Security Challenges of BYOD: a Security Education, Training and Awareness perspective

Authors: Hanlin Chen, Jiao Li, Thomas Hoang, Xiaowei Lou

Abstract

This paper explores the security challenges of Bring Your Own Device (BYOD) for users and organisations by identifying the security threats to mobile devices. Based on these challenges, this paper will aim to identify the security education, training and awareness approaches and concepts based on existing literature to form an understanding of how users can be motivated to commit to BYOD policies and practices. The extent in which users are accountable for the security threats related to BYOD is found to be significant in this paper. It is therefore critical that organisations considering implementing BYOD should focus on developing the education, training and awareness programs for its employees based on concepts of motivation, commitment, knowledge retention and the tradeoff between user/device monitoring and user privacy.

Introduction

Bring Your Own Device (BYOD) is the organisational policy that allows employees to bring personally owned mobile devices to the workplace, and use those devices to access authorised company information and applications (Morrow 2012). However, not all organisations adopt BYOD due to the security challenges and threats that mobile devices pose on the organisation's assets.

With the shift in paradigm from a standardized platform of organisation infrastructure and devices towards the Bring Your Own Device (BYOD) paradigm, there are now diverse mobile device platforms that expose an organisation's assets and information to even more threats. Thomson (2012) believes that the implementation of BYOD is inevitable and the sooner organisations address the issues and challenges of BYOD, the better it positions itself in the future.

This paradigm suggests a change from a technology-centric to a user-centric view in security since the standards for security across different devices are inconsistent. This means that security education, training and awareness strategies need to be developed around its users who own and hold the most control of mobile devices.

In the current literature, there is insufficient research into the security education, training and awareness aspects of BYOD, possibly due to its developing nature in organisations. This paper will aim to develop an understanding of BYOD security challenges from the perspective of user awareness, education and training. The research questions that this paper will address are:

1. What are the security risks of BYOD?
2. How can security education, training and awareness programs address these risks?

Literature review

Despite the benefits of BYOD in the value that it provides with employees and organisations such as increased productivity (Thomson 2012), there is also many risks associated with BYOD that have been explored in literature. Perakovic et al. (2012) identified the assets at risk to threats and attacks on mobile devices which can be classified into two categories of user assets and organisational assets:

User assets	*Organisational assets*
• Personal Data • Personal reputation	• Corporate Intellectual Property • Classified information • Financial assets • Device and service availability and functionality • Political reputation

Table 1. Categories of Assets (Perakovic et al. 2012)

Markelj and Bernik (2012) believe that users who use their personal devices for both work and personal put both their personal data and their employer's information and assets at risk. The threats introduced by BYOD on these assets can be classified into four categories: physically based threats, application based threats, network based threats and web-based threats (Perakovic et al 2012).

Physically-based threats	*Application-based threats*	*Network-based threats*	*Web-based threats*
• Device loss/theft • Attacks on devices intended for recycling	• Malware attacks • Inadvertent disclosure of information • Surveillance attacks	• Network spoofing attacks • Network exploits	• Web browser exploits • Automatically downloaded applications

Table 2. Categories of Threats (Perakovic et al. 2012)

Mobile device users are increasingly downloading and installing third-party applications to their devices which enables attackers to target users who disregard security concerns when selecting and installing applications (Mylonas et al. 2012). Users are also at risk of exposure to security threats when using their mobile devices on unsecured networks or browsing malicious webpages that users are often unaware of (Perakovic et al 2012). Mylonas et al. (2012) found that a majority of mobile device users did not install any third-party security software and a considerable amount of users did not believe that security software was essential. Perakovic et al. (2012) also states that the different operating systems of mobile devices increase the complexity of security risks. Each of the four identified operating systems (BlackBerry OS, iOS, Android OS and Windows Phone OS) were seen to have varying levels of security standards. What this signifies is the complexity of security concerns when BYOD will require security to take into consideration the individual OS of user devices as well as their versions when assessing the security threats.

Although threats to the corporate network and the mobile devices can be addressed through technical approaches such as encryption, anti-malware software and firewalls, threats that involve users require a focus on security education and awareness approaches (Markelj et al. 2012). Markelj et al. (2012) argues that the current security education and awareness in users is lacking for mobile device security. Although the education and awareness issues of BYOD are documented in security guidelines and policies, they are dependent on the user's capability and motivation to comply. The phrase "A chain is only as strong as its weakest link" amply illustrates the implications of this BYOD paradigm and the importance of end users to the security of organisational assets. The users are the weakest link in even the most sophisticated security systems and, for the majority of organisations, security remains a box-ticking exercise for compliance requirements (Caldwell, 2012). Moreover, although some organisations invest heavily in the deployment of advanced security solutions to protect corporate networks, many overlook the human behaviour and fallibility factor which is something hackers appear to be exploiting (Robert, 2012).

Morrow (2012) stated that organizations should be highly aware of the security consequences of user devices, the risks introduced by devices, and the need for the organization to educate the users of those to increase their awareness with the BYOD security issues. Thomson (2012) argues that policy and governance is critical to the success of BYOD and that managing BYOD is much broader than managing the endpoint device and should also focus on the user and the security policies that affecting these users. The organizational security policy, user guidelines, education and training should be designed together with the users (Hagen and Albrechtsen, 2010) which would need to explicitly address and clarify device ownership, security, support and maintenance of employee devices as advised by Markelj et al. (2012). It is therefore important to explore the different approaches to security education, training and awareness that help address the security challenges of BYOD affected by the actions and behaviour of users.

User Awareness and Motivation

In regards to the human fallibility factor, Albrechtsen (2007) argues that a key issue is the user's lack of motivation and knowledge regarding information security. Albrechtsen (2007) found that users often do not follow information security guidelines and procedures and prioritise other work tasks over security. The findings from Post and Kagan's (2007) study also found that users perceived security practices that are too restrictive as a hindrance and interference, who may then find ways around security in order increase productivity in their work tasks. These findings are complemented by Stanton et al. (2005) where

users were found to have a dismal record of behaviour complying with basic security guidelines. Stanton et al. (2005) believes that rewards or motivational approaches help improve user's security behaviour.

To address the subject of motivation, Siponen (2000) provided a conceptual foundation of principles and approaches to motivate users to commit to security guidelines through security awareness programs. Siponen discusses the role of human factors in the success of security initiatives and argues that it is critical for users to be intrinsically motivated in order to comply and commit with security guidelines and policies. As such, one of the behavioural theories that Siponen (2000) focuses on is the intrinsic motivation theory. This theory refers to the user's self-determination, which is their freedom to make their own choices regarding their behaviour. They need to justify their actions in terms of internal reasons such as their own aspirations instead of extrinsic motivations such as financial gain. Forming such intrinsic motivations to commit to security guidelines is defined as *internalization* which drives long-term commitment.

Siponen (2000) argues that users need a rational and logical presentation of facts and information in order to improve their understanding of security. Stewart and Lacey (2012) also state that the security issues involving user behaviour are assumed to be caused by a lack of facts and information available to the user. Security policies and guidelines that are logical and rational will pave the way for intrinsic motivation to be achieved through other principles such as the user's morals and ethics, feeling of security and well-being (Siponen 2000).

Eminagaoglu et al. (2012) also believe that user motivation is a critical success factor for security awareness programs and states that security should be easy, quick and simple to understand. Goucher's (2009) argues that the most successful motivator is peer and cultural pressure to normalise. Pahnila et al. (2007) found that the user's attitudes and the perceived behavioural expectations that their peers and the security culture place on them (normative beliefs) have a significant effect on a user's intention to comply with security policies.

Education and Training

Albrechtsen and Hovden (2010) have claimed that user participation, discussions and collective reflection in groups in training and awareness programmes were shown to provide positive changes in short term security awareness and behaviour. The intervention programme in this study, which aimed to improve the information security attitudes of users, found that the most powerful and effective factor of the programme was the workshops which aimed to impart procedural (Albrechtsen and Hovden, 2010).

The frequency and duration of the workshops were low but efficient in delivering information which is supported by Goucher's (2009) element of *attention* in training which states that, due to the short attention span of users, training will need to convey information concisely and effectively. It was also found that the effects of the workshops on security awareness and behaviour remained for more than half a year after the education and training programmes, but the detailed knowledge on information security issues diminished. Walsh and Homan (2012) found in their study that computer-based security training programs, when compared to instructor-based programs such as workshops, were much more effective in retention of information. Users from the instructor-based programs had a statistically significant decrease in results when taking a 60-day test quiz. The knowledge transferred by instructor-based training was at a higher rate than computer based but does not necessarily mean that the information will be retained. Furthermore, Walsh and Homan (2012) found that after 90 days, users from both instructor and computer based training had no significant difference in the knowledge retained from training; they had reverted to the level of knowledge prior to training.

The intervention programme study (Albrechtsen and Hovden, 2010) claimed that workshops which were not interesting or motivating were unlikely to lead to any changes in behaviour; reinforcing Siponen's (2000) suggestion of intrinsic motivation in education through *excitement* which can achieved by the education program and the instructors. Hagen et al. (2010) also highlighted that a '*fun factor'* could be further developed into their Information Security Awareness program as it is a significant factor that keeps users engaged and motivated.

Discussion

Influence of Users in BYOD Security Risks

As the security standard for mobile platforms is so diverse due to the amount of different operation systems and application software, the security risk of one user's device will differ from another user's. Organisations will have less expertise and experience in providing support for every user's device. Furthermore, many of the different security threats identified by Perakovic et al. (2012) were related to either a negligence or human fallibility issue from the User. Users should therefore be required to assume the responsibility of their devices and be aware of the security risks that their device has to the corporate network as well as the organisation's assets.

In order to facilitate this shift in responsibilities, users must firstly be informed and made aware of the security threats from their mobile devices. Many users don't understand the extent to which the mobile device platform is being maliciously targeted (Mylonas et al., 2012) and because of this, they do not take the necessary safeguards to protect their devices. This places their mobile device at risk to all four categories of threats: physically-based, application-based, network-based and web-based threats.

A basic safeguard against physically-based threats that users may neglect is the locking of their devices using passwords. Having a password will prevent non-sophisticated attempts of unauthorised access to the device and can give the organisation time to take countermeasures when a device is lost or stolen, such as remotely wiping the information on the device. Perakovic et al (2012) also identified the dangers of unsecured devices recycled by users when personal or organisational information and assets are still accessible by that device. Organisations should therefore develop and communicate device recycling policies regarding user's devices which may require users to recycle their devices through the organisation to destroy sensitive information about the user and the organisation.

Application, network and web-based threats are more technical in nature which will be challenging for non-technical users to take precautions against. A basic precaution against these threats is to install organisation approved third-party security software onto the devices, although such software may not be effective against sophisticated and targeted attacks on the device. Users should also be aware of the possible security risks of using their devices on unsecure networks outside of the corporate network and installing unverified applications. When installing an application, users may unknowingly give privileges to the application to access and use the GPS data of a device or take control of certain functions of the device such as the camera (Markelj and Bernik, 2012).

Many of the threats to mobile device security originate or facilitated by uninformed or negligent users. It is therefore crucial for security education, training and awareness programs to inform users about the different security threats of mobile devices and the consequences of those threats in order to shift some of the security responsibilities onto the user. An informed user who is responsible for the security of their device is less likely to perform actions that may compromise their personal data and the corporate data.

Education and Training of BYOD

The BYOD security issues as identified by Perakovic et al (2012) will require education and training approaches to raise awareness of threats that are facilitated by user negligence or unawareness. If a user is informed through education and training that their identity could be stolen when using a mobile device, they will be more wary of its physical security.

It should also aim to raise awareness of the security vulnerabilities of mobile devices, especially within the application, network and web-based security threats since users were inclined to believe that there wasn't a need for installing security software onto their devices (Mylanos et al. 2012). Workshops tailored to demonstrate these mobile device vulnerabilities should aim to be interactive and 'fun' and invoke excitement within users while also be related with the user's work processes and tasks. In order to avoid users perceiving education and training to be a hindrance, the education and training programs should be short in duration and concise but still effective in conveying information.

Workshops and Instructor-based training programs were found to be more effective at relaying information to the user, however computer-based training programs were seen to be more effective in

retaining information (Albrechtsen and Hovden 2010; Walsh and Homan 2012). In order for the training to achieve a long term effect, organizations should provide users with a combination of computer-based training material and schedule multiple workshops and instructor-based training programs to reiterate BYOD security knowledge. These scheduled workshops and training programs should be held approximately every 90 days which was found to be the time it takes for users to revert to their old security habits and knowledge (Walsh and Homan, 2012).

User Motivation and Commitment to BYOD

Some organisations focus on formulating the security policies guidelines within the company but overlook the aspect of motivation to encourage users to commit to security guidelines and policies. Although training and education will raise the awareness of security issues of BYOD, users who are not motivated are less likely to commit follow the security guidelines.

In BYOD, a lot of the responsibility of the devices needs to be shifted to the user where they are expected to manage the security issues of their devices. Because of this, it is essential that users have more of an active role in the development of security policies, guidelines and the education and training programs. This will help users feel more related to the security policies and encourage security commitment.

In order to motivate users to adopt BYOD security practices, Siponen (2000) has explored a range of persuasive principles and approaches that aim to intrinsically motivate users. These approaches include:

Morals and ethics: This approach is based on the concept that if users were to understand the moral and ethical dimensions of BYOD security practices and the possible morally negative consequences of security breaches on their device, they would probably be more likely to follow the guidelines.

Well-being: this approach aims to make users aware of the security implications of poor mobile device security and how it may affect the well-being of the user and the. The consequences of well-being may be moral or non-moral such as financial loss or violation of employment contracts. Users that are made aware of the consequences of mobile device security breaches on their well-being as well as the well-being of the organisation help increase motivation to comply with BYOD security policies and guidelines.

Feeling of security: this approach aims to satisfy the user's need and desire to feel safe and secure. Siponen (2000) states that it is reasonable to assume that people want to achieve and maintain a feeling of security through adherence to security procedures. Feeling of security aims to allow users to recognize the implications of security issues and threats on the user personally by highlighting the invasion of privacy and unauthorized access to their personal information.

Organisations should therefore incorporate these principles in security education, training and awareness programmes in order to increase user commitment and responsibility to security and address the security challenges of BYOD that are influenced by the device usage behaviour and security habits of users.

Monitoring BYOD and User Privacy

A key challenge for the success of BYOD is how organisations can monitor, manage and control users and their device (Markelj and Bernik, 2010) without invading their privacy. There is a blurred line between personal data and organisation information on user devices and the security policies, education, training and awareness programs will need to clearly define this line for employees to mitigate future issues which may cause a user to feel that their privacy is violated. For example, if a user's device was discovered to be compromised with malware and spyware, the organisation may need to seize the device. A violation of privacy may cause employees to lose motivation as it may conflict with their feeling of security, well-being and morals and ethics.

The trade-off between monitoring and user privacy will be a challenge for BYOD as it will require users to have more responsibility in reporting security issues if there is little monitoring and control of the user's device by the organisation. However, in the case where there has been a security leak, users may not be inclined to report the security breach to the organisation as it conflicts with their personal interests. In the end, it depends on the extent to which an organisation can trust users to behave morally and ethically in order to respect the user's privacy.

Conclusion

In conclusion, many of the security challenges of BYOD are related to the behaviors and security habits of users and therefore security education, training and awareness can help mitigate the threats posed by mobile devices. Mobile devices are currently highly susceptible to security risks due to the inconsistent security standards across different operating systems and applications which also expose traditional corporate network security to those risks. Users need to be made aware of these risks through effective education and training in order for the organisation to transfer the responsibility of security to users when implementing BYOD.

Although BYOD security policies, guidelines and education can be developed and communicated to users to raise awareness, without motivation and incentives, it is unlikely for users follow them. There is a need for awareness programs to complement BYOD security education and training in order to motivate users. This motivation can be addressed by appealing to the user's morals and ethics, feeling of security and well-being by raising the awareness of the BYOD security consequences. By understanding the moral and non-moral consequences of their actions, users will be more inclined to internalise BYOD security policies and guidelines.

Monitoring and controlling of how users use their device through software will significantly help mitigate the security threats on mobile devices. However, due to fact that these devices are not owned by the organisation and it contains personal data, there is a trade-off between the extent to which an organisation can monitor the mobile devices and the user's privacy. This balance between monitoring and privacy should be decided by both the organisation and users and well communicated in order to prevent users from feeling that their privacy is violated.

Organisations will need to clearly define the extent to which they will implement BYOD in terms of how much access and responsibility is placed onto users. Security policies and guidelines will need to be developed with the contribution of users in order to align with the user's perception of morals and ethics, security, well-being and privacy. Even in organisations that currently do not implement BYOD policies, BYOD is an inevitable change in security paradigm since employees will want to use their own devices for both personal and work reasons. Employees may even try to find a way around security to use their devices in order to increase their work productivity and accessibility from outside the corporate network, introducing security risks that organisation are unaware of.

Bibliography

Albrechtsen, E. 2007, "A qualitative study of users' view on information security", *Computers & security*, *26*(4), pages 276-289.

Albrechtsen, E. & Hovden, J. 2010, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security,* volume 29 Issue 4, pages 432 – 445.

Caldwell T, 2012, "Training – the weakest link Original Research Article", *Computer Fraud & Security*, Volume 2012, Issue 9, Pages 8-14.

Cohen, F. 1999, "Managing network security: The limits of awareness", *Network Security*, 1999(6), pages 8-10.

Goucher, W. 2009, "The challenge of security awareness training". *Computer Fraud & Security*, *2009*(10), pages 15-16.

Hagen, J., Albrechtsen, E., & Johnsen, S. O. 2011, 'The long-term effects of information security e-learning on organizational learning", *Information Management & Computer Security*, *19*(3), pages 140-154.

Kruger, H. A., & Kearney, W. D. 2006, "A prototype for assessing information security awareness", *computers & security*, 25(4), pages 289-296.

Kruger, H., Drevin, L., & Steyn, T. 2010, "A vocabulary test to assess information security awareness", *Information Management & Computer Security*,18(5), pages 316-327.

Markelj, B., & Bernik, I. 2012, "Mobile devices and corporate data security", *International Journal of Education and Information Technologies*, 6(1), pages 97-104.

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

Mylonas, A., Kastania, A., & Gritzalis, D. 2012, "Delegate the smartphone user? Security awareness in smartphone platforms". *Computers & Security*.

Pahnila, S., Siponen, M., & Mahmood, A. 2007, "Employees' behavior towards IS security policy compliance". *In System Sciences*.

Perakovic, D., Remenar, V., and Husnjak, S. 2012, "Reseach of security threats in the use of modern terminal devices"

Post, G. V., & Kagan, A. 2007, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks", *Computers & Security*, 26(3), pages 229-237.

Robert, G. 2012, "Challenges and benefits in a mobile medical world: Institutions should create a set of BYOD guidelines that foster mobile device usage", ISSN: 1074-4770, 2013 Feb; Vol. 34 (2), pp. 6-7.

Siponen, M. T. 2000, "A conceptual foundation for organizational information security awareness", *information Management & Computer Security*, 8(1), pages 31-41.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. 2005, "Analysis of end user security behaviors", *Computers & Security*, 24(2), pages 124-133.

Stewart, G., Lacey, D. 2012, "Death by a thousand facts; Criticising the technocratic approach to information security awareness".

Thomson, G., 2012, "BYOD: Enabling the chaos", *Network Security*, Issue 2, pages 5-8.

Walsh, P. W., Homan, J. V. 2012, "Measuring the effectiveness of information security training: A comparative analysis of computer based training and instructor-based training, Issues in Information Systems", 13(1), pages 215-224.

White, D., Rea, A., 2008, "Just Trying to Be Friendly: A Case Study in Social Engineering", *Journal of Information System Security*, 4(2), pages 56–85.

Author/s:
Chen, Hanlin; Li, Jiao; Hoang, Thomas; Lou, Xiaowei

Title:
Security challenges of BYOD: a security education, training and awareness perspective

Date:
2013

Citation:
Chen, H., Li, J., Hoang, T., & Lou, X. (2013). Security challenges of BYOD: a security education, training and awareness perspective. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33347

File Description:
Security challenges of BYOD: a security education, training and awareness perspective