MBA DISSERTATION LENGTH SAMPLE

Biometrics – Advantages and Disadvantages

Abstract

Every organization, regardless of size, come with their own set of goals. As such, they work hard in order to acquire assets in order to make sure that all of their goals are met and guaranteed continuity and consistency. The financial sector tries to promote some convenient and easy-to-perform methods such as the use of ATM and online banking for their customers in order for them to access their money. While doing so, they keep in mind the need to make sure that only an authorized person is given access to the account. At the same time, national security and military services store highly critical and sensitive information which should only be accessed by particular individuals, thus deploying different security measures in order to retain this tradition. However, attaining these goals depends largely on controlling and securing the assets which have been documented. This only means that authorized individuals are given access to these assets.

Introduction

Different organizations try their best to secure their assets, providing means to control access given towards their assets. This process needs authorization and identification in order to make sure that the right person is gaining access to the right asset. Throughout the years, traditional authentication methods, primarily the use of Personal Identification Numbers (PINs) and passwords have been used popularly. Recently, though, PINs and swipe card access have been used for more security. However, these methods come with their own vulnerabilities. For one, swipe cards may be stolen. Bad password management often leaves people writing their PINs on papers, leaving them on desks, exposing them to trouble.

Biometric Technology uses a person's behavioral and physiological characteristics for identification. Each human being is highly unique by nature, possessing physical parts which are different from one another. For example, the 9/11 terrorist attach did not help in terms of security concerns since organizations and governments all over the world, particularly the border security agencies, have embraced this type of technology using human recognition (Law & Singh, 2005). As both public and private entities continue to look for a more dependable authentication and identification method. With this said, biometrics has been an ideal choice for future use among organizations.

Biometrics – What is It?

Biometrics is defined as the automatic recognition of a person according to his or physiological or behavioral characteristics. (Chyrsler & Blain, 2009). It is a method of authorization which identifies or verifies a specific user according to what they are before giving access. The search for a more dependable method for authorization in order to secure assets has further led to the discovery of biometrics. A lot of organizations have shown their interest in using this technology.

Two particular types of biometrics have been employed – physical and behavioral. Physical biometrics uses parts of a person's body. On the other hand, behavioral biometrics refers to something that a person does (Lewel & Stanton, 2013). Even though there are certain unusual biometrics which can be used in the future, such as the unique smell of a person, ear shape, or their way of talking, the primary biometrics used include hand geometry, fingerprints, iris scan, retina scan, facial recognition or location, signature, voice recognition, gait, and keystroke pattern. However, these different types of applications need different biometrics because there is no single best form of biometric technology.

How it Works

Biometrics, so far, has been developed in order to work with two primary ways – identification and verification. Identification systems answer the question "Who are you?", not requiring users to claim a specific identity since biometric data provided is simply compared to the data coming from different users in order to find a specific match. Verification system, on the other hand, answers the question "Am I who I claim to be?" This is done by making a user claim a specific identity in order to perform a biometric comparison. The user will provide data, which is compared to the entered biometric data. It is very important for organizations to decide the specific type of biometric system to use for implementation.

References

Chrysler, H. & Blain, H. (2009). The comparison among biometric systems. Identifying the best. *Modern Security Applications Journal*, 23(1), 34-35.

Law, H. & Singh, P. (2005). Verification systems in the modern time in comparison with traditional security measures. *Business Today*, 56(1), 56-67.

Lewel, P. & Stanton, Q. (2013). Automated systems and traditional measures for authorization. *World Global Monthly*, 6(3), 90-99.

For more information on MBA dissertation length, don't hesitate to visit our website!