School Standardized Test Security – From Paper and Pencil to Computer-Based Testing

In April of 2015, 11 staff members from the Atlanta Public Schools were convicted and sentenced to prison terms of up to seven years for inflating standardized test scores of students. Twenty additional Atlanta educators accepted plea deals.¹ These sentences are just the latest development in the long and sordid history of test tampering in the age of high-stakes testing.

As a result of the 2002 passage of the No Child Left Behind Act, public schools receiving federal funding are required to administer an annual statewide standardized test to all students. Schools that do not show that students are making “adequate yearly progress” toward achieving proficiency are penalized in various ways. Underperforming schools may incur the loss of federal funds, replacement of school staff, or even the restructuring of the school.² The pressure to succeed has resulted in administrators and teachers resorting to providing improper assistance to their students to ensure that their schools report the required level of improvement.³


As many states move from paper and pencil test administration to computer-based tests (CBTs), administrators need to reconsider their approaches to preventing, detecting and investigating testing irregularities. Though CBTs remove some of the security risks associated with paper and pencil tests, they also introduce a new set of issues that could affect the security of the tests. The changes in risks require a change in the approaches to preventing, detecting and investigating irregularities.

Prevention

As the old adage goes, “An ounce of prevention is worth a pound of cure.” The internal controls put in place by states, schools and test vendors can limit a school system’s exposure to test security breaches.

In the paper and pencil testing environment, controls center on the physical custody of tests from the moment they are delivered to the school to the time they are returned to the test vendor. Emphasis is placed on limiting the number of people who handle the tests and on ensuring that more than one person is present when tests are accessed. Tests are usually administered by teachers, who typically distribute and collect the tests and also are present as the students take their exams. Both the test administrator and a school-designated coordinator are required to sign out each student’s test booklet and answer sheet at the commencement of each testing session and also sign in each student’s test booklet and answer sheet at the end of the session. The aim of limitation of access is to prevent teachers, school administrators and students from getting unauthorized access to a test – before, during or after the test.

Unauthorized access can lead to various types of security breaches. These include the sharing of test questions before the test and the changing of answers by test administrators or others who may have access to the tests during or after the test session.

With the introduction of CBTs, the risk of unauthorized access to the test questions remains, albeit in different form. There are no physical test booklets and answer sheets to be stored or distributed; however, risks lie in the unauthorized access to tests and in improper test taking by such means as:

- Failure to authenticate a test taker, which could lead to the incorrect person taking the test
- Failure to limit Internet access during the test, which could result in students searching the Internet for answers to questions
- Unauthorized retention of test questions through viewing, printing, saving or emailing test questions
School systems can address these issues in a number of ways, a few of which include issuing a test ticket with unique login information to each student, blocking access to the Internet during testing, and securing cell phones and other personal electronic devices in a location outside of the testing environment.

Because some schools do not have a sufficient number of computers for testing, CBTs normally require longer testing windows, increasing the exposure to unauthorized access to the test. To address this issue, many school systems administer the test to all students in a class at the same time, reducing the likelihood that students will discuss test questions and responses with classmates who have not yet been tested.4

In both CBT and paper and pencil test settings, the use of test monitors is also an effective method to deter violations of test security.

Detection

No internal control system is perfect. Regardless of the number of measures in place to secure the test environment, it is inevitable that someone will find a way to breach test security. To the extent that internal control security measures fail to prevent a security breach, there are steps that may be taken by the school system to detect signs of cheating. These methods rely on statistical analysis to determine the likelihood that a security breach has occurred.

One of the most significant indicators of cheating as it relates to paper and pencil tests is the number of wrong-to-right (WTR) erasures on the optical answer (“bubble”) sheets used in paper and pencil exams. The erasures are measured and then analyzed to determine the performance of a particular class as compared to a system-wide average. A higher than average number of WTR erasures might indicate cheating within a classroom e.g. among students or as a result of inappropriate assistance provided by test administrators or mass erasing by teachers or administrators after the test. States can perform a number of other statistical analyses of student performance, including (but not limited to) analysis of a student’s growth from year to year and analysis of irregular response patterns between constructed responses and multiple choice questions.

With CBTs, there are no erasures to be analyzed; however, states may utilize many statistical techniques to detect signs of cheating. The most common statistical approaches to detecting

cheating on CBTs include analyzing latent response times and looking at score differences from year to year at the classroom, school and system levels.5

Investigation

Detection techniques provide an indication of testing irregularities. These irregularities must then be corroborated by on-the-ground investigations that may further validate statistical results or provide an explanation for the irregular statistical results.

Whether testing is paper and pencil-based or computer-based, the need for on-site investigation remains. The approaches to the interviews of educators and students may differ, as the questions posed to interviewees are directly related to the testing platform used and possible ways that cheating can occur.

On-site investigations look not only at the classroom that had the irregular testing results but also the culture of the school as a whole. Examiners interview school administrators, testing coordinators, teachers and students to determine whether and what type of cheating may have occurred. Questions are geared to scrutinize statistical results down to the individual student level so that investigators can determine how cheating occurred or understand the potential causes for the irregular statistical results.

Conclusion

Whether tests are computer-based or administered by paper and pencil, the risks of test security breaches refuse to go away. Obviously, every effort should be made to prevent security breaches from occurring. However, to the extent that breaches do occur, states and schools need to implement detective and investigative methods to identify cheating and to deter future acts of cheating.

Irrespective of one’s opinion regarding the benefits or disadvantages of standardized testing in schools, cheating on these tests is a disservice to the schools and the students they serve. Moreover, as the convicted Atlanta educators learned, violations of the rules can result in long

---

prison sentences for offenders. The stakes in standardized testing are higher than ever. Rigorous application of internal controls to prevent cheating, supported by measures to detect and investigate irregular testing results, can make an honest difference in American school systems.

Author:

Ingrid Christian, Director, (+1) 202 729 2133

Professional Spotlight:

Dhruv Phophalia, Managing Director, (+91) 22 6129 6038

Dhruv Phophalia is a Managing Director with Alvarez & Marsal and leads the firm’s Global Forensic and Dispute Services practice in India. He has more than 18 years of experience and specializes in anti-bribery and corruption consulting, fraud investigations, anti-fraud programs and controls, regulatory compliance, litigation support and bankruptcy matters.

For More Information:

Global Forensics, Disputes and Investigations