Action Learning Project: Bring Your Own Device (BYOD)

21 November 2012

Executive Sponsor:
Tim Slottow

Team Members:
Michael Daley, Information and Technology Services
Ben Havens, University Audits
Beth Manning, U-M Flint Human Resources
MaryBeth Stuenkel, Information and Technology Services
Ken Wilson, Financial Operations
# Table of Contents

Executive Summary ........................................................................................................... 1
Recommendations at a Glance .......................................................................................... 2
Introduction ......................................................................................................................... 3
Methods ............................................................................................................................... 4
  Literature Review ............................................................................................................. 4
  Stakeholder Interviews ...................................................................................................... 4
  Business and Finance Town Hall Survey ........................................................................ 4
  U-M User Survey ............................................................................................................ 4
  Higher Education Survey ................................................................................................. 4
  IT Support Group meetings .............................................................................................. 4
  Other Information Gathering ............................................................................................ 4
Data Summary ..................................................................................................................... 6
  Industry Trends ................................................................................................................ 6
  BYOD in Higher Education ............................................................................................. 6
  BYOD at U-M ................................................................................................................... 7
Analysis .................................................................................................................................. 14
  Spectrum of Options ....................................................................................................... 14
  Benefits and Risks ............................................................................................................ 15
Recommendations ............................................................................................................. 18
  Suitability ......................................................................................................................... 18
  Governance and Policy ...................................................................................................... 18
  IT Support ......................................................................................................................... 19
  Secure the Data! ................................................................................................................. 20
  Training and Awareness ................................................................................................. 21
  Stipend ............................................................................................................................ 21
  Pilot .................................................................................................................................. 22
Conclusion .......................................................................................................................... 23
Appendices

Appendix A: Surveys from industry

Appendix B: Survey results from peers

Appendix C: Survey results from U-M users

Appendix D: Survey Results from Business and Finance Town Hall

Appendix E: Standard Practice Guide (SPG) policies

Appendix F: BYOD Productivity Savings Example

Appendix G: Resources
Executive Summary

In recent years, there has been an explosion of technology that has led to the “consumerization of IT”. Devices and services historically available only in the workplace and provided by IT departments are now widely available to and affordable by consumers. The introduction of devices such as the Apple iPhone and iPad, Google Android smartphones and tablets, and lower-cost laptops has increased consumers’ appetite for the latest technology, and they crave that same technology in the workplace. IT departments typically lag behind the technology curve due to the effort to test new technologies, expense of procuring them, and the depreciation of assets which leads staff members have taken it upon themselves to bring in their own equipment. This has resulted in the Bring Your Own Device (BYOD) trend seen across most industries today.

In writing this paper, we employed a number of sources to gather data, including research conducted by Gartner and Forrester. In addition, we crafted and conducted three surveys. The first small, initial survey was completed by 290 B&F staff members. The second survey was sent to 5,002 University staff member that included the Health System to determine how Personally-owned Devices were being used today within the University. Another survey was sent to CFOs and Windows administrators from a number of Higher Education institutions to understand how other institutions were handling the phenomenon. Based on our research, the BYOD landscape is diverse and there is an opportunity for the University of Michigan to become a leader in adopting a formal strategy.

We recommend that Business & Finance pursue leadership in the following areas:

<table>
<thead>
<tr>
<th><strong>Suitability</strong></th>
<th>Encourage BYOD where appropriate for the job role and requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance and Policy</strong></td>
<td>Establish flexible representative governance to develop principle-based policies that allow for device choice and provide reasonable controls.</td>
</tr>
<tr>
<td><strong>IT Support</strong></td>
<td>Establish a flexible IT environment that includes innovative software licensing, responsive support, and infrastructure services that support doing U-M business on personally-owned devices.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Protect the data through policy, training, use of cloud services to keep data off of the devices and a robust set of tools to increase security.</td>
</tr>
<tr>
<td><strong>Training and Awareness</strong></td>
<td>Develop a training program to establish and reinforce awareness of and compliance with policies, security requirements, and HR, FOIA and legal issues.</td>
</tr>
<tr>
<td><strong>Stipend</strong></td>
<td>Provide stipends to encourage BYOD, leveraging the stipend to emphasize security, require training and enforce policy.</td>
</tr>
<tr>
<td><strong>Pilot</strong></td>
<td>Pilot with several small, diverse groups to test and measure effectiveness of recommendations and suggest changes where necessary.</td>
</tr>
</tbody>
</table>
Recommendations at a Glance

Suitability
1. Personally-owned device must be capable of performing work functions
2. Individuals who access sensitive or regulated data on device may want to keep university data separate
3. Overall job responsibilities must be suited for a personally-owned device

Governance
1. Implement representative governance including IT, security and employee representatives
2. Revamp and consolidate policies addressing BYOD into a single policy that is principle-based and not prescriptive
3. Make BYOD opt-in initially
4. Allow any device

IT Support
1. Negotiate flexible licensing models with key vendors to provide access to software on personally-owned devices
2. Create new IT capability to support personally-owned devices for work use, staffed with people that have the ability and desire to tackle the unknown, not just follow set documentation and processes
3. Continue to develop services to support BYOD and expand mobility efforts to accommodate the challenges brought by BYOD
4. Provide loaners for emergency use
5. Don't forget the network

Security
1. Integrate security policy with general BYOD policy
2. Consider a Mobile Device Management (MDM) solution to enforce security especially for devices that access sensitive or regulated data
3. Encourage use of supported cloud services to keep data off of devices
4. Provide loaners for international travel
5. Increase security awareness with training
6. Provide robust set of tools to increase security

Training & Awareness
1. Develop a BYOD training and awareness plan
2. Make it multi-dimensional, covering security, policies and IT services
3. Enforce it each year at Performance Review

Stipends
1. Use stipends to encourage BYOD and to use as a lever to enforce policy
2. Evaluate cost/benefit of instituting stipend program for tablets, laptops and other mobile devices

Pilot
1. Run pilot with several small groups of different types of users within B&F
2. Measure and validate recommendations
**Introduction**

In recent years there has been an explosion of technology that has led to the “consumerization” of what were previously IT components and services. Technology once reserved for the workplace and only provided by IT Departments is now widely available to consumers from a variety of sources such as BestBuy and Walmart. The introduction of devices such as the Apple iPhone, iPad, Google Android devices, and lower cost laptops has led people to desire the same functionality in the workplace that they now purchase for their personal use. IT departments typically lag behind the technology curve due to the effort to test new technologies, expense of procuring them, and the depreciation of assets, which leads staff members to take it upon themselves to bring in their own equipment. This has resulted in the BYOD trend seen across industries today. If you look around most meetings today, you will see a number of smartphones, tablets, and even some laptops in use - most of which are purchased by the staff member and not the University. The graph below further illustrates the point that this trend will increase at a staggering rate.

![Global Internet Device Sales](image)

The charge to the BYOD Action Learning Project Team was to provide an assessment and recommendations around key areas such as funding, policies, and security, regarding the use of personally-owned devices to access University resources. For this project, we intentionally limited our scope to University Staff members. We believe that any program developed could pertain to Faculty members with some modifications; however, in some cases their needs are different than general staff members. Students were intentionally taken out of scope as well, primarily because they have been doing this for a number of years already and there is an expectation that they bring their own. With this in mind, our paper will explore the industry trends both external to, and within Higher Education, examine the current state within our university, and provide our recommendations that we would like to see carried forward.

---

Methods

As the BYOD team researched the topic, we employed a number of ways to gather data, summarized below.

Literature Review

We began to gather data on this subject using on-line resources and technical journals such as Gartner, Forrester, Information Week, eWeek, and many others. While many of these articles were written from a corporate perspective, many of the issues and benefits easily translated into our environment, with the exception being that our network is more open than most in the corporate world.

Stakeholder Interviews

We conducted interviews with those who would be most affected by our recommendations. We wanted to capture any concerns and address them in the paper, as well as to make sure that our recommendations would not adversely impact them. We were surprised to find overwhelming support for instituting a BYOD program from those we talked to.

Business and Finance Town Hall Survey

A one-question survey was printed onto slips of colored paper and distributed to tables at the B&F Town Hall in May. We received 290 completed surveys. The single question asked what personally-owned devices are used by the respondent to do work or access work data.

U-M User Survey

The research team surveyed 5002 randomly selected University of Michigan staff members (including the Health System). The questions in this survey were crafted to understand how our own staff were using personally-owned devices to access University resources in their day-to-day work.

Higher Education Survey

The team also designed a survey to help understand how other institutions viewed the trend of BYOD and what measures they had taken to deal with the trend. This survey was sent to CFOs and Windows technologists at a number of higher education institutions.

IT Support Group meetings

We attended an ITCommons meeting and a meeting of LSA IT staff to get a sense of the attitudes of those tasked with supporting end users toward BYOD. As with our stakeholder interviews, we found general support for BYOD where we expected to hear stories of support nightmares.

Other Information Gathering

A non-trivial amount of information was gathered by the team in casual encounters throughout the ALP process. The enthusiasm of the team for the topic provided unforeseen opportunities to gather information.

The team was invited to present at a daylong BYOD Summit held by Merit Networks in E. Lansing in September. Two members of the team were able to take advantage of this opportunity, participated in panels
and heard from higher education colleagues across Michigan on their thoughts and efforts on their campuses on BYOD.

We spoke with staff of U-M Medical Center Information Technology (MCIT) and Medical School Information Services (MSIS). With the different concerns and perspective of our Health Systems, these interviews helped us understand the UMHS perspective on BYOD, including concerns about data privacy and the necessary controls in addition to the need for access.

We leveraged the personal connection of one team member to the Chicago Mercantile Exchange (CME) to host a conference call with five of their top IT personnel. The meeting allowed us to learn how this organization, with a very high security and privacy need, is dealing with the personally-owned device trend.

And last but not least, our involvement in this project sparked conversations with numerous colleagues around campus, allowing us to get their insight and perspective into this phenomenon.
Data Summary

Industry Trends

“The train has left the station.”

Many in industry are grappling with the problem of BYOD. In some respects, we are ahead of this trend. The University has been dealing with many of the issues for some time. Our open academic environment has a culture of allowing, not restricting, access. So, while industry is trying to decide whether to allow personally-owned devices past the firewall, we always have. Our task now is to formally recognize the opportunities and risks that use of personally-owned devices present and to establish guidelines, policies and practices to take advantage of the opportunities and manage and mitigate the risks.

Appendix A summarizes a number of surveys conducted by industry analysts and others.

BYOD in Higher Education

In our survey of a number of Higher Ed CFOs and a global Higher Ed IT Support listserv we received 47 responses from institutions such as Michigan State University, Indiana, Princeton, Yale, and Stanford. The responses were varied as we expected, particularly in relation to education, training, policies and procedures. Nearly all of the university respondents allow for personally-owned devices, and they also allow access to university data. Most provide some level of technical support for personally-owned devices, however most see no or limited financial impacts of BYOD. Employee satisfaction and enhanced productivity were common advantages, while data and IT security and lack of awareness is by far the largest concern. It appears most allowed BYOD before getting a handle on various security and policy risks that may be associated.

Fifty-six percent (56%) of respondents were public institutions; nearly all respondents were from the IT organization. Thirty-eight (38%) percent had more than 10,000 employees and twenty-six percent (26%) had between 5,000 and 10,000 employees.

Notable findings include:

- All respondents provide desktop and laptops; 88% iPads or tablets, 84% smartphones and 82% cell phones.
- For desktops, laptops and iPads, only one respondent (2%) stated the organization monitored for personal use. Only five (11%) monitored smartphone usage and seven (16%) for cell phones.
- Eleven percent of responding organizations stated they allow personal use on devices.
- Ninety-three (93%) allow personally-owned devices.
- Ninety percent (90%) allow some access to data. All (100%) respondents with greater than 10,000 employees allow some access to data.
- Seventy-six percent (76%) provide some level of technical support. From the comments, the types of services are variable.
- For personally-owned devices, 37% had policies regarding usage, 76% for data security, and 59% for stipends. Seventy-eight percent (78%) are considering additional personally-owned device policies (92% of those have more than 10,000 employees).

---

2 See Appendices for detailed data collected.
3 A complete list of schools responding is found with the survey data in Appendix B.
Education and training programs are varied. Respondents have just guidelines, self-service training, large education campaigns, security of data education, web-based training, “tips of the week.”

One school is developing computer based learning on their BYOD policy to ensure adherence to policies as well as FERPA, HIPAA, GLBA, FISMA, Red Flag, FDA part 11, and PCI. In addition, they will use emails, flyers, and website postings, to reinforce BYOD security principles, including mentoring regarding safe data practices.

Regarding the financial impact (effort, dollars) of personally-owned devices, 86% estimated it to be low or none, compared with 14% that said the costs were high.

Some of the advantages noted by respondents: employee satisfaction, enhanced productivity, improved communications, mobility, some reduced institutional expense. The most noted disadvantage was security and security awareness.

See Appendix B for complete results.

BYOD at U-M

U-M Staff Survey

We distributed a survey to 5002 randomly-selected U-M staff to get an understanding of the current level of BYOD practice on campus. 941 complete responses were received. Several interesting observations arose from that data, including:

- 21% of respondents indicated that their department does not provide any of these communication/computing devices for them
- 71% of staff are using their own devices for work with the primary driver being convenience. The average number of devices per person is 1.8.

The following data applies only to those who reported using their personally-owned devices for work.

- The most common personally-owned device was the smartphone (46%) followed by laptops (38%) and tablets (20%). We expect the number of personally-owned tablets to grow as these devices become more common and affordable
- Most people (81%) use one or two personally-owned devices for work, with an average of 1.8 devices per person. This trend of more than one personally-owned device per person (primarily mobile devices) added to the mobile university-owned devices has implications for the scale of the wireless network on campus.
- Convenience was by far the most common reason to use a personally-owned device for work. This aligns with industry data that indicates that convenience and productivity are the two biggest reasons to have a BYOD program. While the survey did not address productivity directly, the majority of the comments provided under “other reasons” are about the ability to work from home, after hours and from anywhere, leading to increased productivity.
  - Faculty, research and student staff said that their unit can’t/won’t buy a device more than administrative staff did.
  - Faculty and student staff preferred a less restrictive device more often than administrative staff.
  - Student staff were more concerned about privacy of activities and data than other staff.
- Most users are not reimbursed for using their personally-owned devices for work indicating that compensation as an incentive for using personally-owned devices is not necessary.
  - Staff in administrative units are more likely to be reimbursed (15%) than staff in academic units (3%)
- Staff access email and browser-based applications most frequently on their personally-owned devices.
If this trend continues, we can focus on providing access to University resources through the browser
and making sure those apps are secure. However, the 43% that access other applications needs further study to understand the risks

- Staff reported high voluntary adoption of security measures (85% using password/pin, 51% using automatic lock, 43% using anti-malware software, 33% using VPN, 14% with remote wipe capability), showing that staff are aware of the need for security on their personally-owned devices and are tolerant of inconvenience presented by these measures. It indicates that staff may be receptive to registering their devices with a mobile device management (MDM) solution to increase the ease of securing their devices.
- Supporting their devices requires very little to no work time for 99% of them.
  - More staff in academic units use work time to support their devices (43%) than those in administrative units (28%).
- Most staff (89%) receive little or no IT support for their devices.
- Most staff (93%) who use personally-owned devices for work perform work outside of their normal working hours. This can be an opportunity for increased productivity but also has HR implications.
- 70% of staff save time (and are therefore more productive) by being able to use their personally-owned device for work.
- Supporting their devices requires very little to no work time for 99% of them.
- Most staff are not getting support from IT.
- Staff are voluntarily using various security measures, the most used being passwords/PINs, anti-malware and automatic lock.
- Staff who use their personally-owned devices for work are receptive to new technology (51% welcoming and 35% enthusiastic) indicating that enabling BYOD rewards staff who are forward thinking and interested in trying new things - traits to be encouraged in our current atmosphere of nearly constant change.

See Appendix C for complete results.

**Business and Finance Town Hall Survey**

290 B&F staff members responded to a one-question survey at the B&F Town Hall in May. In response to the question “How many personally-owned devices do you use to do work or access work data?” only 7% did not use any personally-owned device for work.

- Most people use 1, 2 or 3 different devices (32%, 32%, 21% respectively) and some (8%) use 4.
- Those responding use personally-owned laptops, desktops and smartphones in approximately equal frequency (28-29%), with about half as many (14%) using tablets, showing how quickly work use ramps up for new types of computing devices.

See Appendix D for complete results.
Stakeholder Analysis

We began by considering who on campus would have an interest in this topic. We were amazed when we completed our analysis and decided that the answer was ‘pretty much everyone’. The following diagram illustrates the campus constituents we interviewed to get a complete picture of the BYOD concerns at the University of Michigan.

As the stakeholder map indicates, we heard overwhelming support for BYOD. All recognized that BYOD is already happening on campus. Each had a different take on the trend, with most seeing opportunities but also recognizing concerns. All of them were enthusiastic about our project and glad to see that attention was being paid to this topic, but some cautioned us about legal risks and uncertainties.

Policies in the Standard Practice Guide

Several University policies relating to BYOD cover security, privacy, and proper use of University resources, including data. These policies, with the exception of Standard Practice Guide section 514.04 (Tech Tools: Cell Phones and Portable Electronic Resources), were written before BYOD was even a concept and are past their review dates. While not framed as a BYOD policy, SPG 514.04 addresses crucial aspects of personally owned devices in the workplace such as funding. It does not address the other elements and impacts of BYOD discussed here.

A new SPG section Security of Personally-Owned Devices that Access or Maintain Sensitive Institutional Data is currently in draft pending approval. The authors of this policy and the Tech Tools policy indicated in stakeholder interviews they were unaware of the work each other was doing on their respective policy, despite the clear link between the topics.
Appendix E enumerates SPG sections that touch on issues related to BYOD while pre-dating the start of the trend. This list, which may not be complete, is meant to illustrate the wide-reaching impact of BYOD on University policies.

Current IT Services that Enable BYOD

Information and Technology Services and local unit IT groups already provide services that enable access to data and services by personally-owned devices. The availability of these services puts us ahead of the curve in enabling BYOD, because the University culture has always been to provide access to data and resources beyond the campus boundaries. These services were designed to provide access from stationary and mobile devices to University resources. As such, they are great resources for access to University resources from personally-owned devices. These services are already being used by the University population to access University data and some have the potential to being improved to provide even better support of BYOD.

The services described below are restricted to University faculty, staff and students (with some available to alumni and retirees) and require authorization through a UMICH uniqname and password. Nevertheless, the security of these services should be reviewed in the context of being used on personally-owned devices.

Virtual Private Network (VPN)

ITS provides a Virtual Private Network (VPN) service to allow the campus community to access resources normally restricted to the campus network from off campus, providing encrypted access for all network-computing needs. Windows and Mac OS X are supported and provide access for laptop and desktop computers, whether University or personally-owned. Software and information are also provided for Linux, iPhone, iPod touch and iPad, but is unsupported. The VPN appears to be unavailable to Android phones and tablets.

Wireless

Wireless connectivity to the campus network is available in three flavors

- **MWireless** is the most secure and WiFi network. Once the device is configured to use MWireless, all transmissions are encrypted and secured with your UMICH password and there is no need to re-authenticate on each access.
- **UM Wireless** is an alternative for devices that do not meet the technical standards required by MWireless. It is less secure and less convenient than MWireless.
- **MGuest** is a WiFi network provided for University visitors. it is a limited, open network with no encryption.

MWireless is supported on modern Windows and Mac operating systems, Apple mobile devices (iPhone/iPod touch/iPad) and Android devices. This will cover most personally-owned devices. Information on connecting with other less common operating systems that are capable of working with MWireless is provided, although unsupported.

Desktop Virtualization (VDI)

ITS’ VDI service provides the hosting infrastructure for virtualizing Windows desktops. It enables remote computing and thin client access from any Internet-connected device. This service is available for campus units to leverage. If a University employee’s unit is utilizing this service to provide virtual desktops to their

---

4 [http://www.itcom.itd.umich.edu/vpn/](http://www.itcom.itd.umich.edu/vpn/)
5 [http://www.itcom.itd.umich.edu/wireless/](http://www.itcom.itd.umich.edu/wireless/)
6 [http://www.itcs.umich.edu/virtualization/desktop/](http://www.itcs.umich.edu/virtualization/desktop/)
users, their users will be able to access the desktops and installed software from their personally-owned device.

**Virtual Sites**

Campus Computing Sites provides a rich computing environment for University students, faculty and staff at physical locations across campus. Through Virtual Sites, you can use the software on Campus Computing Sites Windows computers remotely from any Mac or Windows computer with an Internet connection.

Virtual Sites offers a standard Windows 7 desktop and several specialty sites, providing limited access to specialized software applications in addition to the standard Sites software. Virtual Sites is built on the VDI service described above.

**Terminal Services**

Some campus units provide terminal servers for users to connect to, providing remote access to a Windows desktop. An example of this is the B&F mr1 and mr2 servers, available to B&F staff. The availability and support of this type of service will vary with campus unit.

**M+Google**

The University’s collaboration suite, provided by Google, provides lots of opportunities for BYOD. Because it is built on technology developed for consumers, the ability to easily access the data stored there from anywhere on the Internet is baked in. On one hand, this is ideal for BYOD, as the data is stored in the cloud and accessed from an Internet-connected device. There is a downside, though, in that Google also provides the ability to sync data, including email, calendar, contacts and documents, to many devices. In addition, setting up a mobile device to access Google data generally includes storing the UMICH password on the device.

**M+Box**

M+Box provides 50GB of file storage to all U-M students, faculty and staff. Box is similar to Google in that it was designed for easy access from any Internet connected device, including synchronizing the data to computers and apps for access data on mobile devices. It provides many of the same benefits and risks to BYOD.

**MPrint**

MPrint provides the ability for the university community to print from a computer or mobile device from a computer or mobile device after logging on with uniqname and password. MPrint provides a simple way to print documents stored on your computer or in Box. You can even print documents stored in Box from your smartphone.

When a full mobile-friendly version is released (November/December), it will support the full feature set that the non-mobile version of MPrint supports, with the exception of uploading a job. You will be able to submit jobs from a service (Box, Dropbox, AFS and MPrint Locker), manage and view job status (cancel jobs) and see queue information (location, health). A user should also be able to see their allocations and usage. Support staff will be able to perform more actions (disable queue, cancel any/all jobs) and see more information about a queue (IP, support tier info, etc.). These functions will be supported in both the legacy/student system as well

---

7 [http://virtualsites.umich.edu/](http://virtualsites.umich.edu/)
8 [http://google.umich.edu](http://google.umich.edu)
9 [http://www.itcs.umich.edu/storage/box/](http://www.itcs.umich.edu/storage/box/)
10 [https://mprint.umich.edu/](https://mprint.umich.edu/)
as MiWorkspace. We will also take advantage of QR codes on printers for release of jobs, ‘Follow Me’ and ‘MPrint Locker’.

**MiApps**
A component of the NextGen MiWorkspace project, MiApps provides access to Windows applications from any browser to subscribers of MiWorkspace. Through this service, the application runs in the browser and enables the user to open and save files to U-M-hosted file servers. This service differentiates itself from other virtualization services (see VDI, Virtual Sites and Terminal Services above) in that it is accessible from just about any device. No client needs to be installed; only a compatible browser is required.

**Michigan iOS and Android apps**
Mobile apps developed around campus are available through the U-M Mobile Apps website. The huge overlap between mobility and BYOD make this new effort a big win for personally-owned devices. The number of U-M-specific apps will only continue to grow, making mobile devices, both University- and personally-owned, ever more functional for performing work.

**MCommunity**
This robust enterprise directory service provides a basis for securing via authentication and authorization access to University data. This important piece of infrastructure is critical in securing data accessed by personally-owned devices.

**University of Michigan Health System (UMHS)**
Jack Kufahl, Director of the Medical School Information Services Solutions Center, said that UMHS is seeing the Health System device to user ratio is around 7:1. Medical Center Information Technology (MCIT) currently has about 26,000 managed ‘core image’ devices with another 8,000 or so mobile devices. The Health System has about 36,000 appointments (excluding volunteers and dry appointments), so that could mean there are up to 252,000 devices hitting the UMHS network which "on paper" means that the Health System manages about 10-20% of those devices. Not all of those devices should be managed but it is hard determine until we have a service model that accommodates it.

The UMHS approach is to support based on use and roles, not on platforms and ownership, managing the service to their users better so they can help with their data and data use. To that end UMHS has been re-negotiating software contracts, setting up a new service desk support model focusing on role support rather than purely technology support, and partnering with MCIT/MiChart on a virtualization infrastructure to help operationalize the BYOD world.

Melissa Minuth, MCIT Business Systems Analyst, spoke to us about a Mobile Device Management (MDM) RFP. MCIT plans to use the product to manage both UMHS-owned and personally-owned devices that access UMHS services. The recent introduction of MiChart will provide leverage to encourage UMHS staff to register their devices, both university and personally owned, to the future MDM service. Mobile access to MiChart will be available only through the MDM software. Data is not stored on, only accessed from, the device which additionally protects the data in MiChart. With their focus on use and roles, there is no list of supported devices, although minimum operating system levels are required.

---

11 [https://miapps.it.umich.edu/](https://miapps.it.umich.edu/)
12 [http://mobileapps.its.umich.edu/apps](http://mobileapps.its.umich.edu/apps)
13 [https://mcommunity.umich.edu/](https://mcommunity.umich.edu/)
14 [http://revcycle.med.umich.edu/michart](http://revcycle.med.umich.edu/michart)
Mobile Device Security Guidance\textsuperscript{15}

ITS Information and Infrastructure Assurance group has already been thinking about the challenges mobility brings to security. They provide a web site and a paper document providing guidance and links to tools to better secure a variety of mobile devices, including smartphones, tablets and laptops, the most common personally-owned devices used for University business. The guidance provided applies equally to university-owned and personally-owned equipment, but it is especially important to make sure this information is disseminated and communicated well to people using their own devices.

Sensitive Regulated Data: Permitted and Restricted Uses\textsuperscript{16}

This Information Technology Standard, published by the Office of the Chief Information Officer, describes types of sensitive regulated data and University data repositories that are appropriate for their storage. This is important for BYOD because some of these data repositories are readily accessible from personally-owned devices.

\textsuperscript{15} \url{http://www.safecomputing.umich.edu/MDS/}
\textsuperscript{16} \url{http://cio.umich.edu/policy/sensitive-regulated-data.php}
Analysis

Spectrum of Options

Our analysis has found that there are a number of approaches to managing the BYOD trend that range from prohibiting the use of personally-owned devices to requiring that employees purchase their own device, with many different perspectives in between, as illustrated below.

Based on a conversation with Laurita Thomas, AVP for Human Resources, TIAA-CREF is an organization currently utilizing the “prohibit” side of the spectrum. We also talked with members of The Chicago Mercantile Exchange (CME Group) who were also on the “prohibit” side of BYOD but recently recognized the increasing need for their executives to have the flexibility to use data on their personal devices. While the CME group is only six months into this new venture, they are already proving the worth of such a policy. They continue to explore ways to keep the data secure in an increasing data threat environment. For the University, a prohibitive environment would mean taking a step backwards since students, faculty and staff are already bringing their own devices to work. To prohibit these devices would be an unrealistic option for the University.

While the University did not plan to be in an “allow” or “enable” stage of this spectrum, this is indeed where we currently are. The Information Technology Services areas have been supporting these personally owned devices for a while now and there are a large number of employees who are indeed performing some of their work functions using their own laptops, tablets and phones. Employees who are utilizing the Information Technology Services areas for their own devices have stated they have received good customer service.

Moving along the spectrum we come to the “enable” and “encourage” approaches which recognize that BYOD is here and increasing in demand. This is where our group believes the University should be heading. We recognize by aiming toward this part of the spectrum we need to establish some reasonable policies which allow the employee and the University to be able to work successfully, striving to fulfill the University mission.

On the far right of the spectrum is the required option. This approach requires an employee to bring their own laptop, tablet or phone to work in order to perform their work functions. The University recently moved towards this end of the spectrum in the Tech Tools policy.
Benefits and Risks

Benefits of BYOD

Two primary benefits of allowing personally-owned devices to be used for work were seen consistently in both the literature review and in our own surveys and conversations with campus staff - employee satisfaction and productivity.

Employee Satisfaction

Industry research and our own surveys indicate a primary benefit of BYOD is employee satisfaction. When employees are able to choose their own device, they enjoy using it more and are more likely to spend time exploring it and understanding it. They are less likely to require technical support, and when they do receive support from University staff, they are more appreciative of it, perceiving it as more personal instead of just supporting the device.

Increased Productivity

In our survey of other Higher Ed institutions, we asked what the responders thought were the advantages (and disadvantages) of BYOD, and 34% (10 of the 29 responses) indicated productivity increases as an advantage of allowing personally-owned devices for work use. Our user survey also indicated that BYOD results in increased productivity. Of the 941 university staff members responding to our survey, 70% of the U-M staff surveyed reported that they saved time using their personally-owned device for work - anywhere from 1 to more than 10 hours per week. Our survey found that 56% of staff saved 1-5 hours a week, 9% saved 6-10 hours a week and 5% saved more than 10 hours. Using these results extrapolated on 2,500 U-M staff at an average salary of $35/hour, the productivity savings would be approximately $15.3 million. Along with productivity, there are employee satisfaction improvements with staff using their own devices. Clearly, these results must be analyzed further.

Cost Savings

A tertiary benefit inferred from our survey data indicates that costs could be lower with BYOD. People feel more invested in the technology when they are able to choose it for themselves and are willing to put in more effort to learn and support it. At the same time, they spend little to none of their work time supporting these devices. Additionally, most staff do not depend on IT personnel to support their devices. Cisco reported that they saved money with their BYOD program, primarily by reduced support costs.

Additional cost savings can be realized as adoption of BYOD increases, even in cases where a stipend is given to employees (provided it is less than the cost of a machine to the University). The University saves not only on acquisition costs, but also on the ancillary costs such as inventory management, costs to load software, costs for spare parts, etc. In Fiscal Year 2012, data obtained through Procurement Services indicated an approximate spend of $5,473,933 on 3416 laptops through Purchase Orders. Another $115,352 was identified as being purchased via P-Cards for another 77 laptops. These purchases included models from Apple, Dell, HP, Lenovo, and others that could not be readily identified. Based on this information, the average cost per laptop in FY ’12 was $1600. It is important to note that the current average cost of a laptop is now

17 See Appendix F for details
18 Data obtained was for the University overall for FY’12
19 These amounts are estimates, with this being more of the minimum, as the vouchers do not include model or manufacturer for identification. All identification has been determined by the item description. All of the ITS Showcase PO vouchers are excluded as these are “cost of goods” and not departmental purchases. The ITS Showcase SUB vouchers are included, as those are the department purchases from Showcase.
$1077.13. For example, using the current pricing, if the University were to provide a stipend of $500.00 for each mobile employee who participated in a BYOD program and roughly 30% of the laptop users participated, the University would see a savings of ~$500,000.00 in acquisition costs alone.

While the University is already experiencing some of these benefits, a program that moves from simply allowing personally-owned devices at work to one that enables and encourages it with a well-constructed BYOD program can amplify these benefits.

Risks with BYOD

There are three main categories of risks associated with BYOD: Security, HR and Financial.

Security

Our survey of CFOs from other institutions of higher education revealed concern around security of personally-owned devices. Fifteen of twenty-nine respondents (51%) indicated that security was the greatest shortcoming of BYOD. In most cases, the concern was centered around the security of data, since that is the institutional asset at risk. The risks associated with increased mobility of institutional data via university-owned mobile computing devices have been with us for many years. BYOD has reawakened us to those risks by reinforcing the drive toward mobility.

The pending Standard Practice Guide section on **Security of Personally-Owned Devices that Access or Maintain Sensitive Institutional Data**, drafted by IIA, identifies several security risks associated with BYOD.

- Inadequate security safeguards implemented on personally-owned devices
- Employees retaining sensitive institutional data on personally-owned devices after they have changed roles or left the institution
- Lost, stolen, misused, or hacked devices not reported as a security incident
- Impairment of the University’s ability to fully investigate security incidents when it involves a personally-owned device

U-M staff indicated in our survey that they are implementing security measures on their personally owned devices. Eighty-five percent of respondents use a password or PIN to protect their devices. About half use their devices’ automatic lock feature. These findings are promising, as they indicate staff are relatively comfortable implementing security measures on their personally owned devices. However, some uncertainty remains. We do not know whether the individuals who are accessing sensitive institutional data from their devices are the ones implementing these safeguards. We also have no assurance apart from the staff member’s word that these safeguards are in place and configured to provide meaningful protection.

---

20 Based on an average cost of Apple and HP laptops available through M-Marketsite on 11/16/12
HR

It is important to consider the impact bringing your own device to work could have on the legal and human resources side of administration. The Freedom of Information Act (FOIA) requires that certain documentation, including emails, texts, files, data, etc., are subject to outside review. If this information related to the business of the University is on personally owned devices, the University must have a policy in place which enables the gathering of such information while not invading the employee’s outside of work information.

Managers will need to understand and implement ways to ensure employees utilizing their own devices understand their responsibilities and respect their workload. This is most important when working with non-exempt employees under the Fair Labor Standard Act (FLSA) since the University is required by law to report hours to the nearest tenth of an hour. Employees who utilize their personally owned devices at work tend to continue to do so after hours which could place the manager into a situation where overtime must be paid. Managers also have the responsibility to monitor the workload appropriately since employees who utilize their own devices may tend to blend their outside life into their work schedule.

We need to be mindful of the potential view of inequity related to stipends and household incomes. While the University cannot determine or inquire of an employee’s household income, if a stipend provided to employees is the same amount, an employee who has a lower household income may not be able to afford the same high-tech personally owned device as an employee with a higher household income. One way to avoid this particular situation is to allow the employee the choice of purchasing their own, or using a University owned device.

Financial

There are financial risks that should be considered when implementing a BYOD program. These include any increase in infrastructure, support, and security costs. Purchasing discounts for University-provided devices (such as the HP contract) would need to be reviewed if contract volumes are not achieved. For example, our research found one company who experienced an increase in cell phone carrier costs because with users choosing their own, they were not able to leverage savings of a volume contract.

Risk Mitigation

Since people are already using their own devices for work, we have an opportunity to reduce the risks already present. In addition, many of the risks and concerns around BYOD are already there with University-owned mobile devices. The BYOD trend is increasing the visibility of these risks and providing an opportunity to mitigate them.
Recommendations

The BYOD team recommends that the University of Michigan “enable and encourage” the use of personally-owned devices for work purposes wherever possible. Our research has shown that the University has a great opportunity to be “The Leaders and The Best” by instituting a comprehensive BYOD program that allows employees to use their personally-owned devices for work purposes. We recommend that any program should address the following areas:

Suitability

It is important to note that not every employee’s work responsibilities are going to be suitable for BYOD. For example, employees who handle sensitive or regulated data may not be good candidates for using their personally owned devices. Some employees may feel they need to keep their work and home life completely separate. Others may require specialized equipment or software that would be too expensive for an employee to purchase on their own. Policies and their enforcement should depend on the business purpose and departmental needs. It is also very important to emphasize that any personally-owned device must be capable of performing the tasks necessary for the employee’s job.

Governance and Policy

Currently there are University policies governing the use of personally-owned devices for work\textsuperscript{21}, but they address specific areas and have not kept up with the current trends. In addition, existing policies are not built around a comprehensive program regarding the use of personally-owned devices. In fact, policies dealing with different aspects (such as stipends and security) are often developed without knowledge of each other. We recommend that:

- As part of a BYOD program, establish a flexible, representative governance system. Technology is changing rapidly and it is unrealistic to have policies that take years to approve. We must have a governance structure that can quickly adjust to changing landscape (remember: the tablet as we know it is only 2 years old and already has huge adoption) and considers all aspects from a variety of perspectives (ex. Finance / Purchasing, IT Support, etc.). Because BYOD touches many areas including IT, Security, HR, Legal and Finance, governance must be representative of these interests.

- Ensure that any policies developed that have implications for BYOD are “principle-driven”, rather than “prescriptive”. Policies that attempt to prescribe the list of technologies covered or are similarly detailed are typically out of date by the time they are approved due to the ever changing technology landscape. A governance structure will also facilitate the communication of policies so that they may become more holistic in nature. Examine existing SPG’s that touch on BYOD for revision or incorporation into a comprehensive BYOD SPG.

- Make the BYOD program opt-in. Not every employee is comfortable with choosing and supporting their device and not every job function is a good fit with personally-owned devices. This is important to gain the benefit of reducing the amount of support seen in our user survey where 99% reported using little to none of their work time to support their device\textsuperscript{22}.

\textsuperscript{21} See Appendix E
\textsuperscript{22} See Appendix D
• Allow the employee to use a device of their choice, as long as it is able to perform the required work functions. The two primary benefits of BYOD found in our research are increased productivity and employee satisfaction23. These benefits are maximized by allowing the user to choose their devices. Since technology changes today faster than University IT departments can keep up with it, allowing the user to choose their device benefits the University by putting the newest devices in employees' hands much more quickly.

Given the current popularity of the BYOD trend, there are a number of good references for creating BYOD policy. Of particular value are those that do not provide a template per se, but rather present a number of questions that need to be considered when developing BYOD policy. See Appendix G: Resources for some of the more valuable resources we found. While some of these resources are written by vendors pushing their product, they also identify many of the issues that need to be considered when developing BYOD policy.

IT Support
The University of Michigan has been supporting personally-owned devices through the many services that support mobile computing. We recommend that this support continue and expand, and that conscious attention be paid to the need for personally-owned devices to leverage it. Specifically, we recommend:

• Negotiate or renegotiate flexible licensing models with key vendors to provide access to software on personally-owned laptops. While this could extend to mobile devices as well, many mobile apps are inexpensive and may not need subsidy. However, it should be noted that more robust apps may need to be subsidized or purchased by the University. Therefore, who pays for what apps may differ depending on the situation. Any license tracking must take this into account as well.

• Create new IT capability to support personally-owned devices for work use, staffed with people that have the ability and desire to tackle the unknown, not follow set documentation and processes. Campus IT staff reported that supporting their users' personally-owned device generates greater customer satisfaction since many don't expect it and that the service feels more personal. It is also important to note that in our research we also found that almost all (99%) say that it takes little to no work time to support their own device.

• Continue to develop services to support BYOD and expand mobility efforts to accommodate the challenges brought by BYOD. As described above, the University already provides a wide array of infrastructure support that is leveraged by personally-owned devices. As further IT services are developed, conscious attention should be paid to how these services support BYOD. In particular, we see opportunities in the following areas:
  ○ accelerating Mobile application development
  ○ providing Virtualization options for accessing secure data
  ○ expanding the MiWorkspace depot service to provide emergency (short-term) loaner equipment in the event that a personally-owned device is out for repair

• Don’t forget the network. A greater emphasis should be placed on the wireless network across campus. Today, many people carry between 2 and 5 mobile devices24 and industry predictions are that this trend

23 See Appendices A, B and D
24 See Appendices C and D for survey results from campus employees
will continue\textsuperscript{25}. With traffic from these devices going over the 3G / 4G (cellular) networks as well as the wireless networks, attention must be paid to both of those infrastructures on campus. While the campus network infrastructure is robust, with each of these devices requiring an IP Address, the wireless infrastructure in some buildings is strained. We heard reports that in some buildings the unit-provided wireless infrastructure was taxed. While the core network infrastructure is capable of handling the load, wireless capability in specific locations needs to be addressed.

Secure the Data!

Next to its people, data is one of the University’s greatest assets. “Sensitive Institutional Data”\textsuperscript{26} must be safeguarded particularly well, since inappropriate disclosure could cost the University competitive advantage and expose the University to fines, lawsuits, and penalties. Sensitive institutional data is the focus of the pending Standard Practice Guide section on \textit{Security of Personally-Owned Devices that Access or Maintain Sensitive Institutional Data}, drafted by IIA.

- A BYOD program should seek to reduce the storage of data on devices by actively promoting use of University-approved cloud-based and on-premise IT services that fit the sensitivity of the data. This will ensure that data is securely stored, preserved, and accessible to the University.
  - Data stored primarily on the device increases the magnitude of loss should the device be lost or stolen (barring any mitigating controls), and is not readily accessible by (or perhaps even known to) U-M management, and may not be securely and reliably backed up.
  - Data stored in non-approved cloud services, in addition to being inaccessible to management, does not have the protection of a University-vetted contract and may not be appropriate for sensitive institutional data.

- A mechanism for selective, verifiable enforcement of security safeguards on devices accessing sensitive institutional data should be implemented. At a minimum it should be used to provide the security assurance sought by research sponsors, government agencies, and other partners who entrust their data to the University. Based on both guidance from Gartner\textsuperscript{27} and informal benchmarking against Big Ten peer institutions, the enforced safeguards should minimally encompass a password/PIN requirement, automatic lock after a reasonable period of non-use, and remote wiping of lost or stolen devices. Enforcement could be carried out through Google Apps Mobile Management\textsuperscript{28} or a dedicated Mobile Device Management (MDM) system.

- Users accessing sensitive institutional data, if not subject to safeguard enforcement, should be required to certify that they will implement these recommendations themselves, as well as make their devices available for FOIA, legal discovery, and any other process that requires the device’s contents to be inventoried or searched as permitted in the \textit{Security of Personally-Owned Devices} SPG.

- The University should protect employees traveling with a laptop on University business outside of the United States by providing loaner equipment. Some units in the College of Literature, Science, and the Arts issue a loaner laptop loaded with the minimum data necessary for the trip, and wipe it free of any malicious software upon its return to protect University networks from exposure. The Office of Investments, on the other hand, keeps spare devices ready for dispatch to international travelers after their device has been lost, stolen, infected, or damaged, keeping travelers productive.


\textsuperscript{26} See Glossary

\textsuperscript{27} “Address the Risks of BYOD Within Higher Education” (G00235518). Gartner, Inc. 11 July 2012. Retrieved from http://www.gartner.com/id=2079115

\textsuperscript{28} http://support.google.com/a/bin/answer.py?hl=en&answer=1408902
Training and Awareness

The University’s diverse, open computing environment compels users to protect themselves by making smart, informed choices. A U-M BYOD program should reflect this by educating participants on the risks and best practices around BYOD in a variety of venues and formats. Initial training should take place when users opt-in to the program and/or at new employee orientation. Participants should refresh this training each year, perhaps at the time of their annual performance review. Ongoing security awareness efforts targeting the overall campus population should also include BYOD issues.

The message and materials should address potential Freedom of Information Act and other legal obligations and should educate managers on the implications of after-hours use, impact on remote work agreements, and other priorities. Units with special concerns may need to augment this training with material that speaks to their unique environment. A significant portion of the material, however, should be devoted to securing mobile devices, such as:

- **Basic physical protection** - Laptops are stolen regularly across all U-M campuses.
- **Encrypting and backing up data** - Backup is crucial to prevent data loss when a missing device must be remotely wiped.
- **Reporting lost/stolen devices to U-M** - The University has a stake in the loss, too, if the device contained or accessed sensitive institutional data.
- **Using remote locating services or apps to find a lost device** - Smartphones and tablets come with these built in, but they can’t help if you don’t know how to use them.
- **Using the U-M VPN on public Wi-Fi networks** - These convenient “hotspots” may conceal malicious eavesdroppers.
- **Recognizing reputable apps** - Especially important for Android devices, since malicious apps have been distributed through official channels like the Google Play store.

Stipend

The University should institute a stipend program to encourage the use of Personally-owned devices. This would include extending the existing Tech Tools policy to include devices such as tablets and laptops (and any other devices that appear in the future). The stipend program would apply to users who demonstrate a need for a mobile device. For users who do not have a need for mobility, the University will still provide a desktop, but would not provide a stipend for a secondary mobile device that the user might bring. The principle here is that the University would only pay for one device, unless the unit requires the employee to have more than one as a part of their job description (ex. on-call personnel). Any stipend should be directly tied to compliance with all of the policies implemented or any future policies developed. Based on current offerings from the University catalog (M-Marketsite), the average cost of a laptop is $1077.13\(^{29}\). An example stipend program might provide a 50% stipend (in this case ~$500.00) to mobile users every 4 years. This would result in a linear savings to the University for acquiring equipment and a predictable spend moving forward.

At some point in time, depending on the rate of adoption, the stipend program could be withdrawn similar to the way that Internet connectivity and cell phones were handled in the past. At one point he University paid for the device / connectivity, but as the technologies became more ubiquitous, we moved to a stipend model and then finally withdrew the stipend.

\(^{29}\) Includes Apple and HP offerings.
Pilot

For a successful BYOD program, a pilot program must be implemented in several units within B&F to test and measure the above recommendations. The most important aspect of implementing any new program is to test it to be sure it works as expected. Initially, we recommend measuring and evaluating the level of employee satisfaction/productivity, financial impact (What are the direct costs for stipends, increased IT capacity, additional IT security software hardware or other necessary solutions?), and policy effectiveness and adherence. (Do policies need to be updated, changed? What areas of weakness in internal controls exist? What is too rigid or prescriptive?) We also recommend that IT support and security controls be tested and evaluated in a BYOD environment at the U-M. (Where are the deficiencies? What additional stresses are there? What additional controls are necessary?). The pilot will help flush out issues, identify weaknesses and opportunities, and strengthen the overall U-M BYOD program before rolling it out.
Conclusion

Bring Your Own Device (BYOD) symbolizes the maturation of computing technology. The tools have become simple, reliable, and inexpensive enough for the user community to adopt, learn, and implement with much less IT management and support. Personally owned devices are not right for every person or every work situation. But when BYOD is a good fit, freeing staff to choose that option can save the University money and increase those staff members’ workplace satisfaction. A pilot program would validate the costs and benefits of BYOD for Michigan staff and evaluate program controls and the need for staff incentives. This information is crucial for building an accurate business case.

The University has always embraced diverse technologies, believing that teams and individuals know best which tools fit the task at hand. BYOD expands Michigan’s opportunity to apply that philosophy to promote dynamic forms of collaboration that will lead to innovations and efficiencies. The University is asking staff to do more with less so that precious resources are preserved for Michigan’s core mission. The flexibility of BYOD, combined with lean and modern NextGen technology services and a modest set of risk-based controls, will help us achieve that goal.
Appendices

Appendix A: Surveys from industry

2012 Consumerization of IT Survey, Information Week

Executive Summary
“Our second annual InformationWeek Consumerization of IT Survey shows that IT leaders are realizing how the consumerization of IT can be good a thing for the enterprise. Fifty-six percent of companies now consider themselves proactive toward or accepting of consumer-centric tech; two years ago, just 32% did—that’s a 24-point swing. A whopping two-thirds of companies cite positive benefits related to consumerization, and only 2% say it pulls IT from its strategic focus. Apple is now a true enterprise player, with iPhones, Macs and iPads each supported by more than half of companies, up 10 percentage points or more from two years ago. We also see increased use of the types of applications that demand tech-savvy end users, such as IM, video conferencing and enterprise social networking.

“So is this the dawn of a new era, when we finally blend the best of business and consumer tech into a seamless whole? Unfortunately, no—and that’s IT’s fault because we’re slacking on support, even as consumerization expands. Just over half of companies provide some level of technical support to end users connecting personal devices to the network, but that’s almost identical to two years ago. Another 23% still “officially” say no, but end users call in anyway (likely with spotty results). The rest leave employees on their own.

“That’s not smart, considering that security still dominates worries about the consumerization of IT, cited by 59%, up a tick from 2010. Concerns about not having the support staff and budget to help end users adopt technology have fallen, but they’re still cited by more than one-third of respondents. And about a quarter say end users have better technology at home than at the office, up six points from two years ago.

“Netting it out, though, we see IT embracing consumer tech for employees more than it’s fighting it. The tension from that won’t go away. Personal tech favors convenience over security, individual applications over a grand system design, and short-term fixes (and costs) over long-term investment. Here’s the latest on the consumerization of IT and how you can take advantage on your terms.”

Consumerization Survey Report: The Consumerization of IT, Trend Micro

Survey Highlights
- 56% of companies worldwide (75% in the U.S.) allow employees to use their own devices at work
- 63% of companies polled have installed security software on employee-owned devices
- 74% of respondents say companies should offer full (38%) or limited (37%) IT support for employee-owned devices

---

2012 Healthcare Mobility Trends: Survey Results, Aruba Networks, Inc

Survey Highlights
- 85% support their physicians’ and staffs’ use of personal devices at work
  - 53% currently limit users to Internet access only
  - 24% provide limited access to hospital applications
  - 8% enable full access to the hospital network with user-owned devices
- 50% are planning to expand/refresh their Wi-Fi network in the next 12 mos.
  - 35% said the same for their wired networks
  - 93% reported that they owned and managed their own network infrastructure vs. outsourcing
- 83% support the use of Apple iPads on the network
  - 65% support iPhones and iPod touches
  - Blackberry use still outpaces Android-based devices in health care, with 52% supporting the former and 46% support Android tablets and/or phones
- 58% currently use or plan to use desktop virtualization solutions such as Citrix to enable hospital application use on iPads
  - 45% said they would use in-house or third-party applications
- 60% are supporting EMR applications on mobile devices
  - PACS, Secure Messaging, and Voice over IP (VoIP), were each in the 30% range

Impact of Bring Your Own Device on Enterprise Security, AirTight Networks

Survey Highlights
- 87% think the use of personal smart devices is somewhat or very pervasive in their enterprise
- 61% view the BYOD trend as both a threat to enterprise security and an opportunity to reduce IT costs and increase employee productivity
- 64% support applications users are using on their personally owned devices, at least those directly related to the business
- 78% enforce security policy for managing BYOD with one or more system(s)

Good Technology State of BYOD Report

Key Findings
- Highly Regulated Industries Embrace BYOD: Large companies from the Finance/Insurance and Healthcare industries dominate the overall BYOD picture, with Retail/Wholesale and Government less likely to support BYOD, at least right now.
- Big Companies Get BYOD: 80 percent of those supporting BYOD have over 2,000 employees; 60 percent have over 5,000 employees; and 35 percent have over 10,000 employees.
- Employees Are Willing to Pay for Personal Choice: 50 percent of companies with BYOD models are requiring employees to cover all costs - and they are happy to do so; 45 percent provide their

---

employees with a stipend or "expense back" option to help subsidize the cost of their mobile device or service plan.

- Offering BYOD Stipend Increases Adoption: Companies that offer BYOD stipends have the highest rate of employees using mobile devices when compared to companies that require employees cover all BYOD costs themselves, or allow for expense-back of service plan costs, but limit to users with management pre-approval.

- BYOD Goes Global: Many believe that BYOD “doesn’t work” outside U.S. due to international privacy laws and/or greater exposure to highly variable roaming costs. Our data clearly shows otherwise - with nearly half (44.9 percent) of respondents indicating they are already deploying BYOD programs in multiple countries.
Appendix B: Survey results from peers

All respondents provide desktop and laptops; 88% iPads or tablets, 84% smart phones and 82% cell phones.

For desktops, laptops and iPads, only one respondent (2%) stated the organization monitored for personal use. Only five (11%) monitored smartphone usage and seven (16%) for cell phones.

Ninety-three (93%) allow personally owned devices (POD). Ninety percent (90%) allow some access to data. All (100%) respondents with greater than 10,000 employees allow some access to data.
Seventy-six percent (76%) provide some level of technical support. From the comments, the types and levels of services are variable.

**Survey Respondents (Those that self-identified)**

<table>
<thead>
<tr>
<th>California Institute of Technology</th>
<th>St Louis University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cornell University</td>
<td>St. Lawrence University</td>
</tr>
<tr>
<td>CSU East Bay</td>
<td>Stanford University</td>
</tr>
<tr>
<td>Duke University</td>
<td>Tulane University</td>
</tr>
<tr>
<td>Emory University</td>
<td>University of California - Office of the President</td>
</tr>
<tr>
<td>Gallaudet University</td>
<td>University of California, Berkeley</td>
</tr>
<tr>
<td>Grace College</td>
<td>University of California, Santa Barbara</td>
</tr>
<tr>
<td>Harvard University</td>
<td>University of Illinois</td>
</tr>
<tr>
<td>Indiana University</td>
<td>University of Miami</td>
</tr>
<tr>
<td>Michigan State University</td>
<td>University of North Carolina at Greensboro</td>
</tr>
<tr>
<td>Oklahoma State University</td>
<td>University of the Sunshine Coast</td>
</tr>
<tr>
<td>Palm Beach State College</td>
<td>Vanderbilt University</td>
</tr>
<tr>
<td>Princeton University</td>
<td>Wake Forest University</td>
</tr>
<tr>
<td>Purdue University</td>
<td>Washington University in St. Louis</td>
</tr>
<tr>
<td>Riverside Community College District</td>
<td>Yale University</td>
</tr>
</tbody>
</table>
Appendix C: Survey results from U-M users

This survey was sent to 5002 randomly selected staff at the University of Michigan. 941 completed surveys were received. The data is for all staff types (see the demographics at the end of this appendix).

University departments furnished computers for their staff more often than tablets or smartphones.

Staff use every type of personally-owned device surveyed, and most more than one device.

While very few staff received reimbursements to cover personally-owned devices, keep in mind that this survey was taken before the Tech Tools policy took affect.
Staff are motivated by convenience and increased productivity (most often mentioned under ‘other’) and are not burdened by supporting the device.

Staff use their personally-owned devices for a variety of work functions, and also use a variety of security measures.
While many staff do not get IT support for their personally-owned device, of those that do, support for smartphone and laptops is highest.

These results show increased productivity as well as increased number of hours working outside of normal working hours.
Not surprisingly, student staff rate their technical knowledge the highest (89% above or way above average). Staff who use their personally-owned devices for work are receptive to new technology (51% welcoming and 35% enthusiastic) indicating that enabling BYOD rewards staff who are forward thinking and interested in trying new things - traits to be encouraged in our current atmosphere of nearly constant change.

Demographics
Appendix D: Survey Results from Business and Finance Town Hall

290 people responded to the BYOD survey at the B&F Town Hall held on May 30-31. The survey contained one question:

Which of these personally-owned devices do you use to connect to the U-M network for work (e-mail, access to files or anything else related to your job)?

laptop computer desktop computer smartphone tablet other___________ none of these

From that one question, the following data were derived:

Of the 290 staff members responding, only 7% (21) do not use any personally-owned device to do work. Most people use 1, 2 or 3 different devices (93, 93, 52 respectively) and some (22) use 4.

Laptops (157), desktops (155) and smartphones (159) are in use about equally. Tablets are used by about half as many people (75) as these, but that number is expected to grow as more tablets become available and become less expensive. The devices in the ‘other’ category (5) were all iPods (probably the iPod Touch).
Appendix E: Standard Practice Guide (SPG) policies

SPG 514.04 Tech Tools: Cell Phones and Portable Electronic Resources
Revised: New
Date Issued: 5/31/2012
Review Date: 5/31/2017

The newly issued Tech Tools SPG provides guidance regarding use of and reimbursement for personally owned devices for work. It covers cell phones, smart phones, laptops, tablets and similar devices, with differing guidance for the different types of devices.

Stipends may be offered to employees with a business need for cell phones, smartphones and other similar telecommunication resources provided the resource is used more than 50% for business use. Stipends are the recommended practice for cell phones and smartphones.

Laptops, tablets and similar computing devices may be provided by the University directly to the employee with a demonstrated business need. Stipends may not be offered for these types of resources.

The SPG outlines responsibilities of the University and of staff receiving either a stipend or a University-provided device, including criteria for providing tech tools either directly or through a stipend, guidance on stipend amount and the requirement for the employee to complete a Verification Statement.

SPG xxx (draft) Security of Personally-Owned Devices that Access or Maintain Sensitive Institutional Data
Revised: 
Date Issued: 
Review Date: 

This policy addresses use of personally-owned devices to access or maintain sensitive institutional data. It recommends actions to take to secure the device, puts in place guidance for returning data maintained on personally-owned devices when they are no longer an authorized user of the data, and requires incident reporting of lost, stolen or otherwise compromised devices. It also outlines obligations of employees in producing university-owned materials to FOI and eDiscovery requests.

The policy has been drafted and is in the approval process.

SPG 520.1 Acquisition, Use and Disposition of Property
Revised: 6/7/05
Date Issued: na
Review Date: 6/7/09

SPG 520.1 provides guidance on using University-owned equipment off the campus property. It describes allowed and prohibited personal use of University-owned equipment, in essence allowing limited personal use

36 http://spg.umich.edu/policy/520.01
except for illegal or profit-generating purposes as long as that use does not result in a material incremental cost to the University.

This SPG is relevant to BYOD in the inverse - it provides guidance for use of University-owned equipment for personal use, demonstrating that the University has policies that permit mixing of personal and business use on computing devices.

**SPG 601.11 Privacy and the Need to Monitor and Access Records**

Revised: 9/7/2004
Date Issued: 12/1/93
Review Date: 9/7/08

SPG 601.11 provides another example of University policies recognizing the business and personal records may reside on the same device. It offers guidance for protecting personal information in the event that information on the University-owned device must be examined.

**SPG 201.65-1 Conflicts of Interest and Conflicts of Commitment**

Revised: 7/15/05
Date Issued: 9/1/81
Review Date: 7/15/09

Mixing personal and business use and information, whether on a University-owned or personally-owned device, creates the potential for conflicts of interest and conflicts of commitment. Personally-owned devices in the workplace increase the possibility of using work time (time during which employees are compensated by the University) to conduct personal business. This possibility also exists on University-owned resources, but it could be argued that the potential is higher on personally-owned one.

SPG 201.65-1 provides guidance on these issues, requirements to disclose potential conflicts of interest or conflicts of commitment, and consequences of violations. The SPG addresses University-owned resources, but does not preclude applying to personally-owned devices.

**SPG 601.7 Proper Use of Information Resources, Information Technology Resources, and Networks at the University of Michigan**

Revised: 15/5/02
Date Issued: 5/25/90
Review Date: 12/5/04

SPG 601.7 covers proper use of University IT resources, including hardware, software and data. When it was last revised, use of personally-owned devices to access University information was not prevalent. However, in a footnote it states “Information resources in this document are meant to include any information in electronic or audio-visual format or any hardware or software that make possible the storage and use of such information.” which certainly covers personally-owned resources.

---

37 [http://spg.umich.edu/policy/601.11](http://spg.umich.edu/policy/601.11)
38 [http://spg.umich.edu/policy/201.65-1](http://spg.umich.edu/policy/201.65-1)
39 [http://spg.umich.edu/policy/601.07](http://spg.umich.edu/policy/601.07)
This SPG establishes policy for the management of University institutional data and the responsibilities for the protection of this data, regardless of its form or storage location. This includes data that can be accessed and potentially stored on personally-owned devices.

**SPG 601.27 Information Security Policy**
Revised: 10/14/2008
Date Issued: 01/02/2008
Review Date: 01/02/2012

This policy establishes University-wide strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, managed, and/or controlled by the University. It places the responsibility for implementing and ensuring compliance with the policy on the University Deans and Directors. This policy shows the importance of awareness of BYOD issues by unit leadership and imposes a responsibility for protecting University information on unit leadership. The Chief Information Technology Security Officer is charged with determining unit-level compliance with the policy.

**SPG 601.25 Information Security Incident Reporting Policy**
Revised: 10/14/2008
Date Issued: 07/10/06
Review Date: 07/10/10

This SPG instructs University users on the appropriate response when an information security incident occurs. The policy covers University information resources, including data that may be accessed by personally-owned devices. Although the policy makes no mention of BYOD, it clearly applies to University data that may be accessed by or stored on a personally-owned device. It may not occur to users to report a security incident on their personally-owned device to the University Information Security office, it is important that this be explicitly called out in this policy.

**SPG 201.51 Remote Location Pay and Reimbursement of Dependent Relocation Costs**
Last updated: 7/1/2005
Review Date: 7/1/2009

This SPG could be seen as a precedent distributing funds to staff, including what happens when a staff person to whom funds have been distributed sever their relationship to the University. In addition, consideration should be given to a BYOD model to provide computing capabilities necessary to do a job from a remote location.

---

40 [http://spg.umich.edu/policy/601.12](http://spg.umich.edu/policy/601.12)
41 [http://spg.umich.edu/policy/601.27](http://spg.umich.edu/policy/601.27)
43 [http://spg.umich.edu/policy/201.51](http://spg.umich.edu/policy/201.51)
### Appendix F: BYOD Productivity Savings Example

**70% of staff responding to the staff survey reported saving time**

- 56% saved between 1-5 hours
- 9% saved between 6-10 hours
- 5% saved more than 10 hours

If 2,500 EE’s experienced productivity savings:

<table>
<thead>
<tr>
<th>Time Saved</th>
<th>Percentage</th>
<th>Hours Saved</th>
<th>EE’s</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5 hours</td>
<td>56/70</td>
<td>80%</td>
<td>2000</td>
<td>$4,375.00</td>
</tr>
<tr>
<td>6-10 hours</td>
<td>(9+5)/70</td>
<td>20%</td>
<td>500</td>
<td>$13,125.00</td>
</tr>
</tbody>
</table>

2.5 time in hours saved per week (Midpoint between 1 and 5)
50 work weeks
125 hours saved per year
35 $35/hour average
4,375.00 $/year
2,000 #EE’s
8,750,000.00 $/year X #EE’s

7.5 time saved per week (Midpoint between 6 and 10; estimated low)
50 work weeks
375 hours saved per year
35 $35/hour average
13,125.00 $/year
500 #EE’s
6,562,500.00 $/year X #EE’s

15,312,500.00
Appendix G: Resources

Note: Copies of these resources are available to anyone at U-M at https://umich.box.com/byod-resources


