Case Study

The **Right** Approach to Test Security

Background

The Indian Institutes of Management (IIMs) are a network of India's most prestigious business schools. In April 2009, the IIMs announced the decision to collaborate with Prometric to migrate the largest, most competitive and most influential of India's exams, the Common Admission Test (CAT), from paper and pencil to computerized format. The CAT is the premier admissions test used in the selection process for admission to the IIMs, as well as more than a hundred business schools in India.

Challenge

Doing well on the CAT is the first step for candidates to take in gaining admission to one of the prestigious IIMs. More than 200,000 candidates prepare for—and take—the CAT every year. What's more, the test is only available for a fixed window each year. Only top-performing candidates advance to the next round of the selection process. In such a highly competitive environment, the CAT puts tremendous pressure and responsibility on the IIMs to provide a fair opportunity to all eligible candidates so that they can better their lives. The process of acquiring, verifying and maintaining the identity of candidates has never been more critical. Are individuals taking the CAT really who they say they are? Is CAT content and/or credibility at risk by dishonest and disingenuous candidates?

Strategy

Physical security of the testing environment, protection of the test content and verification of the candidate's identity became of utmost strategic importance to the IIMs in order to safeguard the integrity and validity of the CAT exam when converting to a computerized platform. In addition to ensuring that candidates test at the right location, date and time, the IIMs needed a way to accurately identify candidates who attempted to gain an unfair advantage by appearing more than once within the testing window or getting someone else to test on their behalf.

Solution

To address the IIM's test center security concerns in a computerized environment, Prometric put in place a mix of elements—including comprehensive biometrics and monitoring devices; standardized processes; well trained staff; strict compliance policies and audits; advanced data management encryption; and in-depth investigations to name a few.

+ Test content was securely stored on a central server and transmitted to each test location using advanced encryption methods. To minimize exposure of the test content, unique launch codes were provided to the test center staff just prior to each testing session.

IIM Fast Facts:

Location: Throughout India

Challenge: To ensure a secure testing environment to protect the integrity of the largest computerized exam delivered in the shortest period of time.

Outcome: Between 2009 through 2012, more than 800,000 candidates across 36 cities have successfully tested for CAT. More importantly, each candidate received a fair, valid and secure exam.

www.prometric.com

+ Security cameras recorded both audio and video throughout the testing areas.

+ Online systems accurately captured the information of each registered candidate to verify their identities. The customization of an online registration and scheduling portal also allowed candidates to enter their personal details as well as select their choice of location, date and time for their tests.

+ Two forms of on-site identity verification during the test were used. The first was a visual identification through a list of acceptable photo IDs that candidates presented at the time of their scheduled test. The second and more unique form of ID identification was biometric fingerprinting and digital image capture.

As a proven and widely accepted form of ID management, scanning of every candidate's fingerprint is quick — the perfect solution for verifying thousands of candidates. For the CAT, fingerprints were scanned and enrolled during the check-in process. They also were used during break periods — sign-in and sign-out — to verify that it was the same candidate moving in and out of the testing room. The candidate's day-of-test photo was captured, too, as the final step in the secure check-in process and was electronically linked to the candidate's test appointment and results.

The fingerprints captured were then securely stored and compared against a secure database to verify the candidate's identity and test history — identifying candidates who were found to have tested more than once during each testing window.

+ As an added security measure beyond test day, Prometric used an on-campus biometric kiosk which allowed the IIMs to verify the identities of the candidates at the point of admission into the IIMs. Candidates' fingerprints were scanned and verified prior to them being enrolled as a formal student of the IIM. This additional step provided the IIMs with the assurance that the candidate who took the CAT is the same one joining their institute.

+ To implement its strict ID management process, security policies and procedures, Prometric also required that all test center staff receive intensive training and undergo certification prior to the start of the testing window.

Outcome

Since the computerization of the CAT in 2009, Prometric has been successfully capturing the biometric data of approximately 200,000 candidates each year, enabling them to test in a secure environment where they can be assured that no one has an unfair advantage. By 2012 alone, Prometric has successfully delivered close to 800,000 tests across 36 cities and trained more than 1,000 test center administrators, proctors and test center staff.

Find Out More

Learn more about our *Test Development and Delivery Solutions* by visiting **www.prometric.com** or by calling toll-free **1-855-855-2241**.