The Impact of Bring Your Own Device (BYOD) to the Architectural Development Process

James S. McKinney

ICTN 6880: Advanced Topics in Information Infrastructure

Dr. John L. Pickard

6 November 2016

Abstract

In this paper I will discusses the impact of the Bring Your Own Device (BYOD) business model on the network architectural development process. The potential impacts of BYOD to future network architectural design are derived by looking at the evolution of BYOD, how BYOD's impact to the business process has steadily increased and changes to current network architecture because of this technology. As BYOD becomes increasingly more popular, concerns over the security of sensitive, organizational data becomes increasingly more prevalent. Challenges in the infrastructure to facilitate the required heightened security systems and procedures, are just some of the new obstacles facing today's network architect when developing a BYOD solution. Also discussed is how the benefits of BYOD, such as increased productivity, will mandate increased network storage capacity along with greater digital throughput requirements. With every new technology comes a learning curve. During the employee's transition from one method of operation to the next, the level of training prior to the migration will determine the size of the curve. A reduction in company owned end user resource requirements is shown and an increase to network infrastructure requirements when implementing a BYOD business solution. The infrastructure increase, in either a supporting or a primary role, will significantly alter the organizational network architectural topology. These reductions and increases in resource requirements will prove to have a cascading effect. Logistical operation will alter current operations to account for less organizationally owned hardware where as technical support will change current operations due to the increase of personally owned equipment. I discuss the rework of operational policies, procedures, the technical support system and training in addition to the physical infrastructure. Through research, data collection and business intelligence analysis; the identification of impact to the architectural process is possible.

Table of Contents

Introduction: page 04
Bring Your Own Device (BYOD): page 05
Network Architectural Process Begins: page 06
Non-Technical Impact: page 11
Other Considerations: page 12
Conclusion: page 13
Bibliography: page 15

Introduction

When tasked with designing a network architecture, a holistic understanding of the customer's organization is required. The architect will research, interview, and collect data for analytical purposes so that he or she can choose how to provide the best solution to meet all customer requirements. Detailed knowledge of a business' process' provides the architect the basis needed to select the correct technologies to use in a network design. Each technology comes with strengths and weaknesses. In the case of a BYOD solution, the architect has well documented industry best practices to use during the architectural development process. I will discuss what BYOD is both positive and negative, in addition to the aspects considered during the process of choosing a technology option. Furthermore, I will outline the architectural development design process and the areas influenced by BYOD during the design phase of the development process. If selected, a BYOD solution fosters vulnerabilities, technical, economical, and organizational business procedures. The architect must properly address all areas influenced by BYOD or the network will fail to produce the environment intended.

Bring Your Own Device (BYOD)

BYOD is a term that became popular in 2009, and is an acronym that stands for "Bring Your Own Device". Considered a business solution in a corporate environment, BYOD is more than just an acronym; it is a transformation of how the end user communicates with organizational resources. The term BYOD came to describe the growing trend of employees bringing their own device to work. This started when cellular phones became smarter and with the introduction of tablets and the iPad. Employees wanted the flexibility to access the company network resources, without having the constraints of being at their workstation. This flexibility changed how and when a company conducts business. "Every employee can benefit from the increased productivity, flexibility, and efficiency that mobility offers." (13) The adaptation of BYOD has both negative and positive effects on a network along with all aspects of business processes and activities. In order to acknowledge the impact of BYOD, there must first be an understanding of the pros and cons of implementing a BYOD solution. Looking at just some of the benefits, why an organization would evaluate the feasibility appears to be reasonable.

Increased productivity and innovation are some of the most enticing benefits when evaluating BYOD as a possible course of action. When individuals are able to work with preferred applications and devices they accomplish more. There are times that an individual needs to work but is not able to be in the office. Traveling for instance, on the clock but without access they are not able to be productive. Optimizing an employee's time will optimize their productivity. The ability to act upon ideas as they arise reduces the possibility that these ideas will become unrealized opportunities.

From a Human Resource (HR) perspective, there is also an increase to employee satisfaction. Today's employees want to work with technology that is on the cutting edge versus what they perceive to be antiquated resources due to budgetary constraints. Technology has integrated into almost every aspect of life. Because of this, it is easier for the employee when the number of platforms they are required to be familiar working with is limited. Allowing them to bring in and utilize their own devices that they are already accustomed to, reduces stress, increases satisfaction and improves productivity. Another benefit of employee satisfaction is employee retention.

Improved organizational information sharing is another strong selling point for BYOD. Prohibitively expensive, issuing of devices that allowed access to the company resources outside of the business office is restricted to a few key personnel. With the adoption of BYOD things changed because, the burden of ownership was no longer a business concern. Prior to BYOD, only certain employees possessed this capability. Now any employee with a mobile device can check company email or get instant messages. With this capability available at all times, both employees and management have the resource to communicate as needed rather than only when at work.

Logistically speaking, a BYOD solution reduces the amount of Information Technology (IT) equipment that the business would have to purchase for end users. Along with purchasing, a well-designed Life Cycle Replacement (LCR) program is required to insure the operational status while dispersing the cost over time. Licensing is another logistical concern when referring to IT equipment. Licensing is generally an annual expense. There are software licenses and service licenses. It is important to maintain Software licenses to insure accountability and legality during and internal or external audit. Maintenance agreements are another expense that, depending on the desired service level agreement (SLA), can be very costly. These expenses are now the responsibility of the individual who owns the device. This is a cost savings to the company allowing reallocation of resources. Another advantage is reduced training requirements. Since employees are using the device they use on regular bases and are comfortable with, there is a reduction in the need to train them on company provided devices.

Network Architectural Process Begins

When most people think of a Network Architect they think of an individual that only understands the technologies, signaling and hardware of a network. A good architect will understand much more because much more goes into the design and development process. “The Network design should be a complete process that matches business needs to available technology to deliver a System and Services that will maximize an organization’s success”. (9) There is an abundance of technologies on the market today. Each technology is useful in its own way. The architect must understand the business requirements in order to select the appropriate technology for the project. In this respect, business drives technology. IT personnel prefer to stay technical and do not see themselves as primarily business minded. Knowing what questions to ask is important to developing a network that functions to support the business mission. Understanding business is crucial to developing a resilient, reproducible and scalable network design. “Who bridges the gap between business and technology?-the architect”. (10) A good design is of no value if it is not funded. Acquiring funding is not as difficult when both the design and business initiatives align. To insure alignment, the architect must gain comprehensive knowledge of the company, its market place and competitors. To understand the company takes in-depth knowledge of the internal business environment. Having knowledge of the internal business allows the architect to select the technology that best fits the organization. A good knowledge base on the external business environment will provide the information needed to make an informed decision on future growth possibilities. By looking into the landscape of the business' competitors, the possible climate of the industry can be gaged for fluctuations in both business growth and decline. With knowledge of the business aspect of the customers' organization, you can move into network design phase. At this point, I will use the eight-step design methodology for designing a network recommended by CISCO. "The first six steps of the eight step design model is related to CCDA and where you have to design and document the project, whereas the remaining two steps are related to implementation and verification which is the part of CCNP". (7) These eight steps are: 1. Recognize Customer needs, 2. Describe the existing Network, 3. Design networking & topology Solution, 4. Plan the network implementation, 5. Construct a prototype network, 6. Fully Document the Design, 7. Implement the Design, and 8. Verify, monitor & modify as needed. (7) For the purpose of this discussion, I will proceed as if the customer has requested architect design to implement a BYOD solution.

Network Design Process

In step one; the customer's design requirements are identified. The customer requested a BYOD solution, but that is only part of design requirements that the architect needs to know. He or she needs to understand what the organizational goals are in addition to what constraints and or limitations are going to affect the final product? Constraints and limitation are a nice way of saying money. If costs are exceed in one area that cost must be made up in another. Cost overruns are pre-approved so it will be incumbent on the architect to show where a return on investment (ROI) is worth the cost. Because management may or may not be technical, the technical goals and possible constraints are identified for later analysis. Technical goals, in contrast to organizational goals, can be inhibited by interoperability of technology and not just budget. With a BYOD solution, applications that used to be on a workstation now need to be on a server for mobile device access. In addition, there will be increase license requirements. The architect reviews applications ensuring compatible with BYOD. Another possible impact to technical goals is security. Even when a course of action is technically feasible, it may not be practical because of the security risk. Identifying the applications that the customer plans on using will be important later to determine the needed throughput required, internally as well as externally. This is especially important in a BYOD solution because access to the network will be greater and subsequently the usage of resources will be greater.

Step two is the process of defining or describing the existing network. Obviously, if this is an initial build this step will not be needed. When there is an existing network, it makes a very lengthy phase of the process. Performing a network audit will provide you with a lot of information. There are different network auditing and analysis applications available for this task. Using an industry established auditing application provides the most comprehensive orientation of the network. Where auditing gives an architect the physical picture, analytical application will provide the applications level information. In most cases, there will be a large increase to devices, both end user and networking, so it is important to ensure the established naming conventions will support the projected increase. One aspect of BYOD that makes it so popular is the reduction of end user devices, however the reduction is in organizationally owned devices. Once an employee is allowed to "Bring their own device" to work they generally do not stick to one. "A recent survey by iPass found that the average mobile worker now carries 3.5 mobile devices, which might include smartphones, laptops, and tablets." (12) Location of network areas will be analyzed to ensure that current locations provide optimized network operations. The cabling will be assessed to evaluate whether the current infrastructure will align with what is required by the implementation of BYOD. What needs to be looked at is more than just quantity and location. Cable type is important also to insure that it is compatible with future network architecture. Wide Area Network (WAN) technology, if any, should be evaluated to identify the circuit speeds and throughput. Network locations will factor into design plans as well. With BYOD there will be an increase in servers/storage devices. When you increase equipment you increase power requirements as well as the size and or quantity of Environmental Control Units (ECU) needs. Logical network information including Internet Protocol (IP) schemes and availability along with routing protocols, network management and security is required. BYOD will drastically increase the amount of IPs needed. Whether IP version 6 (IPv6) or IP version 4 (IPv4) is used, evaluating the current scheme will determine if a new scheme is needed or if the existing one can be carried forward. Some routing protocols are proprietary such as the Enhanced interior Gateway Routing Protocol (EIGRP). EIGRP is a CISCO developed protocol that only works with CISCO devices. Implementing a BYOD solution, depending of organizational constraints or goals, may not use CISCO equipment exclusively. This would mean that an open source protocol such as Open Shorts Path First (OSPF) would need to replace EIGRP or be incorporated into the routing scheme. Access control list are important aspects of network security. The single most negative aspect of implementing a BYOD solution is security. Network security, in part, is responsible for restricting access to areas based on individual needs. Most organizations restrict access by default. The introduction of what could be potentially a plethora of multi-vendor end points mandates that the authentication protocols and Access Control Lists (ACL) should be evaluated. To facilitate a complete understanding of the network will require the collection of all documentation available. This will also aid in the identification of what the state of the network should be versus its current state.

Step three designing the network topology and solution. In this step you will need all of the information and analysis from the last two steps. In this step, the network topology is selected based on what has been determined to meet the customer's requirements. "The best approach to design the network topology is the structure approach which allows you to develop the optimal solution with lower cost with fulfilling all requirements of customer like capacity, flexibility, functionality, performance, scalability and availability." (7) BYOD, like a wireless network will require a lot of Access Points (AP). These APs will need to be placed throughout the coverage area in a manor to provide overlapping coverage. An employee should be able to travel from area to area without losing connectivity or even noticing a change. Because of BYOD's ability to offer the individual flexibility to access organizational resources at any time or anywhere, there will be an increase to people connecting and using these resources. Access points and Wide Area Network (WAN) devices will be required to accept an increase to concurrent connection. That is to say, that more devices will be connected at the same time and the network devices need to be robust enough to process the increased amount of data. A network solution will encompass all devices, Local Area Network (LAN) services and WAN technologies. LAN services include email and network printing where WAN technologies are concerned with communications between networks. CISCO recommends the use of the Open Systems Interconnection (OSI) seven-layer model in a top down design method. Part of a network solution is a program to maintain it. CISCO also recommends the use of its network life cycle. Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO) "is the network life cycle that is defined by Cisco" (11)

Step four; planning the network implementation requires all accumulated documentation to this point. The implementation plan needs to be documented step by step and then analyzed for possible conflicts. As already stated, BYOD increases the number of devices that will need an IP. Depending on the current IP scheme a new IP scheme may need to be implemented at this time. To do this without a significant loss of connectivity will be a challenge. There will most likely be additional equipment that will need to be integrated as well as equipment that needs to be replaced. Time tables for every step should be defined. Each step should be evaluated to insure that if it is not reliant on a step that has not been implemented thus far. It will be important to factor in time to test each step upon completion.

Step five construction of a prototype network or a pilot site for testing on a network design is recommended. "During the network designing and implementation when you finish a new network module or deploy the design to a small site before the full implementation, it is a best practice to test the new solution." (7) A prototype network is just what it sounds like, a smaller version of the design solution. Being that this is a BYOD solution, I do not believe that this is practical. Any results stemming from the testing of a proto type network would not be an actual representation of what will be found when deployed. A more practical measure of success will be gained from implementing a pilot site. This is where you take a section of the building, area or Campus Area Network (CAN) and install the network solution. By doing this, live data will be gathered based on real world applications. To assure the validity the architect would need to ensure that a large enough sample size of the organization with a diverse enough workflow is used. This would entail not using any one function i.e. accounting or Human Resources (HR) but rather a mixture of as many as possible. Being that there is an increase to wireless/mobile connection, the testing of LAN services is very important. A successful pilot test proves the design functionality and allows progression to the next step. A failure in the pilot site would mean modifications as needed and then the redoing the pilot program again.

Step six is to fully document the design. This is where the architect will document the design process. First will be an introduction that describes the information on the purpose of the project. Then he or she will document the business requirements in the new network design. The old network architecture to include the logical topology and physical topology is documented. Routing protocols, applications along with a list of network devices such as routers and switches are documented. Included also is the configuration and any issues that were identified previously or during the evaluation process. The existing infrastructure showing the cabling types and paths are also documented. Also documented is the result of the pilot site. These results are important to show proof of concept and feasibility in the proposed network design. At this point, the implantation plan will be inserted into the greater documentation. All of this documentation is to identify network changes and provide the enterprise with the documentation needed to manage the network. Finally, appendixes will be created to list all network devices, configurations, and data used during the design process. “Documenting the project is the best practice and has a number of advantages and future benefits.” (7)

Step seven is implementing the design. This step will consist of migrating to the new network by executing the implementation plan. The key to this step is to stick to the plan. Ensure that timetables are adhered to and no steps are skipped. Monitoring activities and verifying progress is a good management tool for keeping a schedule. If corrective action is required, earlier is better than latter.

Step eight is more of a continuous activity. Monitor and modify as needed is a never-ending task. Because this is a BYOD solution, there are particular areas that need attention. What is the throughput on the WAN circuits and is it within acceptable ranges?

What is the Central Processing Unit (CPU) utilization on network devices? How many complaints are there reference connection issues? Monitoring traffic patterns may indicate changes that were not previously identified. One constant is that networks change.

Non-Technical Impact

Non-technical impacts of a BYOD solution are evident in almost all area of the business and influence changes in the business' Standard Operating Procedures (SOP). Implementing a network solution goes beyond the physical/logical network. Programs that support the solution are established along with procedures that govern the use and established parameters to be published.

With the implementation of BYOD the level of service calls is initially going to increase as with any new migration. The difference here is that calls now will be concerning multiple platforms working on various IOSs. The training curve for employees will also result in an increase of service calls. For this reason, it would behoove the organization to bolster up and train the IT staff prior to implementation. Doing this will decrease the time it takes to resolve trouble tickets and user frustration. There should also be a plan to train the users prior to allowing them to gain access to network resources.

Non-technical security measures come in the form of established guidelines, policies and procedures. Because BYOD offers increased flexibility compared to a traditional hardwired network connection, the possibilities for intentional or accidental misuse are greater. That is why a new Acceptable Use Policy (AUP) should be published that establishes how an individual will be allowed to access and use company resources with personally owned devices. There also needs to be detailed repercussions for misconduct. The AUP should be reviewed and approved by the organization's legal department to ensure that the personal rights of the employee are not violated and actions for misconduct outlined in the policy can be taken. A well written AUP prevents misunderstandings and minimizes misuse.

Personal electronic devices operate on their own operating system based on vendor, make and model. "Each device has computing power that was sufficient for navigating a rocket to the moon 40 years ago" (4) With each operating system comes unique trouble shooting procedures and security vulnerabilities. The number of various personal devices on the market today exceeds what is economically practical to support in a BYOD environment. For this reason, an Acceptable Products List (APL) should be generated. An APL will limit the number of devices allowed to connect to network resources. An APL is also a working document that should be reviewed and updated on a regular basis.

With BYOD employees now have the capability to store company data on their personal devices. Although it is a potential security risk even on a normal business day, the true risk is when the employee is not at work. Policies to mitigate this risk should be put into place. For instance if an employee travels on scheduled vacation to another country they are unintentionally putting proprietary information at risk. If the device is lost or stolen, the company may not have a recourse to secure the data after the fact. Remote wiping may be an option if the device is powered on and is in range of a mobile tower. Depending on the time between loss and being reported to the organizational security official there may be nothing that can be done. Some companies require their employees to bring their device in prior to traveling. When the device is brought in, all organizational information is backed up and then cleared from the device. Upon return, the information is restored back on the device and the device is restored to its pre-travel state. Another option would be to have a Mobile Device Management (MDM) solution. This would allow the device to be partitioned so that the individual's personal content is kept separate from the business content. Stronger security measures could be placed on the official portion. "To mitigate these concerns, organizations need to have an effective BYOD policy in place, including a mobile device management (MDM) solution" (5) Another concern when it comes to data stored on an employee's device is in the case of termination or resignation. When an employee leaves the employment of a company that has a BYOD solution in place, the individual's device needs to be cleared of all organizational data. In the case of resignation it is generally not a problem, but when an employee is terminated animosity might exist. There must be a policy or procedure to handle this situation. A process should be developed to enroll personnel into the BYOD program. This process should include the reading of all related policies and procedures. The target device or devices should be evaluated to assess suitability and configured for registration into the program.

Other Considerations

A BYOD implementation into a corporate environment carries vulnerabilities beyond what has already been discussed. The biggest of these involves legal issues. It is important to mention the legal impact because it will factor into the budget constraints outlined in the initial discussion. Cost sharing is where the company pays a portion of the cellular services for time spent conducting company business. A lot of employers object to this feeling that the employee would be paying the bill whether there were using the device for company business or not. In *Cochran v. Schwan's Home Service, Inc., 228 Cal.App.4th 1137 (August 12, 2014)* the courts decided in favor of the plaintiff. There is a California statute that states "[a]n employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer[.]”. The purpose of this bill is to insure that employers do not pass on their operational cost to the employees. There are similar statutes in other states. A 2016 report by Syntonic and Information Solutions Group (ISG) found that 59 percent of enterprises had a reimbursement policy to comply with state laws. In this report it was determined that employees were being over paid for reimbursement. The amount overpaid was found to be more than 2.6 Billion dollars.

Another cost consideration is expenses stemming from overtime hours claimed. If there is not a policy in place that specifies how the logging of overtime hours will be processed the organization will be liable for paying any employee that logs hours whether pre-approved or not. In the case of *Dana Mohammadi v. Augustine Nwabuisi, et al, No. 16-50437 (5th Cir. 2017)* the plaintiff used their mobile device to conduct business outside of established working hours. The employer did not see this as overtime because they were not at their place of duty. Ultimately, the plaintiff was awarded back pay for hours worked. The Volkswagen Corporation, in an effort to put a stop to cost related to extended hours, implemented a policy that shut down email servers for all employees located in Germany. This was successful in the case of employees claiming hours spent checking email.

When an employee puts organizational data onto their personal device, they are placing organizational data alongside their own Personally Identifiable Information. (PII) To insure security of sensitive data, the company will need to have limited access to the device holding the employee’s PII. Privacy is a right that belongs to everyone and cannot be signed away. Even if an organization pressures a person into signing a waiver allowing access, a measure of privacy still exist.

Conclusion

BYOD does not change the process itself but instead changes the course of action taken by the architect during each process. Technically, the dynamic of the network will be transformed into a wireless hub. The data flow will be restructured to optimize the bandwidth between organizational activities and WAN circuits coming in will most likely increase. There will be a need for additional policies, procedures and programs dedicated to outlining how the BYOD program will function. Additional training for both IT staff and end users on the new technologies and processes is required to minimize trouble calls and trouble shooting. Furthermore, budgetary cost associated with legal fees has to be factored in. This is not normally a consideration for a network architect, but BYOD has legal ramification that are still being discovered. Other non-technical budgetary cost are extended work hours and cost sharing. The depth of these expenses makes it noteworthy and should be addressed with the customer. There are business' that are dedicated to BYOD implementation and are a good source for consultation. An in-depth knowledge of current best practices for implementing a BYOD solution would greatly simplify the architectural process. In conclusion, BYOD in one way or another effects virtually all aspects of the architectural design process.

Bibliography

(1) Raths, D. (2012, May 01). Are You Ready for BYOD: Advice from the Trenches on How to Prepare Your Wireless Network for the Bring-Your-Own-Device Movement. Retrieved October 26, 2017, from https://www.questia.com/library/journal/1G1-292008620/are-you-ready-for-byod-advice-from-the-trenches-on

(2) Moyer, J. E. (2013, July 15). Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. Retrieved October 26, 2017, from http://www.tandfonline.com/doi/abs/10.1080/15323269.2013.798768

(3) Fortson, K. (2013, February 01). Creating Device-Neutral Assignments for BYOD Classes. Retrieved October 26, 2017, from https://www.questia.com/library/journal/1G1-324397562/creating-device-neutral-assignments-for-byod-classes

(4) Oppliger, R. (2011, September 12). Security and Privacy in an Online World. Retrieved October 26, 2017, from http://ieeexplore.ieee.org/abstract/document/6017170/

(5) Semer, Lance. "Auditing the BYOD program: the growing business use of personal smartphones and other devices raises new security risks." *Internal Auditor*, Feb. 2013, p. 23+. *Academic OneFile*, Accessed 26 Oct. 2017.

(6) Laird, J. (2014, November 7). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. Retrieved October 28, 2017, from http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore

(7) Azam, W. (2013, July 16). How to design network | Eight step design methodology. Retrieved October 29, 2017, from http://w7cloud.com/how-to-design-network/

(8) McCabe, J. (2007, September). Introduction to network analysis, architecture and design. Retrieved October 30, 2017, from http://searchdatamanagement.techtarget.com/feature/Introduction-to-network-analysis-architecture-and-design

(9) Cruz, Rui Santos (2017). Design Process of IT Infrastructures Network Architecture and Design [PowerPoint slides]. Retrieved from https://fenix.tecnico.ulisboa.pt/downloadFile/845043405444180/AGI.15.16-Lecture-04.pdf

(10) White, R., & Donohue, D. (2014). The art of network architecture: business-driven design. INpolis, IN: Cisco Press.

(11) Klijn, J. (2012). Ongoing 2b/3a inhibition In Myocardial infarction Evaluation. Http://isrctn.org/>. doi:10.1186/isrctn06195297

(12) Romer, Hormazd. "Best Practices for BYOD Security." Computer Fraud & Security 2014.1 (2014): 13–15. Web. 25 Oct. 2017.

(13) "10 Smart Strategies for BYOD Success." Information Management, vol. 49, no. 6, 2015., pp. 1

(14) Crousillac, T. (2016, March 21). Bring Your Own Bill? Reimbursing Employee Use of a Personal Cell Phone for Work-Related Purposes. Retrieved October 26, 2017, from https://lawreview.law.lsu.edu/2016/03/21/bring-your-own-bill-reimbursing-employee-use-of-a-personal-cell-phone-for-work-related-purposes-2/