Chapter 8

Optimized Three-Dimensional Security Framework to Mitigate Risks Arising From BYOD-Enabled Business Environment

Lizzy Oluwatoyin Ofusori  
University of KwaZulu-Natal, South Africa

Ncamiso Nkululeko Jahalenkhosi Dlamini  
University of KwaZulu-Natal, South Africa

Prabhakar Rontala Subramaniam  
University of KwaZulu-Natal, South Africa

ABSTRACT

Bring your own device (BYOD) has infiltrated the work environment and businesses are enjoying the benefits coupled with the adoption of the trend. At the same time, the adoption of BYOD has introduced a number of security threats that businesses are failing to match. In the pursuit of addressing security threats that are introduced by the adoption of this technology trend, this chapter recommends a three-dimensional (3-D) security framework that can be used to mitigate the risks emanating from a BYOD enabled environment. Data was collected from the employees of two banks in Africa that supported BYOD trend to measure individual and organizational practices. This chapter investigates further on these practices in addressing implications of BYOD. Three categories of security threats are delineated in this chapter. A review of existing security frameworks is presented in this chapter. The chapter concludes by outlining a 3-D security framework as a potential solution to protect BYOD enabled business environment.

DOI: 10.4018/978-1-5225-4763-1.ch008
INTRODUCTION AND BACKGROUND

Mobile technologies are increasingly becoming a preferred way of communication as a result of the evolution of the fourth Industrial revolution (Niesen, Houy, Fettke, & Loos, 2016). Most manufacturing organizations continuously evolve into smart and interconnected production systems. As mobile devices are becoming more dependable, they are also becoming prevalent in workplaces (Astani, Ready, & Tesemma, 2013). This pervasiveness has enabled Bring Your Own Device (BYOD) in most organizations. BYOD is a growing trend that allows individuals of an organization to bring their own devices such as smartphones, laptops and tablets to work. This interconnectivity of smart devices has resulted in massive amounts of data from individuals, organizations and society (Niesen et al., 2016). Hence, the likelihoods of millions of people connected by mobile devices, with unprecedented storage capacity, processing power and access to knowledge, are unlimited. This data from individuals results in lack of privacy, data from organizations leads to lack of integrity while data from society leads to security issues. Presently, the number of mobile devices connected to the internet is more than the population of the world. This margin will keep expanding and thus create an avenue for cyber-attack in large scale.

The effect of allowing individuals to access any network with their mobile devices has impacts on network access, network control, helpdesk resources and even information ownership (Astani et al., 2013). Similarly, protection of organizational data becomes a challenge because these personal gadgets are mobile, hence employee are able to carry company data wherever they go. Some other security challenges such as keeping the network malware-free, understanding who and what is on the network, lack of control over the amount of information that should be stored at the endpoint on a BYOD device and giving the appropriate access policies to enforce compliance and audit requirements were identified by Astani et al. (2013). As technological development continues to grow, the threat to individual, organizations and society also increases (Lee, 2015). The major concern is how the connectivity can be harnessed for productive use without affecting privacy, security and integrity.

This chapter provides an overview of the BYOD trend and some key attributes that led to BYOD becoming a business standard. This chapter further presents the security threats and legal issues that confront organizations together with current practices that have been adopted to cushion against these threats. A framework is proposed to illustrate the distinction amongst threats that continuously affect businesses and the society at large through embracing the BYOD trend. A discussion explaining the difference between threats emanating from BYOD adoption and the Cyberspace is provided. Thus, the chapter proposes a 3-D BYOD security framework that can be used to prioritize awareness in order to ensure data integrity is maintained by all means.

In order to measure the BYOD security threats, some data were collected from the banking sectors in the African continent: Nigeria and Swaziland. These two countries are considered from two different extremes: Nigeria is one of the countries where the use of technology is accepted and is being used by the population at large. There are policies and a regulatory framework that have been incorporated to support the use of technology (Umar, 2015). On the other hand, Swaziland is one of the economically under developed countries in the continent. At present, there are no policies that have been implemented that specifically regulate the use of personal gadgets in the work environment. Swaziland has inadequate policy and regulatory frameworks; consequently, the integration of information and communication technologies (ICT) is currently uncoordinated and uncontrollable regardless of the current initiatives (Madzima, Dube, & Mashwama, 2013). As a result, there is lack of adequate planning, technical sup-