Communications of the Association for Information Systems

Volume 41 Article 10

8-2017

A Bring-your-own-device Case for Use in the Classroom

Janice C. Sipior
Villanova University, Janice.Sipior@villanova.edu

James Bierstaker
Villanova University

Q. Chung
Villanova University

Johnny Lee
Drexel University

Recommended Citation
Sipior, Janice C.; Bierstaker, James; Chung, Q.; and Lee, Johnny (2017) "A Bring-your-own-device Case for Use in the Classroom," *Communications of the Association for Information Systems*: Vol. 41 , Article 10.
DOI: 10.17705/1CAIS.04110
Available at: https://aisel.aisnet.org/cais/vol41/iss1/10

Communications of the Association for Information Systems

Teaching Case ISSN: 1529-3181

A Bring-your-own-device Case for Use in the Classroom

Janice C. Sipior
Department of Accountancy and Information Systems
Villanova University
janice.sipior@villanova.edu

James Bierstaker
Department of Accountancy and Information Systems
Villanova University

Q. Chung
Department of Accountancy and Information Systems
Villanova University

Johnny Lee
Accounting Department
Drexel University

Abstract:

Bring your own device (BYOD) refers to the use of privately owned mobile devices for employment-related activities. This paper presents a real-world case study resource for teaching based on an actual consulting engagement of a global accounting firm to bring practical experience with managing BYOD into the classroom. Students, working in teams, assumed the role of consultants and defended their recommendations involving the recognition of benefits and challenges in managing BYOD in an organization. Professionals from five global accounting evaluated the use of the case study in an undergraduate case competition and found that, in general, the students agreed that they had a positive learning experience.

Keywords: BYOD, Bring Your Own Device, Teaching case study, Management of Information Technology, Education.

This manuscript underwent peer review. It was received 07/28/2016 and was with the authors for 6 months for one revision. The Associate Editor chose to remain anonymous.

1 Introduction

IT consumerization refers to the use of IT for both private and business purposes by employees who "invest their own resources to buy, learn, and use a broad range of popular consumer technologies and application tools in a work context" (Niehaves, Köffer, & Ortbach, 2012, p. 2). IT consumerization includes devices such as laptops, netbooks, e-readers, mobile phones, and tablets; applications such as social networks; and IT services such as cloud storage (Steelman, Lacity, & Sabherwal, 2016). We focus on the use of only privately owned mobile devices, a subtrend of IT consumerization referred to as bring your own device (BYOD). BYOD refers to the use of personal devices but not applications and services for employment purposes (Weeger, Wang, & Gewald, 2015). While "BYOD has become associated with the benefits gained from employees using their personal devices" (French, Guo, & Shim, 2014, p. 193), challenges in managing consumer technologies confront organizations.

This paper presents a case study of BYOD for use in the classroom. We found no other case study in previous literature devised to assist the classroom learning experience on this topic. We provide and discuss a real-world case scenario based on an actual consulting engagement of a global accounting firm at an organization that we refer to as the Fairfield Trust Company to bring practical experience with managing BYOD into the classroom. While the situation is factual, names and the company description are fictitious. We conducted this case study due to employees' increasing use of their own devices in the workplace (Buettner, 2015; Chen, 2014; Harris, Patten, & Regan, 2013; Leclercq-Vandelannoitte, 2015; Lee, Crossler, & Warkentin, 2013; Negahban, Windsor, & Bien, 2015; Ortbach, Walter, & Öksüz, 2015; Putri & Hovav, 2014; Shim, Mittleman, Welke, French, & Guo, 2013; Tu & Yuan, 2015; Weeger & Gewald, 2014; Yin, Liu, & Liu, 2014). This case enhances students' understanding of the benefits and challenges of this growing trend. By providing an opportunity for students to experience the challenges confronting an organization that must make decisions in response to BYOD, use of this case can create realism and enliven the classroom.

This paper proceeds as follows: in Section 2, we present the expected benefits for students in analyzing the case study. In Section 3, to provide the background necessary to understand the organizational issues of BYOD, we then review previous literature in which we focus on the benefits and considerations in managing BYOD. In Section 4, we provide implementation guidance in adopting the case for use in teaching and describe the case competition we undertook. To gauge the degree of effectiveness of the case study, we implemented a team-based case competition, which included a survey of students who participated. In Section 5, we present the survey instrument, analyze the data collected from participating students of the case competition, and present the results5. In Sections 6, we present our study's limitations and, in Section 7, conclude the paper. Appendix A provides the Fairfield Trust Company case study and case questions with suggested solution points. The written report of the winning team and their PowerPoint presentation slides are available from the corresponding author. Appendix B present the case competition rules and procedures. Appendix C provides the assessment form that participants from the global accounting firms used to score each team's written report. Appendix D presents the assessment form to evaluate the finalist team presentations.

2 Benefits of the Case Study for Students

The Pew Research Center (2015, p. 3) has concluded that young adults aged 18-29 "are especially likely to be 'smartphone dependent'" and have "deeply embedded mobile devices into the daily contours of their lives" based on a special "experience sampling" survey of smartphone owners in the United States. Thus, students can fully relate to the increasing trend to BYOD for work-related activities. In analyzing the Fairfield Trust Company case study, we expected students to be engaged and to derive the benefits as presented in Table 1.

This case study provides an opportunity for students to experience an actual consulting engagement of a global accounting firm in evaluating the benefits and challenges of BYOD, addressing the risks, and determining recommended policies and procedures. In Section 3, we review existing literature to identify benefits and considerations in managing BYOD.

Table 1. Expected Benefits for Students

1.	Understand the pros and cons of BYOD.
2.	Understand the risks associated with BYOD.
3.	Learn about the concerns of companies regarding sensitive information on mobile devices. Understand security and privacy issues of BYOD.
4.	Gain insight into internal control policies for mobile devices.
5.	Learn about issues companies consider in developing policies and procedures regarding the use of mobile devices.
6.	Learn about ethical issues that arise when companies develop policies regarding the use of mobile devices.
7.	Learn about what compliance issues companies must address for BYOD.
8.	Appreciate the importance of working well together in interdisciplinary teams.

3 Literature Review

BYOD brings organizations both benefits and challenges. We review existing literature addressing BYOD according to each of these areas. In doing so, we explain issues to consider in managing the growing trend of employees' use of their own devices in the workplace.

3.1 Benefits of BYOD

Previous research has discussed the many benefits of BYOD to both employers and employees (see Table 2 for summary). Organizations and their employees who embrace BYOD have an attractive mechanism to recruit and retain the best employees (Loose, Weeger, & Gewald, 2013). For example, younger employees are digital natives and expect to use their devices without distinguishing between personal and business purposes. They perceive that they have the right, not the privilege, to use their own devices (Leclercq-Vandelannoitte, 2015). The constant connectivity afforded by using their own devices allows employees to instantly and widely communicate and share information without needing an Internet connection (Zahadat, Blessner, Blackburn, & Olson, 2015). Building on technology adoption research, Loose et al. (2013) found that ease of use and usefulness are factors that drive employees to BYOD. Employees' use of their privately owned devices for business purposes provides better user experience and greater autonomy (Weeger & Gewald, 2014). It can also foster innovation and creativity (Leclercq-Vandelannoitte, 2015). The increased convenience, mobility, portability, and flexibility that BOYD affords employees increases employees' satisfaction and morale, which, in turn, increases their motivation and performance (Lebek, Degirmenci, & Breitner, 2013). In terms of performance, employees have become more effective, efficient, and productive (Leclercq-Vandelannoitte, 2015).

Employers recognize BOYD's benefits as well. For example, organizations have cited increased employee satisfaction as a primary benefit of BYOD (Niehaves et al., 2012). Employers also benefit by attracting and retaining quality employees who are technologically savvy and expect the flexibility of choosing the devices they use (Leclercq-Vandelannoitte, 2015; Niehaves et al., 2012). Companies are expected to benefit from cost reductions associated with, for example, procurement, hardware, software, licensing, service agreements, and insurance (Loose et al., 2013). However, cost savings may be a misconception since the company may be required to pay voice and data service charges for their employees' devices (French et al., 2014). Familiarity of employees in using their own devices reduces the need to provide training sessions and, in turn, increases the speed of adoption of such devices (Niehaves et al., 2012). Further, employee oversight of their own devices is more diligent than for those that the company provides (Ghosh, Gajar, & Rai, 2013). Companies realize additional benefits in that employees can quickly and easily share information, even at remote locations, and thus, can respond promptly (Zahadat et al., 2015). IT departments can support BYOD in an effort to lead to enterprise growth and development (Thomson, 2012) rather than try to resist this growing trend. However, organizations confront many challenges in allowing or encouraging employees to bring their own personal devices into the workplace.

Table 2. Benefits of BYOD to Employees and to Employers

BYOD benefits to employees	References
Ease of use for employees	Buettner (2015), Hopkins, Sylvester, & Tate (2013), Loose et al. (2013), Niehaves et al. (2012), Ortbach (2015), Ortbach et al. (2015), Rivera, George, Peter, Muralidharan, & Khanum (2013), Zahadat et al. (2015)
Usefulness for employees	Buettner (2015), Chen (2014), Hopkins et al. (2013), Lebek et al. (2013), Lee et al. (2013), Loose et al. (2013), Ortbach (2015)
Better user experience	Weeger & Gewald (2013)
Increased employee autonomy	Chen (2014), Loose et al. (2013), Niehaves et al. (2012), Weeger & Gewald (2014), Weeger et al. (2015)
Increased employee innovation and creativity	Dernbecher, Beck, & Weber (2013), Leclercq-Vandelannoitte (2015), Ortbach (2015), Steelman et al. (2016), Weeger et al. (2015)
Increased employee convenience, mobility, portability, and flexibility	Chen (2014), French et al. (2014), Lebek et al. (2013), Leclercq-Vandelannoitte (2015), Morrow (2012), Negahban et al. (2015), Rivera et al. (2013), Steelman et al. (2016), Thomson (2012), Weeger et al. (2015), Yin et al. (2014)
Increased employee satisfaction and morale	Chen (2014), French et al. (2014), Lebek et al. (2013), Leclercq-Vandelannoitte (2015), Negahban et al. (2015), Niehaves et al. (2012), Ortbach et al. (2015), Rivera et al. (2013), Steelman et al. (2016), Thomson (2012), Weeger et al. (2015), Yin et al. (2014)
Increased employee motivation and performance	Lebek et al. (2013), Leclercq-Vandelannoitte (2015), Lee et al. (2013), Loose et al. (2013), Niehaves et al. (2012), Ortbach (2015), Steelman et al. (2016)
Increased employee effectiveness, efficiency, and productivity	Chen (2014), French et al. (2014), Lebek et al. (2013), Leclercq-Vandelannoitte (2015), Loose et al. (2013), Mansfield-Devine (2012), Morrow (2012), Negahban et al. (2015), Ortbach (2015), Putri & Hovav (2014), Rivera et al. (2013), Steelman et al. (2016), Thomson (2012), Wang et al. (2014), Weeger et al. (2015), Zahadat et al. (2015)
BYOD Benefits to Employers	**References**
Attract/retain top talent	French et al. (2014), Leclercq-Vandelannoitte (2015), Loose et al. (2013), Niehaves et al. (2012), Putri & Hovav (2014), Steelman et al. (2016), Thomson (2012), Weeger et al. (2015)
Reduced company costs (e.g., procurement, hardware, software, licensing, service agreements, and insurance)	Chen (2014), French et al. (2014), Lebek et al. (2013), Leclercq-Vandelannoitte (2015), Lee et al. (2013), Loose et al. (2013), Morrow (2012), Ortbach et al. (2015), Putri & Hovav (2014), Steelman et al. (2016), Wang et al. (2014), Weeger et al. (2015), Yin et al. (2014), Zahadat et al. (2015)
Reduced need for employee IT training	Niehaves et al. (2012)
More diligent employee oversight of their own devices than those the company provides	Ghosh et al. (2013)
Employees can instantly and widely communicate and share information	Leclercq-Vandelannoitte (2015), Steelman et al. (2016), Thomson (2012), Zahadat et al. (2015)
The role of IT departments, as enablers of collaboration and sharing, can lead to enterprise growth and development	Leclercq-Vandelannoitte (2015), Steelman et al. (2016), Thomson (2012)

3.2 Managerial Considerations for BYOD

We summarize prior research to identify considerations in managing BYOD. As Appendix E shows, we categorize these considerations as: compatibility, compliance, culture, IT governance, privacy, security, and support.

3.2.1 Compatibility

Organizations may establish formalized BYOD programs to manage IT infrastructures and to address compatibility issues. Weeger et al. (2015) report that employees' devices have to meet a set of specifications and, further, that employees must agree to an accepted use policy. Pick (2015) note that, in the absence of such a formalized approach, organizational networks, applications, and data must work with a variety of devices that employees select. Steelman et al. (2016) found that compatibility concerns limit device choices, which one may address through a formal BYOD policy. Compatibility should be balanced with freedom, control, and security.

3.2.2 Compliance

Steelman et al. (2016) observe that one may identify and address legal and regulatory issues through a steering committee with representatives from human resources, legal, security, infrastructure, and operations. Rivera et al. (2013) recognize that what security controls an organization uses will vary depending on compliance requirements and that they must periodically review them to ensure effectiveness as changes in BYOD occur. The regulatory demands of an organization's industry segment drive BYOD decisions (Thomson, 2012). Organizations can monitor specific tasks to prevent employees from engaging in behaviors that violate compliance (Lee et al., 2013). French et al. (2014) discuss the necessity for companies to re-evaluate compliance regarding how employees store and share data across the company's network.

Putri and Hovav (2014) empirically examined employees' intention to comply with an organization's IS security policy for BYOD. They found that an employee's perceived response efficacy and perceived justice were positively associated with an employee's intention to comply with BYOD security policy. Further, an employee's perceived cost caused by compliance behavior was positively correlated with an employee's perception of the threat to individual freedom. A security awareness program related to BYOD was positively associated with an employee's perceived response cost in engaging in compliance behavior and perceived response efficacy. Crossler, Long, Loraas, and Trinkle (2014) also examined factors that affect employees' intentions to comply with corporate policies governing BYOD and self-reported compliance behavior by applying protection motivation theory. They found self-efficacy and response efficacy to have a positive influence on individuals' intentions to comply. Threat severity had a positive influence on accountants' intentions to comply but did not affect non-accountants. For actual compliance behavior, threat severity, self-efficacy, and response efficacy had a positive influence, while Response Cost was negatively related to compliance behavior.

Tokuyoshi (2013) views BYOD as having brought to light that organizations may have insufficient levels of control over who can access specific applications and data regardless of who owns a device. BYOD brings additional challenges to compliance because of the need to address a broader set of devices. Zahadat et al. (2015) propose a BYOD security framework, which they validated by a survey, to assist organizations in formulating a BYOD program that meets organizational goals, balances competing interests, and meets regulatory and compliance requirements. Proper planning, implementation of policy through process controls, and training of employees encourages user compliance.

3.2.3 Culture

Current and future employees expect that they will be able to bring their own devices to do their jobs (Thomson, 2012). According to Thomson (2012), three in ten young professionals agree that BYOD practices would influence job decisions such as leaving their current position or declining a job offer. Loose et al. (2013) found that the intention to use BYOD was significantly associated with employer attractiveness. Ortbach (2015) found ease of use of both enterprise-provided and privately owned mobile IT mediates the relationship between personal innovativeness in IT and BYOD intention. Increasingly, organizations are allowing their staff members to bring their own devices through either a passive or active approach (French et al., 2014). Organizations may take a passive approach by simply allowing employees to bring and use their personal devices for work activities. Alternatively, organizations can take

an active approach by formulating and implementing an explicit BYOD policy. Steelman et al. (2016) observed an active approach that evolved over six years, after BYOD arrived at Cisco, one of their case study organizations. As a result, a new corporate culture that accepted BOYD and closely monitored its usage emerged in the company.

Mansfield-Devine (2012) views BYOD as a major cultural shift. Corporations would no longer own the desktop, which necessitates incorporating employees as part of their security framework. Such a shift is difficult not only due to cultural considerations but also technical issues. Ortbach et al. (2015) view the determination of trust factors that influence chief information officers' (CIOs) decisions as the first step in assessing BYOD. Additionally, the specific demands of an organization's corporate culture in terms of risk tolerance versus innovation drive BYOD decisions (Thomson, 2012). In reassessing the effectiveness of a security framework in light of BYOD, one must address a broad range of factors in addition to organizational culture, including risks, controls, policies, and user awareness/training (Rivera et al., 2013).

3.2.4 IT Governance

The development and communication of suitable governance mechanisms and policies that govern the integration of BYOD into the existing environment is one of the most important steps in BYOD oversight (Ortbach et al., 2015). Research regards implementing a BYOD policy as an organizational risk-taking action, which it has empirically found to be influenced by trust factors and moderated by the perceived risks associated with BYOD such as security breaches.

BYOD could bring a new type of IT governance anarchy (Pick, 2015). Employees who use a variety of personal devices for work activities bring a multitude of support, compatibility, and security issues to the workplace when used with corporate networks, applications, and data. If organizations impose restrictions on employees' choices, employees may ignore such policies or push back in other ways. To prevent such uncontrolled "stealth IT" or "shadow IT", which refers to IT use in organizations without explicit organizational approval, organizations should establish official BYOD programs with a set of specifications to enable users to choose and use devices that best meet their needs (Weeger et al., 2015).

IT governance is critical to the success of BYOD (Thomson, 2012). Rather than focusing on whether to allow employees to use the devices they choose, IT governance should focus on devising positive, responsive actions to manage BYOD to remain competitive. Steelman et al. (2016) found that a clear and concise BYOD policy with significant resources devoted to providing and supporting oversight enables employees to innovate and leads to a variety of enhancements in performing tasks.

3.2.5 Privacy

Lee et al. (2013) hypothesize that the monitoring mechanisms that organizations employ play a key role when participants consider participating in a BYOD program. Weeger and Gewald (2014) found that employees' intention to enroll in a BYOD program is a function of perceived risk, which includes privacy risk (the potential that the employer will obtain personal information about an employee without the employee's consent and knowledge). Lebek et al. (2013) found that privacy concerns (and security and legal considerations) significantly impacted employee indecision towards their intention to use their own mobile devices for work activities. Employers have a legitimate interest in monitoring personal devices in order to prevent employees from breaching their security. However, employees may expect privacy when they use their devices for personal activities. Steelman et al. (2016) observe that a central mobile device management (MDM) system reduced employees' privacy concerns.

Garba, Armarego, Murray, and Kenworthy (2015) observe that the trend towards BYOD is creating more information privacy and security concerns. They conclude that many organizations that adopt BYOD are failing to protect their employees' privacy. The necessity for organizations to expend resources to attend to privacy concerns is underscored by the threat of legal action from, for example, those affected by a breach of their personal information (Zahadat et al., 2015).

Corporate BYOD training should increase employees' perceived response efficacy by focusing on how policies respond to security and data privacy threats (Crossler et al., 2014). Employees should understand why they are restricted to use only approved devices for a specific task because of privacy issues (Chen, 2014). Further, ethical values regarding data rights and privacy should be instilled in employees (French et al., 2014). However, Thomson (2012) suggests that enterprises should define a realistic compromise between employees' information sharing and the business requirements of protecting data and information privacy.

3.2.6 Security

Steelman et al. (2016) note that CIOs remain concerned about the control over and security of organizational IT assets. Indeed, as Mansfield-Devine (2012, p. 15) state: "BYOD wouldn't be worrying anyone if it wasn't for the security implications", an opinion that Zahadat et al. (2015) support. Security must be a top priority (French et al., 2014) to protect information and information systems. Vulnerability to security breaches, the need to plan for business continuity, and needs to both comply and document compliance with regulations have pushed organization towards centralized security management (Pick, 2015). Information security management is one of the biggest challenges that large organizations face, and mobile malware attacks in particular have emerged as the primary security threat (Garba et al., 2015).

Decisive Analytics (2012) surveyed 872 IT executives and found that nearly half who allowed employees to connect to their companies' networks reported having experienced a data breach. As a result, 45 percent of these companies responded by restricting BYOD data access rights and 43 percent installed security software. Some companies may restrict employees to use only approved devices for specific tasks due to security concerns (Chen, 2014). Alternatively, companies may choose not to allow BYOD because they do not want to risk increased exposure to security threats (French et al., 2014).

However, Weeger et al. (2015) found that students expect that future employers will permit them to use personal devices for work activities. Loose et al. (2013) found that the attractiveness of a company for a future employee was positively associated with intention to adopt BYOD. Since young employees are likely to use their own devices even if their companies do not permit them to, CIOs should develop a BYOD program with appropriate security measures and usage policies, which is especially necessary since young employees do not believe security is their responsibility (Thomson, 2012). Employers need to balance security and privacy objectives with the effort employees must expend to comply with usage and security policies (Weeger et al., 2015).

Researchers have hypothesized that IT managers' threat appraisal, coping appraisal, and industry norms affect their intention to adopt BYOD security (Tu & Yuan, 2015). Specific BYOD features such as device variety, mobility, visibility, and mixed usage affect the threat appraisal and coping appraisal. Organizations need a combination of multiple security controls to devise a comprehensive security framework. In a comparative analysis of security threats against security controls, Rivera et al. (2013) found what combination of controls organizations adopt varies depending on factors such as the organizations' nature and their risk tolerance, IT security budget, and compliance requirements. Controlling access to applications for particular users and proactively searching for threats is a fundamental challenge in organizations, which the broader group of devices a BYOD program brings exacerbates (Tokuyoshi, 2013).

A further challenge concerns heightening security awareness and behaviors. Putri and Hovav (2014) empirically examined employees' intention to comply with their organizations' IS security policies for BYOD. Their findings reveal that an employee's perceived response efficacy and perceived justice was positively associated with an employee's intention to comply with BYOD security policy. Corporate BYOD training should increase employees' perceived response efficacy by informing them about the severity of potential threats related to unsecure BYOD behavior (Crossler et al., 2014).

Corporate BYOD training should also increase employees' security awareness. From conducting a survey, Harris et al. (2013) found a lack of security awareness among college students entering the workforce. Students inadequately secured their mobile devices and over three quarters (76%) believed that employers have the responsibility to provide security software for BYOD devices.

Lee et al. (2013) suggest that securing corporate information by monitoring personal employee devices to ensure organizational data is safe must be balanced with employee privacy concerns. However, Lebek et al. (2013) found that employees were more concerned about security and legal considerations than about their individual privacy in their intention to use their own mobile devices for work activities.

Researchers have examined decisions by employers regarding BYOD in their organization and by employees to bring their own devices to the workplace. Ortbach et al. (2015) hypothesize that trust influences risk taking (i.e., what risks employees take with their own devices at work) and that IT management's perceived BYOD risk factors, including the probability of BYOD security breach and severity of BYOD security threats, moderate the relationship. Weeger and Gewald (2014) found that employees' intention to enroll in a BYOD program is a function of perceived risk, including security risk, which is a potential loss due to fraud or a hacker's compromising information security.

3.2.7 Support

Employees purchase devices for personal use and incorporate them into the workplace with or without their organizations' IT departments' support (Tokuyoshi, 2013). They also expect the CIO and IT staff members to determine how they can use their devices for work responsibilities, anywhere and anytime, without risk to the company (Thomson, 2012). IT support must be able to respond to requests for assistance from employees using devices with which the organization is unfamiliar (Pick, 2015). Thus, BYOD implementation requires an entire organizational support structure (Rivera et al., 2013). A supporting framework that comprises both technical support and non-technical controls such as policies, user awareness, education, and training must be available to employees who participate in BYOD. Steelman et al. (2016) found that implementing a central MDM system guides employees in their IT selection and ensures adequate control, compatibility, security, and integration across devices.

Conversely, Loose et al. (2013) expect BYOD programs to require that employees assume full responsibility for supporting, installing, and maintaining their own devices and accept their organizations' terms of use and security policies. Buettner (2015, p. 1) concludes that "BYOD user behavior is primarily driven by Perceived Enjoyment as a System 1 IS construct and System 2 IS constructs such as Perceived Usefulness are results of post hoc constructions/justifications of (intended) BYOD usage". System 1 is conceptualized "as the rapid, parallel and automatic driver of behavior and System 2 as the slow and sequential post hoc construction instance justifying behavior (Buettner 2015, p.1), according to dual process theories of cognition (Evans, 2008).

Ortbach et al. (2015) analyzed service quality based on the SERVQUAL approach (Parasuraman, Zeithaml, & Berry, 1985) as adopted in the IS context to measure IS service quality (Jiang, Klein, & Carr, 2002). They assessed SERVQUAL according to five quality classes: 1) reliability (which involves consistency of performance and dependability), 2) responsiveness (which is the ability to provide prompt service), 3) assurance (which concerns employees' knowledge and courtesy, 4) empathy (which refers to individualized attention), and 5) tangibles (which concerns physical facilities and equipment).

Yin et al. (2014) investigated BYOD through the gift economy. When a gift is given, the giver expects a return from the recipient. What gift the receiver receives determines what gift they may return. BYOD programs are a gift to employees that comprises both an informational aspect (which includes flexibility, convenience, and autonomy) and a controlling aspect (which includes workload and controls). In return, recipient employees may return both positive outcomes, such as satisfaction and/or organization commitment, and negative outcomes such as stress and/or burnout.

4 Implementation Guidance

One can use the Fairfield Trust Company case for case competitions, as an active learning exercise in class, or as a homework assignment to support teaching in undergraduate and graduate courses programs. In this section, we discuss our experience in using the case study for a competition among freshmen student teams. We then discuss using the case in class and as homework. The written report and the PowerPoint slides of the winning team are available on request from the corresponding author.

4.1 Case Competition

We implemented this case as part of a case competition with first-year university students that took place from January to September in 2015 with a between-semester break from the end of May to the end of August. Students formed teams of four or five members. Partners, directors, and associates from five global accounting firms, including Deloitte, Ernst & Young, Grant Thornton, KPMG, and PwC, advised the student teams and guided them in preparing a written case analysis that addressed the questions at the end of the case. To facilitate fair and consistent proceedings, we set up the rules and procedures before the students formed teams or we distributed the case materials. We established the rules, communicated them among the partners of the global accounting firms, and announced to the first-year student pool of potential participants. The rules helped to establish expectations in all parties involved and served as guidelines to keep up with the agreed-on schedule and to handle major milestones. Appendix B presents the rules and procedures we used.

Professionals from the firms evaluated the participating student teams' written case analyses using the written case report assessment (see Appendix C), which resulted in five finalist teams. The finalist teams prepared a case presentation, and the professionals from the firms again advised the student teams and

guided them in preparing their presentations. The professionals judged the finalists' presentations with the finalists presentation assessment form (see Appendix D).

4.2 In-class Active Learning Exercise

Alternatively, one could use the case during class as an active learning exercise. The instructor could introduce BYOD by reviewing the benefits and managerial considerations (as Tables 2 and 3 summarize). The instructor could also make lecture notes available to serve as a reference for students.

Students would form teams of three, four, or five members (depending on the number of students) in class. The instructor would provide each student with the case study. One could reduce the number of questions at the end of the case to accommodate the class's duration. Optionally, students could select specific roles to play such as chief information officer (CIO), senior management, and other employees such as management, investment advisors, and administrative support. Role playing starts active discussion in the team to form initial ideas and further develop them (Lincke & Green, 2012). Student teams would prepare responses to the end-of-case questions, which serve as the basis for class discussion. For active learning, students could be given credit for participation rather than the work done (Lincke & Green, 2012). Those students who miss the in-class exercise can complete it as homework.

4.3 Homework Assignment

Lastly, one can use the case as a homework assignment for students to work either individually or in teams. The instructor would introduce BOYD in class by reviewing the benefits and managerial considerations as Tables 2 and 3 summarize. The instructor would then distribute the case in class to individual students or to already-formed teams. The instructor could make lecture notes available to serve as a reference for students.

As homework, students would be required to read the case study and prepare written responses to all or selected end-of-case questions. The instructor would grade the quality of the written responses. Optionally, the students could discuss the case study in class on the due date.

5 Evaluation of the Team-based Case Study Competition

To evaluate the team-based case study competition, we gave students a survey after they completed the finalist presentations to assess how well they learnt the case learning objectives. Table 3 displays the survey questions. A total of 17 out of 20 participating students (12 males and 8 females) returned surveys. All were in their first year when the case competition began and in the beginning of their second year when it completed.

5.1 Degree of Agreement Questions

As Table 4 shows, students generally agreed that they had a positive learning experience with mean responses of almost 5 and above for questions 1 through 16. Specifically, students indicated that they learned a lot about: 1) the potential risks in allowing employees to bring mobile devices to work, 2) what issues companies consider in developing policies and procedures regarding the use of mobile devices, 3) how the pros and cons of a BYOD policy differ from corporate-owned devices, 4) how the expenses of a BYOD policy differ from corporate-owned devices, 5) mitigating the risks of using mobile devices, 6) ethical issues that arise when companies develop policies about using mobile devices, 7) how companies can protect sensitive information, 8) security and privacy issues, 9) the potential risks of allowing employees to bring mobile devices to work, 10) how the risks of a BYOD policy differ from corporate-owned devices, 11) sensitive information that company servers and databases may store, 12) internal control policies for mobile devices, 13) compliance risks related to employees' use of mobile devices at work, and 14) compliance issues companies must address for a BYOD policy. They also generally agreed that they learned a lot about the importance of interdisciplinary teams and how to work more effectively in teams. Moreover, students indicated they were more likely to pursue a career that involved knowledge of accounting and information systems as a result of completing the case assignment.

However, at least one student expressed a strong response against pursuing a career that involves knowledge of accounting information systems. A carefully developed and executed case study, based on an actual consulting engagement of a global accounting firm, may serve as a learning experience to introduce career expectations and, thereby, serve as an early filter to direct students away from or toward suitable careers.

Table 3. Case Competition Participant Survey

Please indicate the extent to which you agree or disagree with the following statements as a result of completing the Fairfield Trust Company case assignment.								
Questions		**Disagree**			**Neutral**			**Agree**
		1	**2**	**3**	**4**	**5**	**6**	**7**
1.	I learned a lot about the potential risks of allowing employees to bring mobile devices to work.							
2.	I learned a lot about sensitive information that may be stored in company servers and databases.							
3.	I learned a lot about internal control policies for mobile devices.							
4.	I learned a lot about the importance of interdisciplinary teams.							
5.	I learned a lot about mitigating the risks of using mobile devices.							
6.	I learned how the risks of a bring-your-own-device policy differ from corporate owned devices.							
7.	I am more likely to pursue a career that involves knowledge of accounting information systems.							
8.	I learned how to work more effectively in teams.							
9.	I learned how the pros and cons of a bring-your-own-device policy differ from corporate owned devices.							
10.	I learned how the expenses of a bring-your-own-device policy differ from corporate owned devices.							
11.	I learned a lot about how companies can protect sensitive information.							
12.	I learned a lot about security and privacy issues.							
13.	I learned a lot about what issues companies consider in developing policies and procedures regarding the use of mobile devices.							
14.	I learned a lot about ethical issues that arise when companies develop policies regarding the use of mobile devices.							
15.	I learned a lot about what compliance issues companies must address for a bring-your-own-device policy.							
16.	I learned a lot about the compliance risks related to employees' use of mobile devices at work.							
17.	Please indicate if you are male or female (circle).							
18.	Please add any comments about the case below:							
Thanks for your feedback!								

Table 4. Descriptive Statistics of Degree of Agreement Question Responses

	Question	N	Mean	Std. dev.	Median	Min.	Max.
1.	I learned a lot about the potential risks of allowing employees to bring mobile devices to work.	17	5.88	0.93	6	4	7
2.	I learned a lot about sensitive information that may be stored in company servers and databases.	17	5.82	0.81	6	4	7
3.	I learned a lot about internal control policies for mobile devices.	17	5.82	0.95	6	4	7
4.	I learned a lot about the importance of interdisciplinary teams.	17	4.94	1.20	5	3	7
5.	I learned a lot about mitigating the risks of using mobile devices.	17	6.12	0.78	6	5	7
6.	I learned how the risks of a Bring Your Own Device policy differ from corporate owned devices.	17	6.35	0.86	7	4	7
7.	I am more likely to pursue a career that involves knowledge of accounting information systems.	17	4.94	1.92	5	1	7
8.	I learned how to work more effectively in teams.	17	5.47	1.33	6	2	7
9.	I learned how the pros and cons of a Bring Your Own Device policy differ from corporate owned devices.	17	6.29	0.85	7	5	7
10.	I learned how the expenses of a Bring Your Own Device policy differ from corporate owned devices.	17	6.18	0.73	6	5	7
11.	I learned a lot about how companies can protect sensitive information.	17	6.00	0.87	6	4	7
12.	I learned a lot about security and privacy issues.	17	5.88	0.86	6	4	7
13.	I learned a lot about what issues companies consider in developing policies and procedures regarding the use of mobile devices.	17	6.35	0.79	7	5	7
14.	I learned a lot about ethical issues that arise when companies develop policies regarding the use of mobile devices.	17	6.06	0.90	6	5	7
15.	I learned a lot about what compliance issues companies must address for a Bring Your Own Device policy.	17	5.59	0.87	6	4	7
16.	I learned a lot about the compliance risks related to employees' use of mobile devices at work.	17	5.76	1.20	6	3	7

5.2 Qualitative Comments

The last question asked students for any other comments they had about the case competition. Table 5 shows their responses. Overall, the qualitative comments indicate students had a very positive experience and found the case interesting and relevant.

Table 5. Individual Student Comments in Response to Being Asked If They Had Any Other Comments about the Case Competition

"I like the case. Very relevant to businesses today."
"I thought the case was very interesting to read and that made the case study more enjoyable to write."
"I thought the case was really interesting and relevant with the increasing popularity of technology in the workplace."
"The case was interesting and relatable."

6 Limitations

As with any study, ours has several limitations. First, we used a small sample size because we surveyed only those students who made it to the final round of the case competition. The small sample limited data analysis to descriptive statistics and qualitative comments. Thus, we report general findings and perceptions rather than objective measures that quantify the benefits that the students attained. Further, one should note that the responding students represent a high-performing subset of the 63 students who registered to participate in the case competition. As high performers, the responses of these students may be more positive than the remainder of the class and, therefore, not be a representative sample.

Second, we focused only on BYOD, a subtrend of IT consumerization. Future research could explore additional privately owned IT resources that are used for business purposes. Finally, we need research in other disciplines with larger samples and in cross-cultural settings to examine the benefits of roleplaying in the use of real-world case studies.

7 Discussion and Conclusions

In the workforce, many knowledge workers could not function effectively without their devices and apps (Jones & Wong, 2016). Some employees are developing new mobile apps themselves. Young employees in particular have the willingness and even the demand to bring their own devices into the workplace (Loose et al., 2013). As such, BYOD is an increasingly important and engaging topic for students to understand. Indeed, the recognition provided as feedback from students characterize the case study as “relevant to businesses today”, “very interesting…and more enjoyable to write”, “really interesting and relevant with the increasing popularity of technology in the workplace”, and “interesting and relatable”.

The use of a real-world case study, based on an actual consulting engagement of a global accounting firm, offered students an opportunity for experiential learning either individually or in teams. Their interaction with a professional from a global accounting firm who served as an advisor, which is unique for many students, enhanced their experience. This case competition was open to all first-year students who wanted to participate and gain experience with a real-world problem and interact with a working professional. Through this experience, students could see the complex implications of bringing their own devices into the workplace while a professional guided them as they analyzed the benefits and challenges and formulated recommendations for managing BYOD.

We believe that we generally achieved benefits for our students. Interestingly, in responding to the questionnaire, students learned more about BYOD than about working in teams. They reported that they learned most about the risks and the pros and cons associated with BYOD and what issues organizations consider in formulating policies and procedures for using mobile devices. This finding reveals a need to teach students who will be entering the workplace about the threats that confront organizations from employees bringing their own devices for use in work activities. Also, students learned about how expenses of BYOD differ from those of organization-owned devices. Further, students learnt about mitigating risks in using mobile devices, ethical issues that arise with corporate policies, how companies can protect sensitive information, risks of allowing BYOD, security and privacy issues, and sensitive information that companies store. Among the 16 questionnaire items, the students reported the lowest agreement for being more likely to pursue a career involving knowledge of accounting information systems, with a standard deviation of 1.92 (highest of all survey items) for the agreement rating.

The response from the five global accounting firms has been extremely positive. The case competition is an important avenue to bring them on campus and to expose them to our students. The accounting firms continue to hire IS majors for both their accounting practice and consulting services. The case competition provides an opportunity for our students to demonstrate their interest in employment with the firms by interacting directly with these professionals, to develop important career skills, and to gain valuable speaking points for interviews and a line item for their resumes.

We recognize that others may not be able to involve working professionals for a variety of reasons. Thus, we offer alternative approaches in using the case to bring realism to students. As an in-class active learning exercise, students work as a team to assume the role of consultants or to role play in the Fairfield Trust Company. As a homework assignment, students are not restrained by the limitations of class time and, thus, may research BYOD to a greater extent than is possible in class. Either approach allows for discussion in class for students to gain experience and insights into the benefits and challenges of BYOD.

Acknowledgments

Gabriele Ralph, CPA, and Laura Iacona, Partner, both of Grant Thornton LLP, wrote the case study and questions at the end of the paper based on an actual consulting engagement of a global accounting firm. We thank them for contributing the case study and for supporting our student case study competition by serving as advisors to our students. Any opinions, findings, and conclusions or recommendations expressed in this papers are those of the authors and do not necessarily reflect the views of the contributors or Grant Thornton LLP.

References

Buettner, R. (2015). Towards a new personal information technology acceptance model: Conceptualization and empirical evidence. In *Proceedings of the Americas Conference on Information Systems.*

Chen, C.-W. (2014). BYOD flexibility: The effects of flexibility of multiple IT device use on users' attitudes and continuance intention. In *Proceedings of the Americas Conference on Information Systems.*

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-gap. *Journal of Information Systems*, *28*(1), 209-226.

Decisive Analytics. (2012). Mobile consumerization trends & perceptions IT executive and CEO survey. *Trendmicro.com*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Dernbecher, S., Beck, R., & Weber, S. (2013). Switch to your own to work with the known: An empirical study on consumerization of IT. In *Proceedings of the Americas Conference on Information Systems.*

Evans, J. S. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology*, *59*, 255-278.

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*, 191-197.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy & Security*, *11*(1), 38-54.

Ghosh, A., Gajar, P.K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Global Research in Computer Science*, *4*(4), 62-70.

Harris, M. A., Patten, K., & Regan, E. (2013). The need for BYOD mobile device security awareness and training. In *Proceedings of the Americas Conference on Information Systems.*

Hopkins, N., Sylvester, A., & Tate, M. (2013). Motivations for BYOD: An investigation of the contents of a 21st century school bag. In *Proceedings of the European Conference on Information Systems.*

Jones, N., & Wong, J. (2016). Best practices for managing the unstoppable trends of BYOA, DYOA and BYOT. *Gartner.* Retrieved from https://www.gartner.com/doc/3206817/best-practices-managing-unstoppable-trends

Jiang, J., Klein, G., & Carr, C. (2002). Measuring information system service quality: SERVQUAL from the other side. *MIS Quarterly, 26*(2), 145-166.

Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. In *Proceedings of the Americas Conference on Information Systems*

Leclercq-Vandelannoitte, A. (2015). Leaving employees to their own devices: New practices in the workplace. *The Journal of Business Strategy*, *36*(5), 18-24.

Lee, J., Crossler, R., & Warkentin, M. (2013). Implications of monitoring mechanisms on bring your own device (BYOD) adoption. In *Proceedings of the International Conference on Information Systems.*

Lincke, S., & Green, D. (2012). Combating IS fraud: A teaching case study. In *Proceedings of the Americas Conference on Information Systems*

Loose, M., Weeger, A., & Gewald, H. (2013). BYOD—the next big thing in recruiting? Examining the determinants of BYOD service adoption behavior from the perspective of future employees. In *Proceedings of the Americas Conference on Information Systems*

Mansfield-Devine, S. (2012). BYOD and the enterprise network. *Computer Fraud & Security*, *2012*(4), 14-17.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5-8.

Negahban, A., Windsor, J., & Bien, D. (2015). BYOD in practice: A comparison of four BYOD programs. In *Proceedings of the Americas Conference on Information Systems.*

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT consumerization—a theory and practice review. In *Proceedings of the Americas Conference on Information Systems.*

Ortbach, K. (2015). Unraveling the effect of personal innovativeness on bring-your-own-device (BYOD) intention—the role of perceptions towards enterprise-provided and privately-owned technologies. In *Proceedings of the European Conference on Information Systems.*

Ortbach, K., Walter, N., & Öksüz, A. (2015). Are you ready to lose control? A theory on the role of trust and risk perception on bring-your-own-device policy and information system service quality. In *Proceedings of the European Conference on Information Systems.*

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of model service and its implications for future research. *Journal of Marketing*, *49*(4), 41-50.

Pew Research Center. (2015). *The smartphone difference*. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Pick, R. A. (2015). Centralization and decentralization in information technology governance. *International Journal of Management & Information Systems*, *19*(2), 61-68.

Putri, F. F., & Hovav, A. (2014). Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In *Proceedings of the European Conference on Information Systems.*

Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). Analysis of security controls for BYOD (bring your own device). Melbourne: The University of Melbourne.

Shim, J. P., Mittleman, D., Welke, R., French, A. M., & Guo, J. C. (2013). Bring your own device (BYOD): Current status, issues, and future directions. In *Proceedings of the Americas Conference on Information Systems*

Steelman, Z. R., Lacity, M., & Sabherwal, R. (2016). Charting your organization's bring-your-own-device voyage. *MISQ Executive, 15*(2), 85-104.

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5-8.

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, *2013*(4), 12-13.

Tu, Z., & Yuan, Y. (2015). Coping with BYOD security threat: From management perspective. In *Proceedings of the Americas Conference on Information Systems*

Weeger, A., & Gewald, H. (2014). Factors influencing future employees' decision-making to participate in a BYOD program: Does risk matter? In *Proceedings of the European Conference on Information Systems.*

Weeger, A., Wang, X., & Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems*, *56*(1), 1-10.

Yin, C., Liu, L., & Liu, L. (2014). BYOD implementation: Understanding organizational performance through a gift perspective. In *Proceedings of the Pacific-Asia Conference on Information Systems.*

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81-99.

Appendix A: Developing a Mobile Device Strategy for Fairfield Trust Company

Client Background

The Fairfield Trust Company ("Fairfield") is an independent investment and wealth management firm headquartered in Philadelphia, PA. The firm serves individuals, families, foundations, and other institutions throughout the United States. It was founded in 1975 by Andrew and Annie Fairfield in Philadelphia to serve as the corporate trustee for the trust they had endowed to honor their parents. The Fairfield Trust makes donations to support charitable organizations that share the family's beliefs and philosophies in the fields of education, medicine, and social welfare. It remains in the ownership of the Fairfield family.

In 1982, Fairfield began offering formal investment services to families, corporations, public plans, foundations and endowments. They built a comprehensive range of wealth advisory services to complement their primary services of investment management and trust administration. Fairfield's SEC-registered investment advisor, Fairfield Investment Management ("FIM"), provides access to Fairfield's investment strategies. FIM has US$3 billion of assets under management for Fairfield's proprietary family of mutual funds.

By 2001, Fairfield had expanded its presence outside of Philadelphia to include offices in New York, Delaware, Illinois and California. As of 2012, Fairfield was a national trust company with 12 offices throughout the United States, employed 210 people, and served more than 2,500 clients across the country.

Use of Mobile Devices by Fairfield Employees

The proliferation of mobile consumer devices in the workplace has the potential to create opportunities for employees to work in innovative and productive ways. Technology continues to evolve at a rapid pace and companies must adapt accordingly. People are becoming more familiar with new technologies and want to use them at work without in many cases knowing or considering the potential risks.

Fairfield currently has a corporate-liable BlackBerry program for its employees. Over the last decade, the nature and use of mobile devices by Fairfield employees has changed dramatically. Originally, a few management personnel used corporate-owned BlackBerrys and a few employees had personal cell phones. Currently, all employees at Fairfield are eligible to participate in the corporate-liable BlackBerry program. Of the company's 210 employees, there are 189 participants in the program and approximately the same number of devices to manage and support. Today, the expansive use of these devices results in significant costs associated with paying for the infrastructure and supporting its users.

The company's BlackBerry service contract will end in the next three months at which time the infrastructure is due to be replaced. As such, the company is now at a decision point regarding the future direction of its mobile device policy. The chief information officer has been in contact with their current provider and has informed senior management that costs under the new service contract will increase by approximately 10 percent. In addition, the provider will no longer offer unlimited data usage. At this time, it is not clear what impact this change would have on employee expense amounts in terms of incurring overage charges.

Fairfield has three general categories of employees: management, investment advisors, and administrative support (including human resources, compliance, accounting and IT). The management team and investment advisors travel frequently to meet with current and potential clients, particularly during each quarterly reporting cycle in January, April, August, and October. Personal client service is an important part of the company's culture, which they feel differentiates them from their larger competitors. Regardless of whether or where they are traveling, investor advisors require access to market information from the New York Stock Exchange, NASDAQ, and other exchanges around the world. Changes in technology and personal mobile use have led some employees to request devices that are not currently supported by Fairfield's IT department. Only BlackBerrys are permitted to access company email; therefore, employees find themselves using both their BlackBerry and personal mobile device. Some investment advisors have also asked about bringing their personal tablets to assist with presentations to their clients.

While BlackBerry devices may access company email, there is no external access to the company's network other than through VPN on company-issued laptops. The CIO recently asked the IT department to conduct an in-depth data security survey. It was determined that, while the majority of data stored on the company's servers is low risk, there is some highly confidential client information including social security numbers, addresses, bank and investment account numbers, and detailed information about trusts and wills.

Balancing Client Service Expectations and IT

As a smaller firm, Fairfield walks a delicate balance between meeting client expectations by providing personal service and simultaneously dealing with changing technologies. They want to demonstrate to their clients that they can be as "leading edge" as the larger investment firms, but they are limited by their use of technology and current business practices. They do not allow for online trading via the Internet or via a mobile device-based app. Clients can check on their portfolio by contacting their investment advisor, but they do not have on-demand access to this information.

As Fairfield continues to grow, management is looking for ways to save costs, retain key personnel, and provide comprehensive client service. The BlackBerry program has become an area they want to investigate. Certain management personnel have questioned the costs and benefits of renewing the BlackBerry contract and, instead, have suggested implementing a "bring-your-own-device" ("BYOD") policy as an alternative. Others have suggested keeping the BlackBerry program but limiting it to employees who have the frequent need to use a mobile device for business.

Fairfield has hired your company to assist with developing a mobile device strategy project. They are seeking your recommendations on whether to remain with their current corporate-liable BlackBerry program or move to a BYOD program. Your main point of contact is John Mason, the CIO at Fairfield and head of the mobile strategy project steering committee. The other steering committee members include Janet Richardson (Chief Financial Officer), Sanjay Sunderji (IT Security Manager), Catherine Wu (Chief Compliance Officer) and Jason Manning (Head of Human Resources).

Case Study Questions

Please develop a detailed written report for Fairfield that addresses the questions below (10 to 15 pages maximum). Be sure to include the client's background and issue, your recommended mobile device strategy, and why you recommended it.

1. What risks are associated with implementing a BYOD policy, and how can these risks be addressed? Consider how BYOD risks differ from those in a corporate-owned mobile strategy.

   BYOD risks

   - Tablets and smartphones present the same risks as laptops but are typically protected by a limited set of controls
   - Heavy reliance on employees to patch/update their own device and keep it secured
   - Highly confidential data may be kept on personal mobile devices, and this data may leave the company when an employee resigns or is terminated. It is difficult to manage the data life cycle.

   How risks can be addressed

   - Employee training and awareness
   - Implement and enforce BYOD policies
   - Technical security solutions applicable to any device on any platform. For example, the company could require the use of Mobile Device Management (MDM) software. Today's MDM software can enable a device to access the corporate environment, secure the device and data stored on it or passing through it, and manage all devices from a central location, with real-time access to inventory, configuration, and help desk functions.

   How BYOD risks differ from corporate-owned risks

   - More reliance on users (employees) to manage and secure the device rather than the company's IT staff. Full-time IT personnel tend to be better trained in security issues.

- Employee may inadvertently leave with corporate data on their personal mobile device in cases of termination or resignation. A corporate-owned device would have to be returned to the company.
- Company must be aware of risks unique to different devices and platforms

2. What are the advantages and disadvantages of a corporate-owned mobile device strategy versus a BYOD mobile strategy?

BYOD advantages

- Employee choice results in increased user acceptance and goodwill, since employees tend to choose the right device for their needs
- Enables employees the flexibility to work in a way that optimizes their productivity
- Reduces reliance on a single platform which mitigates technology industry volatility
- Lower travel and expense management requirements: employees deal with carrier billing directly; cost to company is predictable each month under partial subsidy reimbursement plans (i.e., reimbursement of a set fee each month)
- Employees tend to minimize excessive use since this cost comes out of their wallet
- Company has reduced life-cycle asset management costs (i.e., administrative costs associated with replacing equipment every few years, as well as maintaining an inventory)

BYOD disadvantages

- Loss of control over devices by corporate IT
- Proper implementation requires advanced security controls
- Security capabilities and knowledge will vary, both among different technology platforms and among users (employees)
- Employees are expected to self-support but not all will be able to do so; IT department's costs may increase if corporate IT personnel must support multiple devices under multiple platforms

Corporate-owned advantages

- The company procures and owns the device and all data on the device, and only allows this device to access company systems and information
- Company may be able to negotiate lower rates for service than individual employees
- Security management capabilities are well defined and controlled by knowledgeable IT personnel. These personnel will have an in depth knowledge of the corporate-owned device and how to support it.
- Corporate-Owned Disadvantages
- Lack of employee choice over latest technology resulting in dissatisfaction and reduced productivity
- Employees may try to circumvent the system and move data to their personal devices
- Cost of tracking and managing devices (i.e. "phantom" devices for separated employees may exist)
- High travel & expense management costs: recurring carrier billing negotiations and expense management
- Potential for increased cost due to excessive use ("abuse") by employees

3. Should Fairfield allow the execution of trades using electronic devices, or continue its current policy?
   - Benefits of allowing for online trades and/or app trades include convenience for customers, real-time data
   - Risks include how to make the entire process secure, app development issues, etc.

4. How can a company handle the payment and administration of employee expenses related to mobile devices?

   BYOD

   - The company reimburses the employee a flat fee each month for the use of their personal device for work use
   - Employee must be able to provide evidence that costs were business-related
   - Employee pays for excess usage over the flat fee
   - Employee handles all payment administration with the carrier

   Corporate owned

   - The company fully pays for the employee's expenses and handles all payment administration with the carrier
   - The company may opt to subsidize employees differently based on their requirements (for example, employees who travel frequently receive full reimbursement while those who do not travel receive a partial subsidy)

5. How can a company protect its data if it allows access through mobile devices?
   - The company should take an inventory of its data (i.e. low, medium and high sensitivity) and plan its mobile device strategy accordingly. Identifying the type of data to which employees need access can help define the selection of allowable platforms under an employee-owned device model.
   - Companies with highly sensitive data may consider maintaining a corporate-owned device strategy to help ensure the company can effectively minimize its risk exposure to data breaches and data loss. This also avoids ambiguity as to who controls the device and the applications and data on it.
   - Company may choose to limit mobile device access to its internal systems – for example, strict control of access to enterprise applications, prohibit or restrict data movement via email or files, etc.
   - Company may choose to use mobile device management (MDM) software to monitor all devices that access corporate systems and data

6. Which policies should be in place to help companies manage the risk of using mobile devices?

   Effective policies and procedures to cover mobile technology use should:

   - Consider diverse mobile technologies (i.e. phones, laptops, tablets)
   - Consider different employee usage requirements
   - Consider different data classifications (i.e. low, medium, high risk)
   - Be affirmed in writing with any employee prior to granting access to the corporate network

   Best practice mobile device policies should include:

   - Acceptable device usage guidelines
   - User responsibility, including control over the mobile device's life cycle – Procurement, maintenance, decommissioning
   - Security procedures (i.e., device lock, remote wipe capabilities for lost or stolen devices, anti-virus)
   - Liability / privacy expectations (i.e., if MDM is used in monitoring, random device checks)
   - Rate plans and reimbursement (incorporate into Travel & Expense policy)
   - Mobile device support expectations and role of corporate IT

7. What ethical considerations must a company make when defining the "acceptable use" of mobile devices?
   - Policies must define "acceptable use" from both the individual's and the company's perspective

- Should accessing certain websites be restricted, when an employee is also using a personal device for work?
- Since personal mobile devices will be used for both personal and business purposes, they will contain personal information
- Policies must document the process for an employee to safeguard personal data if / when a time comes where the company needs to wipe the device
- Under what circumstances (if any) should the company have a right to remove any non-work-related content from an employee-owned device?
- Mobile Device Management solutions may include the monitoring of mobile devices
- Monitoring could include emails, website visits, and the ability to track a device's location (and consequently the employee's location as well)
- Employees must be made aware of any monitoring and give their consent

8. What compliance issues must be addressed?
    - With personal devices, evaluation of compliance is a complex task
    - **Expense management considerations:** an employee must be able to demonstrate that expenses are business-related; company uses this as evidence that expenses were not compensatory in nature and to support tax deductibility (IRS compliance)
    - Address this by requiring evidence to be submitted along with expense report
    - Privacy considerations: highly confidential data can be stored on mobile devices, which may subsequently be lost/stolen
    - Address this through device security requirements (for example, device lock and remote wipe capabilities)
    - **Legal considerations:** in case of corporate litigation, personal owned mobile devices will increase the complexity and ability to comply with eDiscovery and data retention requirements
    - Address this through back up requirements (this likely would necessitate mobile device management solutions)
    - **Labor considerations:** ensure compliance with Fair Labor Standards Act (FLSA) requirements (e.g., institute policies to ensure non-exempt employees do not conduct work after-hours unless directly authorized/instructed)
    - Address this through maintaining policies and procedures, such as an Employee Handbook

Appendix B: Rules and Procedures

1. Teams will comprise three to five students who are in their first year of study.
2. Teams will be asked to register by Wednesday, February 11, 2015.
3. Teams will meet and be prepared to ask questions, about the case, of advisors from the global accounting firms at the Advisory Kickoff Meeting on Thursday, February 12, 2015, in Bartley TBD.
4. Teams will be advised by an associate at a global accounting firm. Advisors will be able to direct students to resources to help them understand the case but cannot give students direct advice on the answers to case questions or directly assist in preparing the written report. If advisors are unsure about guidance, they should contact their supervising manager.
5. The advisors will be supervised by a manager at a global accounting firm. If the manager is unsure about an advising issue, they should contact the steering committee, made up of five global accounting firm partners and five VSB faculty.
6. Teams will submit a draft of written responses to the case questions by Monday, March 23, 2015. Teams will use a week of advisement with the associate at a global accounting firm, March 23-30, to finalize their written response.
7. Teams will submit a final written response to the case questions by Monday, March 30, 2015. Each team must sign a statement indicating that their report is their own work, and they have followed the university academic integrity policy.
8. Five partners from global accounting firms and five VSB faculty will judge the quality of the cases based on content, presentation quality, and the team's working relationship with the advisor at a global accounting firm. Finalists will be announced Wednesday, April 8, 2015.
9. Finalists will make an oral presentation using PowerPoint slides to the panel of judges on the morning of Saturday, September 19, 2015, during Parents' Weekend.

Appendix C: Written Case Report Assessment Form: Determine Finalists

Table C1. Written Case Report Assessment Form: Determine Finalists

Name of judge	Name of team

Please place a check mark (X) in an appropriate box for each assessment item.

Assessment item		Score (10 = highest, 1 = lowest)									
		1	2	3	4	5	6	7	8	9	10
1.	Organization of the report										
2.	Presentation (professionalism in writing style, grammar, vocabulary, etc.)										
3.	Quality of answer to Ques #1: what risks are associated with implementing a BYOD policy										
4.	Quality of answer to Ques #2: what are the advantages and disadvantages										
5.	Quality of answer to Ques #3: should Fairfield allow the execution of trades										
6.	Quality of answer to Ques #4: how can a company handle the payment										
7.	Quality of answer to Ques #5: how can a company protect its data										
8.	Quality of answer to Ques #6: which policies should be in place										
9.	Quality of answer to Ques #7: what ethical considerations must a company make										
10.	Quality of answer to Ques #8: what compliance issues must be addressed										
11.	Comprehensive understanding of issues, as reflected in the report										
12.	Thoroughness and level of effort evident in the report										
13.	Is there anything that stands out as commendable and noteworthy?										

Appendix D: Finalists Team Presentation Assessment Form

Table D1. Finalists Team Presentation Assessment Form

Name of judge	

Please score each of the five teams by entering a value of 1 to 10 (1 = lowest, 10 = highest) for each of the seven assessment items below. For each team, total the seven scores. Then, rank order your five teams.

Assessment item		**Team 1**	**Team 2**	**Team 3**	**Team 4**
1.	Organization of presentation				
2.	Issues raised and answered: quality				
3.	Issues raised and answered: validity				
4.	Professionalism in delivery				
5.	Effectiveness in communication				
6.	Preparedness and level of effort				
7.	Quality of recommendation				
Total					
Rank (1 = 1st place, 2 = 2nd place, etc.)					

Please provide brief comments, for each of the five teams, in the given space.

	Is there anything that stands out as commendable and noteworthy?
Team 1	
Team 2	
Team 3	
Team 4	
Team 5	
	Room for improvement?
Team 1	
Team 2	
Team 3	
Team 4	
Team 5	

Appendix E: Previous Research on BYOD

Table E1. Previous Research on BYOD

Reference	Research objective	BYOD considerations	Research conclusion
Buettner (2015)	Empirically examine whether employee intention to BYOD is driven by intuitive and automatic reasoning or post hoc rational reasoning.	Support	BYOD user behavior is primarily driven by perceived enjoyment as an intuitive and automatic reasoning construct and perceived usefulness as a post hoc rational construct.
Chen (2014)	Empirically examine how flexibility of multiple personal IT device use interacts with task complexity to influence users' continuance intention of use.	Privacy, security	(Research in progress)
Crossler et al. (2014)	Empirically examine the factors that determine whether employees follow BYOD policies according to the protection motivation theory.	Compliance, privacy, security	Users' intentions to comply with a BYOD policy were motivated by self-efficacy and response efficacy. Threat severity was more salient for accountants than non-accountants. Employees are sensitive to the costs of compliance.
French et al. (2014)	Conference panel discussion of BYOD current use, real-world cases, adoption, pros and cons, issues, and future directions.	Compliance, culture, privacy, security	BYOD action plans should clearly establish the objective, baseline, and stakeholders. Evaluate the program and revise it according to technical/ behavioral changes.
Garba et al. (2015)	Review security and privacy, mobile computing, and current organizational practices regarding BYOD and its adoption.	Privacy, security	Mechanisms or approaches for BYOD security and privacy either sacrifice or expose data or destroy the users' experience.
Harris et al. (2013)	Empirically examine the lack of security awareness among college students entering the workforce.	Security	Security awareness is lacking, demonstrating the need for security awareness and training in organizations.
Hopkins et al. (2013)	Empirically evaluate antecedents to behavioral intention to BYOD among secondary school students.	Non-corporate setting	Students' behavioral intention to BYOD is substantially influenced by their attitude and moderately by their subjective norms and perceived behavioral control.
Lebek et al. (2013)	Empirically investigate the influence of security, privacy, and legal concerns on the intention of employees to use BYOD mobile devices.	Security, privacy	Security, privacy, and legal concerns significantly impact employees' acceptance of BYOD. Employees are indecisive in their intention to use their private mobile devices for work purposes.
Lee et al. (2013)	Investigate the impact of monitoring mechanisms, privacy concerns, and job performance on BYOD program participation.	Compliance, privacy, security	Research in progress.
Loose et al. (2013)	Empirically investigate the determinants of BYOD adoption and acceptance behavior among college students entering the workforce.	Culture, security, support	Performance expectancy is the strongest determinant of intention to use BYOD. Perceived threats negatively impacts adoption behavior. Intention to use BYOD is significantly associated with employer attractiveness.
Mansfield-Devine (2012)	Discuss concerns with BYOD and how networks are managed.	Culture, security	A 10-step process for managing BYOD.

Table E1. Previous Research on BYOD

Ortbach (2015)	Empirically determine the relationship between personal innovativeness in IT and BYOD intention of individuals.	Culture	Ease of use of both the enterprise-provided and privately owned mobile IT mediate the relationship between personal innovativeness in IT and BYOD intention.
Ortbach et al. (2015)	Propose a theoretical model based on organizational trust literature to determine the influence of trust and risk perception on BYOD policies and outcomes.	Culture, IT governance, security, support	Research in progress.
Pick (2015)	Examine IT governance response to changes in technology, organizational goals, and regulatory climate.	Compatibility, IT governance, security, support	BYOD brought a new type of IT governance anarchy.
Putri & Hovav (2014)	Empirically examine employees' intention to comply with an organization's IS security policy in the context of BYOD.	Compliance, security	An employee's perceived response efficacy and perceived justice is positively associated with an employee's intention to comply with BYOD security policy.
Rivera et al. (2013)	Analyze threats introduced by BYOD and how existing control mechanisms will address the most common security threats.	Compliance, culture, security, support	A combination of technical and non-technical security controls is necessary for a secure adoption of BYOD.
Steelman et al. (2016)	Develop a four-wave model that describes the evolution of BYOD and lessons learned based on in-depth case studies.	Compatibility, compliance, culture, IT governance, privacy, security, support	BYOD progressed from prohibiting employee-owned devices to embracing BYOD as a driver of both productivity and innovation.
Thomson (2012)	Examine the BYOD practice, based on questionnaire responses.	IT governance, privacy, security, support	Devise flexible and creative solutions to secure networks and data types that require protection based on organizational needs, regulations, and laws.
Tokuyoshi (2013)	Examine the BYOD conflict between usability and security.	Compliance, security, support	Steps to mitigate risks.
Tu & Yuan (2015)	Propose a theoretical model to identify factors affecting organizations coping with security threat of BYOD.	Security	(Research in progress)
Weeger & Gewald (2014)	Empirically analyze how employees' perceive the benefits and risk associated with BYOD.	Privacy, security	Employees' intention to enroll in a BYOD program is a function of perceived risk, perceived benefits, and personal innovativeness.
Weeger et al. (2015)	Empirically examine what factors determine employee intention to participate in company BYOD programs and how employer attractiveness is affected.	Compatibility, IT governance, security	Perception of BYOD as improving job performance, effortless, contributing to social standing, and resulting in negative outcomes. BYOD programs increase attractiveness for employment.
Yin et al. (2014)	Propose a theoretical model based on gift economy and cognitive evaluation theory, which indicates the informational and controlling aspects of BYOD.	Support	Research in progress.
Zahadat et al. (2015)	Examine BYOD risks balanced by benefits and propose a BYOD security framework, validated by a survey.	Compliance, privacy, security	Present a validated BYOD security framework is the solution to security concerns.

About the Authors

Janice C. Sipior, PhD, is a Professor in the Accounting & Information Systems Department at Villanova University. Her academic experience includes faculty positions at University of Warsaw, Poland; Moscow State Linguistic University, Russia; University of North Carolina at Greensboro, USA; and Canisius College, USA. She is Chair of the Association for Computing Machinery - Special Interest Group on Management Information Systems (ACM-SIGMIS) and serves as Editor-in-Chief of *Information Systems Management*, Senior Editor of *Data Base*, and Associate Editor of *Information Resources Management Journal*. Her research interests include ethical and legal aspects of information technology, system development strategies, and knowledge management.

James Bierstaker received his PhD in Accounting from the University of Connecticut in 1995, and also holds a BS in Accounting from Fordham University. He is an Associate Professor at Villanova University, where he teaches financial auditing and fraud examination. He is on the editorial board of the *Managerial Auditing Journal*. His primary research interests include behavioral auditing research, auditor technology research, and instructional research. He has over 40 publications in accounting journals, including *Accounting, Organizations & Society, Auditing: A Journal of Practice & Theory, Behavioral Research in Accounting, Accounting Horizons, Issues in Accounting Education,* and *Advances in Accounting*.

Q. Chung is a Professor of Information Systems at Villanova University. He received his PhD from Rensselaer Polytechnic Institute, MBA from SUNY at Albany, and BS from Seoul National University. His current research interests include: theorizing big data phenomena, role of social networking in location-based mobile marketing, digital convergence and value creation, trust and deception in digital commerce, and Radio Frequency Identification (RFID) applications in healthcare. His work has been published in such journals as *European Journal of Information Systems, Information & Management, Intelligent Systems in Accounting, Finance and Management, Electronic Markets, Industrial Management & Data Systems, Journal of Operational Research Society, Annals of Operations Research, Omega, INFOR*, and *Expert Systems with Applications*.

Johnny Jiung-Yee Lee is an Associate Clinical Professor of Accountancy at Drexel University. He earned his PhD in Accounting and Information Systems from University of Utah. He has published in journals, such as *Communications of the ACM, Journal of Business Research, Journal of Real Estate Portfolio Management, Accounting Perspectives, Management Research Review,* and *Information Systems Management*. His current research interests are in working capital management, auditing fees, financial report quality, accounting information systems, management accounting, supply-chain, consumer behavior, and business value of information systems.