A Systematic Research of Internet Security: Security Policies and BYOD

Archie Watt

Level 6, B.Sc. (Hons) Computer Networks

Abstract

A good security policy is an essential element to ensuring the security of any computer network, and should be the first step in the development of a network security plan. This paper emphasizes the importance of security policies and also studies some of the main factors that can hinder their effectiveness, including insufficient security training for employees. Bring Your Own Device (BYOD) is also examined in detail, including the various advantages and disadvantages that it can bring to an organization supporting it, and the various factors, such as advances in wireless network technologies and the greatly increased use of mobile computing devices, such as tablets and smartphones, that have led to its growth over the last few years. The main focus of this paper is on security policies for a BYOD network, and the additional challenges that can be faced when developing a security policy for such a network – for example, the organization's lack of control over the device and employee negligence. Finally, based on the research carried out, the paper puts forward several recommendations for the development of an effective security policy for BYOD.

Key words: Network security, security policies, BYOD, mobile devices, data protection
Introduction
A network security policy [1, 2] is a crucial element of network security, and is the first step in the development and implementation of a network security programme. Its primary objectives are to define the objectives of the security programme and state how these objectives will be fulfilled.

This paper is structured as follows. Chapter 1 provides a general overview of the importance of security policies and their crucial role in keeping a network secure. It also discusses some of the common issues that can potentially result in a security policy being less effective, specifically insufficient security training and security policy violations. Chapter 2 provides an overview of BYOD and its benefits, as well as the additional security implications it can cause for an organization supporting it. Chapter 3 presents a set of recommendations for developing an effective BYOD security policy based on the issues identified in Chapters 1 and 2. Finally, the paper will end with conclusions drawn from the research.

Chapter 1: Security Policies
Request for Comment (RFC) 2196 [3] describes a security policy as follows:

“A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.” The specifics of a security policy will naturally vary depending on the nature of the organization that is implementing it; however, any security policy should at least incorporate the following:

1. A policy should be in place that identifies the security-focused objectives and requirements of the network;
2. Access control rules should be in place to determine whether a user is permitted to access certain objects;
3. All users and applications accessing the network should be identified to the security system;
4. All users should be briefed and trained on security principles on an on-going basis. A security policy should evolve over time to consider, for example, new developments in security threats to a network, and it is therefore important that users are familiar with any updates to the policy. Therefore, security training should happen regularly and not be a one-time affair. It is thought that this point is the most crucial, since a security policy is near useless if those it applies to do not know how to follow it.

Despite the importance of security training, it has been indicated by a number of surveys [4, 5] that the training received by many employees in the workplace is insufficient and, in some cases, non-existent. Of more concern was the fact that a significant portion of the Information Technology (IT) professionals surveyed did not have any knowledge of many of the security threats that it was their job to prevent occurring. This indicates the need for organizations to have skilled IT staff that are always aware of the latest threats to the security of the network and how to mitigate them, as well as to ensure that all staff are trained on the basic principles of network security on a regular basis.
However, even with security training for staff, the effectiveness of security policies can still be greatly diminished in the absence of sufficient enforcement of the policy. This is evident in a recent report by the Corporate Executive Board (CEB) [6], which showed that of the 165,000 employees polled, 93% not only violated security policies, but did so in the knowledge that their actions violated company policy. However, the CEB also observed [7] that “Security policies are written in a way that’s too risk-averse or not reflective of ways people get work done”, indicating that many of these employees may have needed to violate the security policies to carry out work-related tasks. Two conclusions can be drawn from this:

- Security policies cannot be written as a one size fits all, but must be written taking into account the type of tasks employees need to carry out. This may necessitate the security policy being adapted for different departments.
- Better enforcement of security policies is needed and appropriate sanctions should be in place when violations occur.

**Chapter 2: Bring Your Own Device (BYOD)**

BYOD [8, 9], also known as BYOT (Bring Your Own Technology) refers to a programme operated by an employer which allows staff to bring their own devices – such as notebooks, tablets, and smartphones – into the workplace and use them to access the corporate infrastructure.

In recent years, the use of mobile computing devices such as tablets and smartphones has greatly increased, with the sales of tablets expected [10] to reach 197 million units by the end of 2013, which shows a 69.8 increase in comparison to 2012 sales. With the advances of mobile computing devices and wireless networking technology, BYOD has become a very popular practice. The results of a 2012 study by Good Technology indicated [11] that more than 75% of companies with more than 2000 employees formally supported BYOD. Furthermore, it was predicted [12] by Gartner in mid-2013 that by 2017, 50% of employers will require their staff to supply their own devices for work purposes as a condition of employment.

Providing a BYOD programme has the potential to benefit an organization in a number of ways, including:

**Cost Savings**

BYOD is able to reduce costs for the organization, since they will avoid having to pay the upfront fees for the device. In addition, it has been suggested that the majority of BYOD users are happy to pay service plan charges as well [11].

However, it may not always save the organization money overall. For example, the organization has a primarily Microsoft Windows based infrastructure and only has the staff expertise to support this platform. Allowing employees to use personal devices for work (which are likely to span various platforms, such as Linux, Android etc.), may necessitate the recruitment of additional staff expertise in order to support a greater range of devices – which may, in the long term, result in greater expenses. It is therefore important to observe the cost savings aspect of BYOD from different perspectives, and whilst it is a valid a factor when attempting to determine whether the organization should support BYOD, it should not be the sole decision factor and must be carefully assessed.
Simplified Infrastructure
Since employees will be primarily responsible for managing their own devices, BYOD can have the benefit of reducing the work of the IT support staff. However, as discussed in the previous point on cost savings, employee devices are likely to span a variety of platforms, which may lead to a greater workload for IT staff in order to support them all.

Employee Satisfaction
Most employees will be more familiar and more comfortable using their own devices, and the devices that an organization provides may well be different. For example, if an employee is an Apple Mac user, it can be difficult and irritating if the organization requires them to use, for example, a Windows PC, which would necessitate extra learning/training and potentially reduce their work output. BYOD enables the employee to work on a device which meets their needs and one which they are familiar with and competent using.

BYOD also allows for greater flexibility, with a single device being used for both work and personal activities. As a result, work that might normally only be possible at the office can be done anywhere. The benefits of this are highlighted in a recent iPass survey [14], which indicated that the average mobile worker put in 240 hours more work annually when using the same device for both work and personal use than those who did not.

However, allowing employees to use their own devices for work purposes also presents a number of significant security implications, and indeed, the fear of the increased security risks with BYOD were highlighted in a 2013 survey by Kaspersky [15], which claimed that 65% of the IT professionals surveyed saw a threat in allowing BYOD. In addition, BYOD potentially makes the development of a security policy more difficult.

Security risks associated with BYOD include:

Viruses/Malware
This is always a security concern for any network, but the risk of them infecting the corporate network is increased when an employee is using the same device for both work and personal use. Viruses were highlighted as the biggest concern related to BYOD at InfoSec 2012 [16].

Less control
Employees using their own devices for work related purposes increase the challenges associated with securing them for network administrators. Firstly, safeguards and restrictions are more difficult to implement when an employee is using their own device as opposed to a network account which has the necessary security policies in place by default. Secondly is the issue of office politics; many employees are likely to take issue being told how they can and cannot use a device which is owned by them. Finally is the issue of compatibility; different employees will use a range of different devices running operating systems (e.g. Windows, Linux) that are not compatible with the organization’s security software (and, indeed, other software applications the organization uses). This also makes the task of providing user support more complicated; the employee’s own device may not be one the IT support staff are familiar with.
Employee negligence
As indicated earlier, employees are more comfortable using their own devices, which, whilst having the benefit of potentially increasing productivity, has the possible disadvantage of increased negligence. Since the employees are likely to be more at ease when using their own device, a lack of security awareness could lead to their device(s) being compromised, and potentially, compromising the whole corporate network as a result. A ‘click first, ask questions later’ attitude also has the potential to cause many security issues, such as falling victim to phishing and malware; again, this highlights the importance of security training.

Lost/stolen devices
Employees using the same devices for work and personal use could potentially compromise corporate data in the event that the device was lost or stolen.

Legal issues
Legal legislation must also be considered with BYOD, such as recently released guidance [17] from the Information Commissioner’s Office (ICO). Thus, having an effective and well enforced BYOD policy is very important to avoid potential legal issues.

Also of concern is data protection. With reference to the previous point made about lost/stolen devices, if an employee-owned device is lost or stolen, and the device contains customer data which is subsequently compromised, this could result in legal implications for the organization in relation to the Data Protection Act.

Chapter 3: BYOD Security Recommendations
Based on the security issues identified in the previous two chapters, the following recommendations are put forward to develop an effective BYOD security policy. Whilst the focus is on BYOD, certain points are also relevant to the development of security policies in general.

1 Regardless of who owns the device being used to access corporate data, the data is owned by the organization they therefore need to have the right to access it. It is essential that these points are made clear to employees, since if corporate data is being stored locally, this will mean that the organization will require a certain level of access to the employee’s personally owned device. Depending on the tasks the device is being used for, the organization may require the ability to remote-wipe the device. In many cases this could cause concerns of a privacy related nature to arise for employees, hence the next point made that BYOD should not be compulsory.

2 As mentioned in Chapter 2, Gartner has predicted that many employers will make BYOD compulsory by 2017. Despite the benefits BYOD can bring, it is thought that an ‘all or nothing’ approach is the wrong one, since it would have unfair impact on employees unwilling to share their devices with their employer. In addition, since the employer would require a certain level of access to the device (see previous point), there could also be legal implications from a privacy perspective. It is therefore suggested that employees are given the option to opt-out of a BYOD programme and use company owned equipment should they wish to.
Mobile Device Management (MDM) enables personal employee devices to be identifiable to the organization's network administrators. An MDM client should always be used by staff to access the corporate infrastructure using their personal devices. The device should be registered with the MDM, which would involve authentication, ensuring that the device meets the security requirements of the organization before network access is granted.

The process of registration with the MDM should at minimum involve the following:

- User authentication.
- Agreement to comply with BYOD policy and any other applicable policies.
- Ensure that the device is running up to date antivirus software approved by the organization.
- Run a security scan to ensure that the device is free of malicious software.
- The device should be scanned on a regular basis, at minimum once a week. Ideally, the antivirus software should work in collaboration with the MDM, thus if malicious software was detected by the antivirus software, the MDM could immediately disconnect the device from the network, reducing or even eliminating the risk of damage to other devices on the network.

The above process could either be an automatic process carried out by the employee or could require the employee to have their device manually registered to the network by the IT staff. Whilst the latter option would enable more thorough checking of the device, it is suggested for the convenience of staff that it is an automated process. The flow chart in Figure 1 provides a basic illustration of the recommended process.

1. Data should be classified based on its sensitivity; its classification dictates how it should be handled by staff. As an example, data classified as TOP SECRET or similar should not be stored on employee devices.
2. Encryption is an important element of securing any data, particularly if that data is sensitive corporate information. As mentioned previously, the storing of highly confidential data on employee owned devices should be avoided; however, any data that is stored should be protected using an appropriate encryption technology, such as TrueCrypt [18]. As with antivirus software, encryption technologies could be integrated with the MDM client to provide a more seamless security solution.
3. It is suggested that data stored on employee-owned devices is limited to a particular amount, for example one gigabyte (GB). This could limit the potential damage in the event that the data was compromised. An alternative to this is to not permit storage on the local device at all, and take advantage of a cloud based storage solution. With this approach, if the device was lost or stolen, the data that it was used to access would not be at risk since it was not locally stored on the device, and any credentials used to access the data could be remotely disabled. In many cases a cloud storage service such as Dropbox or Google Drive may be suitable, though for more sensitive data investment in a private cloud service may be necessary.
4. Installed and up to date anti-virus software is a crucial security aspect of any system. Any employee-owned device should have a regularly updated
Figure 1: Device Registration Process
anti-virus package approved by the organization installed on any devices they use to access the corporate infrastructure.

However, it should be noted that no antivirus package can be 100% effective. Therefore, other safeguards should be in place as well. Aside from regular virus definition updates and security scans, it is, as has been emphasized already, important that staff are educated regularly about IT threats and how to help prevent them occurring.

1 Identified in Chapter 1 as being one of the most important aspects of a good security policy; employees cannot follow a policy when they do not know how to do so. Regular training is crucial not only for a basic understanding of network security but also to ensure that they are kept up to date on the latest security threats and how to avoid falling victim to them.

2 As shown in the survey discussed in Chapter 1, it is common in the workplace for employees to violate network security policies. Whilst there are caveats to this (covered next), this indicates a significant lack of enforcement of security policies. It is essential that policies are well explained and that disciplinary procedures are taken in the event of a policy violation.

3 As mentioned in Chapter 1, the remarkably high rate of security policy violations was often as a result of the fact that employees were required to carry out tasks that violated the policies. This indicates a lack of consideration for the tasks which will be carried out on a corporate network when developing a security policy. It is therefore suggested that security policies be ‘task-tailored’, developed in collaboration with staff (e.g. department head) who have a good knowledge of the tasks employees will need to carry out. This may make it necessary to have different security policies for different departments based on their requirements, for example staff in the sales department would not have to carry out many of the tasks that staff in the human resources department would.

Conclusion

This paper has evaluated security policies with an emphasis on Bring Your Own Device (BYOD). Based on the research carried out, the following conclusions have been drawn:

- Security training for staff is the most important aspect of ensuring the success of a network security policy;
- There is an apparent general lack of security training given to employees by their employer;
- Security policies are generally poorly enforced, evidenced by the high percentage of employees who had knowingly violated them. This indicates that better enforcement and disciplinary procedures are required;
- Many employees violate security policies because they need to do so in order to complete tasks. This indicates the need for security policies to be developed in collaboration with staff, in order to take into account the type of work the employees will be doing when developing the policy;
- BYOD can bring a number of benefits to an organisation supporting it; however, it is believed to increase threats to the security of a network. It is thought
that the recommendations presented in Chapter 4 can mitigate at least some of these threats;

• Should an organization decide to support BYOD, it is vital to implement and enforce a security policy sooner rather than later. If a policy is not defined by the organisation, it is likely that its employees will define it for them, which could be problematic.

Acknowledgement
I would like to thank Dr Carlene Campbell for her encouragement and support, and for nominating my work to be published. Thanks also to Dr Stephen Hole and Professor Kelvin Donne for approving this paper to represent the Faculty of Applied Design and Engineering in The Student Researcher.

References

Bibliography
‘Best practices to make BYOD simple and secure’, Citrix Whitepaper, 2012
'Meet BYOD challenges', HP Whitepaper, 2013
Miller, K., Voas, J. and Hurlburt, G. 2012. 'BYOD: Security and Privacy Considerations', IT Pro