BYOD: A Security Policy Evaluation Model

30

Melva M. Ratchford

Abstract

The rapid increase of personal mobile devices (mainly smartphones and tablets) accessing corporate data has created a phenomenon commonly known as Bring Your Own Device (BYOD). Companies that allow the use of BYODs need to be aware of the risks of exposing their business to inadvertent data leakage or malicious intent posed by inside or outside threats. The adoption of BYOD policies mitigates these types of risks. However, many companies have weak policies, and the problem of exposure of corporate data persists. This paper addresses this problem by proposing a BYOD policy evaluation method to help companies to strengthen their BYOD policies.

This initial research proposes a novel BYOD security policy evaluation model that aims to identify weaknesses in BYOD policies using mathematical comparisons. The results are measurable and provide specific recommendations to strengthen a BYOD policy. Further research is needed in order to demonstrate the viability and effectiveness of this model.

Keywords

BYOD • Policy Evaluation • Evaluation Model • Risk • Security

30.1 Introduction

With the rapid increase of personal mobile devices accessing corporate data (a phenomenon called BYOD – Bring Your Own Device), companies need to be aware of the importance of maintaining corporate data protection in order to ensure the confidentiality, integrity, availability (CIA) of its data [1]. In 2012, a survey conducted by Cisco reported that 95% of the organizations polled permitted the use of employee-owned devices in the workplace [2]. In 2013, another study by Cisco indicated that 9 in 10 Americans used their smartphones for work, where 40% do not password protect them, and 51% connect to unsecured wireless networks using their smartphones [3]. The Gartner Group also predicted that by 2017 half of all companies will actually require employees to use their own mobile device for work [4].

New security risks are introduced with the use of BYODs to include devices easily tampered, lack of security awareness among users, threats and attacks (e.g. spoofing, phishing, data leakage, sniffing, spam, denial-of-service) [5]. BYODs are consumer devices that lack the strict compliance requirements of devices accessing corporate-sensitive data [6]. Security policies are less likely to be enforced in devices the company does not own [7]. Today's workforce expect to be able to access work-related information via their BYOD, and it is up to the company to protect its network and data [8]. A BYOD security policy needs to be in place and enforced. 'A system can be considered secure and trustworthy if the policy enforced by its security administrator is trustworthy too' [9]. However, many companies do not have a BYOD security policy in place, or their policy is weak, lacking technical or organizational considerations, or enforcement mechanisms. This is a problem because their

M.M. Ratchford (✉)
Dakota State University, Madison, SA, USA
e-mail: melva.ratchford@trojans.dsu.edu

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 558, DOI 10.1007/978-3-319-54978-1_30

corporate data may be exposed to inadvertent data leakage or users with malicious intent (inside/outside threats). Therefore, a company's BYOD security policy should to be evaluated in order to identify the weak strategies that the policy makers can modify and enforce. 'It is possible to evaluate the system security by evaluating its policy' [9].

Current policy evaluation methods involve human intervention to analyze or parse policies written in a natural language (e.g. English) where comparisons are made against published guidelines. This process can produce ambiguous results based on subjective analysis (i.e. the opinion of an individual).

Using design science research methodology, this paper proposes a novel method to evaluate BYOD security policies. The model utilizes an evaluation process based on mathematical analysis that produces quantifiable measurements to provide security levels, identify weak strategies, and provide recommendations. With this information, the company can be in a better position to strengthen the security of its corporate data and mitigate the risks introduced when adopting BYODs.

The organization of the paper is as follows: after this introduction, Sect. 30.2 identifies the literature review, the research gap found in the literature, the requirements needed to fill the gap, and the supporting theories & literature needed to meet the requirements. Section 30.3 presents an overview of the model design. Section 30.4 describes a suitable context to demonstrate the model followed by an evaluation of the problem resolution. Section 30.5 concludes and states future work.

30.2 Literature Review and Underlying Theories

Prior literature provide valuable information in regards to understanding the BYOD paradigm [5, 6, 10, 11]. Several National Institute of Standard and Technology (NIST)'s publications provide further recommendations and guidelines in order to create awareness regarding risks and vulnerabilities to corporate data when BYODs are permitted [1, 12, 13]. However, the literature research finds a gap for a specific and non-ambiguous process to evaluate a company's BYOD security policy.

In order to fill this gap, the following requirements need to be researched and understood:

1. Risks and vulnerabilities associated with BYODs.
2. Methodologies for building security policies.
3. Non-ambiguous evaluating process for policies.

30.2.1 Risks and Vulnerabilities Associated with BYODs

The first requirement (risks and vulnerabilities associated with the adoption of BYODs) involves a thorough understanding of the risks and vulnerabilities introduced to a company when BYODs are allowed. For this purpose, the frameworks proposed by Vorakulpipat et al. [10] and the specific recommendations provided by recognized authorities such as NIST provide the foundation for building a baseline for technical and organizational considerations when mobile devices are allowed. The NIST's 800 publications include the 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise [1], 800-114 User's Guide to Telework and Bring Your Own Device (BYOD) Security [12], and 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device [13]. Main categories such as architecture, authentication, access control, cryptography/encryption, device provisioning, configuration, application requirements, security policy enforcements, auditing, training, and technical support can be expanded to include risks and vulnerabilities at a granular level.

30.2.2 Methodologies for Building Security Policies

The second requirement, (methodologies for building security policies), requires the understanding and developing of a process whereby the BYOD-related risks and vulnerabilities identified above can be addressed in a form of a security policy. Known methodologies for building security policies include McCumber's Cube [14], Peltier's basic concepts for Topic-Specific Policy [15], and Wood's framework for building security policies using the concept of a 'coverage matrix' [16].

The McCumber's Cube methodology is suitable for building a BYOD policy because it ensures that the CIA (Confidentiality, Integrity and Availability) of data is addressed. The data need to be protected while is being transmitted, at rest, and during processing. The security measures to protect the data during its various states need to include the use of technology, creation of policies and the development of training/awareness programs.

Peltier's Topic Specific Policy describes basic components that narrow the topic to one issue [15], making this method appropriate when considering BYOD policy analysis. The policy needs to have thesis statement with clearly identified objectives; it needs to be relevant by

specifying to whom/where/how/when does the policy apply; identify roles and responsibilities by position/job/title/job-function; specify terms of compliance to include unacceptable behavior, its consequences and monitoring of compliance; and include additional information providing specific contact information and policy location [15].

In addition, Wood's methodology for writing information security policies describes a coverage matrix [16] that can be further expanded to map the individual provisions (i.e. security requirements) into a data (tree) structure where the main nodes, sub-nodes, and end-nodes delineate the individual policy elements at its most granular levels.

30.2.3 Non-ambiguous Evaluating Process for Policies

The third requirement (a security policy evaluating process), requires the development of a method whereby an ambiguous evaluation process (i.e. based on natural language analyses) becomes a non-ambiguous evaluation method based on mathematical analyses with quantifiable results. This can be achieved using a model proposed by Casola et al. [9]. Their evaluation process consists of a series of algorithms that convert a natural language of a written policy into a binary matrix. It then applies the Euclidean algorithm to calculate the distance between matrices to identify the differences between two security policies (quantifiable data) [9].

The combination of the above underlying theories are used to build the evaluation model proposed in this research.

30.3 Overview of Model Design

The model proposed in this paper, as shown in Fig. 30.1 below, describes a process via which a company's BYOD policy is evaluated against a set of security standards (referred as a reference policy). The evaluation process is a comparison that identifies the differences between the company's BYOD policy and the reference policy. The results of this comparison are non-ambiguous and measurable. The main components of this model are 1) the reference policy and 2) the evaluation process.

30.3.1 The Reference Policy

The natural language of a reference policy proposed in this paper, is built using known and established principles and methodologies defined by the McCumber's Cube methodology, Peltier's Topic-Specific Policy basic concepts, Wood's coverage matrix, and the NIST's recommendations for data

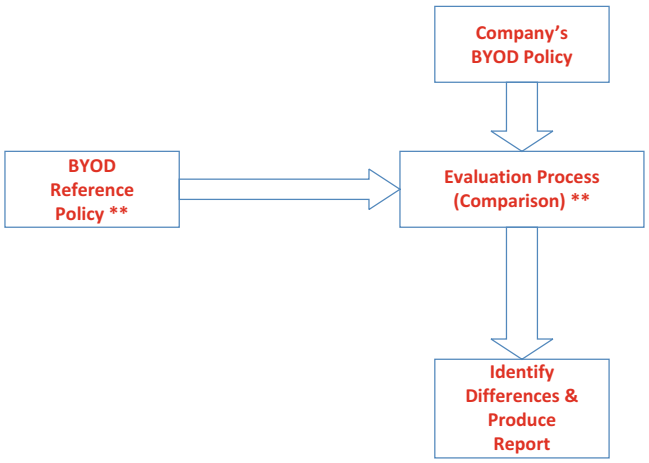

Fig. 30.1 High Level Model

protection when using BYODs. For example, McCumber's Cube methodology is used to ensure that the CIA of data is addressed for each security attribute. For example, data confidentiality during transmission needs to specify measures that include the use of technology (e.g. encryption/VPNs), policy specifics, and human factors that address the need for training/awareness.

Peltier's basic components (as explained in Sect. 2.2) are also included in the construction of the natural language of the reference policy. Then, Wood's coverage matrix is used to organize/format the policy to prepare for the series of transformations required during the policy evaluation process.

30.3.2 The Policy Evaluation Process

The BYOD policy evaluation process presented in this model uses a series of algorithms proposed by Casola et al. [9]. This method performs a number of transformations to convert a natural language of written policy into a binary matrix. It then applies the Euclidean algorithm to calculate the distance between the matrices to identify the differences between two security policies (quantifiable data). In this proposed model, Figs. 30.2, 30.3 and 30.4, show an example comparison between the BYOD reference policy and a company's BYOD policy. These figures show the end-result of this transformation process. The description of the transformation steps themselves (and the weights assigned) are outside the scope of this paper. The examples show the binary matrices created for the reference policy and the policy being evaluated. In this example, matrix R (Fig. 30.2) represents the reference policy, and matrix C (Fig. 30.3) represents a company's policy. The resulting matrix in Fig. 30.4 (after applying the Euclidean algorithm) shows a number value representing the distance between the two matrices.

1. Let R be the matrix that represents the reference policy

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
1	1	1	1
1	1	1	0
1	1	1	1
0	0	0	0
1	1	0	0
1	1	0	0

Fig. 30.2 Example binary representation of a reference policy

2. Let C be the matrix that represents the company's policy

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
1	1	1	0
0	0	0	0
1	1	1	0
0	0	0	0
1	0	0	0
1	0	0	0

Fig. 30.3 Example binary representation of a company's policy

Fig. 30.4 Example Euclidean's distance between matrices

Multiply (R-C)x[(R-C)^T] to find the Trace

0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	0	0	0	1	1	0	0	0
0	0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	1	1
0	0	0	0	0	0	0	1	0	0	1	1

So Trace is = Tr(R-C)(R-C)^T)= 1+3+1+1+1 =7

The smaller the value the closest the policies are to each other, indicating that the policy being evaluated is a strong BYOD policy. Likewise, if the distance is represented by a higher value, it indicates the policy being evaluated is weak. In the same manner, each policy provision can be calculated in order to identify the specific weaknesses and thus provide specific recommendations for the weak provisions.

In addition, a visual representation of each policy provision can be provided using a Kiviat's diagram. In Fig. 30.5, one can visually see the weak/strong provisions of a company's policy as they compare to the reference policy. In this example, policy R represents the reference policy and policy C represents the company's policy being evaluated. Each policy provision (Kn) represents an item of the policy (e.g. provide confidentiality via encryption/VPN, etc). This Kiviat's diagram example shows that the policy being evaluated lacks strength in almost all its policy provisions.

Figure 30.6 below shows the high level model and added steps to reflect more detail. The blue boxes represent the incorporation of the steps for 1) building the reference policy, 2) the steps that involve the transformation from natural language to binary matrix, and 3) the final step of policy comparison (matrix distance calculation) where the results are produced. The creation and transformation of the reference policy is a one-time process. The repetitive process is the evaluation of a company's policy.

30.4 Model Demonstration and Evaluation

30.4.1 Artifact Demonstration

The model can be demonstrated in a case study that uses the natural language of an existing BYOD policy where the process is applied manually.

30.4.2 Artifact Evaluation

Measuring the success or failure of the model can be determined based on the answers to the following questions:

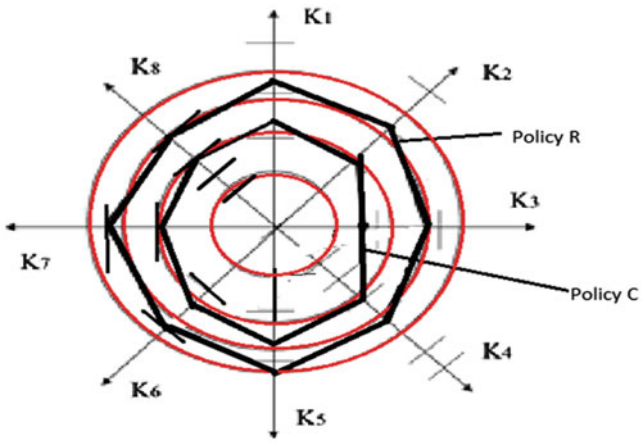

Fig. 30.5 Example Kiviat's representation of a policy comparison

Can this policy evaluation method identify the BYOD risks the company is not addressing in its policy?
Can the level of data exposure be effectively measured?
Does the company find the results of this evaluation useful and clear so that they can implement the necessary changes to their BYOD policy?
Is a reference policy based on the McCumber Cube/Peltier/NIST methodology suitable to create a generic/reference BYOD policy?
Is the reference policy a 'generic' and robust policy to use as an acceptable standard to measure BYOD policies for all size companies of multiple sectors?
Is it feasible/possible to automate the steps proposed by this model?

30.5 Conclusion and Future Work

30.5.1 Conclusion

Corporations need to address the vulnerabilities and security risks introduced when BYODs are allowed. In order to maintain control and mitigate the risks of data leakage/exposure there is a need to have a BYOD security policy in place. However, the policy may be weak. Therefore, an evaluation method that produces measurable results may provide the company with valuable information to strengthen their

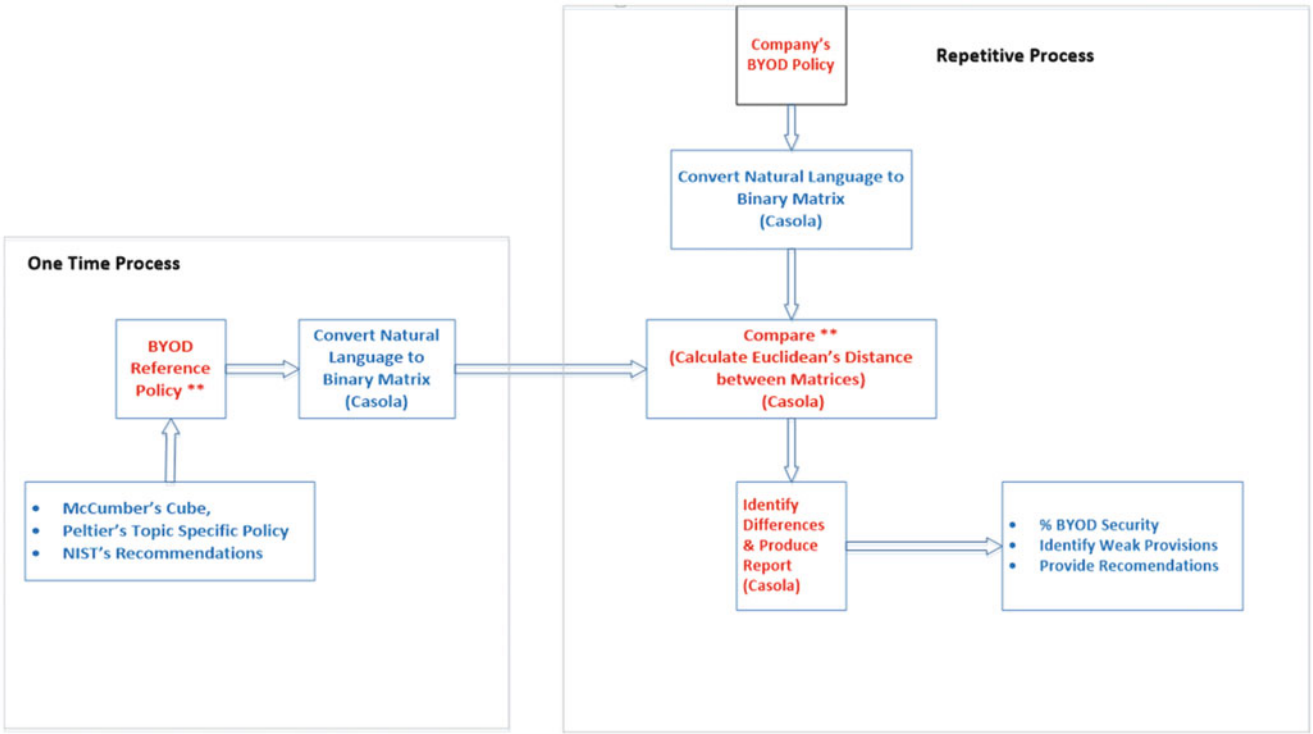

Fig. 30.6 Detailed model

policy hence strengthening the security of its corporate data when BYODs are allowed.

Current literature only provide guidelines to build BYOD policies. Current policy evaluation methods involve human intervention to analyze or parse policies written in a natural language (e.g. English) where comparisons are made against published guidelines. This process can produce ambiguous results based on subjective analysis (i.e. the opinion of an individual). This paper proposes a novel method to evaluate BYOD security policies. The process utilizes an evaluation process based on mathematical analysis that produces quantifiable measurements, security levels and identification of weak strategies.

Using design science research methodology, this work aims to find out if an evaluation model based on a BYOD reference policy built upon established theories such as McCumber Cube methodology, Peltier's basic concepts, and the NIST guidelines for BYOD security coupled with an evaluation process (such as the one presented by Casola) can be used to successfully evaluate a company's BYOD policy.

30.5.2 Future Work

The analysis and description presented thus far represent an initial work into this research. Extensive work is needed in order to build a BYOD reference policy that defines a wide-range of security rules for the reference policy for each main provision/requirement of the natural language of a policy while applying policy concepts based on McCumber's Cube, Peltier and Wood.

At the time of this writing, the intention of this research is to build a 'generic' (but comprehensive) BYOD policy evaluation model independent of the type of organization. However, it is possible to tailor the policy evaluation process by modifying the reference policy in order to meet an industry-specific security requirement(s).

If the model works successfully/effectively, it may be desirable to explore the possibility of automating certain steps of the model by using tools suitable for parsing text, matrix analysis and computation.

References

1. Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise NIST Special Publication 800-124 Revision 1.
2. Cisco's Technology News Site. (2012). *Cisco study: IT saying yes to BYOD*. Retrieved September 19 from https://newsroom.cisco.com/press-release-content?articleId=854754
3. BYOD Insights. (2013). *A cisco partner network study, report*. Retrieved September 2016 from http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&SWTHEMEID=12949
4. Gartner. *Gartner predicts by 2017, half of employers will require employees to supply their own device for work purposes*. Retrieved August 31, 2016 from http://www.gartner.com/newsroom/id/2466615
5. Wang, Y., Wei, J., & Vangury, K. (2014). *Bring your own device security issues and challenges*. Consumer Communications and Networking Conference (CCNC), 2014 I.E. 11th, pp. 80–85.
6. Holleran, J. (2014). Building a better BYOD strategy. *Risk Management, 61*, 12–13.
7. Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional, 14*, 53–55.
8. Thompson, G. (2012). BYOD: Enabling the chaos. *Network Security, 2012*, 5.
9. Casola, V., Mazzeo, A., Maxxocca, N., & Vittorini, V. (2007). A policy-based methodology for security evaluation: A security metric for public key infrastructures. *Journal of Computer Security, 15*, 197–229.
10. Vorakulpipat, C., Polprasert, C., & Siwamogsatham, S. (2014). *Managing mobile device security in critical infrastructure sectors. Proceedings of the 7th international conference on Security of Information and Networks*, p. 65.
11. Kumar, R., & Singh, H. (2015). A proactive procedure to mitigate the BYOD risks on the security of an information system. *SIGSOFT Software Engineering Notes, 40*, 1–4.
12. Souppaya, M., & Scarfone K. (2016). *NIST 800-114 Rev 1 user's guide to Telework and Bring Your Own Device (BYOD) security*. Retrieved from http://csrc.nist.gov/publications/drafts/800-114r1/sp800_114r1_draft.pdf
13. Souppaya, M., & Scarfone, K. (2016). *NIST 800-46 Rev 2 guide to enterprise telework, remote access, and Bring Your Own Device (BYOD) security*. Retrieved from http://csrc.nist.gov/publications/drafts/800-46r2/sp800_46r2_draft.pdf
14. McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*. CRC Press. Boca Raton.
15. Peltier, T. R. (2016). *Information security policies,procedures, and standards: Guidelines for effective information security management*. Chicago: CRC Press.
16. Wood, C. C. (1995). Writing infosec policies. *Computers & Security, 14*, 667–674.