IS CLOUD STORAGE TOO FLUFFY FOR YOUR MOBILE DEVICE?

Joe Sturonas, CTO van PKWARE, schrijft over de risico's van informative in de cloud. Dit keer beschouwt hij de BYOD-trend, waarin hij stelt dat het niet "jouw" apparaat is, maar "ons" apparaat, dat device management niet gelijk staat aan beveiliging van deze apparaten en dat gebruik van de cloud door deze apparaten niet uit te sluiten is. Daarom sluit hij af met twee belangrijke vragen die we onszelf horen te stellen.

By Joe Sturonas, Chief Technology Officer for PKWARE. PKWARE offers software solutions to critical IT problems, namely the explosive growth of data, the need to secure data, and the emergence of data in the cloud. He can be reached at Joe.Sturonas@pkware.com.

With the proliferation of mobile devices, companies are increasingly adopting "Bring Your Own Device" (BYOD) policies – whereby employees use their personal phones and tablets to access corporate applications and data. Gartner has projected that by 2014, ninety percent of organizations will support corporate applications on personal devices. This raises significant security challenges for enterprise IT departments on how to secure and protect corporate data on a wide range of mobile devices.

Knowledge workers in an enterprise are notorious for finding the path of least resistance in order to be productive, much like a river finds the path of least resistance in a valley. The river will find its way around a large boulder until it erodes the boulder to gravel. Today, knowledge workers use mobile devices to fuel efficiency like never before. And in an ironic twist, smart phones and tablets have become the network computers that IT organizations have been trying to propagate for years.

More and more, employees are bringing their personal technology devices into the workplace to access company information. As a result, companies are challenged to enable collaborative access to sensitive information while ensuring data security and privacy. The trend significantly blurs the line between enterprise and personal computing, and further complicates the job of governance, risk and compliance management. Left unbridled, this practice can lead to a significant loss of sensitive information.

> The river will erode a large boulder to gravel

In many organizations, there has been a tremendous focus on security technologies, such as *Data Loss Prevention (DLP),* with which organizations attempt to detect sensitive data at rest and in motion within the fortified borders of the enterprise network. Frequently, and quite often in parallel, knowledge workers are moving data to their BYOD smart phones and tablets, bypassing the MIS/IT policy and procedures completely. Picture your data management guru repairing a leak in the middle of a dam, while at the same time, water cascades by the gallons over the top of his/her head.

The not so hidden costs

Yes, at face value it seems like an excellent deal…*employee purchases wireless device, not us*. But, not so fast, there's a host of security and compliance costs associated with mobile BYOD. Typically, BYOD brings the iOS® iPhone® and iPad®, BlackBerry®, and Android™ tablets together into one shop. Now CIOs have to invest in a multi-platform mobile device management solution as well as other software, and possibly a virtual private network (VPN) layer.

And, while most mobile devices have some type of management tool to help

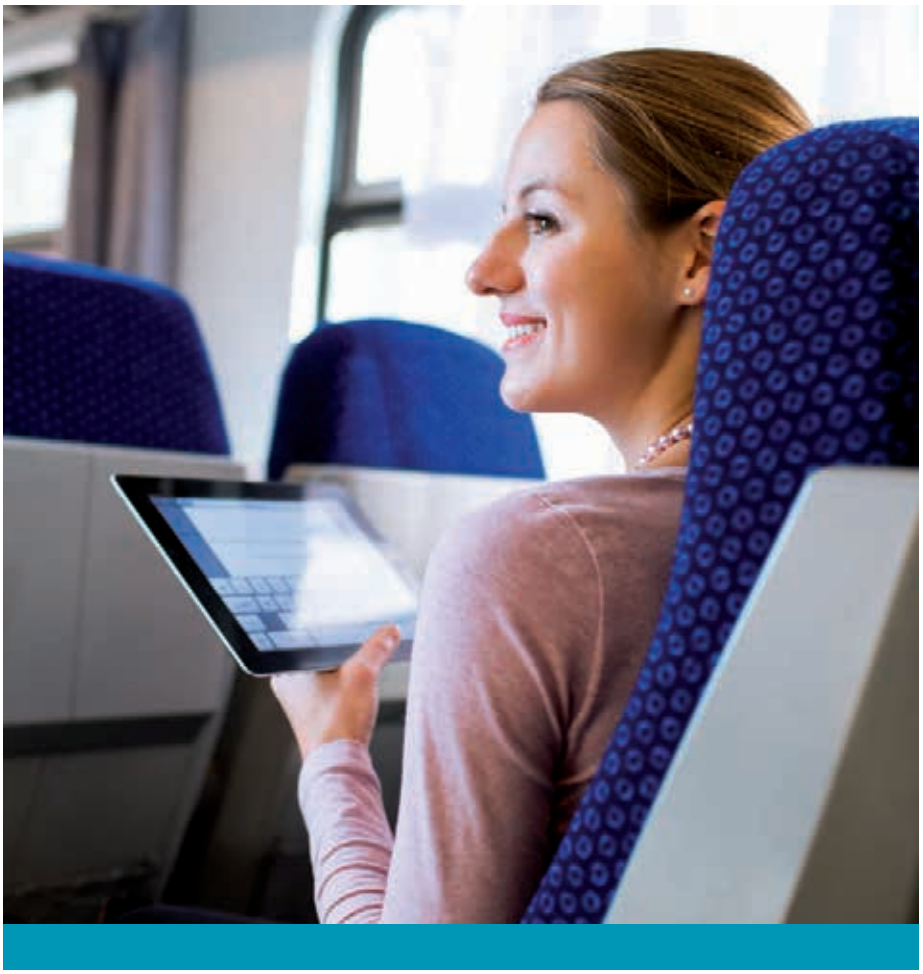
locate a lost phone, perform a remote lock or wipe, or even change the pass code remotely, the tools may not meet your enterprise standards. What's more, you can't force fit an Android phone into a BlackBerry Enterprise Server paradigm.

Aberdeen analyst Hyoun Park adds, "The cost of compliance - ensuring governance, risk management and compliance - is also more difficult when devices must be chased down individually." It's quite different for an organization to inventory and set-up a hundred devices from a hundred directions than a bulk upload of machines from one vendor.

Avanade, a business technology services firm, surveyed more than 600 IT decision makers late last year and discovered that more than 50% of the companies reported experiencing a security breach as a result of consumer devices.

According to Jim Reavis, executive director of the Cloud Security Alliance, "The challenge for administrators is to provide business data to end user devices while keeping that data separated, segmented and managed."

Time to sharpen your pencil when examining the overall cost savings of employee owned devices, don't forget to factor in additional management time, increased risks for a breach and the need for policy enforcement.



Consider theses sceneries to see how companies quickly turn "your" into "our" device.

A Closer Look- taking the "Y" out of your

The BYOD culture can create very interesting situations. For example, when an employee purchases a device, it is thought of as *their own* device. But in reality, if they really want to increase their own productivity, they will want access to company resources via the device requiring a connection to enterprise data network devices.

Before the employee has permission rights to connect the BYOD to the company network, the employee may need to agree that the BYOD be managed by policy. Such policy often includes mandatory password protected screen timeout, data encryption, and the ability to wipe the device if it is lost or stolen. The policy granularity can go very deep and may actually encroach on personal data. So at this point, is it really still the employee's device?

50% of companies experienced a security breach because of BYOD

Recent headlines spotlight a very large international company that allowed BYOD, but prohibited the use of voice recognition command software.

The rationale cited a remote server that translates the spoken queries into text, a process not done locally on the phone. Fears loomed around the potential for data leakage if the voice recognition was used for sensitive data and the phone provider (aka the third party systems) did not treat it as such. A natural language interface is often viewed as a very useful feature of a smart phone. And it could easily be deprecated by the policy administrator, thus becoming a cost of policy enforcement in order to access enterprise data. Is this still the employee's device?

If an employee agrees to use a device for company business, they might need to call on a corporate IT person for assistance or support. More likely than not, that IT person will have some access rights to the personal information, if even temporarily. A company may also set forth certain rights to "snoop"

A company may "snoop" your device

on the device, requiring random access and possible review of private files, e-mails, web history, even passwords. Now, is it the employee's device?

Lastly, pretend the BYOD device has been found to be out of compliance with agreed upon security standards. As a result the device is quarantined, and access to corporate networks shutdown, a virtual lockout of everything, even family phone numbers, needed by the employee. Now, is it the employee's device?

Device management ≠ data security

Regardless if the BYOD culture gets the traction many expect, it is still a force that requires attention. A recent survey by Gartner suggests global companies have BYOD on their radar. The 2011 survey results found CIOs believe 38 percent of laptops, tablets and mobile phones will be employee-owned in the US and 20 percent in the UK in two years. The survey also showed BYOD demand was highest in countries where Gen Y employees make up more of the workforce.

With all the buzz around Mobile Device Management (MDM), it might be tempting to believe your data will be locked down with use of these tools. Not always the case. Determining efficiencies and creating management dashboards to control a sea of smart phones does not equate to data security. Instituting a policy that wipes a device clean if lost might be just a few seconds too late at the hands of a professional hacker.

> The content consuming devices need the content producing devices

Perhaps there is comfort in knowing the MDM strategy articulates the acceptable apps employees can access. Think again. Even the best efforts will fall short trying to control the plethora of employee owned devices and enforcing policy. For example, the Android Malware Genome Project hopes to improve the efficiency of mobile malware detection-- claiming mobile security software can miss as much as 80% of malware with the best apps letting approximately 20% slip by today.

Those challenges may quickly pale in significance when you consider the dangerous combination of employee owned devices accessing corporate information connected to third party cloud services and using cloud storage.

100% Chance of cloud cover

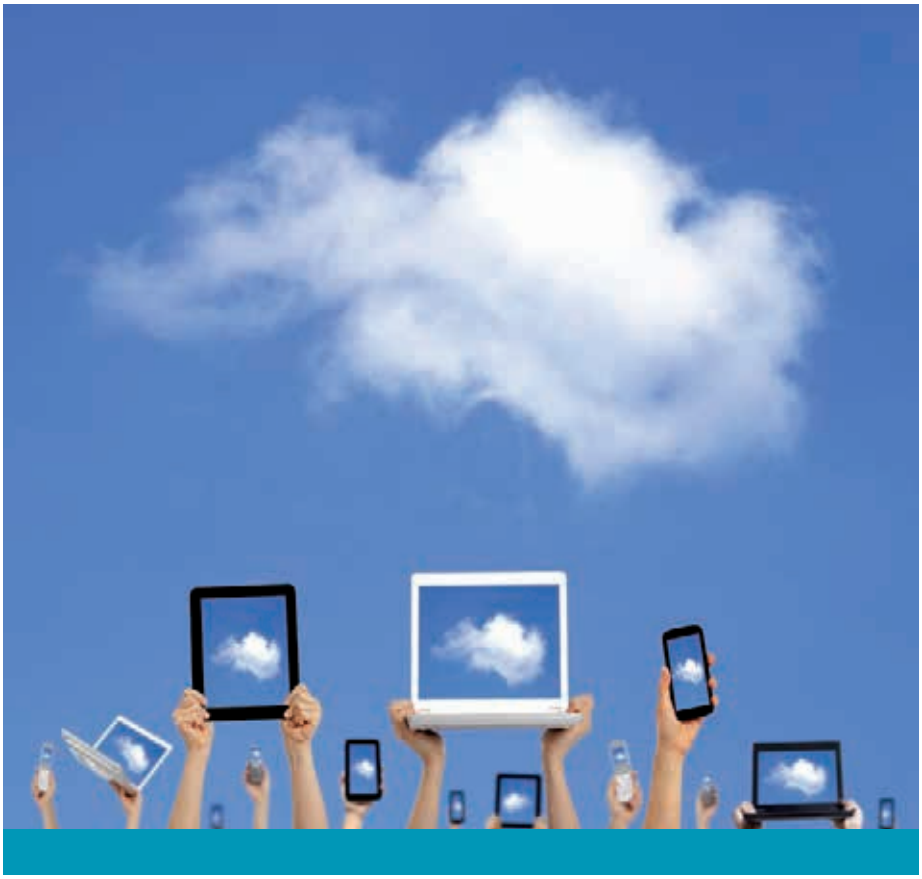
Why is cloud so closely related to mobile? Mobile devices are for the most part, content consumption devices where content (emails, documents, books, articles, etc) is mostly consumed (read) on these devices. The content producing devices-- such as desktops and laptops-- need to be available to the content consuming devices.

> Data has to actually get to the cloud

The very productivity potential of the mobile device requires automatic content delivery, not premeditated, through cloud storage services that synchronize data from each device and the cloud. Consider this result:

An employee works on a desktop to prepare a presentation needed for the next day. That evening, he wants to go over the presentation one last time. He takes out his smart phone, downloads the latest presentation from the cloud storage where it was last updated from the desktop, and reviews the presentation. The next day when he arrives at the office, he goes into the conference room with his tablet, accesses the latest file, connects to a projector and presents to his peers.

While cloud storage synchronization might sound like a very intimate activity with very little security exposure, the reality is that unless the data is encrypted, the data could be very exposed.



And, depending on the cloud storage service that is being used, it might actually be public. Exactly the case when a 2011 software update mishap yielded a four hour security breach, temporarily allowing any password to access any user account in the vendor's cloud storage system.

Because mobile devices are mainly content consumption devices they don't have the same resources in terms of memory. What's more, almost all mobile data plans are capped in terms of the amount of data that can be transferred in a month. This means the majority of data must reside in the cloud which allows the user to pick and choose the data they need on the mobile device, conserving the memory and bandwidth.

Cloud concerns

Data is often comingled on shared servers and exposed to users you don't know. If your Cloud storage provider encrypts your data but holds the key, anyone working for that Cloud storage provider can gain access to your data. Cloud providers have root access to all your unencrypted data in the cloud, and they are not your employees.

Data also has to actually "get to" the cloud, which usually means leaving your trusted infrastructure and overcoming compounded transfer vulnerabilities as data moves to and from the cloud.

Contactless transactions

More data vulnerabilities are present with Near Field Communications (NFC) and Bluetooth Low Energy, both short-range communication technologies which are integrated into mobile phones. Cleverly coined a "virtual wallet", retailers are looking to capitalize on this opportunity to personalize the consumer experience. Although the transmission range is fairly short, such as waiving your phone over a NFC capable device for a coupon or payment, worries are still justified about personal information stored in NFC tags.

This wireless exchange of data between a reader (a phone) and a target (a microchip embedded in an object) is essentially a subset of radio frequency identification (RFID). Man-in-the-middle attacks are at the forefront of concern, where a participant in one transaction drops some form of malware onto the phone, subsequently infecting other phones that the original interacts with later. And the bottom line…any broadcasted data can be intercepted, period.

Key ideas

Using Public/Private key pairs (X.509 digital certificates and/or PGP key pairs) can greatly increase the ease of use for regular crypto use. Using Public/Private key pairs eliminates the need to have to manage a dozen or more passwords in order to decrypt information.

> The cost and complexity of implementing secure data exchange can get overwhelming

With Public/Private key pairs used for encryption/decryption operations, the public key is used for encryption. Public keys are intended to be public and can exist in local key stores or in LDAP directories where they can be searched and used for encryption operations.

The use of Private keys for mobile devices is a bit more delicate. For certain, concern arises that if the private key must exist on the mobile device itself, that the mobile device be sufficiently protected so that the private key could not be exposed if the mobile device were lost or stolen. Best practices to ease anxieties include policy around timeouts and screen locks that require authentication in order to protect the private key on a mobile device.

In contrast, mobile interaction does not always require the private key to reside on the device for decryption operations. For example, where attachment

processing is managed by a server it is only necessary for the private key to exist on the server, which is essentially out of control of the owner of the private key. This can have some serious security implications depending on the nature of the data and the applications that are securing the data.

Think outside the device-- data-centric not device-centric

A device-centric strategy is a costly infrastructure to keep up and almost destined for failure. There's no dispute, organizations are confronted with increasing amounts of sensitive data and ever changing compliance statutes. Simple encryption solutions, in a complex world of mobile devices won't get the job done. Faced with a wide variety of computing platforms and operating systems, the cost and complexity of implementing secure data exchange can get overwhelming. Damaging costs due to a breach could essentially cripple an organization.

Think outside the device for a more realistic strategy and protect data at its native-use level. The only way to protect data in the cloud is if you encrypt the data before it leaves and you maintain control of the private key.

This approach ensures that virtually any type of sensitive data kept in file, folder, or email format is protected while the data is in transit or at rest.

A data-centric security strategy helps organizations address their daily data security challenges, including protecting sensitive data and meeting compliance requirements. When used in conjunction with a compression tool, less bandwidth is required for transmissions and less storage space is required in the cloud. This helps companies reduce overall costs and operational overhead.

The regulatory standards issues that you deal with today in your own data center are just as important in the Cloud. Compliance with PCI DSS, EU Privacy Act, Sarbanes-Oxley, and FIPS140-2, etc. are just as imperative. If you know that the data is encrypted before it goes into the Cloud, you may be compliant with any number of these regulations. Even if the Cloud vendor is hacked or someone uses an administrative password improperly, your data is still impregnable at that location. A breach? No worries, really. You can prove your data is protected.

Important questions

Since the productive use of mobile devices requires spontaneous access to data that must reside in the cloud, then ask yourself a couple important questions:

1. Do you trust your cloud provider?
2. Do regulations on certain data allow you to trust your cloud provider?

If you answered "no" or even "maybe" or hesitated, it's time to encrypt the sensitive data. Then, you don't need to trust your cloud provider.

Data-centric security, allows you to decrypt the data on your mobile device when you need to consume the information, and leave it encrypted otherwise. As "data-centric" becomes the standard for information security, it eases concerns over the platform, the device, the transmission for moving and storing that data.

Reversing BYOD is not an option

Bill Bodin, IBM® chief technology officer for mobility, summarized that whatever the challenges of supporting workers' equipment might bring, reversing BYOD practices is not an option for IBM nor the business world in general. "The genie is out of the bottle," he said.