# Using Human Factor Approaches to an Organisation's Bring Your Own Device scheme

Jodie Ward, Huseyin Dogan, Edward Apeh, Alexios Mylonas, Vasilis Katos

Department of Computing & Informatics, Bournemouth University, Bournemouth, United Kingdom.

{i7933001, e.apeh, hdogan, amylonas, vkatos}@bournemouth.ac.uk

**Abstract.** Bring Your Own Device (BYOD) is an emerging trend that is being adopted by an increasing number of organisations due to the benefits it provides in terms of cost efficiency, employee productivity, and staff morale. However, organisations who could benefit from implementing BYOD remain sceptical, due to the increasing threats and vulnerabilities introduced by mobile technology, which are amplified due to the human element (insider threats, non security savvy employees). In this context, this paper investigates the application of human factor techniques to the BYOD scheme of an anonymised, real-life organisation (referred to as "Globex"). Questionnaires and Interactive Management are the two Human Factor methods used in this case study to help determine areas for improvement. Results from the experiment highlight an issue with employee satisfaction towards their employers' BYOD scheme, which could negatively impact their organisational culture. The paper concludes with recommendations for additional information within the BYOD policy and the review of reimbursement eligibility and entitlements.

**Keywords:** BYOD, Bring Your Own Device, Mobile Devices, Mobile Device Management, Security, Interactive Management, Human Factors.

## 1 Introduction

THE emergence of smartphones and other mobile devices with advanced capabilities has encouraged organisations to introduce them into the workplace. These devices coupled with high-speed mobile internet increases productivity by enabling employees to work on-the-go. Recently, many organisations are considering the concept of Bring Your Own Device (BYOD), which enables employees to use a personal device of their choice to connect to company resources whenever they like. Besides increased productivity, organisation's also benefit from reduced costs as the responsibility of purchasing and maintaining the device lies with the employee (Ali et al. 2015;

Eshlahi, et al. 2014). Another potential benefit is increased staff morale as a result of having more flexibility (Downer and Bhattacharya 2015).

BYOD is a relatively new domain and comes with various security challenges that must be considered before adoption. Mobile security is not as advanced as computer security, and research has found attacks typically aimed at computers are increasingly targeting smart devices (Clay 2015; Eslahi et al. 2012). Additionally, by shifting the responsibility of purchasing and maintaining a mobile device to employees, the company relinquishes control over the device making security mechanisms harder to enforce. If BYOD implementations are not properly secured the organisation risks leaking sensitive information and damaging their reputation.

There are multiple trust and privacy issues acting as barriers to the uptake of BYOD. Employees must be able to trust their employer not to use technical security mechanisms to access or monitor their personal information, but in the same respect the employer must be able to trust their employees to follow company policy and safeguard corporate information. This research contributes to the cyber security policies and user behaviour domains by applying human factor approaches to investigate information confidentiality and privacy issues that tend to arise between corporations and their employees from the adaptation of BYOD.

This paper critically evaluates an organisation's BYOD scheme and makes recommendations for improvement based on research and experimental case study results. This paper is ordered as follows: Section II elaborates on BYOD security threats and challenges. Section III discusses Human Factors as a discipline and how various approaches can be used to improve security. Section IV presents the case study results i.e. information gathered about the organisation's security solution in addition to questionnaire and IM results. Section V discussed the research with final remarks and recommendations and section VI proposes future work.

## 2 Bring Your Own Device

### 2.1 BYOD Security Threats

Attacks aimed at mobile devices are heavily increasing (Wang 2014). A report published by Symantec show mobile vulnerabilities rose by 214% in 2015 compared with 2014 (Symantec 2016). It is therefore important to understand the types of attacks to defend against them.

**Loss or Theft.** Mobile devices present an increased risk of compromise due to their size and mobility as it makes them susceptible to loss and theft (Souppaya and Scarfone 2013). Globex should therefore assume an attacker will gain access to a lost or stolen device in the future, and think about what tools they want in place to prevent access corporate information.

**Malicious Applications.** In 2011, it was estimated that 11,000 malicious applications were residing in Google's Play store, which hosts a multitude of applications for downloading to devices running the Android operating system (Miners 2014). This

number quadrupled by 2013. Such applications contain malicious code commonly designed to steal the user's data for committing fraud. A recent example of a malicious application involves WhatsApp, Uber, and Google Play (Kan 2016). The malware spread through an SMS prompting victims to click a link which then downloads the malware. The malware then creates an overlay to spoof a trusted application and requests credit card information. Once the victim submits the information, it is sent to the attackers.

**Phishing and Smishing.** A phishing attack is a form of social engineering designed to trick recipients into divulging sensitive information, such as credit card details, by masquerading as a legitimate and trustworthy entity. The attack comes through various channels such as email and malicious applications. A phishing attack in the form of a text message is referred to as 'smishing'. Phishing is difficult to defend against as attackers are constantly changing their techniques to evade security mechanisms (Wu et al. 2016). There are many technical solutions available for phishing, however many researchers agree the most effective solution is staff education, training, and awareness (Dodge, R. et al. 2007; Symantec 2016).

**Mobile Botnets.** A botnet is an interconnected network of infected computers used to spread malware. It is fully controlled by an attacker through a command and control server. A botnets potential for inflicting damage increases as more machines are infected and become a part of the zombie network (F-secure labs 2016). Botnets are considered one of the most dangerous cyber threats as they can be difficult to detect and shut down due to their dynamic nature and complexity. In recent years' researchers have discovered botnets operating on mobile devices. The lack of security knowledge of many mobile users and less advanced security solutions has motivated botmasters to migrate (Eshlahi et al. 2012). While the threat of mobile botnets is not as prevalent as traditional botnets, security experts expect it to grow (Winder 2016). Table 1 lists some well-known examples and their attack vectors (Eshlahi, et al. 2012; Winder 2016).

**Disgruntled Employees.** Employees can leave an organisation feeling disgruntled for a variety of reasons: being made redundant, having a poor relationship with their managers or colleagues, or feeling unappreciated for their work. A disgruntled employee is more likely to have motive for an attack or data leakage over one who left amicably (Kumar 2015). Therefore, it is vital to ensure corporate data is removed from personal devices before every employee's termination date.

**Unsecured Wireless Networks.** Most organisations encourage staff to use Wi-Fi wherever possible to save on costly data usage bills. This means staff may connect to unsecured public wireless networks whilst travelling, which is an easy target for attackers to gain access to sensitive information.

**Table I.** Examples of Mobile Botnets

| Name | Attack(s) | Mobile OS |
|---|---|---|
| Zeus (Zitmo) | Fraud<br>Private data theft (mobile banking)<br>Illegal transactions | Symbian<br>Windows<br>BlackBerry<br>Android |
| DroidDream | Private data theft<br>Malicious applications | Android |
| Android.Bmaster | Revenue<br>Private data theft | Android |
| Viking Horde | Fraud<br>DDoS<br>Revenue generation | Android |
| Ikee.B | Revenue<br>Private data theft | iPhone |

### 2.2 BYOD Challenges

There are many other challenges involved in BYOD besides security threats. The National Cyber Security Institute (2014) and Information Commissioners Office (2016) divide BYOD challenges into eight main categories, namely:

**Limiting Information Shared by Devices**. Personal devices are often set-up for easy or automatic sharing of data such as backing up to the cloud or automatically connecting to nearby wireless hotspots. Appropriate consideration should be made into how to protect data from unlawful access, regardless of storage location. Additionally, organisation's must also think about how personal applications may interact with company applications and what methods are available to keep them separate.

**Creating an Effective BYOD Policy.** A BYOD policy clarifies the responsibilities of the employer and employee for protecting corporate information on mobile devices. A policy is only fully effective when it is enforced and regular compliance checks are carried out. This is because people tend to forget over time or are not made aware of changes (Downer and Bhattacharya 2015). An effective BYOD policy is also realistic and flexible. Employees who strongly disagree with a policy may ignore it or actively seek loopholes if there is a benefit for them (Thomson 2012; Mathias 2013).

**Technical Controls.** There are a range of technical controls available to help organisations remotely manage, secure, and support BYOD devices. Such controls may support compliance and policy enforcement, password enforcement, a remote wipe facility, locate device function, containerization and more. While technical controls provide measures for protecting corporate data on personal devices, they do not come without their limitations. The limitations for various tools are explored in the next section.

**Planning for Security Incidents.** Mobile devices can be easily lost or stolen. It is vital for an organisation to plan for such incidents to protect corporate data. An organisation must be able to act immediately to limit losses, prevent the spread of any compromise, and learn lessons from the incident (NCSC 2014).

Technical controls are useful in events such as the loss or theft of a device as it will enable the organisation to remotely wipe corporate data. Although this will only work if the server is able to establish communication with the device over a network connection. It is crucial that staff understand the process of reporting such incidents to the organisation and the importance of doing so in a timely manner for technical controls to be effective.

**Alternative Ownership Models.** The National Cyber Security Centre (2014) advise considering alternative ownership models before jumping into BYOD. A 'choose your own device' policy is one where the company purchases the device and maintains control over it, but the employee can choose from a selection of models that best suits them. There is also a 'corporately owned, personally enabled' policy that allows staff to use corporately owned devices for personal use. An option that gives the organisation full control but allows flexibility to the employee. The main problem with the aforementioned policies is the organisation remains responsible for expenditure of devices and so would not appeal to one looking to cut costs.

**Encouraging Staff Agreement.** Some staff may resist BYOD as it transfers the costs of purchasing and maintaining the device over to them. Some will likely have privacy concerns with technical controls the organisation enforces and sharing their personal contact number to clients or colleagues. Moreover, staff may not receive the same level of technical support from IT services as they did for corporate liable devices as it widens the scope for technical issues.

The National Cyber Security Centre (2014) advise communicating their BYOD policy through employee training and education to ensure staff understand their responsibilities and the decision-making processes behind the company's decision. Organisation's should consider how they present training materials to staff depending on their local organisational culture. To ensure maximum impact, the right information needs to be presented in the right way through the right communication channels (Lacey 2009). Sources of influence play an important role in changing attitudes and behaviour in staff. Three sources of influence include:

- Hierarchical: those that respond well to authoritative figures such as the CEO;
- Democratic: those that respond better to peer discussions;
- Sophisticated: those that respond better to thought leaders.

**Increased Device Support.** A BYOD policy invites the use of a wider range of mobile devices, which increases demand for device support. Technicians may have to keep multiple operating systems compliant and up-to-date, support a greater number of device types, and respond to security incidents across a variety of devices (NCSC 2014). For a successful BYOD approach organisation's must have sufficient support capability and expertise to support a growing range of devices. Increased device sup-

port is likely to come with an associated cost for training or hiring additional support staff.

**Understanding Legal Issues.** There are myriads of legal issues surrounding BYOD, many of which are ill-defined and do not yet have solid solutions. Laws and regulations are continuously evolving as technology grows, so policies and standards must be regularly maintained to demonstrate good practices (Mavretich 2012). Additionally, legal issues will present various constraints for IT managers implementing a BYOD policy, so it is important to prepare for changes and allow room for flexibility.

A BYOD policy is largely influenced by local government laws and regulations, and so organisation's looking to implement BYOD on a global scale should customise their policy for each country (Absalom 2012). A comprehensive policy constructed around local laws is a strong way of ensuring legal compliance. It ensures that employees are fully aware of the implications of using their own device and understand their responsibilities.

## 3 Human Factors Approaches Adopted: Questionnaire and Interactive Management

Human factors (HF) is a scientific discipline also referred to as ergonomics. It combines knowledge from various fields of research to design systems that complement the natural abilities of people to improve efficiency and safety at work (Chartered Institute of Ergonomics 2016). The term 'ergonomics' is mostly used to describe human interactions with physical environmental factors at work, whereas HF covers the broader aspects such as interaction with systems, processes, and products. HF has contributions from such fields as psychology, engineering, physiology, cognitive science, human computer interaction (HCI), and more. BYOD is centred on managing the way humans interact with their devices and corporate systems. Human error and malicious intent are the most common causes of security breaches (Greenburg et al. 2015; PWC 2015), so considering HF is essential for a strong scheme.

There are various human factor approaches available to help see a broader picture of the problem, which presents a wider range of solutions. Applying HF helps to design a system for people that is user-friendly yet effective. One approach is Heuristic Evaluation, which is used to identify usability issues in the design of a user interface. Another approach is Soft Systems Methodology (SSM), which is a decision support tool typically used to help develop a better understanding for a problem to prevent premature solutions that do not work or are not effective enough. Focus groups is another methodology which is used to gather qualitative research from a group of people, usually based on their thoughts, perceptions, and attitudes towards a certain product or system. As another example, there is also Cognitive Walkthrough which is typically used to evaluate the usability of a system by asking participants to work through a series of tasks while answering questions posed by the researcher.

This paper utilises questionnaires and an approach called Interactive Management (IM), and applies them to an organisation's BYOD scheme with the aim of identifying areas for improvement. These approaches are discussed next.

### 3.1 Questionnaires

The most commonly used technique for gathering information from people is questionnaires. They are useful for obtaining large amounts of information because they can be distributed widely and therefore can get more response. However, due to the lack of social cues from respondents and the inability to ask for clarification, the validity of the data received is always questionable (Wickens et al. 2003). For this paper, questionnaires were used to gather information from IT managers regarding what BYOD solutions Globex have in place as the information required is purely factual and does not require human interaction. This information helps to recognise if and where Globex's solutions need improvement.

### 3.2 Interactive Management

Interactive Management (IM) is a system designed to manage complex situations through structured group discussions between a group of people knowledgeable to the problem. Focusing on the problem in detail and building a deeper understanding of it prevents premature solutions not fit for purpose (Warfield 2002).

IM supports consensus decision-making where group members reach an agreement on a solution together rather than voting and leaving some members unhappy with the outcome. It promotes effective communication, participation, and is an efficient use of participants' time. IM can also be considered as a 'soft' systems approach that helps to capture the stakeholder requirements in order to better contextualise the problem space (Dogan and Henshaw 2010). To support consensus decision-making there must be a facilitator, participant group, a set of methods for reaching decisions, a computer or flip chart for organisation of ideas, and a decision support room (Broome and Keever 1986). IM is made up of three phases:

**The Planning Phase**. The first and most important step in this phase is to make sense of the situation at hand. This is achieved with scope and context statement writing, actor identification, and definition of the state. These methods encourage members to think about who and what is involved, and how it is effecting them to gain a broader picture of the problem. Defining the state of the problem helps to reveal questions that if answered, may significantly contribute towards an effective solution (Warfield 2002).

**The Workshop Phase**. The workshop is where participants come together to answer any questions derived from the planning phase and put consensus decision-making into action. The workshop is largely focused on three key concepts: Context, content, and process (Warfield 2002). Discussions are led by the facilitator, who provides the group with context derived from the planning phase. The group provides content based on the contextualisation through discussion and idea sharing. The facili-

tator manages the process of the workshop to ensure discussions remain on topic and members are making the best use of their time.

The IM workshop will consist of three methods: Idea Writing, Nominal Group Technique, and Interpretive Structural Modelling. In idea writing, a trigger question is presented to participants to silently write down ideas for. The written ideas are then exchanged with others and additional ideas are added. Everything is then collated and divided into categories, and presented to the group. Next is the Nominal Group Technique, where participants generate further ideas after a more holistic view of the problem is gained from idea writing. This also allows for clarification and editing of problem statements. Participants then rank each idea based on importance. The final part of the workshop is to transform idea statements into objectives and then create an interpretive structural model (ISM) to identify relationships amongst various items surrounding the problem (Attri et al. 2013). To gather participants for the group discussion, an email was sent to a group of people either enrolled in BYOD or likely have a good understanding of it due to their role and responsibilities. Five participants were selected in total.

**The Follow-up Phase**. This phase puts into action the objectives derived from the workshop and begins the planning phase of solution implementation. If, during this stage it is realised that the issue had been misunderstood or new issues arose afterwards that were not taken into consideration before, a new planning phase would be entered (Warfield 2002).

## 4 Case Study Results

This section examines Globex's BYOD security solutions and assesses them based on professional guidelines from the previous section. Findings contained within this section were obtained by analysing Globex's BYOD policy, and conducting questionnaires and informal interviews with IT management staff.

### 4.1 Company Profile

Globex is a global company exercising BYOD in various countries. They began rolling it out to employees earlier this year. The deciding factors for Globex adopting BYOD were to reduce costs, allow employees to choose their own device, and to keep up with modern technology trends. New hires are enrolled in BYOD by default, and employees with corporate liable devices before the introduction of BYOD are allowed to remain on a corporate liable plan until further notice. Employees can opt in to BYOD at any time, subject to managerial approval. Users can expense a capped amount of their network service costs to Globex for business-related usage.

### 4.2 BYOD Policy

As Globex is a global company, it would not have been possible to analyse every policy. This section focuses only on the BYOD policy for the UK. Globex's BYOD policy is very detailed and quite clearly communicates the responsibilities of the employee for both BYOD and corporate liable devices. It covers reimbursement and eligibility, device selection, corporate applications, separation upon termination, maintenance and repair, technical support, invoicing, and more. The employee's responsibilities are clearly conveyed followed by a best practices guide for avoiding additional costs and using mobile devices safely.

**Corporate Responsibilities.** One of the first aspects of this policy that stood out is how it lacks a clear definition of Globex's responsibilities. The employee's responsibilities are clearly illustrated in a sizeable list, but the company's responsibilities appear to be lesser and are embedded in text. From the employee's perspective the policy may be interpreted as a set of rules telling them what to do rather than a policy that represents both the interests of the company and the employee.

**On-boarding process.** Results from the questionnaire found that the BYOD policy is not currently a part of HR's on-boarding process for new hires. This is concerning since the majority of new hires are not entitled to corporate liable devices and would have no choice but to enrol in BYOD if they needed a mobile device for their role. Imposing BYOD on an employee's first day may come as a surprise and give an unprofessional first impression of the company.

**Policy enforcement and compliance.** At present, employees are not required to re-read and sign the BYOD policy at regular intervals, which makes it easy for them to forget about.

**Social media policy.** Globex should consider writing a social media policy to prohibit the disclosure of confidential information on social media (ICO 2016). Such a policy will aim to clearly define the types of information that must not be shared with each one supported by an example (Lawrence-Hardy 2016). This helps to cover the Globex's liability should a situation arise where corporate information is accidentally leaked due to inadequate care.

**Encryption.** Globex's policy makes no mention of device encryption for additional security for data at rest. It might be deemed too inconvenient for a lot of Android users due to the fact it enforces a strong password rather than a passcode, but for security conscious staff, the mention of device encryption may encourage some.

**Anti-Malware.** The policy does not advise employees to install anti-malware solutions. Research presented earlier in the paper shows that mobile malware is on the rise, particularly on devices that install open source applications from Google's Play Store.

### 4.3 Technical Controls

**AirWatch MDM.** AirWatch is a mobile device management (MDM) application used by Globex which employees must enrol in before being accessing corporate resources. AirWatch has many features and supports multiple platforms, making it an easy choice. Of the many features included with AirWatch, Globex use: passcode enforcement, containerisation, device visibility excluding GPS tracking, and remote wipe.

To enrol in AirWatch, employees are provided with documentation with step-by-step set-up instructions. Globex have documentation for Android, Windows 8, Windows 10, and Apple iOS devices. Once enrolled in AirWatch, the user can access their corporate emails. The user is also given access to an AirWatch portal that they can sign into from their PC to manage their device. Users can still access their corporate OneDrives without AirWatch enrolment.

As highlighted by Eshlahi et al. (2014) and Ali et al. (2015), BYOD security models like MDM only provide a basic security solution and focuses mainly on management of the device. Because MDM is a reactive solution, it's effectiveness is only as good as the reaction time in the event of a security breach NCSC 2014). MDM is a controversial model because of employees' privacy concerns and the inconvenience of security protocols enforced on the device (Downer and Bhattacharya 2015). MDM solutions like AirWatch can also be high maintenance due to regular updates and the number of devices connecting is constantly changing.

**Alternative Solutions.** An alternative solution to MDM is mobile information management (MIM), where corporate information is secured rather than devices and stored in a central location for secure access. The problem with MIM is it requires an internet connection to access resources which is inconvenient to staff who travel a lot (Eshlahi et al. 2014). This limitation is also shared by the VPN-based access model (Ali et al. 2015). Similarly, there is mobile application management (MAM), which is used to install, manage, and audit enterprise applications. Since MAM requires unique coding for each enterprise application to work properly, it is not a popular option (Steele 2013). Finally, another option is kernel modification, but employees may feel uncomfortable allowing the organisation to make changes to their devices operating system (Ali et al. 2015).

It is evident that more work is needed to address BYOD challenges. However, as it stands at the time of writing, MDM is the most feasible option for Globex to manage personal devices.

**Improvement of MDM.** Globex could use more of Airwatch's features to their advantage. The use of encryption enforcement would provide an extra layer of security for data at rest and should be considered in the future when BYOD develops. Training and awareness methods can be utilised to win employees over for such security protocols if done correctly. Blacklisting is another feature currently not in use that prevents jailbroken devices from connecting to corporate resources.

### 4.4 Planning for Security Incidents

As mentioned in the previous section, organisation's must be able to act quickly in the event of a lost or stolen device. AirWatch MDM is a good tool for this, but it's only effective with quick reaction time and a network connection to the device.

Globex's BYOD policy states it is the employee's responsibility to report a lost or stolen device to IT immediately. Globex have a dedicated 24-hour helpdesk that can be reached via telephone or email. However, if an employee doesn't have a spare phone or has lost all of their contact information, the reporting process might be delayed. Helpdesk staff have administrative privileges to the AirWatch portal so they can perform a remote wipe quickly in a security event. Employee's also have access to the AirWatch portal to perform a remote wipe, but only on their own device. Research discovered that IT are meant to perform remote enterprise wipe for terminated BYOD users, but there is currently nothing within in their leavers process that communicates this.

### 4.5 Encouraging Staff Agreement

Globex communicated the shift to BYOD primarily through line management and email newsletters from the CIO (chief information officer). The introduction newsletter outlined basic policy information and expected time of introduction to each region. Subsequently, Globex held a series of Q&A webinars.

Training and awareness is provided in several documents available on the corporate intranet. These documents were also included in the email newsletter. The problem with email communication is it is easy to miss and removes the human element from communication, which makes it easy to be misinterpreted.

Communication and change management is a complex task requiring in-depth knowledge of the company, as well as advanced planning techniques.

### 4.6 Increased Device Support

The policy reads that IT support will not support mobile devices unless the issue is related to AirWatch. From a cost and resources perspective this makes sense because it would impose an increased demand on IT staff, but BYOD users may feel abandoned by company. In the long term this may negatively contribute to the organisation's culture and attitudes.

The policy also states employees are responsible for maintaining and repairing their own device, which makes sense as they hold the warranty information.

### 4.7 Understanding Legal Issues

Exploring legal issues surrounding Globex's BYOD policy is out of the scope of this experiment as it requires background information from the Legal team and Human Resources. However, it is worth mentioning the value of employing risk man-

agement techniques to identify legal risks and develop strategies to outsource, mitigate, or transfer them.

### 4.8 Interactive Management (IM) Results

One of the authors acted as the facilitator for the IM session. The session took place in a meeting room situated in one of Globex's offices for the participants' convenience. Five participants were selected in total to participate in the IM workshop. Two of five participants are enrolled in BYOD, one by choice and the other as part of their on-boarding process to the company. One participant is from the legal department, another from the facilities department, and the final participant is from customer support.

As explained in the previous sections, idea writing requires a trigger question which participants can write down ideas for and then exchange them. However due to the limits set by the participants' schedules, it was not possible to spend much time on this phase so ideas were exchanged aloud from the beginning. Ideas were recorded on a computer connected to a projector. The trigger question presented was:

*"What are the issues with Globex's BYOD scheme?"*

Table II presents the ideas generated from the trigger question. The ideas are numbered for ease of referring to, they do not represent the order of importance.

Table III presents the categories in which each idea falls into. The categories are ranked based on how many ideas belong to each category. Based on this data, the biggest concerns for BYOD are to do with privacy and lack of communication. The next most occurring concerns are for the inconvenience presented to BYOD users and monetary issues. Following on from that is the users lack of understanding. Finally, the least concerns fall under culture and other. 'Other' represents ideas that are too generic to fall under any category.

**Table II.** Results of Idea Generation

| | |
|---|---|
| 1 | Privacy of personal information being accessed by AirWatch. |
| 2 | Lack of control over what information Globex can and can't see. |
| 3 | Users have to accept permissions for AirWatch to access the device in but it states on the set-up document Globex does not monitor it. |
| 4 | Don't understand why higher level executives are entitled to corporate liable devices. |
| 5 | The standard cap is not enough for some users and should be flexible depending on the employee's role. |
| 6 | The principle is a good idea but it needs more work. |
| 7 | There's no clear definition of where the office ends and begins. Employees can end up bringing work on holiday. |
| 8 | Sharing your personal number with customers and/or colleagues. |
| 9 | It seems like IT are able to wipe your device and control your personal data. |
| 10 | Clients may still be contacting people after leaving the company. |
| 11 | Getting the workers council to approve it. |
| 12 | It's not clear what BYOD leavers do in terms of wiping their device when they leave and cutting contact. |
| 13 | There's nothing in the mobile policy about insuring the mobile devices. |
| 14 | There's no advice about what to do if your device breaks. Will IT provide you with a temporary one in that situation? |
| 15 | The admin work involved in separating business and personal usage involves time. People may end up not bothering. |
| 16 | Most people nowadays take out a package of minutes, texts, and data with their network supplier and don't necessarily get a break down of their usage which is covered under their contract so you can't expense it. In the mobile device policy, it states no contribution will be made to packages. |

.

**Table III.** Categorization of Ideas

| Category | Ideas | Ranking |
|---|---|---|
| Privacy | 1, 2, 3, 8, 9 | 1 |
| Culture | 4, 7 | 4 |
| Monetary | 5, 13, 15, 16 | 2 |
| Lack of communication | 3, 7, 9, 12, 14 | 1 |
| Lack of understanding | 2, 3, 9 | 3 |
| Inconvenience | 7, 10, 14, 15 | 2 |
| Other | 6, 11 | 4 |

Next is the nominal group technique, where participants were asked to pick their top five issues from the list of ideas and rank each one between the numbers one and five, with one being the most important. Table IV displays the results.

**Table IV.** Participant's Ranking of Ideas

| Idea | P1. | P2. | P3. | P4. | P5. |
|---|---|---|---|---|---|
| 1 | 3 | 5 | 1 | 3 | 1 |
| 2 | 2 | | 4 | 2 | 2 |
| 3 | | 3 | | | |
| 4 | | | 1 | | |
| 5 | | | | 5 | |
| 7 | 4 | | 2 | | 4 |
| 8 | 5 | | 5 | | 5 |
| 10 | | 2 | | | |
| 12 | | | | 4 | |
| 15 | 1 | 4 | | | 3 |
| 16 | | 1 | | 1 | |

Based on this data, ideas that were ranked most important are privacy of personal information, the additional administrative work, and not being able to get reimbursement for network packages. Interestingly, one participant ranked higher-level executive's eligibility to corporate liable devices as their most important issue. During idea generation one participant commented that they 'were used to senior level executives getting more out of the company'. This could indicate an organisational culture issue that Globex's BYOD scheme is contributing to. It also shows a lack of understanding for security from the participant. The reason Globex may have implemented

this rule is because senior executives handle more sensitive information in their roles and therefore the company requires complete control over the device to protect corporate data. On the contrary, it could be argued that the responsibility of ensuring employees understand this lies with Globex.

The final part of the workshop involves transforming idea statements into objectives and creating an interpretive structural model to demonstrate the relationships. Table V displays the objective statements from ideas deemed important enough by participants to rank in their top five.

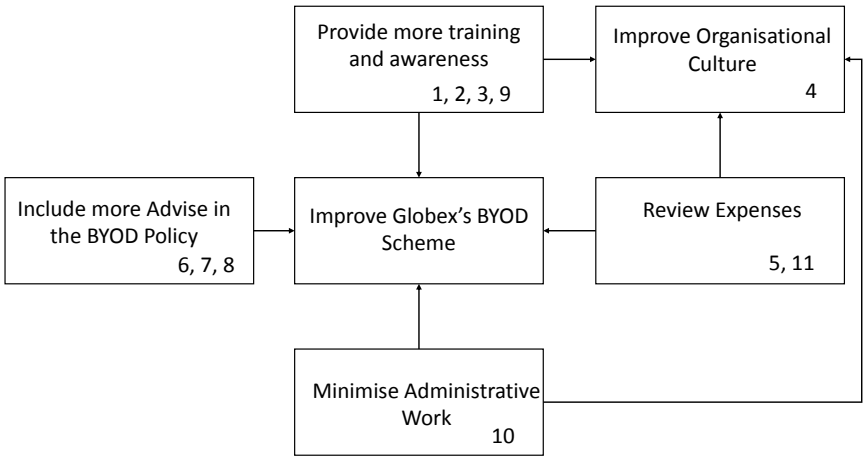
**Table V.** Objective Statements

| | |
|---|---|
| 1 | Elucidate what personal information corporate installs like AirWatch can and cannot access through training and awareness methods. |
| 2 | Improve employee's awareness of the control they have over corporate installs through training and awareness methods. |
| 3 | Improve employee's awareness of how application permissions to personally owned devices work and what they really access through training and awareness. |
| 4 | Provide clarity as to why higher level executives are entitled to corporate liable devices. |
| 5 | To implement a flexible re-imbursement cap for employees based on their role and travel frequency. |
| 6 | Include a section in the BYOD policy that covers the employees right to separate work from their personal life with tips on how to practice it in BYOD. |
| 7 | Include an advice section in the BYOD policy on how to manage sharing your personal number with customers and colleagues. |
| 8 | Include an advice section in the BYOD policy on how to manage client contacts upon termination from the company. |
| 9 | Advise users on how to wipe corporate information from their device upon termination with tips on how to detach. |
| 10 | Minimise the administrative work to make it as easy as possible for users to expense network usage. |
| 11 | Look at allowing employees with a bundled network package to expense a certain percentage back, perhaps based on their role. |

To make ISM simpler, objectives from Table V are grouped by similarity to derive more generic objectives. The numbers grouped in the bottom right-hand corner of the boxes in Diagram I represent the objectives from Table V in their new group.

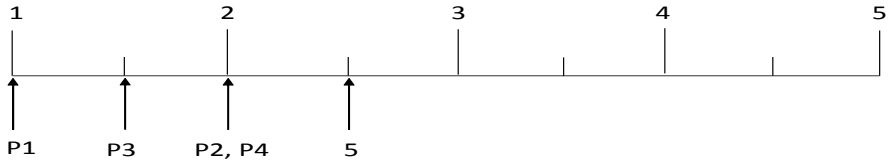
Diagram I shows the interpretive structural model derived from the objective statements and their relationships.

**Diagram I.** Interpretive Structural Model




To conclude the workshop, participants were asked to rate their overall satisfaction with Globex's BYOD scheme on a scale of one to five, with one being very unsatisfied and five being very satisfied. Diagram II shows the ratings.

**Diagram II.** Participants Satisfaction with BYOD




The overall result of the IM session shows that all of the participants are unhappy with Globex's BYOD scheme to some extent. Of course this only represents a miniscule percentage of Globex as a whole. The participants all belonged to the same office, which will have its own unique culture to other offices. It could also be coincidence that brought five people together who share similar feelings towards Globex's BYOD scheme. In spite of having a small study group, some interesting points were made which are used to produce a clear list of objectives that Globex can use to improve employee satisfaction with BYOD.

## 5 Discussions

Bring your own device provides many benefits for an organisation and its employees. It is cost effective, increases productivity, and can improve staff morale if planned carefully. This paper surveyed the challenges and threats surrounding BYOD in general, and then critically analysed a given organisation's BYOD scheme against professional research. Two human factor approaches were applied to this case study: questionnaires were used to gather information about the scheme from IT management; and interactive management (IM) was used to explore the problem scope and build a list of objectives for improvement of Globex's BYOD scheme. The results of these experiments highlighted plenty of areas for improvement. The key outputs are discussed below.

**Policy changes.** Align HR's on-boarding process with the BYOD policy so it does not come as a surprise to new employees, as this may not give them the best first impression of the company. Globex should consider including a social media policy to prohibit the disclosure of confidential corporate information and to demonstrate to employees what types of information must not be shared outside of the company. Employees should also be required to re-read and sign the BYOD policy at least once per year so they are less likely to forget how to adhere to it. There should also be controls in place to ensure adherence. It is advisable to encourage the use of anti-virus software for mobile devices as many people are unaware of threats transferring to mobile devices. Device encryption should also be recommended to protect data at rest. It would not be a good idea to enforce encryption until employee satisfaction towards BYOD improves as this may cause more resistance and negative feelings.

There should be an additional section in the policy with separation advise for cutting ties with the company upon termination. Finally, the policy could be re-worded to sound less like a set of rules and cover more of the employer's responsibilities to 'even the scales' between the company and employee. This will make the policy appear more friendly.

**Technical controls.** The use of mobile device management (MDM) as a technical control is the most feasible solution for the company at this time, but some features are not being used to their full potential. For example, additional policies could be set to prevent jailbroken devices connecting to corporate resources, ensure an up-to-date anti-malware solution is installed, and device encryption enforcement could be considered for the future. In addition, the set-up instructions for configuring AirWatch on mobile devices need to be reviewed and updated more regularly as it quickly becomes outdated with updates to the graphical user interface. Interestingly, results obtained from the questionnaire state IT staff are meant to performing remote wipes upon an employee's termination, but there is no formal documentation on this in the leavers process. This means there might be staff leaving with company with corporate information still on their device. This item should be actioned immediately.

**Encouraging staff agreement.** It is clear from the experiments that there is bad energy amongst the employees about the Globex's BYOD scheme. Certain aspects are still misunderstood by employees and will have easily been forgotten since they were made to read and sign the policy. Therefore, more creative methods of training and awareness should be developed rather than using email newsletters and Q&A sessions. People are less likely to speak out in large groups and people can often miss email communications. Role-playing activities, games, and demonstrations are proven to be more effective in the long-term (Lacey 2009). Of course this will come with additional costs, but it would be incomparable to the potential losses of a security breach. The re-imbursement caps should be reviewed on an individual basis depending on the employee's role and recent travel requirements. Two participants from the IM session felt it was unfair of Globex to send them to a country with high data roaming charges where they could not expense it all back. Moreover, employees with network bundles should be able to expense some of their usage to the company without a breakdown of the business and personal costs. Particularly if they are someone who uses their mobile device for business on a daily basis. Globex should consider awarding employees with a one-off contribution to their employee's mobile devices in order to improve staff morale and encourage the shift. If Globex issued £50 to each user, they would feel less disgruntled and resentful. Doing this would still significantly reduce IT costs because corporate liable devices are purchased above £100, and that's not including the monthly network usage plan. Finally, the company should try to find ways to reduce the amount of administrative work involved in expensing business usage so staff are not discouraged from doing so.

**Device support.** The final note for improvement to this case study is, not to rule out device support completely. No additional training will be required from IT, nor will they be under any obligation to the support BYOD devices, but if they have pre-

vious experience with the device in question, it should be down to the engineer's discretion to help the user.

## 6 Future Work

This work could be expanded upon in the future with the use of other Human Factor approaches, as mentioned in section 3. One area of particular interest is the use of Cognitive Walkthrough. Here, the participants are given a goal that needs to be accomplished with a particular system and are then asked to work through specific task-based scenarios set by the facilitator. The facilitator observes the participant and evaluates the usability of the system based on the participant's actions of thought-processes. Cognitive walkthrough could be used in this case study to evaluate the usability of the AirWatch set-up. By identifying problem areas in the set-up of devices, the company could save a lot of time that employees spend in IT support and improve overall efficiency in the configuration.

## 7 References


1. Absalom, R., 2012. A guide for BYOD policies. *International Data Privacy Legislation Review*, 1, 1–23. Available from: http://www.webtorials.com/main/resource/papers/mobileiron/paper5/Guide_for_BYOD_Policies.pdf [Accessed 2 November 2016].
2. Ali, S., Qureshi, M. and Abbasi, A., 2015. Analysis of BYOD Security Frameworks. *2015 Conference on Information Assurance and Cyber Security (CIACS)*. Pakistan: The Military College of Signals (MCS).
3. Attri, R., Dev, N. and Sharma, V., 2013. Interpretuve Structural Modelling (ISM) approach: An Overview. Research Journal of Management Sciences, 2 (2), 2319–1171.
4. Broome, B. J. and Keever, D. B., 1986. Facilitating group communication: The Interactive Management approach. Available from: http://files.eric.ed.gov/fulltext/ED273997.pdf [Accessed 6 November 2016].
5. Chartered Institute of Ergonomics, 2016. What is ergonomics? - chartered institute of ergonomics & human factors. Chartered Institute of Ergonomics & Human Factors. Available from: http://www.ergonomics.org.uk/what-is-ergonomics/ [Accessed 6 November 2016].
6. Clay, J., 2015. *Continued rise in mobile threats for 2016*. Trend Micro. Available from: http://blog.trendmicro.com/continued-rise-in-mobile-threats-for-2016/ [Accessed 12 October 2016].
7. Davi, L., Dmitrienko, A., Sadeghi, A.-R. and Winandy, M., 2011. Privilege escalation attacks on Android. *Lecture Notes in Computer Science*, 6531, 346–360.
8. Dodge, R., Carver, C. and Ferguson, A., 2007. Phishing for User Security Awareness. *Computers & Security*, 26, 73–80.
9. Dogan, H. and Henshaw, M.J.D., 2010. Transition from soft systems to an enterprise knowledge management architecture. In: International Conference on Contemporary Ergonomics and Human Factors 13-15 April 2010 Keele University, UK.

10. Downer, K. and Bhattacharya, M., 2015. BYOD Security: A New Business Challenge. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*. Australia: IEEE.
11. Eshlahi, M., Salleh, R. and Anuar, N., 2012. MoBots: A New Generation of Botnets on Mobile Devices and Networks. *2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE 2012)*. Malaysia: IEEE.
12. Eshlahi, M., Var Naseri, M., Hashim, H., Tahir, N. M. and Mat Saad, E., 2014. BYOD: Current State and Security Challenges. *2014 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. Malaysia: IEEE.
13. F-secure labs, 2016. *Botnets. A quick guide to botnets - what they are, how they work and the harm they can cause.* Available from: https://www.f-secure.com/en/web/labs_global/botnets [Accessed 14 October 2016].
14. Greenberg, A., Reporter, S. and Colón, M., 2015. Human error cited as leading contributor to breaches, study shows. SC Magazine US. Available from: https://www.scmagazine.com/study-find-carelessness-among-top-human-errors-affecting-security/article/535928/ [Accessed 8 November 2016].
15. Information Commissioners Office, 2016. *Bring Your Own Device (BYOD) Guidance*. Available from: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf [Accessed 4 October 2016].
16. Kan, M., 2016. *This malware pretends to be WhatsApp, Uber and Google play*. PCWorld. Available from: http://www.pcworld.com/article/3089514/security/this-malware-pretends-to-be-whatsapp-uber-and-google-play.html [Accessed 12 October 2016].
17. Kumar, R., 2015. A Proactive Procedure to Mitigate the BYOD Risks on the Security of an Information System. *ACM SIGSOFT Software Engineering Notes*, 40 (1), 1–4.
18. Lacey, D., 2009. Transforming Organisation Attitudes and Behaviour *In: Managing the Human Factor in Information Security*. West Sussex, England: Wiley & Sons Ltd, 237–240.
19. Mathias, C., 2013. Potential BYOD legal issues you may not have thought of. SearchMobileComputing. Available from: http://searchmobilecomputing.techtarget.com/tip/Potential-BYOD-legal-issues-you-may-not-have-thought-of [Accessed 7 November 2016].
20. Miners, Z., 2014. *Report: Malware-infected Android apps spike in the Google play store.* PCWorld. Available from: http://www.pcworld.com/article/2099421/report-malwareinfected-android-apps-spike-in-the-google-play-store.html [Accessed 12 October 2016].
21. NCSC, 2014. *BYOD guidance: Executive summary*. GOV.UK. Available from: https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary#create-effective-byod-policy [Accessed 4 October 2016].
22. *PWC, 2015. 2015 Information Security Breaches Survey. HM Government.*
23. Rieman, J., Franzke, M. and Redmiles, D., 1995. Usability evaluation with the cognitive Walkthrough. CHI '95 Proceedings. California: University of California. Available from: http://www.sigchi.org/chi95/proceedings/tutors/jr_bdy.htm [Accessed 6 November 2016].
24. Souppaya, M. and Scarfone, K., 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. USA: National Institute of Standards and Technology (NIST).
25. Steele, C., 2013. *Mobile device management vs. Mobile application management*. Search Mobile Computing. Available from: http://searchmobilecomputing.techtarget.com/feature/Mobile-device-management-vs-mobile-application-management [Accessed 6 November 2016].

26. Symantec, 2016. Internet Security Threat Report. Vol. 21. Symantec.
27. Thomson, G., 2012. BYOD: Enabling the chaos. *Network Security*, 2012 (2), 5–8.
28. Wang, Y., Wei, J. and Vangury, K., 2014. Bring Your Own Device Security Issues and Challenges. *The 11th annual IEEE EENC- Mobile Device, Platform and Communication*. Las Vegas, NV: IEEE.
29. Warfield, J. N., 2002. A Handbook of Interactive Management. 2nd edition. USA: Ajar Publishing.
30. Wickens, C., lee, john, Liu, Y. and Gordon-Becker, S., 2003. An Introduction to Human Factors Engineering. 2nd edition. USA: Pearson.
31. Winder, D., 2016. *Viking horde: Are mobile botnets a thing now?* SC Magazine UK. Available from: http://www.scmagazineuk.com/viking-horde-are-mobile-botnets-a-thing-now/article/496002/ [Accessed 14 October 2016].
32. Wu, L., Du, X. and Wu, J., 2016. Effective Defence Schemes for Phishing attacks on Mobile Computing Platforms. *IEEE Transactions on Vehicular Technology*, 65, 6678–6691.