Chapter 8
Information Security Governance Using Biometrics

Shrikant Tiwari
IT-Banaras Hindu University, India

Sanjay Kumar Singh
IT-Banaras Hindu University, India

ABSTRACT

To establish the identity of an individual is very critical with the advancement of technology in networked society. Thus, there is need for reliable user authentication technique to solve the growing demand for high level of Information Security Governance (ISG) depending on the requirement. Biometrics can be explained as the method to recognize an individual based on physical (face, fingerprint, ear, iris, etc.) or behavioral (voice, signature, gait, etc.) features to identify an individual person. Nowadays, biometric systems are being used for different purposes for information security like commercial, defense, government, and forensic applications as a means of establishing identity and to mitigate the risk which is one of the important objectives of Information Security Governance. In this chapter, an attempt has been made to explain the use and proper selection of biometric trait to help in Information Security Governance.

INTRODUCTION

According to NIST (National Institute of Standard and Technology) Information Technology (IT) governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk. Information Security Governance consist of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages identity and risks appropriately, uses organisational resources

DOI: 10.4018/978-1-4666-2083-4.ch008

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

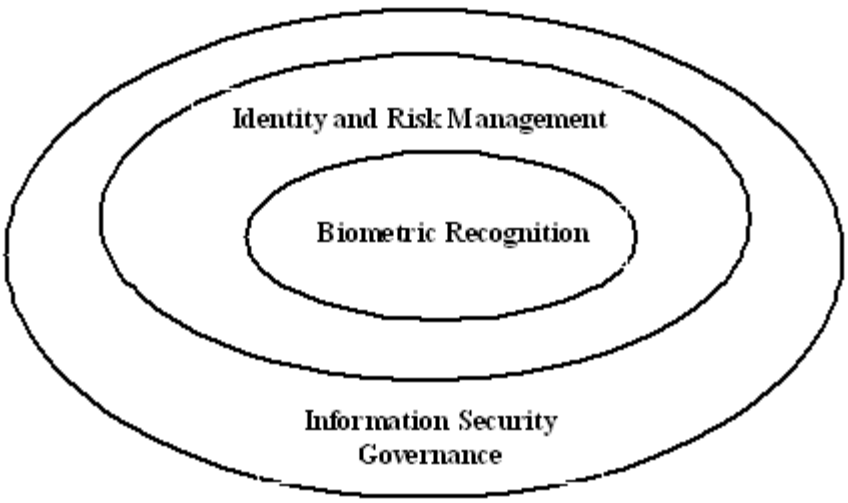
judiciously, and monitors the success or failure of the enterprise security programme.

The concern about the Identity Management (IM) which is a subset of Information Security Governance is increasing across the public and private organisations. In private organisation it is most frequently thought of in the context of identity theft. According to FDIC figures, 10 million Americans suffered identity theft in 2003 resulted with a cost to business in excess of US$50 billion and a personal impact that is difficult to estimate[1]. As large amount as this sum is, identity theft is at the core of significantly broader economic vulnerabilities and national security concerns. Thus using biometrics to develop identity theft countermeasures has direct impact on civil infrastructure protection. Authentication and identification of people are critical to eliminating threats to organization security and public safety, and securing business transactions. As technology advances and public policy debates continue over the pros and cons of personal identity programs, the identity management industry continues to grow and change. Information and the knowledge based on it have increasingly become recognised as information assets, i.e., a business-critical asset, without which most organisations would simply cease to function. It is a business enabler, requiring organisations to provide adequate protection for this vital resource.

Organizations depend heavily on Information Technology to run their daily operations and deliver products and services efficiently. With an increasing reliability on IT, a growing complexity of organization IT infrastructure, and a constantly changing information security threat and risk environment, Information Security has become a mission-essential function. In order to ensure the organization ability to do business, security must be manage and govern to mitigate the risk to organization. To support their mission organization ensure that agencies are actively implementing appropriate information security control in a cost effective manner to reduce the risk at the required level.

Information Security Governance is a subset of Information Technology Governance and both come under the purview of Corporate Governance. Information Security Governance has recently expanded so much that organisations employ a specific person to handle only Information Security issues (Von Solms, S. H., 2005) Figure 1

Figure 1. Information security governance consisting of a number of disciplines



32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/information-security-governance-using-biometrics/69420

Related Content

A Value Framework for Technology Potentials: Business Adoption of Emotion Detection Capabilities
Stefan Kochand Kemal Altinkemer (2021). *International Journal of Digital Strategy, Governance, and Business Transformation (pp. 1-13).*
www.irma-international.org/article/a-value-framework-for-technology-potentials/302636

Organizational Structure's Influence on Business-IT Alignment: Looking Back to Look Forward
Gideon Mekonnen Jonathan, Lazar Rusuand Erik Perjons (2018). *International Journal of IT/Business Alignment and Governance (pp. 15-29).*
www.irma-international.org/article/organizational-structures-influence-on-business-it-alignment/220438

Use of New Technologies in Organizational Change Process in Aprosub
Juan Antonio Gonzalez Aguilar (2014). *ICT Management in Non-Profit Organizations (pp. 180-191).*
www.irma-international.org/chapter/use-of-new-technologies-in-organizational-change-process-in-aprosub/107855

Auditing the Blockchain
Prabhat Kumar, Othniel Lambert, Sivajit Sreekumar, Mukesh Ravi Bhatiaand Akash Garg (2023). *Modernizing Enterprise IT Audit Governance and Management Practices (pp. 147-180).*
www.irma-international.org/chapter/auditing-the-blockchain/333181

Auditing Agile Release Management: Balancing Speed and Control
Nikitha Agnew, Manish Guptaand Raj Sharman (2023). *Modernizing Enterprise IT Audit Governance and Management Practices (pp. 25-67).*
www.irma-international.org/chapter/auditing-agile-release-management/333177