Jay Kaplan Course:BCS 300 #90124 Due Date 10/09/2014

Assignment: Case Study: “The Pleasures and Pitfalls of BYOD”

Chapter 5, Pages 174-175. Answer 4 Questions: 1-4 on page 175.

**Question: 1 - What are the advantages and disadvantages of allowing employees to use their personal smart phones at work?**

The advantages of allowing employees to use their own devices in the workplace represent a convergence of work and personal time that creates an ever-connected employee. Employees who are willing to work after hours, whether it be answering emails, completing reports, or creating documents, are becoming today's mobile employees. The creation of these mobile employees has led to an increase in worker productivity with an estimated additional 57 minutes per employee during the work day. Over time, an additional 5 million minutes of productivity is calculated when a company has implemented a successful Bring Your Own Device (BYOD) program.

The disadvantages of allowing employees to use their personal smartphones at work appear to have far greater problems with a company's overall goals than the value of increasing productivity over time. Security risk and data loss are the top issues associated with employees and their own devices. Employees who bring their own devices have the potential to easily allow viruses direct access to an internal corporate system from inside the network rather than allowing viruses to gain access from outside the network. Corporate BYOD programs could give hackers an upper hand as they target mobile employees with third party apps that could contain trojans or malicious software aimed at stealing corporate documents and gaining access to thousands of bots.

Businesses need to address these additional threats with an increase in security and support personnel to manage devices and apps as well as policies and training regarding appropriate device use. This creates a strain on the time and resources of an IT department who has to manage the system security of apps, devices, and support for many different operating systems. This has led many companies to create mobile device management (MDM) software, which helps control the entire BYOD program including devices, apps, and company policies. IT departments will now have to hire new employees who can support and manage with these programs.

**Question: 2 - What people, organization, and technology factors should be addressed when deciding whether to allow employees to use their personal smartphones for work?**

**People**: Management will have a very difficult time when addressing the employee factors and deciding if this program should be implemented. Can employees be trusted not to spend hours of the day on Facebook or sending out pictures to Instagram? Downloading illegal movies, music, and software over a corporate network are additional concerns that need to be included in these decisions. Are employees willing to follow the rules put into place by the IT department? Will these devices contain viruses or malicious apps that can cause harm to the internal network? Employees will need to be trained about which phones and devices are allowed on the network, what devices will be blocked, which apps will be allowed, and made aware of the company's strict guidelines about what can and cannot happen on the network. Human Resources should also be involved in order to create guidelines and policies for personnel issues such as disregard for BYOD policies, cyber stalking, or even online bullying.

**Organization**: The two biggest factors affecting corporate policy regarding personal devices is network security and the costs of a device program. A company needs to fully understand the risks associated in managing network threats and governing corporate device policies. These types of programs have been associated with an increase in costs as IT staff has to devote time and resources away from other projects to focus on managing these mobile devices. The average cost to an organization is $170,000 per 1000 devices. When a large organization has 10,000 devices, that cost now becomes $1,700,000.

Additional factors that an organization should consider are increases in morale and productivity. If a business can gain employee productivity and profitability, is it worth the risk of allowing these device programs? Employees would need to be skillfully trained on the rights and wrongs of bringing their devices to work and the impact to the corporate network. Future training should continue in order to alleviate and reduce any new security risks. If employees are happier at work, would the company benefit overall from a better work environment? Probably, as happier employees are less likely to turnover and more likely to work harder for the company.

**Technology:** Network security is one of the biggest considerations before implementing a bring your own device program. In the last 10 years, as devices have become more advanced, it appears that the devices have become less secure, but it’s the hackers who are now more advanced. BlackBerry was the leader in the corporate landscape because it was able to offer businesses a very secure mobile operating system and companies felt that their networks were protected. Today, BlackBerry is not a popular operating system. The new market leaders are iOS from Apple and Android from Google. While both of these systems are secure, there are a number of potential security risks that can harm a network, where in the past, BlackBerry had a stronger foothold on these problems. IT departments today need to have both an increased knowledge and ability to support many different mobile platforms and providers.

Other technology factors for a company to consider are the reduced security risk of employees forwarding sensitive emails from the office to personal accounts as well as employees who are uploading and storing company documents to personal cloud accounts such as Google drive and Dropbox. Virtualization is a solution to both of these issues. Employees can now access their desktop space from a number of devices, all by accessing one server, thereby eliminating any risks between work and non-secure personal accounts. The ability to access the same desktop from work, home, and the road now creates a very efficient virtual mobile employee.

**Question: 3 - Compare the BYOD experiences of IBM and Intel. Why did BYOD at Intel work so well?**

IBM and Intel had very different experiences when comparing their BYOD programs. IBM’s CIO Jeanette Horan had a very negative attitude towards BYOD, where she saw more problems than solutions. Intel’s CIO, Diane Bryant, had a very different approach. She was far more positive and wanted to find a way to make it work. According to Osterman Research, three out of five companies agree more with IBM than they do with Intel.

IBM saw a large increase in costs because of its BYOD program. These costs were associated with a number of problems that hurt IBM during implementation of the programs. IBM was unable to create effective company-wide security and device management policies. Employees were unaware of security problems related to third party apps, such as the flow of emails and data from company systems to personal cyber lockers such as Google drive and Dropbox. The use of cloud storage allowed not only the ability for IBM’s corporate documents to get indexed by Google, but also for hackers to gain access to personal email accounts and internal documents.

IBM saw a strain on its IT departments with regard to how it was going to manage all of the different devices. Each device was treated differently depending on the type of employee, the level of the employee, and what type of clearance that employee had. Employees were not happy with these different types of treatment factors. IT also wanted the ability to remote wipe a device in case it was lost or stolen, this way IT could ensure that corporate security and documents were not at risk of getting stolen or leaked to competitors.

Intel had a better approach towards their programs, where they first focused on successfully implementing trainings and then the infrastructure to handle security and device management. Policies were enacted that managed business intelligence, device management infrastructure, and security protection. Intel’s policies included a list of allowed devices as well as a list of blocked devices, thus preventing any issues with employees trying to connect to the network with devices that could cause harm. Intel created an internal app store that allowed employees to access its own apps, including both security and travel apps, and maintained an active mobile app management policy. Intel was able to provide multiple levels of training to employees, management, and support personnel.

Intel’s successful implementation of the bring your own device program increased employee morale and productivity. Employees were happier at work using their own devices which led to an increase in productivity because people were working longer. Whether it be answering emails or communicating with coworkers after hours, Intel was able to calculate that each employee was more productive by 57 minutes on the average day and across its organization found that the company had 5 million hours of increased productivity because of their MDM and MAM policies.

**Question: 4 - Allowing employees to use their own smartphones for work will save the company money. Do you agree? Why or why not?**

It’s clear that allowing employees to use their own smartphones or devices for work will not save a company money. Companies that initiate a BYOD policy will incur a significant amount of time, money, and resources on managing the program as well as the security of the entire corporate network. The costs associated with any type of program can be very substantial to a company that wants to outfit all of its employees with a mandatory program. There are costs associated with staffing and managing the policies, apps, and devices of these programs.

Security risks to the network are also big concerns and come with their own costs. Could an employee’s smartphone become the point of attack of malware or a virus? Companies that rely on their technology for revenue, especially e-commerce related companies, could lose millions of dollars just because their system was compromised by an employee’s device. There are many companies today that implemented these policies only to have an employee’s device unleash a virus into the system that attacked the payment system. These problems have a greater negative impact on costs than just bad public relations, such as credit card hacks and bank fraud.

At the end of the day, a company is really only worried about what type of return on investment can they gain from each activity. Would implementing these programs increase revenue for a company? Is a company even able to measure any return from this type of program? Intel was able to determine that when successfully implemented, they saw a substantial return in productivity hours. Those five extra hours a week that Intel saw is equal to approximately 250 extra hours of productivity over the course of the year. Companies need to figure out the cost savings and benefits of spending for security and implementation of these systems versus the revenue produced from 250 extra hours per employee.