Effectiveness of security controls in BYOD environments

Zoran Marjanovic

Introduction

Mobile computing introduced completely new security risks and increased the potential of the old ones. Remote access as an enabler of mobile computing opened the organisations' systems to various attacks from the Internet, both technical and social ones. Regular access to the Internet outside corporate systems exposed mobile devices to malicious code and hackers which improved the attack success rate. As a response, security experts have been developing technical and non-technical mechanisms for protection of information. They have been trying to identify the most effective approach and combination of security controls that can deliver maximum security without impairing the business processes.

These efforts increased with the introduction of Bring Your Own Device (BYOD) concept. BYOD reduces IT costs and provides more flexible work experience. So far, many organisations decided to allow user-owned devices on the system and the trend is still growing. From information security perspective, BYOD comes with risks common for mobile computing, but it also introduces new technical and legal ones. Technical solution providers have been trying to develop security systems that can help organisation in adopting the BYOD concept, and security experts have been trying to design a complete security strategy that can meet the challenges of BYOD. The focus of these efforts is information security.

Information Security Controls

IT Governance Institute (2006) advises that organisations and businesses must have an effective security strategy in order to enable secure business operations. The top management needs to be fully engaged at the governance level to ensure the security and integrity of critical information assets. The most important part of an information security governance policy is management of security risks. The security risks are identified, classified and mitigating factors applied using the most effective measures. From the information security perspective, these measures or mitigating factors are called security controls and their purpose is to minimise or completely eliminate the potential impact of identified risks.

TOGAF (The Open Group 2011) explains the general risk management approach as an iterative process where initial level risks are identified, classified and mitigated. This is followed by a reassessment of the risk and evaluation of the applied mitigating factors or security controls. The business assesses the severity of the residual risk and decides whether additional or different security controls need to be applied. The process repeats until the risk is reduced to an acceptable level.

The selection of the most effective and suitable security controls is guided by the results of security risk assessment and business impact analysis (Protective Security Policy Section 2012). The goal is to identify and implement the most effective controls that will support and not impair the business. Straub (1990) notes that managerial concern about security is influenced by the perception of the inherent risk and that misunderstanding or underestimating risks may lead to underfunding of security which could expose the organisation to losses that could have been prevented. This is why it is critical for the management to understand the risks and controls that can minimise or eliminate these risks and the impact to the business.

Technical Security Controls

Generally, security controls can be divided into two groups, technical and non-technical controls. Technical controls are implemented at the computer software and hardware level, while non-technical controls are used at the organisational level and are focused on influencing human behaviour.

Venter and Eloff (2003) describe two categories of technical information security controls: proactive and reactive. Proactive controls are technical solutions used to prevent unauthorised access to data and resources, and reactive measures are technical solutions used as a response to a security breach as soon as it is detected.

Table 1: Proactive technical security controls (Venter and Eloff 2003).

Proactive Information Security Technologies	**Description**
Cryptography	Protects data confidentiality and integrity
Digital signatures	Ensure data integrity, authenticity and non-repudiation
Digital certificates	Communicate trust on the Internet and ensures confidentiality
Virtual Private Network	Protects data confidentiality and integrity on public networks
Vulnerability scanners	Discover vulnerabilities on IS
Anti-virus scanner	Provide protection of malicious code
Security protocols	Enable secure communication (e.g. IPsec, Kerberos, 802.1x)
Security hardware	Provides security services at device level (e.g. encryption)
Security SDKs	Development tools used to create secure programs

Table 2: Reactive technical security controls (Venter and Eloff 2003).

Reactive Information Security Technologies	**Description**
Firewalls and proxies	Traffic filtering at network and application level
Access control	Access right management (e.g. access to data, resources, services)
Passwords	Authentication – managing access to the information system
Biometrics	Authentication – managing access to the information system
Intrusion detection systems	System access monitoring and alerting
Logging	Audits and records access to data, resources and services
Remote access policies	Define and enforce restrictions for remote access to the system

Non-technical Security Controls

Non-technical information security controls such as guidelines and policies are used to influence the behaviour of employees. The level of detail and clarity of security policies greatly affect the employees' understanding and perception of security issues. Purser (2002) explains that security policies need to be clear, specific and easy to understand. For example, in the area of access control, the policy should provide clear instructions on granularity of access, ownership of data and resources, and roles and responsibilities relating to access control process. Once the policies are in place, the users need to be informed and educated about the acceptable use of the system. Straub (1990) advises to have employees sign a data contract and effectively have them take the responsibility and accountability for the data they work with.

Deterrents clearly define legitimate and acceptable use of information systems and discourage potential offenders by threatening them with sanctions. Straub (1990) argues that deterrents are successful in lowering computer abuse by weakly motivated employees. He adds that the effectiveness of deterrents depends on two factors: certainty and severity of sanctions.

Straub (1990) notes that it is thought that visibility of certain security controls additionally discourages employees from abusing the system. For example visibility of surveillance and monitoring measures as well as security staff may act as another layer of protection from abuse of computers and leak of information. Regular monitoring of employees behaviour can help to spot unusual and suspicious actions that could alarm the security staff before a breach of the system or leakage of information. Such controls can help with enforcing compliance with the security policies. Examples are monitoring of compliance with password, data and web access policies. Any detected violations need to result in sanctioning the offenders in a visible way in order to ensure future compliance with security directives.

Zviran and Haga (1999) emphasise the importance of monitoring of employees' compliance with security guidelines and policies. In their studies on compliance with user password specifications not enforced through technical means, they found that users rarely followed recommendations and directives defined in policies and communicated in security awareness trainings. So they suggest that organisations need to test the effectiveness of educational efforts that aim to increase employees' awareness of security issues, and have means to monitor the implementation of security directives and recommendations.

Security Strategies

Most organisations rely on a combination of technical and non-technical security controls. Ahmad, Maynard and Park (2012) identified specific approaches in academic literature and defined them as security strategies. They found that all the organisations that were covered by their study used the prevention strategy as the first line of defense, while other strategies were also considered. The organisations combined technical and non-technical controls in order to engineer the best and affordable defense of the information and resources.

Table 3: Security strategies defined in academic literature (Ahmad, Maynard and Park 2012).

Security Strategy	Definition
Prevention	Proactive approach to attacks and abuse of systems and information
Deterrence	Use of sanctions to discourage potential offenders
Surveillance	Real-time monitoring of the system and user activities
Detection	Monitoring of user activities for signs of misbehaviour
Response	Reactive approach to attacks and abuse of systems and information
Deception	Decoys used for misleading attackers and offenders
Perimeter defense	Traffic monitoring and filtering devices
Compartmentalisation	Separation of assets in combination with access restrictions
Layering	Implementation of multiple security controls in a cumulative way

Bring Your Own Device

In today's fast paced and interconnected world, most organisations and businesses use the Internet as an extension of their computerised information systems to support their processes and communicate information. Morrow (2012) explains that the availability of the Internet introduced new trends that boosted business and employees' productivity, including mobile computing and so called road warriors. It enabled employees to connect to the information system from any location in the world and at any time and do the work as if they were in the office. One such a trend in mobile computing is called Bring Your Own Device (BYOD). The idea is to reduce organisation's investment in hardware and software, as well as to enable the employees to connect and work from home or while commuting, effectively making the work more seamless and life more convenient. Neff (2013) argues that organisations can generate substantial savings from reduced IT costs and increased productivity. He refers to the case of Intel who, according to their CIO, saves $150 million a year through a BYOD program.

However, BYOD introduced a range of new security risks. Some of these risks are BYOD specific, while others are common for the systems supporting mobile computing. Neff (2013) suggests that organisations who opt for BYOD need to use a combination of technical measures and crystal-clear policies that define what devices can be used, what data should be accessed from these devices, what applications and services must be avoided for security and compliance reasons, and what happens when such a device is lost, stolen or the owner leaves the company. BYOD is not a great idea for certain industries who deal with sensitive information, such as healthcare and financial organisations. But if they decide to adopt it, they need an exceptionally defined program to ensure that every device follows the rules and compliance functions. Neff suggests that organisations need to focus on policies instead of technical solutions and try to understand the user behaviour, communicate what can and cannot be done, and explain why.

BYOD-specific Risks and Solutions

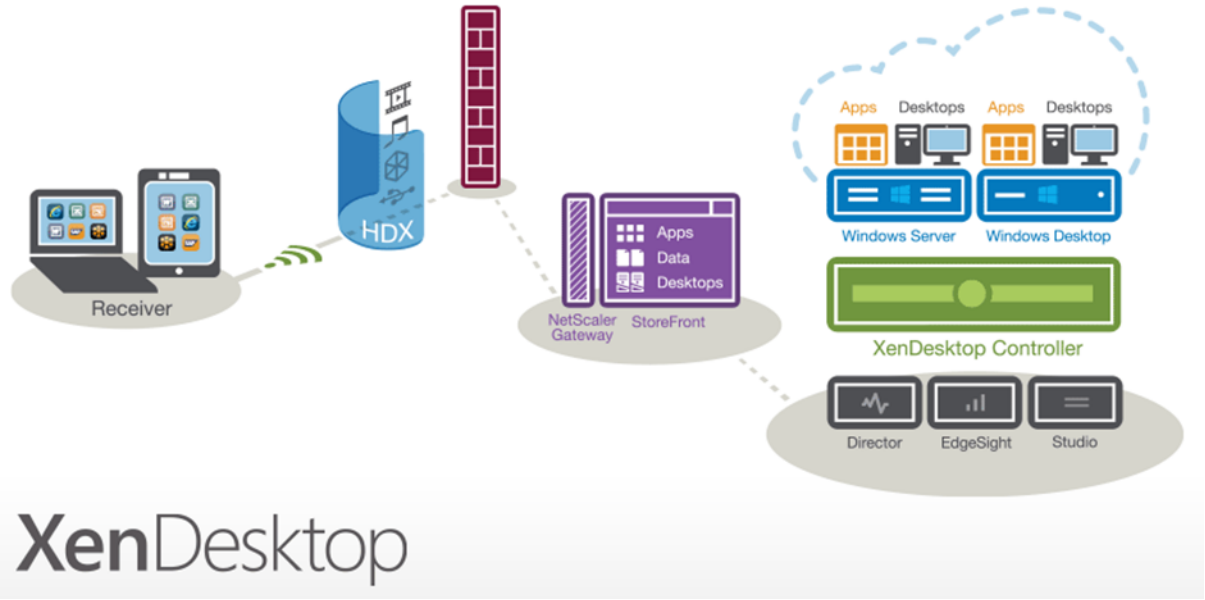
Most organisations address BYOD-specific risks by implementing security strategies described by Ahmad et al (2012) as prevention, perimeter defence and compartmentalisation. Marrow (2012) describes different scenarios for theft and leak of information involving malicious code, unmanaged devices and careless users. He notes that organisations have less control and visibility, as well as fewer mitigation options with unmanaged or partially managed devices. Several studies showed that over two thirds of managers are aware of security risks related to BYOD and admit that they do not have the necessary security controls in place to protect the confidential information. Marrow suggest that organisations need to implement a layered security strategy in order to address the BYOD risks and maintain compliance. It is necessary for organisations to switch their focus from devices to information and compartmentalise sensitive information in order to improve data access control.

Due to the lack of control over devices that often operate outside the organisation's boundaries, excessive privileges granted to mobile users in order to be able to use all the features of their devices, differences in how various vendors address access control and permissions management in their platforms and applications, Payne (2013) suggests that organisations need to follow risk mitigation best practices and advises against allowing users to store information on mobile devices, but keep it at the backend, and only displaying it on the end-user's device through secure channels.

An industry solution that enables compartmentalisation and enforces backend storage of data is Citrix HDX SmartAccess technology in combination with Citrix Access Gateway. It can be used to lock the system down and prevent users from saving data on the local devices, printing documents and even can restrict access to certain applications depending on the device used and the user's current location (Citrix nd). In this case, the backend part of the system with all the servers, applications and storages would be separated from the frontend part of the system with client access points. Effectively, the data and applications reside in one network, while users connect to another network either locally or through remote access. These two networks are connected with a device that allows only a specific protocol for publishing virtual desktops and/or applications.

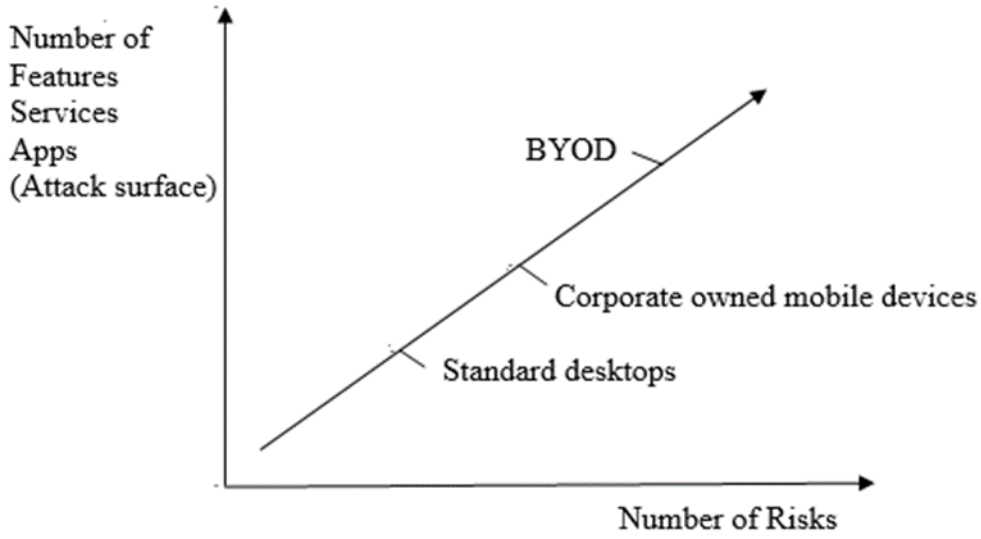
"Citrix XenDesktop is built to be secure by design. Core in the product's DNA is the idea that all data remain in the datacenter unless it can be audited, controlled, and enforced by policy. (Citrix nd, p. 6)"

Figure 1: Citrix HDX SmartAccess – virtual desktop (Citrix nd).



If storing data locally on mobile devices is necessary, then organisations need to look into the most optimal combination of technical and non-technical controls in order to reduce BYOD-related risks as much as possible. According to Payne (2013) a number of features built into the modern mobile technologies reduces the effectiveness of traditional security controls. The system's attack surface enlarges with the increase of the number of functions and services supported by mobile devices. Users should never be trusted by the system and strict security controls should apply across the entire system and at all times, including limiting duration of idle sessions and applying automated responses to a breach of policies.

Figure 2: Relationship between the size of the attack surface and the risk exposure of a system with a different type of devices in use.



Phifer (2012) notes that only thirty nine percent of organisations that use mobile devices implemented security controls to address the risks associated with such devices, and less than half of these were actually able to enforce the relevant security policies. There are many Mobile Device Management (MDM) products available that can mitigate BYOD risks. Organisations can use MDMs to enforce data encryption and two-factor authentication, deploy VPN clients and anti-malware software, as well as to push virtual desktop applications and sandboxed browsers. Phifer (2012) suggests that organisations need to be well aware of the limitations of these technologies before fully embracing BYOD. For example, even though MDMs support a remote wipe of mobile devices, most Android phones will simply be reset to factory defaults with data left on the removable storage in a clear-text format. For these reasons, organisations need to evaluate capabilities of MDM products and match these to the information security requirements defined by the business in order to be able to make an informed decision when selecting and purchasing an MDM product. Marrow (2012) notes that organisations also need to improve their monitoring, logging and alerting capabilities of the systems, and deploy specialised security solutions designed to secure and manage BYOD strategies.

Designing Security Policies

Marrow (2012) argues that most data leaks occur due to a lack of security awareness and not malicious intentions of users, so organisations need to invest in educating their users about security concerns and ensuring that everyone understand and comply with security policies. Mansfield-Devine (2012) explains that once organisations decide to go with BYOD they no longer own the devices, so they have to make the employees part of the security strategy. As BYOD introduces low level of visibility and makes standard security controls less effective, it is critical for the designers of the security strategy to understand the needs and wants of the BYOD users. Organisations first need to increase the visibility of mobile devices, that is, they need to know what they have on the network. The next step is to understand where the edge of the organisation's system is and to lock the access points down with the necessary security control mechanisms. These controls need to be able to identify who and what is connecting to the system, and record and log all activities and behaviour of users and applications. Finally, organisations need to understand who is going to use BYOD and for what purposes, what devices are going to be used and why, what applications will be used and for what reasons, and how and from what locations users need and want to be able to connect.

To answer all these questions, organisations need to engage in a dialog with their users and encourage them to communicate and explain their needs and wants. Once information on requirements, applications and devices are collected and processed, the security staff needs to educate and train users on how to recognise and deal with the security risks that come with a BYOD program. It is necessary to map the risks and threats to specific devices, applications and behaviour identified by the users, and ensure that everyone understands the security issues related to BYOD. Mansfield-Devine (2012) warns that if users are not involved in defining security policies, they are going to perceive these policies as restrictions designed against them and they are going to look for ways to bypass these restrictions. Making the users part of security team, makes information security everyone's concern. Users will respond to this approach by actively participating in designing and implementing the security strategy. Increasing awareness about security also helps users to make more informed decisions when purchasing new devices or downloading applications which reduces the attack surface of the system and makes security management easier.

Methodology

I developed my security policy perspective on Bring Your Own Device security by conducting a literature review on papers from high quality IS journals and relevant security and IT journals. These are: Compliance Week, Computer Fraud & Security, Computers & Security, Information Security, Information Systems Research, IT Professional, Journal of Intelligent Manufacturing, Journal of Management Information Systems, and Network Security.

I used the Science Direct and Elsevier databases as well as Google Scholar. I found 38 articles of which 23 were relevant. I focused on articles with the following themes that related to our research question:

Effective approaches to securing BYOD environments

Risks associated with BYOD programs

Securing ISs that adopted BYOD

Technical and non-technical security controls for BYOD environments

Discussion

Security Controls

Both academics and industry experts agree that information security acts as an enabler of business by protecting the confidential information and keeping the resources available. However, their views of the most effective security controls are not aligned. Academics acknowledge the importance of technical controls, they emphasise the limitations of the technology and argue that the most important component of a complete information security strategy is human element. They believe that only those security solutions that involve employees in design and implementation of security solutions can actually deliver high level of security standards. While industry experts tend to agree with the views of academics, the studies show that in reality most organisations' security strategies focus on technical solutions and security policies enforced by a system of sanctions. Even though many studies showed that this approach is not delivering good results in practice, there are no signs that organisations are genuinely interested in exploring other methods.

BYOD-specific security risks and solutions

Although BYOD seems to be just a variation of mobile computing, it introduces a range of new risks and has a potential to change the way organisations manage their information and resources. Lost and stolen devices, unauthorised devices and applications, insecure communication channels, vulnerabilities in different mobile platforms, inability to manage unsupported devices remotely present some of the challenges the organisations who choose the BYOD path are going to face and deal with. Ultimately, it is a role of the business to assess the risks and benefits and decide whether BYOD presents a value to the business. If they decide to adopt it, it is critical to organise the information storage in an easily manageable and accessible way, and classify and compartmentalise confidential information in order to reduce the risk of information leak. It is also critical to deploy security controls and tools that were designed to support BYOD environments and are capable of increasing the device visibility and control. Additionally, in order to be able to deliver an end-to-end security solution and ensure business compliance with regulations, organisations need to involve their employees in all stages of design and implementation of security solutions.

Conclusion

Designing the most effective security strategy suitable for BYOD environments requires a close collaboration between top management, security staff and end-users. The job of the security staff is to architect the strategy by incorporating both business requirements and users' needs and views. Many academic studies and experience from the industry showed that an attempt to impose security policies without consulting the users usually fails. Even though most organisations implement a range of security controls with focus on prevention and compartmentalisation strategies, it is impossible to have a complete end to end security solution without addressing the human component. Most reviewed papers advise that organisations need to invest in training and education of users in order to ensure a high level of security standards and business compliance requirements. However, it is important to constantly monitor the effectiveness of both technical controls and security policies.

References

Ahmad, A, Maynard, SB & Park, S 2012, 'Information security strategies: towards an organizational multi-strategy perspective', Journal of Intelligent Manufacturing, 22 July, pp. 1-14.

Cirtix nd, Introducing XenDesktop, Citrix, viewed 14 July 2013, < http://www.citrix.com/content/dam/citrix/en_us/documents/products/introducing-xendesktop-built-on-avalon-platform.pdf>

IT Governance Institute 2006, Information security governance: Guidance for boards of directors and executive management, 2nd edn, IT Governance Institute, viewed 13 July 2013, < http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf>.

Mansfield-Devine, S 2012, 'Interview: BYOD and the enterprise network', Computer Fraud & Security, vol. 2012, no. 4, pp. 14-17.

Morrow, B 2012, 'BYOD security challenges: control and protect your most sensitive data', Network Security, vol. 2012, no. 12, pp. 5-8.

Neff, T 2013, 'A winning BYOD policy balances usability & control', Compliance Week, vol. 10, no. 109, p. 42.

Payne, J 2013, 'Secure mobile application development', IT Professional, vol. 15, no. 3, pp. 6-9.

Phifer, L 2012, 'BYOD: Taming the tide', Information Security, vol. 14, no. 4, pp. 16-22.

Protective Security Policy Section 2012, The Australian Government Information security management guidelines-Management of aggregated information, Protective Security Policy Section, Attorney-General's Department, viewed 13 July 2013, < http://www.protectivesecurity.gov.au/informationsecurity/Documents/PSPF%20-%20ISMG%20-%20Management%20of%20aggregated%20information.pdf>

Purser, S 2002, 'Why access control is difficult', Computers & Security, vol. 21, no. 4, pp. 303-309.

Straub, DW 1990, 'Effective IS security: An empirical study', Information Systems Research, vol. 1, no. 3, pp. 255-276.

The Open Group 2011, Risk Management - TOGAF 9.1, The Open Group, viewed 13 July 2013, <http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap31.html>.

Venter, HS & Eloff, JHP 2003, 'A taxonomy for information security technologies', Computers & Security, vol. 22, no. 4, pp. 299-307.

Zviran, M & Haga, WJ 1999, 'Password Security: An Empirical Study', Journal of Management Information Systems, vol. 15, no. 4, pp. 161-185.

Author/s:
Marjanovic, Zoran

Title:
Effectiveness of security controls in BYOD environments

Date:
2013

Citation:
Marjanovic, Z. (2013). Effectiveness of security controls in BYOD environments. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33346

File Description:
Effectiveness of security controls in BYOD environments