Compliance to Governance policy while adopting new Information Technology practices, agility and data fragility– A study on implementation of BYOD policy in Singapore

K.S. Raghuram[1] **Easwaramoorthy Rangaswamy**[2]

Albeit employee friendly, Bring Your Own Device (BYOD) guise challenge to organisations in data security maintenance and application vulnerability. Organisations need to estimate if their Information Technology (IT) Governance policy is agile and makes its data security fragile. This paper helps organisations in widening their horizon of understanding and implementing IT governance. In addition, it addresses issues in compliance and exercising security control to reduce data and application vulnerability. Data was collected through a field survey from IT organisations in Singapore which have implemented BYOD. It is hypothesized that increase in data and device security controls makes employee more compliant. Secondly it hypothesizes training and awareness programs in pursuant with law of the land and best industry practices will reduce the fragility and security compromise. Lastly it is hypothesized that implementation of BYOD increases inventory and platform management risk with increased frequency of malware and application vulnerability threats. The survey was restricted to IT companies located in Singapore. This paper contributes to IT practitioner's understanding and perception of BYOD, its related security challenges while strategising BYOD governance. The results have significant implications to organisations while strategising its IT Governance policies and reduce data and application vulnerability. The findings suggested that organisations need increased constant surveillance and legitimate review of security inventory controls, implement employee awareness programs following policy iteration. Stringent compliance and substitutive procedures reduces application vulnerability.

Keywords: *Data Security, IT Governance, BYOD policy, IT Governance compliance, device vulnerability.*

INTRODUCTION

Employees are excitingly embracing latest business mantra – BYOD. Trends show a phenomenal growth in the number of organisations adopting this mantra. The number of smart phone users is likely to touch 6.1 billion and utilise 80 percent of the mobile data traffic by 2020 (Tech crunch, 2015). Smart phones and tablets have made a dramatic transformation on life style and information sharing. Social media changed the way people use gadgets for personal life, anywhere and everywhere data availability and business requirement had similar impact on their business life. (Disterer & Kleiner, 2013). Gadgets are so advanced and people are mature in its usage and have superior computing at their finger tips everywhere and every time. Employees carry their personal smart phones, iMacs and tablets to their work place.

Organisations adopt BYOD policy and employees are given choiceto select the gadgets even personal devices and bring them to work place. (Citrix, 2013) Employees conveniently continue to enjoy using their personal devices at work and share same devices between personal and business work (Air Watch, 2012).

[1]Senior Lecturer and Research coordinator, Amity Global Business School, Singapore Email: ksraghuram@singapore.amity.edu

[2]Principal, Amity Global Business School, Singapore, Email: erangaswamy@singapore.amity.edu

Organisations aim at developing an information security control policy that will instil confidence, expect honesty from the users and is flexible for timely up gradation to suit the control environment (M. E. Whitman and H. J. Mattord, 2010). Deshmukh and Wadhe A, 2012 report organisations are concerned with loss of physical devices, loss of data into unauthorised networks and gaps in IT governance policies. The essential feature of the devices enrolled under BYOD is mobility and given their size they are prone to theft or getting lost. Organisations will have to wipe data and remote locking as a standard practice. Building firewalls and multi stage password authentications are essentially used for data protection while logging into unauthorised networks and also follow data encrypting. Any policy loopholes make the IT Governance fragile rendering the data and device compromise to Trojans and malwares. They reported that even if organisations have an efficient security policy its success depends on the implementation of the policy. Conversely, good is the IT policy if the company can implement the policy effectively. With a variety of hardware and plethora of software and platforms, enforcement and compliance of the policy becomes a challenge. Providing legitimate updates and maintenance to these devices needs considerable effort by organisations. In the absence of a stringent security policy and non compliance, BYOD can lead to serious consequences like lawsuits and culpability.

(A. B. Garba, J. Armarego, and D. Murray, 2015) indicate that many organisations do not conceive mechanics of BYOD framework without clear knowledge of probable repercussions on the organisations liability. Companies which understood the mechanics failed in creating awareness among its employees. Majority of organisations articulated only mechanics of BYOD, but were reluctant with the policy framework and IT governance.

One other area of security risk is when devices are connected to unauthorised or public Wi-Fi networks. It may result in unintentional delivery of data to unauthorised devices and recipients without the knowledge of device user. Data stored or transmitted without encryption becomes vulnerable. A legitimate attempt to ensure the company policy is strong then it should include identification of training needs for the employees on all the privacy settings. (K. W. Miller, J. Voas, and G. F. Hurlburt, 2012)

Organisations should be keen in defining the practices and implementing IT governance policy. About 5.18 devices per employee constituting a mix of both company owned and personal devices are hooked to company network. Organisations are in persistent pursuit of developing a policy that is inclusive and exhaustive any attempt to incorporate all the possible escape clause is a challenge. Several companies are adopting BYOD policy without an explicit policy in place (Citrix, 2013)

This paper provides greater insights for organisations while implementing an IT governance policy since many organisations adopt BYOD without an explicit policy in place (Citrix, 2013) It also provides insights for creating awareness and leverage the security controls since many companies does not understand the mechanics of implementing, creating awareness and were reluctant in writing a detailed policy (A. B. Garba, J. Armarego, and D. Murray, 2015)

A sudden spurt of dual use of personal devices to keep the employees happy has made organisations to adopt BYOD agile that makes the organisations data vulnerable and fragile in absence of a suitable policy.

REVIEW OF LITERATURE

Employees have ambitiously requesting for using same device for personal and business work as it is convenient and easier to use. (Garlati, C. 2011). Organisations have been adopting BYOD with or without detailed policies in place to make their employees happy and this has resulted in increased productivity, employee

satisfaction and increased mobility at businesses. (Singh, N, 2012)

This makes employees delighted resulting in generating a positive impact in the work environment, greater productivity, reduced turnaround time and attracting new hires. With all these it comes with it a deluge of security issues. (Deshmukh, R., & Wadhe, A, 2012)

(Forrester, 2012) reports that the biggest challenge with BYOD is the device and application security concern and data breach

Smart devices offer the luxury and are suitable to carry easily due to their compact size. This advantage may turn into a potential disadvantage sometimes as the smaller size makes them prone of getting misplaced or lose easily (Calder, 2012)

Reports of employees misusing the organisations resources have increased with organisation adopting BYOD. Few employees indulge in activities like wilful bypassing firewalls, crack passwords making data and device compromise inadvertently. As a result of this when such devices are lost, organisations cannot wipe the data since the employee was not compliant to the policy. (Potts 2012)

BYOD exposes organisations data and devices to malware and Trojan with a possible data leakage. (Cisco, 2012) identifies that the biggest threat to the company with BYOD adoption is from the viruses, malwares and network intrusions. This threat makes organisations vulnerable. Many times organisations are not aware the network to which employees get connected and any such unintentional download into the device may spread into organisations network in a jiffy. (Tzoumas, 2013)

According to (Dilger, D.E, 2013), a BYOD user specifically need not have to download apps to be a potential victim. The user platform will be a victim of malware that leads the user to the unauthorised and restricted sites. He report such issues are increasing since most Android users have not been updating their Android devices making it vulnerable for attacks. Organisations need to educate their employees with every update of its policy or malware version to ensure that the company data and employee device are not victimised.

But organisations are concerned with maintaining the data security when corporate data is accessible by a device which is not owned by the organisation. Unintentional delivery of corporate data to an unauthorised device, gadgets getting compromised by Trojan and application vulnerability by the malwares are the prime issues concerned with adoption of BYOD (Morrow, 2012).

For organisations one of the driving forces to adopt BYOD is it renders savings in investment resulting in its reduction of capital expenses. Organisations tend to transfer these investment costs on to their employees (Wood 2012).

Employees work outside their work place and sometimes connect to open wireless network if they are not controlled by IT policy. (Vickerman.J, 2013) suggests the company should adopt an Information Technology governance policy whether the company likes or not.

(Abubakar Bello Garba et al. 2015) proposed a frame work for security for BYOD implementation. This study considers the framework by analysing the degree of control needed to have strong IT governance.

There has been many academic research work to establish trade-off between cost and benefits of implementation of BYOD but the degree of security controls to strengthen an IT governance policy has not been addressed in much of academic literature, hence the need for the study.

RESEARCH MODEL AND HYPOTHESIS

Majority of BYOD devices are small and have mobility which are prone to lose and there by making the data to be compromised. Mobility

being the essential feature, fear of connecting the device outside the secured network is high. Controls at the gadget level and at the server level should be imposed resulting in multiple levels of authorisation, device lock with more than the prescribed number of attempts to logins with a wrong pass code. Theoretically BYOD was embraced by employees because of ease of use. With increase in the controls and security policy employee often tries circumventing the security protocols. (Vickerman, J. 2013).

IT governance policy should have power to scrutinise and access data in the devices with more checks and balances. Employees find different ways to bypass the security controls if they are aware that the company has the possibility to remotely locate alter and wipe the data partially or completely at the behest of companies' discretion. But the challenge remains that with increased security protocols will the employees adhere to the policy, hence the hypothesis

H1: Greater the control measures to avoid security breach will make the employees more compliant to the IT governance policy.

Influence on Behaviour

Employees carrying their devices many not be comfortable in using multi step user authentication and alpha numeric passwords, or fingerprint scanners for logging into the device especially while they are accessing social networking sites. If the device registered under BYOD is lost, the employee will be more concerned losing their play list and photo albums rather than the company data. Device loss or theft will result in remote locking of the device or partial or complete wipe of the data, hence the hypothesis

H1-1: Increase in security controls has a negative impact on the behaviour and satisfaction of the device user.

INCREASE IN RESOURCES

With a plethora of gadgets coupled with unprecedented flood of updates, organisations have to increase its resources capabilities to keep pace with the updates and controls. Personal and business information lies on an obscure boundary with in a common device. Organisations need to access the data on each device and compartmentalise for better data security controls which needs additional resources, hence the hypothesis

H1-2: Enhanced data security controls require increase in resources at the organisational level

Increase in Responsibility

Personal and business information lies on an obscure boundary with in a common device. Organisations own its data on the device owned by employees. Employees tend to be more concerned with loss of their play list and photo albums in the event of theft of device rather than the companies data. Can organisations impose a liability on the employee for loss of its data? Would this bring in a sense of responsibility in the employee to secure the data and the device? Hence the hypothesis

H1-3: Imposing more responsibility on the employee will make them more compliant towards the IT security policy.

Influence on Employees

What would be the impact on the employees if the IT policy includes words like restricted, compulsory, unauthorised, intended? (Ten-Steps-To-Secure-BYOD, 2014) Would this be binding on their part to abide to the policy? If the policy expressly restricts few websites or applications on the devices, would it have a positive influence on their perception towards BYOD? In the absence of stricter clause any

breach may lead to liability on part of the company, there by spoiling the name of the company for unintentional act of the employee. Hence the hypothesis

H1-4: Using binding clause in the IT Governance policy will influence the user-friendly behaviour of the employees

Law of the Land

Most countries have data protection act in place. In any event of loss or theft of the devices, organisations to reduce liability should write policy that is in complaint with data protection act of the country. Should organisations comply with the best security practice or with the law of the land? Hence the hypothesis

H1-5: Security policy that is in compliance with the law of the land and best industry practices reduce the risk of data and device vulnerability

Employees may be ignorant with the frequent updates at the policy level and the user level. They may not even be aware to what level of policy confidentiality they belong to (A. B. Garba, J. Armarego, and D. Murray, (2015) Some mobile devices registered under BYOD may not receive automatic updates of security making them vulnerable for attack from malware and Trojans Paullet, K., & Pinchot, J. (2014). But it can be argued that the devices are generally owned by the employees and should be mature enough to safe guard the devices from such treats. Organisations have little authority on the gadgets and employees hold a broader responsibility and ownership on the device. But in the absence of adequate knowledge on part of employees, organisations should have to train to mitigate such threats and, hence the hypothesis

H2: Increase in training and awareness of the employees has a positive impact on the reduction of risk of data and device vulnerability.

Training for Compliance

Any security update in policy or practice should be educated to the employees. Both technical and security training in safeguarding the devices and data has to be programmed and scheduled in the training calendar of the organisation. Most employees are unaware the level of security required to be firewalled to their device should be covered. It can be argued that training will educate and bring in compliance, hence the hypothesis

H2-1: Training on policy and practice updates significantly improves compliance to the policy.

Enforcement of Policy

The training needs should be included in the policy enforcement which includes areas like privacy governance and restricted application download. Strict enforcement of policy will ensure users who are non compliance do not violate the standards, hence the hypothesis

H2-2: Strict enforcement of security policy has a positive impact on compliance and reduction in data vulnerability

Initially when the organisation adopts BYOD, data is trafficked among devices that do not comply with the security standards of the organisation. Mobile devices come with a range of applications including gaming and social networking. Applications provide service that is largely obligated only by developer idea it also widens the risk of assisting gadgets in an authorised network. Few operating systems and products in the Original Equipment Manufacturer (OEM) may not support the security environment existing in the organisation resulting in unintentional download of malware and making the application vulnerable. Devices belonging to employees are used to access business information may sometimes become a mobile devices to access corporate data, such

devices will be a fragile point of the companies data security standards. But the devices owned by the organisations comply with such standards. The organisation will have to work on increasing the surveillance of such concern by increasing its support management activities, hence the need to hypothesise

H3: Adoption of BYOD will increase the inventory and platform management risk and increase in threat of malware application vulnerability.

METHODOLOGY

This study investigates the impact of IT security controls on perception of employees' compliance, secondly the influence of training and awareness programs on the compromise of data and device and lastly the relationship of BYOD adoption on frequency of malware threats and organisations inventory and platform management risk. Positivism research philosophy is adopted for this research. A structured questionnaire is sued for the survey. The research approach is deductive methodology with cross sectional study.

A field survey was conducted and data was collected from IT companies that had adopted BYOD in Singapore.

4.1 Sample and Data Collection

From the list of IT companies registered with Accounting and Corporate Regulatory Authority (ACRA), Singapore 678 companies were selected. Initial contact was a request to participate in the survey with a precondition that if they had BYOD implemented. 242 responses were received of which 213 had adopted BYOD. To encourage participation, it was confirmed to respondents that identity would not be disclosed. Electronic form of the structured questionnaire was circulated to 213 companies Chief Information Officers (CIO) or the Chief Compliance Officers (CCO). This form was free from setting up any of login credentials they were free to exercise the option to opt out of the survey. There were 197 responses of which 31 were partially complete and could not be used, thus making the sample limited to 166. This gives an overall response rate of 24.4 percent. The breakdown of respondents shows that 11.45 percent were from product companies, 27.71 percent were from services companies and 60.84 percent were from process or Information technology enabled services. No evidence of response bias was found when the types of companies were compared to the population of IT companies. There was no evidence of any non-bias response when the results of key variables compared between initial and slow responses.

4.2 Measurement

Based on the responses received, the respondents were grouped into two categories depending on the degree of security control. The variable was called as degree of control based on the responses we received. The measurement of this variable was on a scale of 1 to 2. A value of 1 was attached when the company has strong control and 2 when the company has weak control. The structured questionnaire used to evaluate the degree of security controls and perception of employees on IT Governance included 16 items selected from three below listed sources were considered with suitable alteration to match the control environment. To measure the degree of security controls, the technical controls were adopted from (D, Rivera et al, 2013). To measure the training and awareness factors from (M.A.Harris, K. Patten and E. Regan 2013) were adopted. To measure the degree of resources required and control mechanism, items were adopted from (A. B.Gabra et al, 2015). The reliability of the factors considered was evaluated using Cronbach's α which was 0.87 for all the 16 items and showed there was internal consistency. Cronbach, L.J. (1951) the response were collected using five point Likert type scale.

Data Analysis and Hypothesis testing

TABLE I
Demographic details of sample

Criteria	*Detail*	*Value*
Gender	Male	113 (68 percent)
	Female	53 (32 percent)
Age	Mean	44.5 years
Tenure in the company	Mean	8.4 years
Business type	Product	19 companies (11 percent)
	Service	46 companies (28 percent)
	Process	101companies (61 percent)
Size of company	Mean	12.7 years

TABLE II
Correlation and Standard deviation of data

Variable	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Compliant to policy									
1 Influence on behaviour	0.21**	1							
2 Increase in resources	0.33**	0.29**	1						
3 Increase in responsibility	0.47**	0.18**	0.23**	1					
4 Influence on employees	0.47**	0.16**	0.47**	0.27**	1				
5 Law of the Land	0.32**	0.26**	0.41**	0.57**	0.24**	1			
Training and Awareness									
6 Training for compliance	0.58**	0.13**	0.50**	0.39**	0.54**	0.49**	1		
7 Enforcement of policy		0.41**	0.27**	0.49**	0.61**	0.37**	0.54**	0.61**	1
Application Vulnerability									
8 Platform Management risk	0.29**	0.41**	0.15**	0.32**	0.44**	0.67**	0.51**	0.37**	1
Mean	3.1	3.9	4.6	4.1	3.5	2.4	3.8	3.9	2.5
Standard deviation	0.6	1.2	1.3	1.7	1.6	1.7	1.5	1.8	1.3
N = 166									

** Correlation is significant at 0.01 level (2 tailed)

TABLE III
One Way ANOVA

Variable	*F value*	*Significance*
Compliant to policy		
1 Influence on behaviour	8.9**	0.000
2 Increase in resources	12.4**	0.000
3 Increase in responsibility	27**	0.000
4 Influence on employees	18**	0.001
5 Law of the Land	4.6**	0.000
Training and Awareness		
6 Training for compliance	12**	0.002
7 Enforcement of policy	22.6**	0.001
Application Vulnerability		
8 Platform Management risk	31.6**	0.000

N = 166
** Significant at 0.01 level (2 tailed)

RESULTS

It is evident from table II that the correlation between the degrees of control desired and the compliance to the IT policy is significant. This also suggests that organisations need to have greater control on drafting of the policy and also

TABLE IV
t Test

Hypothesis	*Variable*	*Means (μ)*		*Strong Control*			*Moderate Control*		
		Strong	*Moderate*	*Mean*	*t*	*Sig*	*Mean*	*t*	*Sig*
		Control	*Control*	*difference*			*difference*		
H1	Compliant to policy								
H1-1	1 Influence on behaviour	5.69	5.36	1.44**	3.67	0.00	1.59**	3.91	0.00
H1-2	2 Increase in resources	5.61	4.11	1.78**	7.01	0.00	1.80**	6.10	0.00
H1-3	3 Increase in responsibility	5.03	5.62	1.17**	5.84	0.00	0.90**	2.43	0.00
H1-4	4 Influence on employees	5.75	5.14	1.79**	4.11	0.00	1.09**	1.22	0.00
H1-5	5 Law of the Land	4.44	4.45	1.43**	4.06	0.00	1.27**	1.46	0.00
H2	Training and Awareness								
H2-1	6 Training for compliance	5.89	3.53	1.24**	6.33	0.00	1.19**	2.14	0.00
H2-2	7 Enforcement of policy	3.66	3.45	1.29**	4.89	0.00	0.74*	4.22	0.00
H3	Application Vulnerability								
	8 Platform Management risk	5.49	5.44	2.45**	2.47	0.00	0.33**	2.11	0.00

N = 166
* Significant at 0.05 level (2 tailed)
** Significant at 0.01 level (2 tailed)

implementation. The policy should not be agile and rolled out just because the employees want this policy to be implemented.

The output of one way ANOVA in table III shows that there was significant in the *F*-test. This significance made us to accept the hypotheses which had equal group means for a sample size of 166.

Further table IV showed that the evidence supported Hypothesis H1-1. No significant difference was observed in means between the organisations having strong and moderate control. However organisations having a strong control tend to have greater negative influence on the behaviour of its employees since the mean of strong control is higher. It implies that organisations imposing a greater control on data security policy compliance will have a negative impact on perception of employees. Employees many not be comfortable in using multi step user authentication for logging into the device especially while they are accessing social networking sites, alpha numeric passwords, or fingerprint scanners.

Hypothesis H1-2 is supported in table IV. There was significant difference observed in means between the organisations having strong and moderate control. However it suggests that organisations that need to have strong control on the security policy have to invest on more resources to keep pace with the updates and technical controls. Organisations need to access the data on each device and compartmentalise for better security controls which needs additional resources.

Hypothesis H1-3 is supported. There was no significant difference observed in means between the organisations having strong and moderate control. However mean of moderate control is slightly higher than the mean of strong control. It implies that with moderate control organisations can impose responsibility for any loss of data or device on the employees. With moderate control and by inserting clause like attaching liability

to the employees in the policy would bring in a sense of responsibility in the employee to secure the data and the device.

Hypothesis H1-4 is supported. There was no significant difference observed in means between the organisations having strong and moderate control. However mean of strong control is higher than the mean of moderate control. It implies that organisations need to use binding clause in the security policies to have an influence on the employees. Use of words like restricted, compulsory, unauthorised, intended creates a sense of binding on part of the employees which makes the IT Governance policy robust.

Hypothesis H1-5 is supported. There was no significant difference observed in means between the organisations having strong and moderate control. However mean of strong control is almost same as the mean of moderate control. It implies that irrespective of the controls organisations must comply with the best security practice and law of the land. It supports the proposition security policy that is in compliance with the law of the land and best industry practices reduce the risk of data and device vulnerability

The results from table IV support Hypothesis H2-1 and H2-2. For H2-1, there was significant difference observed in means between the organisations having strong and moderate control. The mean for strong control was significantly higher than moderate controls. It implies that organisations should have a strong control in identifying the training requirements and it eventually has a positive impact on the compliance. Hence the hypothesis training on policy and practice updates significantly improves compliance to the policy is supported.

Hypothesis H2-2 is supported. There was no significant difference observed in means between the organisations having strong and moderate control. However mean of strong control is almost same as the mean of moderate control. It implies that irrespective of the controls organisations must impose strict enforcement of security policy for having positive impact on compliance and reduction in data vulnerability

TABLE V
Hypothesis support result summary

Hypothesis	*Variable*	*Supported?*
H1	Greater the control measures to avoid security breach make the employees more compliant to the IT governance policy.	Yes
H1-1	Increase in security controls has a negative impact on the behaviour and satisfaction of the device user.	Yes
H1-2	Enhanced data security controls require increase in resources at the organisational level	Yes
H1-3	Imposing more responsibility on the employee will make them more compliant towards the IT security policy	Yes
H1-4	Using binding clause in the IT Governance policy will influence the user-friendly behaviour of the employees	Yes
H1-5	Security policy that is in compliance with the law of the land and best industry practices reduce the risk of data and device vulnerability	Yes
H2	Increase in training and awareness of the employees has a positive impact on the reduction of risk of data and device vulnerability	Yes
H2-1	Training on policy and practice updates significantly improves compliance to the policy	Yes
H2-2	Strict enforcement of security policy has a positive impact on compliance and reduction in data vulnerability	Yes
H3	Adoption of BYOD will increase the inventory and platform management risk and increase in threat of malware application vulnerability	Yes

Hypothesis H3 is supported. There was no significant difference observed in means between the organisations having strong and moderate control. However mean of strong control is almost same as the mean of moderate control. It implies that irrespective of the controls organisations have to increase surveillance of malware and Trojan concern by increasing its support management activities.

Discussion, Implications and Research Synthesis

This study shows how organisations should exercise control while framing an IT Governance policy. With the growing threat of malware and Trojans organisations must review the degree of capability of their policies. Organisations should develop a policy that is inclusive and exhaustive and encompass all possible areas of practice.

Our study also showed that organisations have to educate its employees on technical and security controls. Organisations should attempt to protect user-friendly interests of its employees and at the same time balance the law of the land data protection act and best industry practices. The research also highlighted that employees may be sceptical and try to bypass the controls when they are aware of the fact that organisations has the right to access and wipe the data on their systems without their consent remotely.

The findings from this research might have implications on organisations that implement BYOD without considering the potential liability it is exposed to and are very informal at adopting the policy. This has further implications on developing policy controls that is a up-to-date with governance roadmap to cater and counter potential and emerging threats and application.

Conclusions and Limitations

Employees are becoming increasingly demanding for using same device for dual purpose of personal and business needs. The demarcation between work and personal life is getting faded and BYOD is influencing the work life balance. (Jamie Pinchot, Karen Paullet, 2015)

Organisations should not adopt BYOD as a policy just because employees demand for it. (James Scott Magruder et al 2015). If done without frequent reviewing its security policy it may potentially lead to serious security breach and liabilities. (Abubakar Bello Garba et al. 2015). Organisations should educate its employees with any updates and potential risk of malware.

The findings suggested that organisations need to have a constant surveillance and legitimate review of security inventory controls, implement employee awareness programs following policy iteration. Stringent compliance and substitutive procedures reduces application vulnerability.

The limitation of this study is that it was geographically restricted to IT companies in Singapore and the sample size was not big, however it was in a testable range. The study can be extended to companies beyond IT sector and different locations.

REFERENCES

A. B. Garba, J. Armarego, and D. Murray,(2015) "Bring your own device organizational information security and privacy," ARPN Journal of Engineering and Applied Sciences, vol. 10, pp. 1279-1287.

A. B. Garba, Jocelyn Armarego, David Murray (2015) A Policy-Based Framework for Managing Information Security and Privacy Risks in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 4, Issue 2, March-April 2015.

A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, (2015) "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments," Journal of Information Privacy and Security, vol. 11, pp. 38-54.

AirWatch. (2012). Enabling bring your own devices (BYOD) in the enterprise. Retrieved from http://www.ciosummits.com/ media/solution_spotlight/byod-whitepaper.pdf

Calder, (2013), 'Is the BYOD Movement Worth the Risks?' Credit Control, vol. 34 Issue 3, p65-70.

Citrix. (2013). Best practices to make BYOD simple and secure (White paper). Retrieved from http://www.citrix.com/ content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf

Cisco (2012), Survey Report: "BYOD: A Global Perspective Harnessing Employee-Led Innovation", CISCO IBSG. Retrived from http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf

Cronbach, L.J. (1951), "Coefficient alpha and the internal structure tests", Psychometrika, Vol. 16 No. 3, pp. 297-334.

Deshmukh, R., & Wadhe, A. (2012). Mobile security: Why to secure your mobile devices? International Journal of Advances in Engineering & Technology, III (IV), 72-74

Dilger, D.E. (2013), Mobile malware exploding, but only for Android, Retrived from https://twitter.com/danieleran.

Forrester. (2012). Key strategies to capture and measure the value of consumerization of IT. Cambridge, MA: Forrester Consulting. Retrieved from http://www.trendmicro.com/cloud-content/us/ pdfs/business/white-papers/wp_forrester_measure-value-ofconsumerization.pdf.

Garlati, C. (2011). Trend Micro consumerization report 2011. Retrieved on Dec 28, 2015 Retrieved from http://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byodpolicy.htmlhttp://bringyourownit.com/2011/09/26/trend-micro-consumerization-report-2011/

D. Rivera, G. George, P. Peter, S. Muralidharan, and S. Khanum, (2013) "Analysis of Security Controls for BYOD, (Bring your own Device)," The University of Melbourne, Melbourne, 2013

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. Procedia Technology, 9, 43-53. doi:10.1016/j.protcy 2013.12.005

James Scott Magruder, Stanley X. Lewis, Eddy J. Burks, Carl Smolinski, (2015) Bring Your Own Device (BYOD)—Who Is Running Organizations? Retrieved from Journal of Accounting and Finance Vol. 15(1) 2015

Jamie Pinchot, Karen Paullet (2015) Bring your own device to work: Benefits, Security risks, and governance issues - Issues in Information Systems, Volume 16, Issue III, pp. 238-244.

K. W. Miller, J. Voas, and G. F. Hurlburt, (2012), "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, pp. 53-55, 2012.

M. A. Harris, K. Patten, and E. Regan, (2013), "The need for byod mobile device security awareness and training," in Americas Conference on Information Systems, Chicago, 2013.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. Network Security, 2012, 5-8. doi:10.1016/S1353-4858(12)70111-3

M. E. Whitman and H. J. Mattord - Principles of information security. (2010) Boston USA: Cengage Learning, 2010.

Paullet, K., & Pinchot, J. (2014). Mobile malware: Coming to a smart phone near you? Issues in Information Systems, 15(2), 116-123.

Potts, M. 2012, The state of Information Security,2012, 7, July 2012, Pages 9–11

Singh, N. (2012). B.Y.O.D. genie is out of the bottle – "Devil or angel". Journal of Business Management & Social Sciences Research, 1(3), 1-12

Tech crunch (2015) http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/#.zocdo8u:RPIH

Ten-Steps-To-Secure-BYOD, www.cadincweb.com / wp- content /uploads/2012/04 /CAD _BRAD _Ten_Steps_to_Secure_BYOD.

Tzoumas, C. 2013, The BYOD World. Retrived from Business West, 30, 45.

Vickerman, J. (2013). Bring your own device to work. Risk Management, 38-41.

Wood, A. (2012), 'BYOD: The Pros and Cons for End Users and the Business', Credit Control, vol. 33 Issue 7/8, p68-70.