THE UNIVERSITY OF
SCRANTON
A JESUIT UNIVERSITY

BYOD Strategy
2014

BYOD Strategy Group
Joseph Casabona
Lee DeAngelis
Adam Edwards
Diane Kennedy
Calvin Krzywiec (Chair)
Timothy Meade
Glen Pace
Jason Wimmer

Planning and Information Resources

Summary

The Bring Your Own Device (BYOD) phenomenon offers a unique challenge to IT departments as more students, staff and faculty bring their personal devices and services to campus. The ease of use and ubiquitous nature of consumer technology has led to an increased demand for access to institutional services and data from non-University devices. Since support for BYOD touches all aspects of technology, the BYOD Strategy Group was formed to develop a three-year, high-level strategy for supporting BYOD as it relates to the mission and the vision of the University.

This document is a collection of strategic objectives for addressing the BYOD phenomenon. This strategy is based upon findings from industry specific research publications and contextual conversation among the members of the group. The group compiled and evaluated industry research recommendations and tailored them to local objectives.

Teaching and Learning

As the population of students and faculty bringing technology to campus continues to rise, this technology can be leveraged as an opportunity to enhance the teaching and learning environment. Students today have high expectations for "anytime anywhere" access to teaching and learning material [3]. Expanding mobile friendly content delivery solutions, such as lecture capture and the LMS, provide students access to lecture resources beyond the walls of the classroom. Additionally, students have a higher demand for the integration of their devices into the classroom [3]. Technology solutions can be leveraged to provide faculty and students untethered access to classroom resources, such as mediation and computing infrastructure.

As we look to incorporate client devices into the classroom, BYOD can be leveraged as an opportunity to eliminate a majority of the traditional computing infrastructure provided within instructional spaces. Given the already successful deployment of virtual desktops into the lab spaces and the fact that the vast majority of students own a laptop or tablet [1], these two technologies could be combined to reduce the physical computing infrastructure deployed to labs. This design would rely on the student's device to connect to a virtual lab desktop or virtual lab applications rather than deploying a traditional computer or VDI thin client into the classroom. This would have a tangential effect of reducing other classroom infrastructure, such as network cabling and switching requirements.

The financial analysis of this is complicated and requires further study. While this may seem like an opportunity for cost reduction, the capital savings associated with traditional PC hardware or VDI thin clients will likely be offset by licensing fees (specifically, Microsoft VDA licenses). Some remaining dollars will likely need to be redirected to fund the network, server, and storage infrastructure required to provide this service. Financial considerations aside, the service provided is

invaluable. Students would now have access to lab resources beyond the borders of the classroom (e.g. specialized software), extending educational resources to their residence halls and off campus locations. This service is beneficial to current students and marketable to future students. This may also allow for the elimination of some open computing labs, resulting in further cost reduction. It's important to note that a complete reduction in lab computing infrastructure is not feasible as virtualization is not currently suitable for some specialized labs. Additionally, some open lab machines will be necessary to address disparities in student computer ownership or provide assistance to users with a failed device [2].

Changing the classroom technology necessitates a change to the classroom and lab workspaces. As future classroom renovations occur, rigid furniture should be replaced with flexible workspaces to accommodate mobile devices. Much of the classroom space on campus is constructed with traditional PCs in mind, with power sources being relatively inaccessible and therefore, limits the use of mobile devices for longer durations. Although specific to smartphones, ECAR research supports this, listing "inadequate battery life" as the top barrier to using such devices as a learning device [3]. Flexible workspaces in general use labs (i.e. open labs) will facilitate increased collaboration among students and help promote the sense of community that is core to our mission. The Library Learning Commons will be an interesting project to monitor and will serve as a litmus test for how students will utilize such an environment.

The increased demand for classroom technology has resulted in the organic growth of lab spaces over the years. This demand continues to grow in contrast to a physical footprint that remains relatively constant. Scheduling complexities occur as the registrar attempts to meet the needs of faculty with the finite lab spaces available. As such, construction projects are leveraged as opportunities for the creation of new lab spaces populated with computing devices to address the demand, which results in an increase in overall operating costs for the lab environments. The combination of virtual labs and mobile-friendly classroom environments will reduce the complexity in classroom scheduling as any classroom could conceivably be converted, on the fly, to a computing lab. This approach should remove the need for the addition of spaces with dedicated lab devices in the future, having an overall positive effect on future operational costs.

As more student devices enter the classroom, some faculty have expressed concerns related to academic integrity, as mobile devices have the potential to allow easier access to outside resources during electronic assessment. This will become more of an issue if BYOD access to lab resources is introduced. As such, additional solutions need to be introduced to address faculty concerns. This group does not have a recommendation on a specific technology to address this concern, but it does recommend that this be investigated further as a prerequisite to BYOD in the lab spaces.

Thus far, we've introduced a number of technology changes both inside and outside of the classroom. As these and future solutions are implemented, support models should be enhanced to accommodate training and support for the students and faculty that will incorporate these solutions into their teaching and learning toolbox. Success of BYOD in this area is tied closely to the institution's ability to proactively support and train their faculty in the integration of this technology into their classroom [4]. As such, this group recommends partnering with the CTLE to develop a model of proactive support for faculty on the use of the proposed technology. Additionally, engaging faculty in the implementation of BYOD has shown to be an effective strategy at other institutions for gaining acceptance for the use of these technologies in the classroom environment.

Strategic Objectives:

- Increase student and faculty interaction with technology in the classroom
    - Investigate and implement untethered teaching / learning solutions
    - Focus classroom upgrades on providing collaborative, flexible workspaces
    - Leverage virtual desktop / application technologies and client devices to reduce reliance on physical lab infrastructure
    - Investigate and implement secure electronic assessment solutions
- Extend access to classroom resources to anytime / anywhere
    - Leverage virtual desktop / application technologies to provide ubiquitous access to lab software resources
    - Expand lecture capture to additional locations
    - Leverage the LMS to provide mobile access to course material
- Partner with the CTLE to provide a proactive approach to classroom technology solutions, including technology support and training

Staff and Faculty

The core issue associated with BYOD for faculty and staff is how to best provide access to campus services from non-corporate assets, while maintaining the security of institutional data and the integrity of campus software licenses. At this point in time, staff is more likely to use BYOD as a supplement to institutionally provided devices for "routine" access to institutional services and data, such as email and documents. In addition, staff is more likely to use their own devices for remote access to institutional services. Faculty will also fall into this model. However, given that faculty have historically required greater flexibility in technology choices to facilitate their teaching and research, they are also more likely to utilize their own devices in place of standard institutionally provided devices. These predictions are mostly based on anecdotal evidence, but ECAR research supports this in terms of the growth of devices accessing institutional networks by population [5]. That said, embracing BYOD for faculty and staff would rely on the same set of technology solutions and security controls.

As faculty and staff bring their devices to campus, they will want to interact with campus services. Classifying and isolating corporate versus non-corporate devices on the network provides for the ability to selectively allow access to campus services from non-corporate devices through the use of technical controls, such as firewalls. For example, a staff member working from their personally owned machine can access common intranet resources, such as printing services, but cannot connect to the ERP.

When access to restricted resources is required, faculty and staff can leverage virtualization technologies to access the resource. This solution allows the employee to interact with the service they need (in this case, the ERP), without the risk of data loss. Virtual desktops and applications have the added benefit for allowing faculty or staff to utilize University licensed software from their personal devices, without violating the license agreement. For example, a faculty member brings their personal laptop to campus and interacts with common software from their own device, such as a Microsoft Office or the LMS. When the faculty member needs to utilize University licensed software (such as SPSS), they can utilize a virtual application to do so without violating the terms of the license. Should more faculty and staff bring their own primary computing devices, this technology would give them access to a University desktop and applications from their own device at a fraction of the cost of a traditional University issued device. This same approach can be utilized for remote access to restricted services, accomplishing the same goals with users' home machines.

As BYOD grows and users begin to utilize their own primary computing devices in lieu of an institutionally provided device, reimbursements models will need to be developed. There is currently no clear industry model for this. Reports from other institutions vary widely by amount, employee type, technology and duration [5]. This is likely due to the fact that this model of BYO primary computing device is not widespread. As this grows, considerations for equipment and software reimbursements should be considered.

While the above technical solutions work well for access to intranet and restricted services from personally owned devices, there is still a risk of data loss from public services. Email and other data storage on mobile devices make them likely sources for a data breach as these devices are frequently lost or stolen. Additionally, as more employees are linking University email accounts to their personal phone, data loss can occur on employee separation, as there is currently no mechanism to ensure that institutional data has been removed from the personal device. Investing in a comprehensive mobile device management (MDM) program can help mitigate data loss by ensuring that the appropriate controls are in place and that corporate data can be wiped from devices when necessary.

In a higher education environment, the same MDM controls are not appropriate for everyone. The following three-tiered approach is recommended:

- *Mandatory*: This tier applies to all University issued devices and requires an enrollment in a MDM system that enforces the implementation of technical controls on the device, such as lock code, lock when idle, remote wipe capabilities, device encryption, and potentially even location tracking for locating a lost device.
- *Optional*: This tier applies to all non-corporate owned staff, faculty, and affiliate devices connecting to University systems, including email. Enrollment in the MDM solution is optional but the expectations of minimal technical controls and the requirement to notify PIR of a lost/stolen device are defined in institutional policy. Employees must agree to allow the University to wipe the device when it is lost/stolen or the employee separates from the institution.
- *Exempt*: This tier applies to student devices. This tier has no requirements but offers guidance to students on how to secure their devices.

The tiered system offers a balance between security controls and end user privacy on their personal devices. Users may object to a full wipe of their device on separation in which case, enrollment in the MDM solution is attractive so as to facilitate a partial wipe of the device, removing only corporate data.

One of the more crucial components of an MDM program will be the policy it's based on. An MDM policy should clearly describe the institution's authority and expectations. In addition, and perhaps more importantly to the success of a MDM program, the policy should be transparent as to what the capabilities the MDM solution provides the University, the data it collects and why it collects it. This will help dispel some of the "big brother" feeling that MDM is sometimes associated with. Stanford University has an excellent example of this on their MDM website[1]. Other policies, such as the *Acceptable Use of Computing Resources Policy* and the *Planning and Information Resources Privacy and Confidentiality Statement* may also need updating to incorporate MDM and other BYOD concerns.

The group identified two important services that should be enhanced to provide seamless integration of BYOD into the work environment. Failure to do so will likely inhibit the growth of faculty and staff BYOD on campus. The first service is one of the most common, routine resources utilized by users: a printer. While our current infrastructure works well for corporate laptops and PCs, we lack a solution for printing from mobile and non-corporate devices. Most printers on campus require special drivers that aren't compatible with mobile devices and introduce security risks for non-corporate workstations. As more of these devices enter our environment, the printing infrastructure needs to be updated to provide a secure and scalable solution.

[1] https://itservices.stanford.edu/service/mobiledevice/management

The second important service is file storage. The current file storage solution, RoyalDrive, lacks important features needed in a BYOD world. First, access from mobile devices is restricted to read-only and the solutions that exist are awkward to use and rarely render the content correctly. Second, when working with files from non-mobile devices, users must either download the file from the web interface or form a persistent connection to RoyalDrive to interact with files. This is a security concern as files containing sensitive data have the potential to be accidentally stored locally on the user's device, which could lead to a data breach as a result of malware or theft of the device. Many free, clouded storage solutions exist today, almost all of them providing mobile-ready features, such as a mobile application and in-browser editing. Lacking a local comparable solution, users are likely to utilize these foreign solutions for their functionality and convenience, resulting in the loss of control over institutional data. This is evident by the fact that IdentifyFinder scans have already detected restricted data in some of these products installed on institutionally owned machines. Many of the consumer services offer corporate solutions as well. These solutions provide the same features of the consumer versions, but also allow administrators to set parameters as to how and where data is stored.

While many technical controls and solutions are recommended, end user behavior will pose the greatest risk to data loss in a BYOD world. Developing a comprehensive Information Security training program to build end-user awareness of the risks and benefits of BYOD is recommended. Mandatory security awareness training at other institutions focuses primarily on staff and faculty knowledge workers [5]. Training should focus on building awareness to data exposure risks and how to use corporate solutions to secure and isolate institutional data from personal data.

Strategic Objectives:

- Implement virtual desktop / application technologies to facilitate ubiquitous access to services
- Deploy new network configurations to facilitate connections from non-corporate devices
- Investigate and implement a mobile device management (MDM) solution utilizing a tiered approach
    - Develop transparent MDM policy
    - Update existing policies as needed
- Develop solutions that allow for secure interaction with the corporate environment from non-corporate devices
    - Mobile printing
    - File storage
- Develop a comprehensive Information Security education program to raise end-user awareness of BYOD risks and controls
- Investigate BYOD reimbursement/stipend models

Infrastructure Implications

Much of the technology solutions discussed are reliant on a high performance, reliable infrastructure. The wireless network is the conduit for access to all BYOD services and a dense wireless deployment is required to handle the number of client devices coming onto campus. Our recent investments in a campus-wide wireless upgrade have put us in an excellent position to meet the BYOD demand. That said, as the recommended lab strategy is implemented, wireless client density in classrooms will grow. These areas need to be monitored for saturation and small investments may be needed to increase the number of wireless access points and maintain proper wireless density ratios.

Much of the recommended solutions are based on virtualization technologies, which are highly dependent on infrastructure services. As these solutions grow, a reliable data center network, storage, and server infrastructure will be required. Continual investments in this area will be required to enhance the redundancy and scalability of the infrastructure.

Strategic Objectives:

- Monitor wireless access point density ratios and deploy additional access points as necessary
- Continue to invest in data center infrastructure
    - Increase redundancy and scalability of network, storage and server infrastructure
    - Expand virtualization infrastructure

Support Implications

Traditional support models focused on supporting devices. As BYOD grows, these support models will evolve to focus on supporting the service rather than the device itself. Many consumers are familiar with the "self help" model so developing "self help" modules or DIY tutorials will likely reduce the BYOD load on support staff. While the number of different devices that users are bringing to campus is vast, the underlying operating systems (Windows, OSX, Android, iOS) are not. Support staff should be familiar with the major operating systems that consumer devices are using in order to better support the services being utilized from these devices.

Strategic Objectives:

- Develop "self help" models for services
- Develop support staff skills across the major BYOD operating systems

Works Cited

1. Institutional Research Office, ECAR Undergraduate Student Technology Survey, The University of Scranton, September 2013
2. EDUCAUSE: What Does BYOE Mean for IT?, May 2013 http://www.educause.edu/library/resources/what-does-byoe-mean-it-it-leader-roundtable
3. EDUCUASE: ECAR Study of Undergraduate Students and Technology, 2013 http://www.educause.edu/library/resources/ecar-study-undergraduate-students-and-information-technology-2013
4. EDUCUASE: Formal Planning Optimizes BYOE Opportunities, May 2103. http://www.educause.edu/library/resources/formal-planning-optimizes-byoe-opportunities-university-florida
5. EDUCUASE: The Consumerization of Technology and the Bring-Your-Own-Everything (BYOE) Era of Higher Education, March 2013 http://net.educause.edu/ir/library/pdf/ERS1301/ers1301.pdf