Byod pro’s and con’s essay sample

Bring Your Own device is a business policy of employees bringing personally owned mobile devices to work and using those devices to access privileged company resources like email, file servers and databases as well as personal applications and data. The types of devices that employees may use are smart cell phones and laptops. The reality is that there is no simple solution when it comes to regulating BYOD. Every organization is different and there are number of different factors that have to be taken into consideration. First a company will have to decide which employees will be allowed access, as well as the types of devices they are going to support.

“ Forrester Research reported in July of 2011 that nearly 60 percent of companies allow employees to use personal devices for work. “ Bring Your Own Device (BYOD)” policies allow employees maximum choice and flexibility but raise new challenges in maintaining the personal privacy of the user, managing and securing valuable corporate information assets, and providing IT with an unpredictable and inconsistent mobile environment. There are also mobile technology considerations, while mobile devices are surpassing PCs and laptops as a user’s primary computing platform, they do have limited access to power, network and hardware resources. Devising a BYOD solution that will support both personal and business roles requires attention to all of these challenges”. The paper will be to identify most of the risks associated with companies allowing personal devices in the work place to access company information. I will also demonstrate the downside of the BYOD policy and the affects to the company and the employee.

There are numerous risks associated with the BYOD policy many of them are security related the loss or theft of a mobile phone could lead to confidential data being stolen and interruption of services this could hurt the company legally as well as financially. Data is discoverable means the device and the information in the personally owned device are subject to litigation and the user has no right to privacy. The device and the information can be examined by the employer and used in a litigation lawsuit. The duty to preserve and disclose electronically stored information is usually initiated by a judicial order, a discovery request, or knowledge of a pending or future legal preceding that is likely to require gaining access to the electronically stored information. Determining what data is required for the matter, and then finding that data’s location across networks and archives is a huge challenge for legal and Information Technology departments, especially if pro-active planning is incorporated.

The scope of data to be preserved or disclosed is determined by the subject matter of the dispute, and the law and procedural rules that a court or other authority will ultimately apply to resolve the dispute. In general, all data is potentially discoverable if it is relevant to the disputed transaction. Failure to preserve or disclose discoverable data may result in serious penalties. Employees need to be made aware that there is no privacy policy and the information may be used in litigation. Litigation expensive, when an employer allows multiple devices to be used this drives up the cost of lawyer fees when litigation is necessary. If there is a data breach an insurance company may not cover the claim if the BYOD program is not involved in the policy it may be only for corporate devices and not personal ones. Dealing with a data breach is expensive and time consuming if found guilty the lawyers fee and penalties can rack up a huge bill. Loss of personal files, employees need to be made aware that personal information may be lost and the company may not be responsible.

When your personal smart phone, laptop or tablet is used for work related activities, such as access to corporate email, calendar or corporate directory, there is a good chance that your company relies on built in features and additional software tools to secure and manage the data in the device… As a first line of defense, many organizations enforce ActiveSync policies, preinstalled in most consumer mobile devices, to enforce password protection and remote wipe and lock. More sophisticated IT departments may request the installation of additional mobile device management software agents to extend corporate IT reach into any application and functionality of your device. While security and manageability are legitimate concerns for the company, most BYOD programs rely on IT tools that don’t make a clear separation between personal and corporate data and applications. As a result, in case of unauthorized access a real or presumed situation the whole content of the device is more or less likely to be deleted and the device will be unusable.

In regards to privacy, from a legal standpoint the fact that the employee owns the device holds no bearing in the event of litigation. As mentioned earlier regarding discovery, the court may require forensic review of all devices in connection with the litigation. An employee participating in a company’s BYOD program may be asked to produce their personal devices for a third party examination. The employee will have to make any personal information stored in the device accessible. This also includes the history of websites visited; songs and movies download and played copies of financial transactions and statements as well as personal contacts. All email and phone call as well as social networking activity is also subject to search. This extends to the personal information of any other family member or third party who may share the use of the device.

Personal data stored is not the only privacy concern for the employee, location and online activity may be exposed to the employer as well. A main feature of mobile device management software is the ability to track in real time the location of the device. The feature is designed to help determine whether a device is lost or stolen before a remote lock or wipe is accessed. It can also be used to selectively disable camera and microphone when a device enters into a restricted company area to prevent sensitive data loss. Although not intended for this use, the IT department may be able to track your whereabouts anywhere and anytime and the employee may not be aware of it. In addition when a personal device is connected to the corporate wifi network, there is a possibility online activity is being monitored and filtered to comply with regulations and to protect the company from liability from improper use.

*Enterasys survey Feb 2012
Are Mobile Devices Risky Business?

“ Among Motorola’s key findings: 2 out 3 people realize that the responsibility falls on them, rather than the IT department, to keep mobile data private and secure. 73% of respondents said they are concerned about smart phone security; in fact, a quarter of them would rather share a toothbrush than their phone.

The survey also found that people:

* Store sensitive data on phones: 34% store sensitive data such as their bank account information or work email passwords on their phones * “ Work around” company mobile policy: 55% admit they’ve sent work email or documents to their personal email accounts on their phones * Chose convenience: 48% have used their devices to log into an unsecure wireless network * Just aren’t that worried: 77% can name at least one thing they’re more familiar with than their company’s IT security policies (67% credit card terms, 57% health insurance policy, and even 33% are more familiar with their home appliance manuals)”

Future Benefits of BYOD

BYOD is here to stay and companies need a plan, in addition to preparing for the potential risk of BYOD and managing the integration. The CIO must evaluate what opportunities does this policy present and determine if it is time to shift gears to application strategy, review the organization’s goals, and strategize how applications can help achieve them. In today’s marketplace, processes occur at a faster pace than in the past, the virtual workforce is increasing, and competition is always trying to stay ahead. Efficient mobile applications can move data closer to the source, which improves sales reporting, streamlines processes and approvals, and provides on-the-go-data to key users. Integrating a mobile application strategy creates new ways to work, and allows redundancy and flexibility that businesses can count on during unfavorable weather, disasters or other interruptions. This continuity is critical whether an organization’s remote workforce is in a home office, at a customer site, or on a battlefield, mobile applications can be the key element. Enabling decisions with accurate data is essential, and indecision or lack of information is surrendering competitive advantage to your peers.

An article written by Courbanou reported that Dell and Intel released findings from the final phase of a multiyear research effort took feedback from 8, 360 workers worldwide and twenty nine interviews with global experts and senior business leaders indicate that bring your own device initiatives and workplace flexibility as a way to generate additional employer productivity and loyalty. (Courbanou, July 2012).

Another benefit to BYOD is cost savings, by allowing the use of personal devices and encouraging employees to pay for their own devices and data plans as a condition of use, there will be substantial cost savings. The savings come by way reduced hardware and software expenditures, and a relief in support costs.

According to a recent Microsoft survey, 53% of organizations responding “ officially” allow BYOD, with 20% providing some financial subsidy to team members and 33% providing no subsidy, as shown below in the graph.

Recommendations for a solution to some of the negative issues associated with the BYOD program would be to have a strong company policy. The following is a list of areas that should be addressed: The policy should be able to support various platforms there are many devices that use different operating systems and they should also include social networking platforms. The employer should keep track of what devices are being used and the applications, these two items should be tested. If budget allows the company should create an application store for the employee to download, however software licensing will have to be addressed. Access control is extremely important user passwords should be issued and controlled, there could be employee access cards distributed and in the future biometrics could be introduced. Awareness, educate employees on how to responsibly protect their device and use company data. Employees who understand the risks and the consequences are less likely to mismanage information. Security software is important in the event a phone is lost or stolen. Maybe to even terminate access. Employees should be made aware that their device is subject to be locked or wiped. Email security is also important because it is regularly used so software to protect email messages is essential.

Out sourcing is an option if the IT department staff cannot handle all tasks involved, possibly using cloud if feasible. Continuous patches and updates to keep up with newer versions of software used.

Out sourcing IT management is a viable option if the budget will allow. This will alleviate some of the pressure on the IT team, also keeping with operating systems and new technology is worrisome. Security wise unless IT safe is completely trained to make important decisions regarding the network and legal decisions regarding locking and wiping devices, this should be done by an expert. Monitoring of device usage and applications can also become a task along with technical support like changing passwords and upgrading applications, so it might be in accompanies best interest to transfer the liability and risk to someone else at a cost. Careful evaluation and research should be done before choosing a company and application, the CIO doesn’t have to worry about Mobile Device Management direct becomes the out sources problem to provide capabilities and services based on changing needs.

Below is a sample of services offered for management of a BYOD policy?

Enterprise Device Management from Smith Micro offers companies of all sizes an easy, secure solution for empowering their mobile workforce—from one central console.

Multi-OS Device Management

- Central, web-based console across major operating systems
- Device configuration
- Inventory management
- Pass code enforcement
- Remotely locate, lock, and wipe devices

Security Management

- Remotely locate, lock, and wipe devices

Administration

- Over-the-air configuration
- Role-based access
- Group-based actions
- Device information access

Enterprise Integration

- Rich web services APIs
- Directory services LDAP
- Manage security certificates

Application Management

- Inventory management
- Publication management
- Installing, uninstalling, updating

Self-Service Management

- Self-registration
- Remotely locate, lock, and wipe devices

Supported Platforms

- Android®
- Apple ions®
- Symbian®
- Windows® Phone 7*
- BlackBerry®*
- webOS®*

* Planned in roadmap

In conclusion the Bring Your Device to work program is becoming popular by default, because so many employees use and rely on mobile devices companies are being forced to address the issue and make a decision. Although there are numerous risk as described earlier in this paper it seems that many companies are willing to take the risk if they can increase productivity, to have employees continue to work long after the company has closed for the day is a benefit and increased productivity means more sales and the end result is prophets and the competitive edge over peers.

Works Cited

The BYOD Conundrum.” Web log post. SecurityInfoWatch. com. N. p., n. d. Web. 09 Dec. 2012. Benigno, Richard. “ 10 Tips for Implementing BYOD Securely.” N. p., 08 Sept. 2012. Web. 09 Dec. 2012. Berkowitz, Philip. “ Corporate Counsel.” Corporate Counsel. N. p., 26 July 2012. Web. 09 Dec. 2012. Messmer, Ellen. “ BYOD-resistance Loosening but Security Practices Lacking.” Consumerization of IT, BYOD. N. p., 25 Oct. 2012. Web. 09 Dec. 2012. Savitz, Eric. “ Developing A BYOD Strategy: The 5 Mistakes To Avoid.” Forbes. Forbes Magazine, 27 Mar. 2012. Web. 07 Dec. 2012. Courbanou, Dave. “ Dell, Intel: BYOD Is Productivity Powerhouse | Channelnomics.” Channelnomics RSS. N. p., n. d. Web. 07 Dec. 2012.