Information Security Culture

Literature Review

Jessica O'Brien, Sabbir Islam, Senjie Bao, Fangren Weng, Wenjia Xiong, Anhua Ma

Department of Computing & Information Systems

University of Melbourne

Abstract

An organisational culture that is information security aware will minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets. With the rise of mobility and BYOD, organisations require guidance in establishing an information security-aware or implementing an appropriately stringent information security culture. Various bodies of literature exist to address the issues that employee behaviour could pose when exposed to the diverse and complex world of BYOD. However, published articles that focus specifically on the relationship between the BYOD wave and the influence it has on the culture in an organisation are limited. Organisations therefore have need of a call for further research on pertinent issues within this area of information security culture. Organisations should understand that the consumer world moves much faster than the enterprise world; the challenge is to try and keep up. There is a need to support repeated platform renewals and mass switching - companies are forever playing catch up and running six to twelve months behind the market. Organisations need to shift the perimeter from the network barriers back towards the information itself. Mobility completely defies this view, and people respond to that. The objective of this paper is to examine how BYOD influences security culture in organisations, discuss findings and apply them to new but untested sights, paving the way for areas for further research. The paper has been divided into the following sections. First, the authors review previous relevant research on both information security culture as well as cultural issues surrounding mobility and BYOD. Second, they deliver what the literature review called out to the group as three pertinent cultural issues surrounding mobility in the workforce. Third, they discuss the results of the review and apply them towards new but untested ideas. In the final section, they discuss contributions, and conclude by emphasizing further research direction in the area.

Introduction

Mobilizing the enterprise is vital for businesses to find success in the dynamic, innovative workforce of 2013. Information security departments can no longer strive to be the impenetrable barrier between the threats of the external world and the vulnerabilities within their organisation. The enterprise must exchange flexibility for controls with which workers can agree (Thomson 2012). Rather than being a matter of deciding whether or not to forge ahead with allowing employees to provide their own mobile devices and access work related applications from them, it is now a matter of strategically incorporating BYOD into the workplace in as secure a manner as possible. Technical controls are a given – the focus should now be on fostering a cultural awareness and understanding surrounding the incredibly diverse range of informational security issues that arise when so many data breach opportunities exist – the total cost of just one data breach in the United States averaging $5.4M (Symantec Corp 2013). Despite advanced technical controls such as client-based firewalls, anti-virus and real time patching, and so forth, company information systems remain vulnerable because of human behaviour (Lacey 2009). The same Symantec study revealed that mistakes made my people – human errors account for the majority of data breaches, with 62 per cent of employees thinking it is acceptable to transfer corporate data outside the company. It is therefore imperative to improve the effectiveness and efficiency of awareness techniques (Thomson 2012). Examining available literature on the topic of culture and information security provides
a very broad understanding of both information security and mobility, including BYOD\(^1\). For the preceding reasons, the research questions in this study are as follows:

*How does BYOD influence security culture in organisations?*

*How can organisational security culture play a significant role to prevent security breaches?*

*What informational security management practices could improve the security culture of an organisation?*

The rest of the paper is divided into the following sections: First, the paper reviews previous relevant research on security culture and BYOD (Bring Your Own Device). Second, it explains several concepts regarding implementing security culture to manage information security for BYOD. Third, it discusses those concepts that can potentially reduce security breaches. In the final section, resulting conclusions are drawn along with an acknowledgement of their implications for the ability of security culture to effectively manage information security for BYOD, with reference to discussion on research limitation and proposition of future research direction.

It would be absolutely impossible to eliminate the risk of breaches entirely, however by adapting appropriate policies and measures, the risk can be reduced significantly. Raising security culture by creating employees awareness about security breaches and focusing on ways to protect both personal and corporate information is a sustainable, educated way to improve employees’ awareness and potentially reduce internal and external security threats.

**Methodology**

We developed our security culture perspective by conducting a literature review on papers from high quality IS journals and relevant security journals. These are shown below in Table 1.0. We used DISCOVERY, the UniMelb library search and Google Scholar, using the keywords demonstrated in Table 2.0. We found several hundred academic articles of which about thirty were relevant. We focused on articles with the themes that related to our research question as per Table 2.0.

The group then reviewed previous relevant research on both information security culture as well as cultural issues surrounding mobility and BYOD, identified some key concepts and areas for further research, and discussed the results of the review and applied them towards new but untested ideas.

<table>
<thead>
<tr>
<th>Table 1.0 Journal Titles</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Computers &amp; Security</em></td>
</tr>
<tr>
<td><em>Computer Fraud &amp; Security</em></td>
</tr>
<tr>
<td><em>BT Technology Journal</em></td>
</tr>
<tr>
<td><em>International Journal of Human-Computer Studies</em></td>
</tr>
</tbody>
</table>

\(^1\) It is important to note that while the BYOD movement encapsulates some of the key issues surrounding mobility in the workforce, mobility encompasses so much more than just employees providing their own devices (Jan 2013).
Table 2.0 Search Terms and Results

<table>
<thead>
<tr>
<th>Library Super Search / Google Scholar Search</th>
<th>Resulting # of Relevant Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational Security Culture</td>
<td>267 academic articles</td>
</tr>
<tr>
<td>Information Security Culture</td>
<td>3528 academic articles</td>
</tr>
<tr>
<td>BYOD</td>
<td>170 academic articles</td>
</tr>
<tr>
<td>BYOD + Security Culture</td>
<td>1 academic articles</td>
</tr>
<tr>
<td>Mobile Security Culture</td>
<td>1 academic articles</td>
</tr>
<tr>
<td>Human factor + information security</td>
<td>3 academic articles</td>
</tr>
</tbody>
</table>

In addition to the literature review, our team also conducted two sets of interviews, one with the Information Security Team at the Research & Development offices in Bundoora, Melbourne, and the other with a Domain Architect who oversees the security functions for ABC Mining Limited, at the Corporate Head Office in Melbourne. These Interviews were transcribed and used to take the concepts from the literature review through to the discussion, to try and formulate a new take on the cultural aspect of information security.

**Prior Research in the field**

**Security Culture**

According to Von Solms (2000), security culture is “to be created in a company by instilling the aspects of information security to every employee as a natural way of performing his or her daily job”. According to Schlienger & Teufel (2003), “Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee. The cultural concept helps to increase trust between the different actors concerning information security within an organization”. The emergence of security culture has been identified and explained by many researchers in various ways. It was found that there is no unique way or any specific parameters to define security culture within an organisation. Elaborating on these definitions, researchers have found various factors involved in managing information security in an organisation and related factors. According to Sasse, Brostoff and Weirich (2001), identification and specification of key behavioural attributes can drive security culture including business impact, penalty and security awareness. They described a predominantly fear based approach with the intention of encouraging acceptable security behaviour.

Adams and Blandford (2005) explained that a security culture must align with business strategy and be amalgamated into standard operational practice. Moreover, they mentioned that the key strategy should be raising awareness and encouraging staff to be alert. Furthermore, they highlighted the importance of informed management and staff by providing training, as security culture wouldn’t be able to be successfully implemented without clear support from management. Thompson, Vol Solms and Louw (2006) mentioned that a security culture was highly influenced by organizational culture and reciprocally related to it. They emphasised learning and development as critical factors to ensure employees’ awareness of security concerns and improved aptitude to implement them. They also argued communal socialization may play as an important factor as people learn by observing one another. Ruighaver, Maynard and Chang (2007) claimed that it wouldn’t be appropriate to assess security culture in isolation
from overall organisational culture as an organisation’s internal culture has an enormous impact on security culture.

According to Whitman and Mattord (2011), attitudes towards the ethics of computer use were affected by various reasons and differences were found among individuals within the same company from the same social background. They added that education was the factor that made the difference, which could be disseminated throughout the organisation by providing training, generating awareness and most importantly creating a culture; an organisational security culture could make a big difference towards the whole approach. Whitman and Mattord (2011) also mentioned three general causes of unethical or illegal behaviour. They indicated that ignorance could easily be reduced through raising awareness, culture and training. Moreover, accidents can similarly be mitigated through raising awareness, training, and creating culture along with process and policy. Furthermore, intent is another cause that is quite difficult to control, however by creating employee profiling and new behavioural patterns along with training, awareness and developing a security culture, this can potentially be prevented as long as appropriate policies and procedures are in place.

**BYOD Culture**

From a survey conducted by Cisco in 2012, approximately 89 per cent of organisations around the world allowed their employees to use employee-owned devices in the workplace and the percentage still keeps rising. Similarly, based on the same survey, Cisco also indicated that the average number of devices that each employee use is expected to increase to almost 21.7% by the year 2014. This means that BYOD is growing more and more important to both organisations and employees. From the organisation’s perspective, the most notable benefit that BYOD’s bring is increased work productivity and mobility. For example, by accessing SAP via mobile device, employees can keep up-to-date with the latest business data and information at anytime and anywhere, which not only significantly boosts their work efficiency, but also increases their collaboration with customers, suppliers and business units. Especially for mobile employees, who have to spend a lot of time travelling or waiting for flights at the airport, SAP mobile no doubt is the most straightforward way for them to eliminate wasted time. Moreover, by allowing employees to bring their own devices, the cost that organisations outlay on IT infrastructure is also reduced. From the employee perspective, the quality of their work and personal life is improved because they can choose the devices, applications and services they prefer for both work and personal use (Santhana & Kumar, 2011).

However, even though BYOD brings a lot of benefits for consumer use, it poses a great challenge for IT professionals to keep the organisation’s data and information secure and protect them from cyber-attack and malware infection. According to a 2012 survey by Infonetics Research, all organisations in the survey said they had found malicious apps on their employees’ devices and 64% of them said their employees had lost their personal devices that contain access to a large number of their organisation’s sensitive resources. Another survey from Duo Security Report (2012) showed that over half of the Android devices had security loopholes that were susceptible to malware attacks, which also indicated that serious security issues arise when employees bring their own devices for work (Semer, 2013). Besides, many organisations didn’t regard mobile security as a business priority (Confidential Document, 2012). Therefore, in order to avoid the security risks caused by BYOD, it is necessary for organisations to deploy some effective BYOD policies.

So far, many organisations consider mobile device management (MDM) is the best solution to secure employee-owned solutions. It provides two independent environments and therefore the business data and personal data that are stored on the same employee-owned device can be separated and organisations only need to monitor the data and set policies for the business environment, which not only guarantees the security of the organisation’s resources, but also effectively protects the employees’ privacy. In addition, managers in the organisations should have continuous risk awareness and assess the BYOD risks and policies frequently. Meanwhile, they should also provide a security culture that ensures each employee in the organisation understands the importance of business data security and follows the security policies and rules relating to BYOD. (Semer, 2013).

**Key Concepts**
**Risks Associated With BYOD**

BYOD offers end users (employees) and businesses several benefits. By enabling employees to bring their own devices into the work place and have the option to choose the most appropriate device for their work, BYOD makes IT in organisations more flexible and cost effective. However, the information security risks presented by BYOD are also a big challenge. Mobile malware and data leakage are two main concerns associated with BYOD (Hunt 2012). With mobile devices becoming more advanced, the increasing prevalence of malicious software on them is almost inevitable. Advanced mobile devices provide a programmable platform, which is the cause of malware on mobile devices and is making malware by no means restricted to PCs (Furnell 2006). Friedman and Hoffman (2008) also pointed out mobile devices such as PDA and mobile phones can improve enterprise productivity efficiently, but are more vulnerable to attack than PCs. They divided mobile device risks into seven categories and claim that firewalls and anti-virus software are necessary but not sufficient. Firewalls cannot block malware spreading through ports that are in use, and some malicious code can also evade signature based antivirus software and mobile devices can move outside the organisation’s firewall area and will be under threat (Friedman & Hoffman 2008). Thus, it is essential for organisations to educate employees to raise their awareness of information security and only use their devices containing company information in a safe environment.

Employee behaviour is strongly affected by the organisation’s information security culture; therefore, cultivating a good information security culture should be combined with technical controls to prevent mobile malware.

Another subtle risk of BYOD is employees may misuse mobile technologies and causing data leakage. Due to effectiveness of mobile devices as business tools, employees’ own mobile devices have penetrated the workplace and 95% of workers have smartphones according to an iPass Global Mobile Workforce Report (Calder 2013). However, this scenario also presents corporations with a serious security risk. Any devices used in the workplace are likely to contain company sensitive information. If companies allow employees to bring their own devices into the workplace, an organisation information security issue will emerge: it is hard to regulate private devices even though these devices contain significant corporate information and increase the possibility of data leakage of the company. From a user’s perspective, employees are likely to ignore the gap between personal life and work and use their mobile devices as both business tools and personal tools. It is almost impossible to stop employees using their own devices to support their business lives and banning these devices may be against the interest of business as employees may be denied access to a potential business opportunity through using their own devices (Furnell 2006). However, businesses may recognise the benefits of BYOD and allow employees to bring their own devices. A survey held by BrightTalk, a netmeeting provider, revealed that 4 out of 5 respondents owned more than one mobile device while more than one third failed to have a passcode to protect information stored on their devices (Calder 2013). Thus, allowing employees to bring their own devices to the workplace without any control strategy and awareness education will expose organisations to a high risk of data leakage. To make the most of BYOD benefits, a BYOD policy is definitely not enough. Technical control methods and an organisation security culture (employee awareness and behaviour) should work together to deal with the risks accompanied with BYOD.

**Mobility - The Enterprise View**

BYOD has advocates across different levels of managerial hierarchy. From the perspective of high-level management, productivity of employees will increase considering the fact that they can now work whenever and wherever they want using their own devices (Baker, 2013). For example, according to Jon Smith, Domain Architect at ABC Mining Limited, middle level managers are a group who will benefit greatly. As now with BYOD, they are able to get information and make approvals on things such as SAP purchase requisitions and purchase orders as soon as possible in order to accelerate the whole process. In addition, employees familiar with current technologies are more willing to use their own advanced devices to fulfil their tasks. By supporting BYOD within the organisation, employees will be more engaged and enthusiastic; problem-solving capacities could be facilitated; and furthermore, the organisation is actually enjoying the merits of new technologies and functionalities that are used by their employees (Gordon, 2013).

Efforts have been made by organisations to both support BYOD and to extract benefits from it, as well as to ensure the security of business operation. According to Baker, T., (2013), applications are the
“backbone” of any mobile workforce. Applications for system integration and interoperability are purchased off the shelf or developed internally by organisations to ensure that employees are able to use organisational information systems or other functional applications on their own devices using the Internet. Although development of applications to support interoperability and functionality of different devices is critical, it is not enough. Security is as important as functionality when developing BYOD programs (Baker, 2013). As a result, programs to protect company information from leakage such as Data Loss Prevention (DLP) have also been developed (Gordon, 2013). Some principles for developing BYOD security applications are identified from literature reviews.

First of all, the idea of security should be embedded into the design of applications, not as an afterthought (Baker, 2013). As different security issues arise every minute, organisations tend to rush in to ensure the deadlines and budgets are met. However, this “short sighted model” not only puts organisational information assets into danger, but also leads to further security costs. Therefore, the better way is to consider security at the initial stage of any BYOD program to eliminate any potential vulnerabilities. Thus, BYOD require flexible and creative solutions from IT staff for maintaining security while enabling access to collaborative technologies (Gordon, 2013). Functional applications and security applications should be able to work together to make sure employees with their own devices are working in a well-functioning and safe environment. Therefore, it is important that security does not act as a barrier to business transformation, and the balance between risk and benefit of BYOD should be found (Gordon, 2013). Ultimately, the nature of devices employees use, the sensitive information that might be held on these devices, the potential threat to the device, as well as the level of security available and likely to be in use, should all be considered (Steven, 2013).

Another complex but important issue that organisations should be concerned about is accessibility and its related security solutions. What kind of information can be accessed by personal devices, the authorisation levels of different employees, and how easily the employees can access business information by using their own devices, should be determined. Several technologies for maximising the probability of information security are available to organisations, for example, strong password protection on information access, enabling file encryption to encrypt data stored in devices, applying automatic locks to close access if an incorrect password is entered too many times or after a period of inactivity, adopting remote wiping to remove data from devices in case of loss or theft, etc.. However, it is not just defining the authorisations and degrees of accessibility that is a complex issue, but applying those security technologies is also not easy. The more secure the technology is, the more organisations should pay. Besides, as Furnell, S. (2006) figured out on his research, too many constraints can impede the use of security. This is also supported by Mansfield-Devine, S. (2012) who indicates organisations would undermine the whole benefit of BYOD if they are too restrictive. (Those technologies may be too secure to constrain the flexibility of using personal devices which may further lead employees’ unsatisfactory so that they may have resistances to follow those necessary security actions) Overly restrictive technologies may constrain the use of personal devices to the extent that employees become reluctant to follow required security procedures.

According to Furnell S. (2006), “technology will never provide the complete solution”. In order to gain benefits from BYOD rather than be trapped by security problems, non-technical solutions such as establishing security policies, implementing efficient controls regarding these policies, building security awareness through training and education programs, etc. are more important. As many academic journals indicate, BYOD brings big cultural change to organisations. Thus, it would be necessary for organisations to address the BYOD issue from the security culture perspective. Based on the information security culture framework of Veiga, A. (2010), the information security culture is cultivated by the behaviour of employees, which is directly influenced by the information security components. In relation to the BYOD, it is important for organisations to adopt appropriate security policies, leadership and governance, and other security components which enforce the behaviours of employees could be in line with the security policies, in order to change the organisation culture into a security conscious one (Vroom, 2004). With an effective security culture, BYOD is more likely to achieve a positive effect for organisations.

**Discussion**
**Social Contract**

Resistance to the mobile computing wave will likely come at great cost to organisations, as the younger generations of tech-savvy professionals have come to expect that their profound attraction for the opportunity to combine work and home life on the one mobile device will be satiated in whatever company they choose to work for. Above all, an organisation is only as good as the people that work for it, and refusing to accommodate these fundamental user needs would undoubtedly mean offering up the best talent to competing companies that will. These ‘millennials’ are coming into the workforce as ‘fully indoctrinated mobile device multitaskers’ (Sybase 2011). These highly sought after individuals expect access to their critical business applications as well as their social media applications whenever and wherever they need them – they will expect no sacrifice in usability. Attracting individuals who have grown up taking basic utilities such as water and electricity for granted in the same way that they take the internet and mobile phones for granted indicates an important cultural shift that every organisation needs to make (Sybase 2011). BYOD can empower employees to be more creative, more efficient, and more productive (Sybase 2011) – realising that it is time for the contractual boundary to shift, placing the onus now on the enterprise rather than the user to ensure that demands are met – this is how truly innovative companies should seek to secure their competitive advantage in the marketplace.

The concepts outlined in this review paper offer more than just a summary of findings – our team builds the support for a discussion of the information security issues surrounding mobility as a cultural paradigm and allow the social contract theory to be examined, which is a new way to examine the two broader issues together. Although supporting BYOD is a way of fostering a positive level of human interaction between corporate environments and personal contexts, the use and growth of information technology change the collective obligations present in the implicit social contract between the user and the organisation (Skovira 2003). Information security in mobility affects the fulfilment of obligations and responsibilities. It is a cultural force that shapes these commitments. According to the Cyber Risk Manager and Information Security Architect the social contract idea is a theory that you have made a social contract with society that allows you to live in it. The challenge that organisations are experiencing today is that there is a breakdown in the social contract with mobility and BYOD - people want to make their own choices and do whatever they want but don't want to be accountable for their actions. An interview with the security team at XYZ mining revealed that the company made the decision to strand / isolate users via the move from GOOD2 to MDM. Previously, users were complaining they didn't have enough freedom of choice with devices. The solution: Organisations need to get an enforceable social contract out; a self-regulating system that pre-empts a move away from people demanding the choice but not being prepared to be accountable for their own actions. The information security team at XYZ developed the idea to write a ‘social contract’. This is not an actual legal document where user needs to ‘sign here’ – it is more about embedding a cultural shift in the way people work than ‘sign here, ask questions later’ change. You can’t look at it as a legal problem, or a technical problem - it’s a social engineering problem. Raising social awareness is done through being transparent and open with people about the requirements and criteria involved.

**Cyber Kill Chain - the effectiveness of war stories**

Security experts at enterprise information protection leader Verdasys say customers are successfully using a defensive strategy known as the Kill Chain Defence3 to guard against Advanced Persistent Threats (APTs) and other targeted and highly sophisticated cyber threats (Verdasys 2013). The idea is, if you can break a link somewhere in that chain of attack (the cyber kill chain), you can stop the attack from working properly. When the topic was presented to them, the InfoSec team at XYZ said they would consider explaining the cyber kill chain to people to try and embed a more aware and active culture surrounding information security and mobility. If you say ‘here's what happens at this stage’, and raise awareness on issues like don’t click on links, report suspicious computer behaviour like reduced performance (could be

---

2 For enterprises and government, Good for Enterprise delivers secure mobile communication that allows IT to protect the enterprise and end users to connect and collaborate on their devices of choice (Good 2013).

3 A Kill Chain Defence collects and correlates threat activities, identifying anomalies that signal malware and challenges that malware’s adaptability and stealth from all possible stages of the attack by rapidly deploying containment controls to the stages where the malware is most vulnerable. Detection and kill capability at each point in the enemy’s attack chain results in the highest probability of a successful defines.
downloading gigs of information over the network) etc. The Cyber Kill Chain is one way to apply the findings discussed in previous sections to new but untested sites. Fundamentally, empirical evidence demonstrates that ‘war stories’ are an extremely effective way to instil the importance of information security into users. Organisations are not placing enough weight on user awareness training (D'Arcy & Hovav 2007), while giving far more attention to ensuring the appropriate technical controls are in place. For while technical controls are important and even critical, procedural controls must also be utilised to ensure that the technical controls are not undermined. For instance, an organisation might invest heavily into ensuring their MDM solution has the ability to remotely erase company data, however, if their users are not made aware of the potentially catastrophic consequences of them being careless with information or not reporting suspicious cyber activity, then the company is still highly vulnerable to attack. The idea with this approach is to ingrain the importance into the very culture of the organisation through educating users from the bottom up. Teaching them about the different stages that occur throughout a cyber-attack, teaching them what signs and symptoms to look out for, and teaching them to always be diligent in reporting suspicious activity – these are ways in which organisations can begin to develop a common defence against threats. See Table 3.0 for a more in depth examination of the second research question offered earlier – an overview of some ways organisations can seek to raise awareness through embedding culture. The security issues pertaining to mobility in the workforce are a largely social problem; they therefore need to be tackled in a social way.

<table>
<thead>
<tr>
<th>Method</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
<td>Educate employees and train them on how to handle confidential information (Symantec Corp 2013).</td>
</tr>
<tr>
<td><strong>War Stories</strong></td>
<td>According to Jan (2013), informally raising awareness is the best way to foster a positive cultural shift in understanding; a chat in the hall, grabbing a coffee, that sort of thing. Giving people war stories about things that have gone wrong is the most effective way to raise awareness about security issues. The team at XYZ talk about APT Threat - Advanced Persistence Threats as the most viable way they believe hackers will try to attack users. Via this method, anyone down to entry level can be targeted, and even lower levels of staff can be monitored for months on end. Technical controls work for the ‘opportunist’; the ones who see a phone left in an airport lounge and pick it up, realise it is a corporate device and consider - this could be worth some money.</td>
</tr>
<tr>
<td><strong>Internal Social Media / Communities of Practice (CoP)</strong></td>
<td>Social media is an extremely effective way to get people involved, interested, and sharing. Yammer is an enterprise social media network designed for company collaboration, file sharing, knowledge exchange, and team efficiency. An interview with information security experts at XYZ revealed that raising social awareness is done through being transparent and open with people about the requirements and criteria involved. They ran surveys on Yammer to gauge an understanding of user awareness on the critical security issues that mobility presents, created an interest group called ‘BYOIT’ (Bring Your Own IT), and set it up so that</td>
</tr>
</tbody>
</table>
Yammer is an accessible app from the mobile device itself.

**National Culture**

Regulations vary widely between industries; with heavily regulated fields including healthcare, pharmaceuticals, and finance incurring breach costs 70 per cent higher than other industries (Symantec Corp 2013). The same Symantec study reveals that while German companies are most likely to experience a malicious or criminal attack, Brazilian companies are most likely to experience breaches caused by human error. Unfortunately the majority of research about information security management has been performed about technologically leading countries such as the USA, the UK, the European Union and Australia (Ponemon Institute 2013), leaving unanswered questions about cultural awareness and understanding from a security perspective in developing countries. The business environment of Saudi Arabia, for example, is vastly different from the environment of a Western country (Alnatheer & Nelson 2009). A study done by Alnatheer & Nelson (2009) applies Hofstede’s 2001 framework to information security culture and how it is influenced by national culture. Hofstede classified national culture into five dimensions, outlined in Table 3.0. Although the study discusses the important cultural differences between developing countries and Western countries and how these relate to information security, an area for further research would be to take the step further and investigate how mobility and BYOD relate to these issues. Hofstede argued that organisational cultures are nested within a national culture, and that national culture influences human resource practices and organisational behaviour (Hofstede 1984).

<table>
<thead>
<tr>
<th>Table 4.0 Hofstede’s Five Cultural Dimensions (1984)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Distance</strong></td>
</tr>
<tr>
<td>Long-term orientation</td>
</tr>
<tr>
<td>Masculinity / femininity</td>
</tr>
<tr>
<td>Individualism</td>
</tr>
<tr>
<td>Uncertainty Avoidance</td>
</tr>
</tbody>
</table>

**Conclusion**

The literature is unanimous - adopting a BYOD policy is a cost effective way to immerse your organisation in the mobility movement. Ultimately, employees who provide their own mobile devices have higher morale and yield significant savings for the company in capital expenditures (Sybase 2011). That being said, formalising such a policy should not be the first or most highly prioritised move – the focus should be on changing the corporate culture to match the mobile nature of the way people want to work today. Businesses that embrace the changing times will be the first to reap the rewards that come with having a happier, more productive workforce. In essence, the literature available on the mobility zeitgeist seems to hone in on one fundamental concept – that being if organisations are going to remain competitive in today’s markets and enjoy fast return on investment, increased employee productivity, and the ability to attract the best of upcoming talent, they need to embrace the move forward into the vulnerable world of
BYOD (Sybase 2011). The discussion provided indicates several innovative areas in which further research would provide value to the issues surrounding BYOD, more broadly mobility, and security culture. Some empirical research on the concept of social contracts and the effectiveness of utilising real life ‘war’ stories to informally ingrain an understanding would be extremely insightful. Additionally, further research on whether an ideal culture exists or whether different industries and departments require different approaches would be beneficial. How does BYOD influence security culture? Through taking a largely technical phenomenon and immersing it into a social engineering challenge, rather than a mechanical challenge. The knowledge retained within the people working for an organisation are the real assets, and if they are going to utilise that knowledge to the advantage and ultimately bottom line profitability of the organisation, balancing the fine line between the end user’s demands and the security risks posed is where organisations should focus their efforts.

References
Calder, A 2013, 'Is the BYOD Movement Worth the Risks?', Credit Control, 34, 3, p. 65, MasterFILE Premier, EBSCOhost, viewed 14 July 2013.
Hunt, J 2012, 'BYOD Policy -- What Businesses Need to Consider', Credit Control, 33, 5/6, p. 69, MasterFILE Premier, EBSCOhost, viewed 14 July 2013.


Publications.

Schlienger, T., & Teufel, S. 2003, Analyzing information security culture: increased trust by an appropriate information security culture. In the proceedings of 14th International Workshop on Database and Expert Systems Applications,IEEE.


Soon Lim, J., Chang, S., Ahmad, A., Maynard, S., (2012), Towards an organizational culture framework for information security practices. Strategic and Practical Approaches for Information Security


Author/s:
O'BRIEN, JESSICA; Islam, Sabbir; Bao, Senjie; Weng, Fangren; Xiong, Wenjia; Ma, Anhua

Title:
Information security culture: literature review

Date:
2013

Citation:

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33336

File Description:
Information security culture: literature review

Terms and Conditions:
Terms and Conditions: Copyright in works deposited in Minerva Access is retained by the copyright owner. The work may not be altered without permission from the copyright owner. Readers may only download, print and save electronic copies of whole works for their own personal non-commercial use. Any use that exceeds these limits requires permission from the copyright owner. Attribution is essential when quoting or paraphrasing from these works.