

September 2013

Bring your own device

Security and risk considerations for your mobile device program

EY

Building a better working world

Contents

Introduction 1

Issues to consider in your BYOD deployment 2

Defining the BYOD risk 3

1. Securing mobile devices 4
2. Addressing app risk 6
3. Managing the mobile environment 7

Addressing governance and compliance issues ... 9

Conclusion 11

Eight steps to secure and improve your BYOD program 12

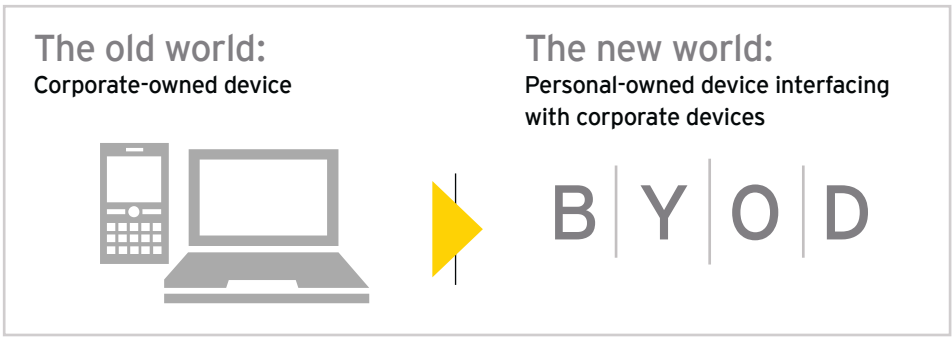
Introduction

Estimates suggest that in about five years, the number of mobile devices will be about 10 billion – 1.5 for every man, woman and child on the planet. With mobile devices increasingly embedded into all parts of our personal lives, organizations are finding that their employees increasingly want to use their own personal mobile devices to conduct work (often alongside corporate-provided devices), and many are reaching out to corporate IT to support this. Employers have concluded that they can't physically stop the use of mobile devices for both work and personal agendas, but they need to know how to control it.

In the current economic environment, companies are demanding that employees be more productive: having a robust mobile program that allows personal devices to be used safely in a work capacity can raise employee productivity and be a significant competitive advantage; it can even yield higher recruiting acceptance rates. An employee IT ownership model, typically called bring your own device (BYOD), presents an attractive option to organizations.

BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership. With personal devices now being used to access corporate email, calendars, applications and data; many organizations are struggling with how to fully define the impact to their security posture and establish acceptable procedures and support models that balance both their employees' needs and their security concerns.

In this report, you will discover what the main risks of BYOD are when considering your mobile device program, and we will propose potential steps to address these risks based on your organization's current and most urgent challenges.



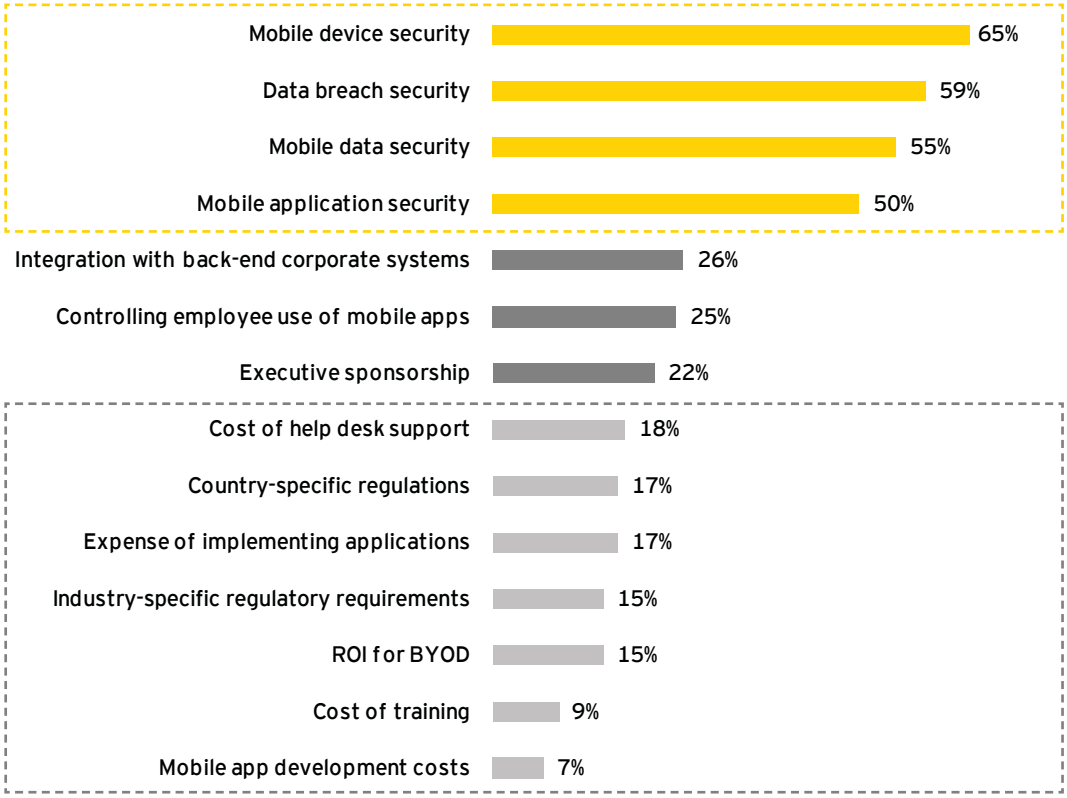
Issues to consider in your BYOD deployment

The risk landscape of a BYOD mobile device deployment is largely dependent on these key factors:

- **The organization's risk profile** – As for all information security risks, how the organization defines and treats risk plays a key role in choosing the type of security controls the organization should employ.
- **Current (and future) mobile use cases** – Organizations should take into consideration the types of data and functionality that are exposed through the deployment. For instance, a retail deployment that allows credit card processing on personal devices would require PCI-DSS compliance on the devices – which includes stronger and more rigorous controls than on non-PCI devices. There is no "one size fits all" use case.
- **The geographic deployment of the devices** – International deployments increase risk levels not only because of the geographic distribution of the devices, but also as a function of unclear and regionally applicable legislation in certain geographic areas. Areas with rigorous privacy legislation such as the EU and Brazil also affect the legal workload and nature of the security controls needed to stay compliant.

Considering these factors at an early stage in the BYOD planning process is key for a secure and successful rollout.

Challenges or barriers facing BYOD deployment



The top concerns for BYOD are related to security.

While there are various costs incurred on BYOD, they are not seen as major barriers for deployment.

Source: Forrester, *Key strategies to capture and measure the value of consumerization of IT*, July 2012

Defining the BYOD risk

As BYOD introduces risk to the organization, a holistic and methodical approach should be used to define this risk and help to ensure that controls exist to maintain both the security and usability of the devices in the enterprise.

Defining the BYOD risk

With the issues of risk profile, usage and geography to consider, an organization can begin to define the BYOD risks and what impact they would have. What is often found is that the risks generally remain the same. The risk introduced by BYOD tends to be an expansion of the current risk landscape — rather than introducing completely new risks, it has the potential to amplify and increase certain risk.

Here, we have divided the risk landscape into three areas:

1 Securing mobile devices

2 Addressing app risk

3 Managing the mobile environment

1 Securing mobile devices

In the former single-phone corporate environment, mobile devices were relatively straightforward to manage and secure as they consisted of a uniform distribution of device types, often from a single manufacturer or brand, that had limited or no access to corporate data. This allowed the organization to consistently apply security policy controls, often through a unified management interface supplied by the manufacturer. BYOD fundamentally changes this architecture as users bring in their own devices of various makes and models. These devices are often designed to exist in their own "walled gardens" with little seamless interaction with an enterprise environment and management utilities.

Security risk expansion happens both on the basis of a more diverse device portfolio, and as a function of the number of devices. As a BYOD deployment invariably will include a wider range of device types, the same security controls that before were applied to a singular device type now have to be applied to a multitude of hardware and operating system combinations, often with differing levels of effectiveness. In addition, end users often have more than one device and would like to connect multiple devices to the organization's infrastructure, which increases the net number of devices that must be secured.

As a result, basic security controls may not be consistently and effectively implemented across the collection of devices. This may occur even when a functional mobile device management (MDM) product is in place, as operating system or app-specific vulnerabilities may be able to circumvent existing controls on the device.

For organizations, the principal goal of technology is to drive and deliver business value. While locking down mobile devices and prohibiting the use of personal devices may mitigate some security risks, policies that are too restrictive will drive down adoption or encourage workarounds. In time, they may also drive employees to use unsafe alternatives to obtain the flexibility and access they have already experienced and now expect. In these instances, neither the policy nor the program will be sustainable.

When it comes to mobile devices, well-developed programs should be based on an understanding of different user types and a clearly defined set of user segments. For example, international organizations should consider the impact of regional device availability, usage habits and cellular network provider capabilities and data plan costs. A clearly articulated set of usage cases should drive the development of experience, as a poor user experience will lead to fast failure. Ultimately, understanding your users and how the technology and product offerings can enable their daily tasks will drive user satisfaction.

Familiarity and awareness of these challenges will help organizations and their employees understand the critical areas which can help secure their mobile devices, thereby promoting enhanced information security. Risks relating to securing mobile devices are categorized into five basic concerns:

- Lost and stolen devices
- Physical access
- The role of end user device ownership
- Always on with increased data access
- Lack of awareness

Lost and stolen devices

Millions of cell phones and smartphones are lost or stolen every year. It is thought that approximately 22% of the total number of mobile devices produced will be lost or stolen during their lifetime, and over 50% of these will never be recovered. Most devices are stolen for the value of the hardware on the second-hand market; however, a growing amount of lost and stolen phones have their content accessed by someone other than their owners. This highlights the importance of basic security features such as password protection, encryption and robust procedures to wipe the device once lost.

Physical access

The high number of stolen and lost devices also means that attackers may have physical access to the actual device hardware. This is a different threat model than for stationary hardware such as servers and workstations, where physical access is less likely. It is much harder to properly secure a device once an attacker has gained physical access.

Consequently, the hardware, operating system and apps all affect the total security state of the device, and this risk increases when employees bring potentially old or insecure devices into the organization. For instance, iPhone models manufactured before the 3GS lack hardware encryption, offering far less effective data protection than newer iPhones. In a BYOD scenario, this risk is accentuated, as organizations that fail to set minimum supported device requirements for personal devices are likely to have more insecure devices accessing the organization's data

The role of end user device ownership

There are two distinct scenarios: employees in the US are expected to supply their own devices to work on, making it difficult to separate work and personal data and apps; in Europe, employees are normally provided with company-owned devices, but will still often use these in their personal life, or want to use their personally-owned devices to work on projects out of the office.

The fact is that whatever the scenario — employees are going to use their own devices in the work environment — this can't be stopped, and it will continue to grow. Employers should accept the situation, manage the risks and welcome their use.

In the US, end users feel an increased sense of ownership of the devices they use at work, and would like to retain as much control as possible. This often includes a sense of entitlement to unlock, "root" or "jailbreak" the operating system of the device, and thereby removing many of the operating system's security features and introducing security vulnerabilities. The sense of ownership may also cause the user to be less inclined to immediately notify the organization of device loss.

Always on with increased data access

One of the greatest advantages of a mobile-enabled workforce — the employee's ability to always be connected — unfortunately also expands risk. While employees previously left their data at work, they are now traveling the world with access to corporate data anywhere, anytime. A lost or stolen smartphone will now potentially compromise both business data located on the phone and corporate data access channels such as VPN connections where further data loss may occur. In addition, this new connectivity also makes it possible to link security bugs in the personal apps (social media, blogs, etc.) to gain corporate access.

Lack of awareness

Lack of user security awareness is the primary contributor to several of the above risks being realized in the organization. Maintaining awareness and good support procedures for handling device loss is critical to the security of the data on the devices.

The risk of the device itself should be assessed as a part of the company's risk assessment framework. In some organizations a tiered device architecture may be viable to deal with varying degrees of risks tied to job functions. For instance, devices that are being used to present sensitive financial data to the board through a custom app will invariably be more sensitive to theft or accidental loss than a mobile device with access to calendar and email updates.

Considerations for mobile device security

How to secure your employees' devices

1. **Evaluate device usage scenarios** and investigate leading practices to mitigate each risk scenario.
2. **Invest in a mobile device management (MDM) solution** to enforce policies and monitor usage and access.
3. **Enforce industry standard security policies as a minimum:** whole-device encryption, PIN code, failed login attempt actions, remotely wiping, etc.
4. **Set a security baseline:** certify hardware/operating systems for enterprise use using this baseline.
5. **Differentiate trusted and untrusted devise access:** layer infrastructure accordingly.
6. **Introduce more stringent authentication and access controls** for critical business apps.
7. **Add mobile device risk** to the organization's awareness program.

2 Addressing app risk

Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games – apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of supporting BYOD devices in a corporate environment.

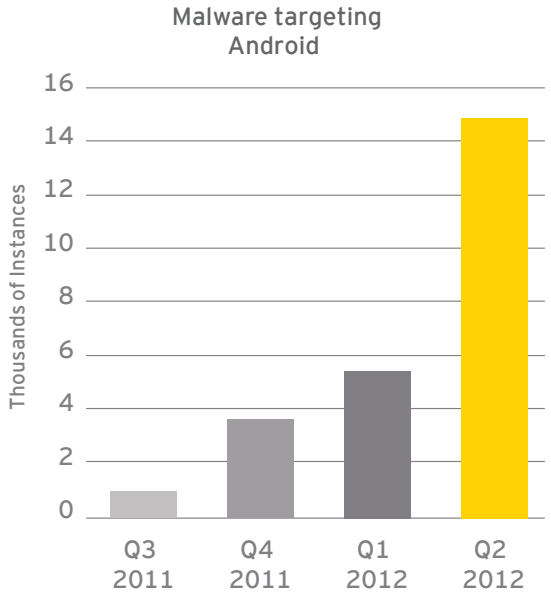
As the organization enables employees to bring their own, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- **Malicious apps (malware):** the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes
- **App vulnerabilities:** apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses

Malicious apps (malware)

Mobile malware are apps with code embedded within them that compromise the security of the device or related data. They can take the form of legitimate apps that have been modified to include malicious code, or code that runs when a user views a compromised site, or code introduced from a data interface separate from the internet (local file sharing, Bluetooth, NFC, etc.).

Mobile malware is quickly going mainstream



Currently, the most common types of malware on mobile devices are versions of pay software that have been "released for free" on illegitimate app stores. These free versions of paid apps have codes imbedded within them that allow premium SMS messaging, or export sensitive data.

At the time of writing, mobile malware is significantly more prevalent on the Android platform: according to Kaspersky,[1] 98% of identified mobile malware target the Android platform, and the number of variants of malware for Androids grew 163% in 2012 compared with 2011. This highlights the need for malware protection and control over personal devices running versions of the Android operating system and the concerns of older technology and non-uniformed platforms. As this is the most common operating system, it is likely that this is a problem that will have to be addressed by every organization that allows multiple devices in their BYOD deployment.

App vulnerabilities

App vulnerabilities and weaknesses consist of issues within custom or commercial software that may unintentionally expose the data within the app, or otherwise assist attackers in compromising the device.

Mobile app vulnerabilities are similar to traditional PC and web app vulnerabilities, but with a greater emphasis on the protection of locally stored data on the device. The impact of these vulnerabilities could impact the end user's device security, the corporate data within the app, or even the corporate infrastructure.

The risk of app vulnerabilities is accentuated when devices are not owned and managed by the IT department, as this model forgoes remote administrative capabilities and the associated control. To counter this risk, app management or compartmentalization of sensitive data and tasks is recommended.

While the threat landscape outlined above is not a set of completely new concepts to most IT organizations, nor is it exhaustive in nature, the BYOD model enhances many of these risks.

First, with less control over the devices and a greater sense of ownership by the employees, and the innate nature of users to search the web on these devices, organizations will be facing a greater number of personal apps on their employees' mobile devices than in a non-BYOD environment. As the line between personal and corporate usage blurs, both on the device and in the employee's mind, non-sanctioned apps designed for consumers will more frequently be used to hold, view, edit and exchange corporate data.

Second, the expansion of mobile device risk surface also applies here. As a more diverse portfolio of devices are supported by the organization, the risk that mobile malware is able to compromise a device increases due to the diverse attack surface.

Third, the organization's IT function will have an increasingly daunting task in monitoring and applying software updates intended to plug security holes.

[1] "Android Under Attack: Malware Levels for Google's OS Rise Threefold in Q2 2012," Kaspersky, 10 August 2012

With the increasingly powerful consumerization of their working world, employees will feel greater entitlement to control every aspect of their device and their experience using it. Employers should assume that if their workforce's functional needs aren't met, or are restricted by IT policy, employees will find ways to circumvent these controls to enable them to perform work more effectively and efficiently on the new devices and take advantage of their technical capabilities. The mechanisms of bypassing technical policies could weaken the overall security of the device or may represent a breach of security themselves.

Considerations for mobile device security

Ways to counter app risk

1. **Use mobile anti-virus programs** to protect company-issued and BYOD malware-prone mobile operating systems with mobile anti-virus.
2. **Ensure security processes cover mobile app development** and leverage tools, and vendors to bridge assessment skill gaps.
3. **Manage apps** through an in-house app store and a mobile app management product.
4. **Introduce services that enable data sharing** between BYOD devices.
5. To increase productivity and security, **continually assess the need for new apps**.

3 Managing the mobile environment

BYOD increases the organization's management effort, both for maintaining an accurate inventory of the mobile devices, keeping mobile operating systems' software up-to-date and supporting the increasing number of device types.

Device evolution and turnover is two to three years in the consumer mobile space, versus the usual four- to six-year hardware cycle in traditional PC asset inventory. Due to the accelerated device turnover and high rate of new user adoption, organizations often struggle with maintaining an accurate inventory of enrolled mobile devices. Additionally, within the hardware life cycle, there are often multiple upgrades to the operating system, which can be customized by individual cellular carriers at their own discretion and pace, and initiated by the end users. While not a direct security risk, unmanaged devices form a hidden security problem as they may lack corporate security controls and patch management.

BYOD increases inventory and platform management risks

A BYOD environment will have significantly more variability in the hardware and software versions of devices holding corporate data and providing employee access. This will further decrease the ability of MDMs to manage and consistently apply technical security policies to the endpoints. This variation in platforms will also complicate device wiping when the phones are replaced, resold or upgraded by employees, or when they change carriers.

Where does this variability come from? Unlike PC operating system (OS) updates, mobile operating system updates often need to go through layers of validation and customization before being applied to a consumer device. In the instance of Android hardware, updates to the OS are reviewed at three different levels before you can install them. Hardware manufacturers ensure that the update doesn't impact their hardware functionality; OEM vendors use software customization to verify that the update doesn't impact the user experience; and local cellular carriers often hold back on updates until they are sure that connectivity to the cellular towers are not impacted by the update. After all of these levels of review, the updates are finally made available to end users, though often installation is optional and the availability of the updates is not obvious.

There are also significant hidden costs associated with a BYOD program: the vast majority being unrelated to hardware, highlighting the importance of choosing the right governance and support models to control these costs prior to implementation. Many of these costs are tied to support – there is often a discrepancy between the support levels provided by the organization and the employee's expectations. This also is a potential security issue – as employees rely upon a company-provided support function that is not prepared to answer an influx of device-related questions, employees turn to workarounds and the internet for answers. Streamlining enrollment and deprovisioning support procedures are therefore key to a secure BYOD deployment; for example, success in establishing moderated employee self-service forums for employee devices has been proven effective.

Another hidden cost is related to reimbursement of data plans – organizations see a significant spike in data usage, especially when rolling out tablets. Setting tiered data caps and providing secure and cheap connectivity options for mobile workers are effective means to control this cost. This is especially important for global firms with employees that frequently travel internationally.

Considerations for mobile device security

Managing support for BYOD devices

1. **Create and enforce** an appropriate BYOD support and usage policy.
2. **Revamp existing support processes** to include secure provisioning and deprovisioning (wipe) of devices, and an increased level of self-help.
3. **Create a patch education process** to encourage users to update their mobile devices.
4. **Introduce a social support mechanism** to augment the existing IT support team.
5. **Implement** a wiki/knowledge base employee self-service support solution.

Hidden service costs of BYOD

User device control	User device control means that IT departments may lose a layer of control that they have with corporate-liable devices
Users' expectations relating to the support of BYOD	Managing users' expectations relating to the support of BYOD will reduce the new support calls relating to incidents that service desks are unable to manage
Costs associated with request fulfillment	Identify the potential costs associated with request fulfillment following requests for paid applications to aid productivity to the service desk
Additional training of service desk staff	Additional training will ensure that the service desk staff are kept up to date as device operating systems are updated

Advances in mobile device security features

By adopting strategies that are flexible and scalable and taking advantage of new and upcoming security features, organizations will be better-equipped to deal with incoming – and even sometimes unforeseen – challenges to their security infrastructure posed by the use of employees' own devices.

Multiple logins and compartmentalization

Some of the large mobile device developers are developing the native ability to have work and personal environments that are sandboxed and securely separated from each other. This feature is a response to users carrying a work and personal smartphone at the same time; it allows the end user to use the device as they desire, as well as allowing an enterprise to manage the work environment to the degree that they see fit.

App virtualization and sandboxing

Virtualized environment providers are continuing to develop their offerings to customize access and experience based on identity while creating seamless integration of app environments across platforms. Some full featured apps on the traditional desktop are not usable within a mobile environment and a hosted cloud version of the apps may make more sense than trying to replicate the in-office experience on a phone or tablet.

Overall the mobile OS sandboxing model will continue to become more prevalent on the desktop. We expect this trend to continue for mobile apps in addition to more focused purpose-built security solutions for mobile platforms.

BYOD endpoint security

More traditional endpoint security products will continue to offer more management and monitoring services through their administrative consoles and policy managers. Certain providers are developing new solutions around anti-malware solutions for virtual machines, virtual desktops and the data center: this capability will be more important as apps become more sandboxed and virtualized on both traditional desktop computing environment and on BYOD devices. Security program vendors are focusing on deploying endpoint anti-malware capabilities for mobile operating systems and integrating it into their MDM platform, allowing enterprises to have dashboard monitoring capabilities for mobile malware.

Addressing governance and compliance issues

As the usage scenarios of mobile devices evolve and mature, guidance around what an organization needs to do to remain compliant is often inconsistent. Additional compliance complexity is introduced in a BYOD environment when employees own the device and use it for personal data.

Handling regulatory risk

1. Talk to legal and HR in the respective countries where BYOD devices are to be supported in order to understand local privacy and data security laws.
2. Create tiered policies per geographical segment that expand on the general BYOD policy.
3. Ensure your policy addresses the risk areas outlined in this whitepaper.
4. Ensure that local IT has the right processes in place to support the policy.
5. Review, monitor and revise policies regularly.
6. Segment business environments and data from personal employee data as much as possible.
7. Create a policy structure that is a streamlined governance workflow to address emerging risk areas, making the policy approval process faster and more agile.

Addressing governance and compliance issues

Using a personal device for work will implicate employee labor law protections in Europe and other data privacy-focused regions, and a range of legal and regulatory risks will be amplified when deploying a BYOD program.

Privacy governance

Increasing privacy legislation is a trend that likely will increase in the near future. As organizations design BYOD security controls, these may interfere with personal expectations of privacy. In order to stay ahead of this concern, organizations are currently addressing privacy concerns in a BYOD policy.

A well-formed BYOD policy should include defined, clear expectations on privacy-impacting procedures. In certain geographical regions, organizations may also be forced to provide employees with a non-BYOD alternative, potentially decreasing the savings potential of the overall BYOD program.

In Europe, for example, it is more common that the employer provides the hardware on which work is performed, prompted largely by the inability to force employees to have their own cell phone: this results in either a hybrid BYOD program where you have both privately and organizationally owned devices, or programs that include provisions for device purchase. Whereas regulations in the US give organizations the right to monitor and wipe the users' device: it is critical that the organization assesses the risk around this practice, establishes a policy and informs the users about the privacy implications of using their own device.

Data protection

In a BYOD deployment, data protection does not only apply to corporate data. EU regulations that govern processing of personal data in a BYOD scenario will apply, and if the organization is collecting personal data from an employee's device, the purpose, expiration, security, etc., of the data collected must be clearly stated in the BYOD policy. The organization also must undertake a risk assessment of the risks associated with the processing.

If data is processed by a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.

Right to be forgotten and erasure

It is increasingly more common for privacy regulation to include provisions for the employee's right to be forgotten — to have a person's personal data erased when leaving the organization — therefore, organizations operating in countries where such legislation exists should assess the impact to the organization and create formalized support procedures to handle such requests. These companies should consider leveraging these processes to also encompass BYOD-enrolled employees.

Monitoring (privacy at work)

There is a wider variety of laws and requirements around monitoring, wiping and data protection in Europe and certain other countries. For instance, EU privacy regulations dictate that monitoring should be restrained to use of the device within the time the employee is at work. Global, organization-wide monitoring may also be restricted, as EU prohibits export of personal data to non-EEA countries.

Labor laws vary by country and restrict an organization from viewing personal employee information. This may limit a company's ability to monitor and control the content delivered to mobile devices for security purposes.

These monitoring requirements are further complicated when, for instance, an employee hands their device to a child to watch a movie. In order to avoid these privacy pitfalls of monitoring controls, a product should be selected that allows for the ability for monitoring to occur exclusively around work-related mobile activities.

Breach investigation and notification

As digital investigations on personal devices in the wake of breaches may be regarded as a privacy invasion, it is important for the organization to retain the right to examine employee devices when an incident occurs. If no such right is reserved in the agreed-upon BYOD usage policy, the organization may face legal challenges and delays when investigation of data on personal devices is needed.

The current trend for new and future legislation is beginning to address data breach notification, with exceptions around notification if certain data protection criteria are met. The organization should prepare for these legislations by keeping an active inventory of the devices, the data on them, and the security controls in place to protect that data.

Data ownership and recovery

"Ownership" should be a key dimension that guides policy settings. As a result, personal and corporate devices will each have different sets of policies for security, privacy and app distribution. The shift from corporate laptop to personal devices has repercussions for data recovery when a device is damaged or lost/stolen.

To mitigate unclear responsibilities for data recovery in a BYOD scenario, the organization should have a clear policy stating who owns what data, and whose responsibility it is to maintain backups of data, corporate as well as private. The policy should also cover liability of loss, state whose responsibility it is to retain data recovery when it is needed, and the privacy implications of such recovery operations.

Conclusion

By leveraging industry leading practices, integrating a thoughtful BYOD policy and adopting strategies that are flexible and scalable, organizations will be better equipped to deal with incoming (sometimes unforeseen) challenges to their security infrastructure posed by the use of employees' own devices.

The introduction of appropriate procedures and regular testing will help organizations become smarter and make their employees more aware of the challenges that the use of personal devices pose for the entire enterprise.

Eight steps to secure and improve your BYOD program

Here are steps organizations can consider to help grow confidence among employees and provide reassurance to stakeholders that information security won't be needlessly imperiled by the use of employees' devices.

1 **Create a strategy for BYOD with a business case and a goal statement**
As technology continues to advance and change the way we live and work, building a smart, flexible mobile strategy will allow companies to explore innovative ways to empower their workforce and drive greater productivity.

2 **Involve stakeholders early through the formation of a mobility group**
A cross-business mobility group will help to vet the needs of the business. The group could consist of executives, HR, legal, support, IT and potentially representatives for key user groups. An effective way of generating powerful usage cases is to model day-in-the-life scenarios that envision how mobility will ease the everyday work situation of key employee groups. Establishing key success factors will help the group to measure the success of the implementation and mold it moving forward.

3 **Create a support and operations model**
Using the scenarios formed by the mobility group, identifying and quantifying costs and benefits, will help build the overall business case for BYOD. Ensure that hidden costs such as increased data bills and support expansion are considered, together with potential advantages such as increased recruiting success rates with younger demographics.

4 **Analyze the risk**
By utilizing the usage cases, you should assess the data stored and processed in the devices, as well as the access granted for the devices to corporate resources and apps. Paying special attention to scenarios that are more likely for mobile devices, such as a lost or stolen device, will help focus the effort. Incorporate geographically relevant data and privacy laws, and consider the impact of the mobile workforce traveling to countries with data import/export restrictions.

5 **Create a BYOD policy**
Creating a flexible but enforceable policy is key to ensuring that it effectively limits risk to the organization. The BYOD policy should complement other information security and governance policies, and should provide the following to the user:
a) General security requirements for mobile devices
b) Authentication (passcode/PIN) requirements
c) Storage/transmission encryption requirements
d) Requirements to automatically wipe devices after a number of failed login attempts
e) Usage restrictions for mobile devices
f) Company liability
g) Rights to monitor, manage and wipe
h) Support model
i) Leading practices for mobile data usage on international travel
j) Acceptable use (if different from the normal acceptable use policy)

6 **Secure devices and apps**
Implementing an MDM solution, or other container-focused management utilities, will greatly help the organization in managing and securing the devices. The policies on the devices or within managed containers should be defined by the risk assessment.

7 **Test and verify the security of the implementation**
Perform security testing and review of the implemented solution. Assessments should be performed using an integrated testing approach combining automated tools and manual penetration testing, and preferably utilizing a trusted third party that has a proven track record assessing mobile deployments. We would recommend assessing the implementation as a whole and test devices, apps and the management solution together. In addition, it is important to test the infrastructural changes that are performed to allow mobile devices to connect to the enterprise network, such as Wi-Fi deployments or VPN endpoints.

8 **Measure success, ROI and roll-forward lessons learned**
Measure key performance indicators of the BYOD program, and use this as means to continually improve the program. Use direct user feedback extensively to identify areas for improvement.

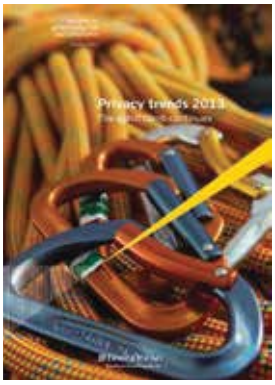
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our *Insights on governance, risk and compliance* series at ey.com/GRCinsights

Fighting to close the gap: EY's 2012 Global Information Security Survey
ey.com/giss2012

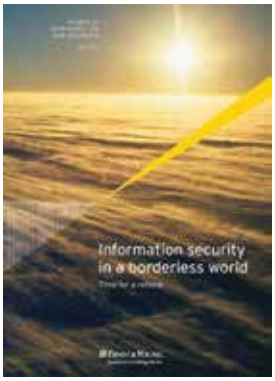
Identity and access management: beyond compliance
ey.com/IAM



Privacy trends 2013: the uphill climb continues
ey.com/PrivacyTrends

Mobile device security: understanding vulnerabilities and managing risk
ey.com/MobileDeviceSecurity

Protecting and strengthening your brand: social media governance and strategy
ey.com/ProtectingBrand



Information security in a borderless world: time for a rethink
ey.com/infosec_borderless

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. AU1850
ED none

ey.com/GRCinsights

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our IT Risk Advisory services could help your organization, speak to your local EY professional, or a member of our team.

Contact details of our leaders

Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Areas		
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Shohei Harada	+81 3 3503 1100	harada-shh@shinnihon.or.jp