Bring Your Own Device (BYOD)--Who Is Running Organizations?

James Scott Magruder
University of Southern Mississippi

Stanley X. Lewis
Troy University

Eddy J. Burks
Troy University

Carl Smolinski
Louisiana State University-Shreveport

This paper will discuss what BYOD is and why it is a current trend in business. This paper will also look at why BYOD may be a disaster for organizations that adhere to this trend. One argument for BYOD seems to be that employees do not want to use more than one device: one for their private lives and one for their business lives. Since employees prefer their device the firm has to be concerned that the internal control system is providing the necessary security required by COSO. The benefits and costs of this type of program must be weighed.

Bringing Your Own Device (BYOD) to the office is a current trend in business. This paper will discuss what BYOD is and why it is a current trend in business. This paper will also look at why BYOD may be a disaster for organizations that adhere to this trend.

> "BYOD (Bring Your Own Device) is a huge trend in corporations, hospitals and universities, where employees and other users are allowed to access the corporate network using a wide range of personal devices. BYOD has wide appeal because employees value the convenience and ease of use, while businesses recognize that it allows their staff to be as productive as possible. However, the growth in personal devices being brought into the enterprise network is also a potential security threat as well as a huge headache for IT departments trying to make BYOD work."
>
> "They now expect and increasingly demand the freedom to use their personal devices for work, accessing the company network to perform their daily tasks." (Ten Steps, 2013)

The two above paragraphs are a good description of the BYOD phenomena. Employees are allowed to use their own personal devices to access the organization's information. These personal devices are also

used for their own personal interests. This usage of personal devices may make the employees more productive. The usage of these personal devices may also bring a major security hole to the organization. Is this "increase in productivity" worth it? The authors argue a definite "No". Note also in the second paragraph above that employees "…now expect and increasingly demand…" they be allowed to use their own personal devices. Who is running the organization? Is management running the organization in a prudent manner? Is management creating an effective control environment to maintain privacy of data that is both proprietary in nature and designated as data that should remain private and confidential under various requirements under law?

One argument for BYOD seems to be that employees do not want to use more than one device: one for their private lives and one for their business lives. One suggested solution is BYOD. However, "…personal devices are generally harder to secure than organization-issued devices." (CDWG, 2013) An "integrated approach" is needed to secure these personal devices.(CDWG, 2013) However, one may be able to argue that having two separate devices is much better for security than putting both "lives" on the same device, where it is harder to keep the two separate.

Other arguments for BYOD are "Cost savings", "Increased Flexibility", " Increased Productivity" and recruitment . (BYOD, 2013) Some consider that a prospective employee may choose an employer based upon the employer having a BYOD program. Disadvantages of BYOD: "Data Security", "Cost" (the BYOD may have unexpected costs), "Privacy", and "What happens when an employee leaves?" (BYOD, 2013)

Consider this likely scenario: A worker wants to turn in her corporate-owned BlackBerry in favor of her personal iPhone. She will enthusiastically personalize her iPhone with productivity tools and apps that deliver up-to-the-minute data, as opposed to the less-customizable BlackBerry." (Kaneshige, 2012) Suppose these "productivity tools" and/or "apps" increases the employees productivity by several factors (unlikely in the real world), but these tools also have a security problem in them that is not known for some time. Then the security problem is found by hackers and a security breach occurs. The organizations database may be compromised. Intellectual property may be stolen. Customer data may be compromised. The good name of the organization may be tarnished. Lawsuits may be lodged against the organization. All of this occurred because employees demanded to use their own personal devices. One small security hole in the chosen apps and tools may eventually lead to this.

A list of steps to secure BYOD is given in Bradford networks. (Ten Steps, 2012) The article discusses each step in detail. Only the steps will be listed here:

1. Determine which mobile devices are allowed on the network
2. Determine which OS versions are allowed on the network
3. Determine which applications are mandatory (or prohibited) for each device
4. Determine which groups of employees will be allowed to use these devices
5. Define the who, what, where and when of network access
6. Educate your employees about the BYOD policy
7. Inventory authorized and unauthorized devices
8. Inventory authorized and unauthorized users
9. Control Access Based on the Need to Know
10. Continuous Vulnerability Assessment and Remediation (Ten Steps, 2012)

This is an excellent list of steps to secure BYOD. However, it could also be used by the business and its accounting function to create a list of steps to secure an organization's (regular) network:

1. Determine the devices (PCs, etc.) to be on the network.
2. Determine the operating systems to be used on these devices.
3. Limit the applications to be used on the devices
4. Limit which employees can use the devices and what they can access on the network.
5. Tell the employees what is allowed on the network and what is expected of them.
6. Determine what devices should/should not be on the network.
7. Determine who should/should not be on the network

8. Determine the network access for each job category.

Also note the limitation-intended words (allowed, mandatory, unauthorized, and prohibited) used in the list. Will employees expect and demand these limitations to be removed? BYOD should only be implemented if the benefits and costs of such a business program are taken into account and the benefits outweigh the costs (short and long term). The program should not be implemented just because employees demand it.

So how is securing BYOD different from securing a "regular" network? It increases complexity of the networking environment. It increases the probability of a security hole that will eventually be found by hackers.

> "Organizations across the world continue to strive for greater agility, efficiency and innovation. But they also need to cut costs, improve productivity and become more competitive. . . . These new requirements create complexity and extra tasks for IT to manage. But with greater complexity it is easy to miss a system vulnerability such as an unpatched application or new device on the network, which in turn can cause major security issues." (Why Complex, 2013)

In addition to which, some apps have malware in them already. "Malware targeting mobile devices is rapidly growing in both the number of variants found in the wild and in their complexity and sophistication, but the only platform being actively targeted is Google's Android, which researchers now say resembles Windows on the desktop PC." (Dilger, 2013) "The research noted that mobile threats are overwhelmingly motivated by profits, with 76.5 percent designed specifically to con users out of money, rather than seeking to just cause damage." (Dilger, 2013) So when it becomes profitable for them to attack other mobile devices, it would be expected that they will do so.

A user does not have to download apps to be targeted. [6] "Users on any mobile platform, including iOS, can be targeted with spam that directs them to malware websites."[6] Expect these incidents to increase. Most Android users have not been updating their Android phones. [6] "In contrast, Apple developed iOS with controls that specifically limit what installed apps can do and tightly regulate what personal information they can access." [6] Users of mobile equipment and organizations can only hope that this kind of diligence continues in the mobile market.

A SUCCESSFUL USE OF BYOD

To show an example of success with BYOD, Kaneshige (2012) offered this:

> "The iPad, a popular candidate for inclusion in BYOD programs, recently changed the way Eaton Corp., a 100-year-old hydraulics maker, sold its products, basically upending the sales workflow process. CIO Justin Kershaw measures iPad worker productivity gains by monitoring order intake rate and length of sales cycle, from opportunity to quote to the actual order."

However, it was not clear from Kaneshige's (2012, 2011) two articles whether the discussion was about a successful BYOD (iPad) program or developing a new app that was used on "some 300 distributor-owned iPads, as well as iPads for a small group of internal salespeople." Nonetheless, it is also important to note successful BYOD programs.

SAP is also putting products into the mobile market. Since BYOD is supposed to make employees more productive, they must have access to the organizations databases. "Exposing those back-end systems is complicated, and companies can face a risk of hacking if the systems are misconfigured or do not have up-to-date patches." (Kirk, 2013) Tools may be developed to help in the configuration of these back-end systems. "Boston-based Onapsis will release a new module for its X1 security suite, a product

that performs automated security assessments, penetration testing and compliance audits for SAP's ERP (enterprise resource planning) software, said Mariano Nunez, Onapsis' CEO." (Kirk, 2013) "We see that companies may not be paying enough attention to that and forgetting the devices," Nunez said. "Our empirical experience shows those systems are usually left insecure because of people not applying the latest patches or not following SAP's best security practices." (Kirk, 2013) Note that this last sentence reference "empirical experience". So organizations are not (at least in some instance) correctly securing the systems they currently have. Adding more complexity will only make the situation worse. Automation tools may help.

It should be no surprise that the cost of cybercrimes continue to increase. These attacks have become more common. (Ponemon, 2012) "The most costly cybercrimes are those caused by denial of service, malicious insiders and web-based attacks. Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, application security testing and enterprise governance, risk management and compliance (GRC) solutions." (Ponemon, 2012) All of these attacks may be performed on mobile devices. Adding another vector of complexity only makes the matter worse.

In a recent survey conducted by B2B International on behalf of the security company Kaspersky Lab, 46 percent of IT professionals said they agreed with the statement that anti-malware vendors have inadequate products and services to cope with the security threats of smartphones and tablets. (Ackerman, 2012) This technology needs to improve.

OpenDNS has announced "the general availability of a solution called 'Umbrella' that combines Anycast DNS routing, selective proxying and encrypted VPN to protect mobile workers wherever they are, regardless of whether they are using their own device or a device provided by their employer." (Ackerman, 2012) This system "which will initially be available for the Mac and PC, as well for iOS, encrypts all data that is transmitted from a device and steers it onto a sanitized network for faster, safer delivery." (Ackerman, 2012) It will allow "contextual security policies" to be set up. (Ackerman, 2012) It will take time to see if this is a solution the BYOD security issue.

THE COSO FRAMEWORK

The National Commission on Fraudulent Financial Reporting (the Treadway Commission) beginning in 1985 sponsored and funded by five main professional accounting associations and institutes headquartered in the United States recommended to the business community and the accounting profession that all five associations and institutes work together to develop integrated guidance on internal control. These efforts continue today. The business community knows the results as the Committee of Sponsoring Organizations of the Treadway Commission or COSO. The efforts of COSO were first published in 1992 as a four volume report entitled *Internal Control— Integrated Framework*. This report became the standard for U.S. companies to use to evaluate their compliance with appropriate laws including the Foreign Corrupt Practices Act, and has served as the underlying basis for several efforts by the accounting profession including AS2 (Auditing Standard No. 2, PCAOB and SAS 55/78 (AICPA). (Treadway)

The COSO Framework described five interrelated components which relate to how a business is operated with awareness of the integration of various processes. Although the components apply to all entities, small and mid-size companies may implement them differently than large ones. Its controls may be less formal and less structured, yet a small company can still have effective internal control.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers," (COSO, 1992)

The business community and accounting profession with responsibilities to ensure the components of the COSO Framework are maintained in a reasonable level of security may realize that all the components can no longer be successfully implemented at any level expected by the organizations comprising the COSO efforts to ensure businesses provide an internal control environment that assures privacy and confidentiality of business and individual data. It is a logical assumption that corporations will need to reconsider especially the efforts established to comply with the components of risk assessment, control activities, and information and communication.

There are several practical limitations that can be drawn from a study about BYOB and serve as items that both the business and eventually the internal/external auditors must consider when determining the control environment of the business. These items include (not all inclusive nor in any priority of importance):

1. BYOD is generally not a good idea, security being the overriding concern.
2. Employees have no right to BYOD. An employee who insists that it is his right to BYOD is either a potential trouble-maker and/or someone who might be planning corporate espionage (extreme case.) In any case, a reasonable, knowledgeable employee should understand the concerns with BYOD.
3. Might be actually good for employees to be proficient in the use of more than one device (organization's devices and their own device.)
4. Problems with departing/terminated employees - can you (legally) get a hold of their device and make sure that it is purged?
5. What if personal information was purged accidentally, another potential liability?
6. Would employees be more likely to lose a personal device than an organization device?

7. Easier to instruct employees in the use of devices and provide new apps if all are using the same type of device.
8. Problems with interfacing of devices?
9. Could lead to more use of devices for personal business? Harder to monitor uses of devices for personal business? If they are supposed to be using organization devices, then it's pretty obvious that whenever they are using personal devices, what they are doing is not work related.

In short, business data maintained and used by on a BYOD is no longer private and confidential as well as being subject to misuse or accidently made public.

External auditors must also consider the implications described from a perspective of ensuring that confidential client information as well as that audit engagement decisions and discussions are not accessible if audit staff is allowed to migrate toward a BYOD environment. To do otherwise would potentially increase the legal liability for public accounting firms. (AICPA)

The Impact of the Millennials

A recent report provides further verification of the seriousness of the issue. Over half of the 4,000 employees surveyed admit to storing, sharing and working on company documents on their personal devices and led the researchers to conclude:

> "If you think your BYOD policy telling employees that they can't put sensitive data on their personal smartphones, laptops and tablets is keeping your company safe, think again. Few office workers are actually aware of their company's BYOD policy…."
> Now for the kicker: The security problem is only going to get worse as millennials flood the workplace. That's because millennials, especially on the younger side of the generation, don't really care about security or the stress it causes the IT department; they just want BYOD without restrictions." (Kaneshige, 2013)

One additional observation from the research conducted is that

> "…18- to 24-year-olds are "gourmet chefs of security breach," because they play loose with corporate documents. That's not good, given that millennials will make up the majority of your workforce by 2015, according to the U.S. Bureau of Labor Statistics." (Kaneshige, 2013)

CONCLUSION

BYOD should not be made an organization policy just because employees "demand" to be able to use their own personal devices. The benefits and costs of this type of program must be weighed. It appears that the benefits do not out way the costs of the greater complexity that occurs—potentially leading to a security breach in the organizations network/database. Although there is new technology to manage a BYOD program, at this time, it appears the costs are greater than the benefits of such a program. An increase in risk assessment for the business and the implications of the changing nature of risk assessment poses additional requirements for both the business and its external auditor if they are to allow the migration toward a BYOD environment. Maintaining the confidentiality and privacy of business (client) data is critical. BYOD has several consequences that directly impact efforts to ensure the adherence to control standards.

REFERENCES

Ackerman, E. (2012), OpenDNS Proposes New Approach To Securing BYOD Devices And Protecting Nomadic Workers, http://www.forbes.com/sites/eliseackerman/. 11/13/2012 @ 10:56AM. Downloaded on 7/16/2013.

AICPA, http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00314.pdf

BYOD – The Good, the Bad and the Ugly: What is BYOD?", http://spectrum-coms.co.uk /byodgoodbadugly/. Downloaded 7/16/2013.

CDWG, SECURING BYOD Guidance on the strategies and tools needed for a secure and productive bring-your-own-device-program, CDWG.COM/BYODGUIDE, www.edtechmagazine.com /higher/resource/securing-byod. Downloaded 7/18/2013.

COSO, http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf

Dilger, D.E. (2013), Mobile malware exploding, but only for Android, https://twitter.com/danieleran. Tuesday, May 14, 2013, 03:37 pm PT (06:37 pm ET), downloaded 7/16/2013.

Kaneshige, T. (2011), Enterprise iPad App: A Deal Closer, Tue, December 20, 2011, http://www.cio.com/article/696869/Enterprise_iPad_App_A_Deal_Closer_?page=2&taxonomyId =3005. Downloaded 7/18/2013.

Kaneshige, T. (2012), Are BYOD Workers More Productive? Mon, April 23, 2012, http://www.cio.com/article/704828/Are_BYOD_Workers_More_Productive_?page=2&taxonom yId=600013, downloaded 7/18/2013.

Kaneshige, T. (2013), CIO's Need To Push BYOD to Lure Millennials, http://www.cio.com /article/2383561/byod/cios-need-to-push-byod-policies-to-lure-millennials.html, 08/05/2013, Downloaded on 09/10/2013.

Kaneshige, T. (2013), Confidential Data is Leaving on Workers' Mobile Devices, http://www.cio.com/article/2382912/byod/confidential-data-is-leaving-on-workers--mobile-devices.html, 08/30/2013, Downloaded on 09/10/2013.

Kirk, J. (2013), Security company to release testing tool for SAP mobile access, July 17, 2013 09:05 AM ET. Downloaded on 7/18/2013.

Ponemon Institute, 2012 Cost of Cyber Crime Study: United States, Ponemon Institute© Research Report Sponsored by HP Enterprise Security, Independently conducted by Ponemon Institute LLC Publication Date: October 2012. Downloaded 7/15/2013.

Ten-Steps-To-Secure-BYOD, www.cadincweb.com /wp- content /uploads/2012/04 /CAD _BRAD _Ten_Steps_to_Secure_BYOD.

Treadway,http://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of the_Treadway_Commission .

Why Complexity is IT Security's Worst Enemy, http://www.kaspersky.com/business-security /whitepaper-complexity. Downloaded 7/18/2013.