Biometric Standards, Performance, and Assurance Laboratory

Department of Industrial Technology
Purdue University

Evaluation of Biometric Implementers to Investigate a Viable Return On Security Investment Technique

R.C. Skinner[1], P.J. Duparcq Ph. D[2], S.J. Elliott Ph. D[3], M.J. Dark Ph. D[1]

[1] *Department of Computer Technology, School of Technology, Purdue University, West Lafayette, IN 47907*
[2] *Center for E-business Education and Research (CEER) , Krannert School of Management, Purdue University, West Lafayette, IN 47907*
[3] *Biometrics Standards, Performance, and Assurance Laboratory, Department of Industrial Technology, School of Technology, Purdue University, West Lafayette, IN 47907*

Problem

Within an enterprise-level organization's IT system, ultimately upper-level management approves of new investments and technologies that are to be deployed or tested. One of the key factors that management takes into account is what the overall effect is on the bottom line, or the return on investment. There are various techniques that organizations use to determine this factor; however the process has not been standardized. The term ROSI (Return on Security Investment) was developed a couple of years ago, with exceptional contributions from University of Idaho (using Network Intrusion Detection Systems) and Stanford, MIT, @Stake (developing Secure Software Engineering). The term did strike interest within a variety of different sources. However, the solution of an ample return on security investment is still being asked today.

There are multiple technologies that allow an organization to secure their IT system. Biometric security is one of the technologies however; it has been a hard technology to adopt based upon a variety of factors including cost to implement, lack of standards, and lack of large scale published deployments.

According to Ernst and Young's 2003 Global Information Security Survey that had responses from over 1,400 organizations, "nearly 60% or organizations say they rarely or never calculate ROI for information security spending."

Security Technique Implementations

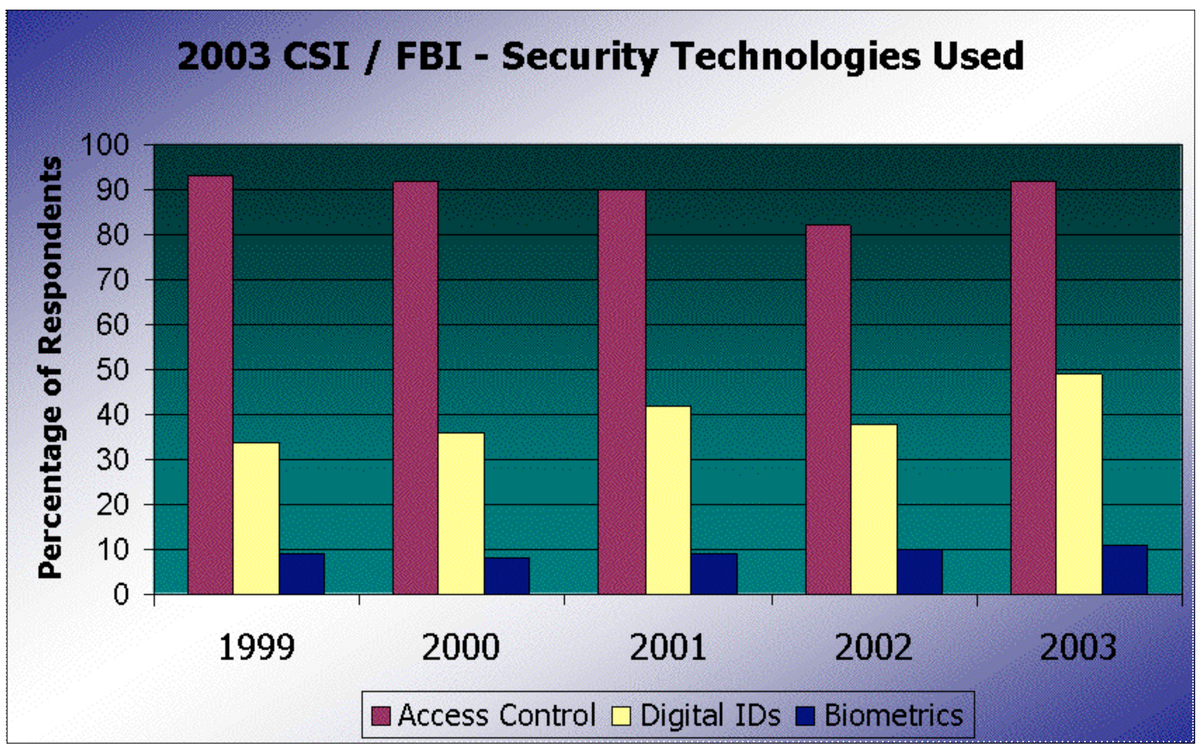

Figure 1 – Security Technologies Used 2003 CSI / FBI Computer Crime and Security Survey

According to Elliott (2004) Biometrics can be used as protective security measures for access control and unique identifiers. This being said the 2003 CSI / FBI survey shows a mature access control sector as well as increasing adoption of digital ID technologies (Figure 1). However, Biometric deployments have remained steady from 1999 – 2003. A number of variables could be causing this disparity.

Population – Future Biometric Industry Sectors Surveyed

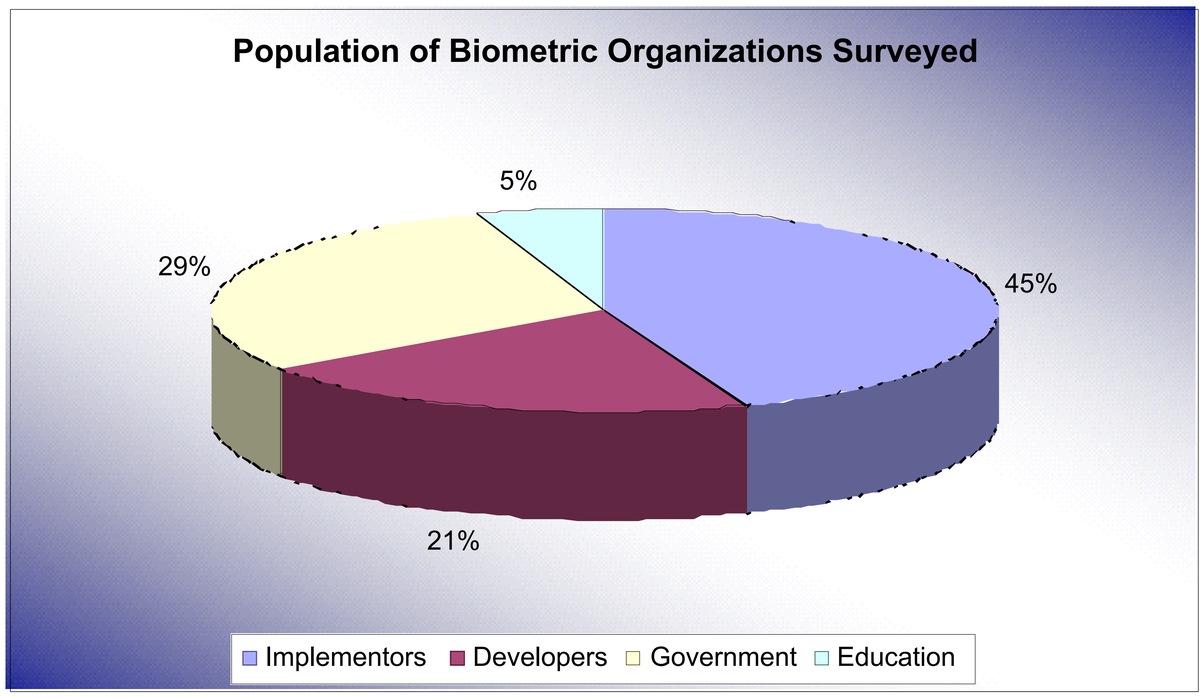

Figure 2 – Population of Biometric Organizations Surveyed

Methodology

Explore ROI techniques that have been published to date for Information Technology

↓

Survey a number of biometric implementers to get their clients' perspectives on the solution they have provided

↓

Analyze results, produce model that organizations can use to influence the investment in Biometric Technologies

Figure 3 – Project Methodology

The author intends to analyze a number of cost / benefit variables that organizations can use to tailor to their specific environment. Variables will relate to specific industries that the organizations surveyed have business and research exposure with (Figure 2).

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise