CLEAR
Exam Review

A Journal

Coeditor
Michael Rosenfeld, Ph.D.
Educational Testing Service
Princeton, NJ 08541-0001
mrosenfeld@ets.org

Coeditor
F. Jay Breyer, Ph.D.
Educational Testing Service
Rosedale Road, MS13-R
Princeton, NJ 80541-0001
fbreyer@ets.org

CLEAR Exam Review

VOLUME XXII, NUMBER 2   FALL 2011

Contents

The Role of Security in Today's Testing Programs

MARIE GARCIA, M.ED.[1]
Administration Manager, Examinations Department, National Council of State Boards of Nursing

ADA WOO, PH.D.
Senior Psychometrician, Examinations Department, National Council of State Boards of Nursing

Risk management is a key aspect of business success in any industry; neglecting risk management could lead to calamitous results (Fitzgerald, 2004). This statement is especially relevant to today's high-stakes testing programs given the prevalence of attempted cheating. Advances in technology have created more opportunities for individuals to cheat by providing new resources and ways of cheating (Cohen & Wollack, 2006). In one instance of high-tech cheating, a Medical College Admissions Test (MCAT) candidate used a pinhole camera to capture images of the test items. The items were transmitted to a co-conspirator who tricked three tutors into answering the test items. The answers were then fed back to the candidate via an open phone line (CSB News, 2011). With the increased instances of cheating, concerns about cheating now extend beyond validity of individual test scores to compromise of an entire testing program. For a $30 fee, the Website Scoretop.com provided candidates a chance to view operational Graduate Management Admissions Test (GMAT) items. Over 1,000 candidates subscribed to the service (Lavelle, 2008).

David Foster (2000) addressed the importance of test security, stating, "any certification program of value to you and the industry will do all that it can to preserve its overall quality, which is most strongly affected by the quality and security of its tests." Large testing programs, such as GMAT, MCAT, and LSAT are aggressively establishing and growing security practices to guard against the potential risks facing testing programs today and into the future. Complete security risk elimination is difficult, but awareness, effective strategies and response can elevate a security program and deter examinees from cheating on an examination. Cohen and Wollack (2006) discussed three categories of cheating countermeasures testing programs can implement: human observation and prevention (e.g., secure location of test materials, establishing authenticity of candidates), electronic countermeasures (e.g., video cameras, fingerprinting), and psychometric countermeasures (e.g., controlling item exposure, detecting aberrant response patterns). Each testing program may implement different security measures to prevent and detect cheating. The purpose of this paper is to provide a case study of the process implemented by one large-

scale examination program. The current paper describes the practices and security methods in place to preserve the integrity of the NCLEX® nursing licensure examinations.

Owned and developed by the National Council of State Boards of Nursing (NCSBN), the NCLEX examination is used for initial nursing licensure for registered nurses and licensed practical/vocational nurses in all U.S. states, Guam, Northern Mariana Islands, Virgin Islands and the American Samoa. More than 280,000 NCLEX examinations are administered annually. Due to the high-stakes nature of the examinations, the temptation to gain an unfair advantage through cheating is great among some candidates. As a result, the NCLEX follows a set of comprehensive procedures to detect and mitigate the impact of potential aberrant test-taking behaviors throughout the test development and administration processes.

Computerized Adaptive Testing Format

The NCLEX employs a multifaceted security design starting with test assembly and administration. The NCLEX is administered using Computerized Adaptive Testing (CAT) format. Each test administered is tailored to the candidate's ability and is variable in length. The difficulty of items seen by each candidate is determined by the person's ability estimate. When a candidate answers an item correctly, he/she will be presented with a more difficult item; when an item is answered incorrectly, an easier item will be administered next. This process will continue until the candidate has responded to a sufficient number of items and his/her ability estimate reaches one of the pre-established termination criteria. The variable length CAT format limits item exposure to only what is necessary to reach a pass/fail decision, thus enhancing security of the item bank.

In addition to exposure control, the CAT design also varies the items administered in each examination. Combined with a large number of items in the operational item pools and frequent rotation of the pools, the likelihood of identical examinations for two candidates or across multiple attempts is low. This property of CAT greatly mitigates the impact of item harvesting and sharing.

The GMAT is another example of a large-scale, high-stakes CAT program. In the GMAT cheating instance described previously (Lavelle, 2008), GMAC announced that the benefit to candidates who utilized Scoretop.com was minimal, because it was "extremely unlikely" that candidates would

see the same questions on their exams as they saw on Scoretop.com.

Application and Candidate Identity Verification Processes

Intellectual and physical security measures make up the second component of the NCLEX security design. In order to ensure the authenticity of all candidates' identities, nursing licensure candidates must follow the multi-step NCLEX Examination Administration, Registration and Eligibility registration prior to scheduling the examination (NCSBN, 2010). Nursing candidates must first submit an application to the Board of Nursing at which they wish to be licensed. Boards of Nursing will then conduct investigations and authorize eligible candidates to take the examination. Candidate's eligibility is managed through a secure online system by Boards of Nursing, NCSBN and its contracted test service staff.

Candidates may only register for the examination after they have met all of the eligibility requirements set by the Boards of Nursing in which they seek licensure. The secure online registration system detects duplicate registrations; ensuring only one registration exists per person at any given time. Once eligible, candidates are issued a NCLEX Authorization to Test (ATT) letter. The ATT letter is a required document for admission to the testing session. It identifies each candidate with candidate identification number, authorization code and test validity date. Candidates may schedule the examination within a specified timeframe after the ATT has been issued. If candidates do not complete the examination within this timeframe, they must repeat the application process to renew eligibility to test (NCSBN, 2011).

Establishing authenticity of the candidate does not end with the examination registration process. The NCLEX is administered at over 200 Pearson Professional Test Centers located in the U.S. and internationally. These testing locations are approved by NCSBN and managed by NCSBN's contracted test service Pearson VUE. Standardized test admission, administration and security procedures are implemented across all testing sites. Test administrators must undergo a comprehensive training program and up to 40 hours of practice before they administer an examination.

Verification of candidate identity begins when candidate arrives at the test center. The NCLEX program has traditionally used a multi-layer identity verification process including

verification of ATT letter, government issued identification document, photograph, signature, and digital fingerprint (NCSBN, 2011). As identification technology evolves, many testing programs have responded by implementing increasingly high-tech methods to authenticate identity of candidates and deter proxy test-taking (Hechinger, 2008). Starting from 2009, the NCLEX added palm vein technology to its existing identity check procedures. Palm vein scans capture the unique patterns of the blood vessels in an individual's palm using a near-infrared light source. Palm vein technology provides an extremely accurate way of identifying individuals and screening proxy test-taking attempts. All mismatches of biometrics and candidate identifications are kept on files and subjected to future investigations.

Test Administration and Incidents Reporting

All NCLEX examinations are administered following standardized procedures. Test administrators thoroughly explain examination rules during the candidate check-in process. Candidates confirm their understanding and agreement by providing digital signatures, noting that violation of any of the rules will result in withholding or cancelation of test results. Non-compliant candidates are not allowed to test. These standardized procedures are subjected to security audits by NCSBN staff. Random site visits and regular review of procedures are part of the overall security plan.

After candidates complete the check-in process, they begin testing in one of the standardized testing rooms. The testing rooms are designed for optimal monitoring by trained test administrators. Video cameras are installed in every testing room to monitor each candidate. Test administrators are able to monitor multiple candidates at once using a video monitor in the proctor station. Continuous video monitoring as well as full sound and motion videos are captured for all testing sessions.

To support test administrators in following examination procedures and prompt reporting of possible security risks, an incident reporting system is put in place. The Examination Incident Reporting System is a real-time reporting and tracking system designed to collect information about candidate and examination issues. Upon observing aberrant test-taking behaviors or procedural irregularities, test administrators are trained to immediately record the incidents. Depending on the nature of the incidents, candidates' results may be placed on hold for further analyses to determine validity of the test scores.

Incidents from testing sites are monitored daily. In addition to NCSBN and test service staff, the incident reporting system is accessible to NCSBN's member Boards of Nursing. All authorized parties can instantly review a report of a candidate who engaged in misconduct or aberrant test-taking behaviors. Depending on severity and nature of the misconduct, further investigations may follow. NCSBN reserves the right to cancel or withhold any test results when testing irregularities occur. This includes, but is not limited to, falsification of candidate identification or breaches to the candidate confidentiality agreement (NCSBN, 2010).

Data Forensics

In addition to putting procedures in place during test application and administration to deter and detect cheating behaviors, the NCLEX also regularly monitor open-source networks for unauthorized information. NCSBN contracts security service providers with expertise in cyber intelligence to monitor internet sites for content that may threaten the integrity of the NCLEX. Through continuous, comprehensive internet searches and sophisticated intelligence analyses, NCSBN staff can quickly identify unauthorized content. Internally, NCLEX item statistics and test data are under constant scrutiny by NCSBN and test service staff psychometricians. All test results undergo a series of quality control checks prior to being released. Any records containing potential irregularities are placed on hold for further review.

Conclusion

In a world where advanced technology is widely available and creative methods of cheating abound, there is great temptation to gain a competitive advantage in high-stakes testing through illegitimate means. In this environment, testing programs must continue to implement and improve their security plans. The need to maintain test integrity continues to drive sound operational procedures and innovative security enhancements. Security risk management should continuously evolve through an established culture of security awareness and immediate responses. In addition to reviewing test development and administrations procedures, testing programs should include regular monitoring of social media or other open-source networks when planning security procedures. A central element of a sound security plan is an established framework that provides a clear path for immediate identification, monitoring, control and mitigation. The benefits of establishing a set of standardized and multi-

faceted security procedures are well documented, not the least of which is to enhance legal defensibility of the test (e.g., Gorham & Woo, 2011). The authors hope that the example of the NCLEX program may provide some insight in developing security processes. With the advent of technology and the computers' capacity of simultaneously processing a large amount of information, the field of test security is growing rapidly to combat the rising sophistication of cheating attempts.

References

Cohen, A. S., & Wollack, J. A. (2006). Test Administration, Security, Scoring, and Reporting. In R. L. Brennan (Ed.), *Educational Measurement* (Fourth ed., pp. 355-386). Westport, CT: Praeger Publishers.

CBS News. (2011, May 31). *High-tech medical exam cheating alleged*. Retrieved September 8, 2011, from CBS News: http://www.cbc.ca/news/canada/british-columbia/story/2011/05/31/bc-high-tech-mcat-scam.html

Fitzgerald, C. (2004, September). *Risk management: Protecting our tests*. Retrieved September 9, 2011, from http://www.caveon.com/articles/fitzgerald2.htm

Foster, D. F. (2000, January). *What's all the fuss about test security*? Retrieved September 9, 2011, from Caveon: http://www.caveon.com/articles/df_article10.htm

Gorham, J., & Woo, A. (2011). The importance of data forensic applications in today's testing programs. *CLEAR Exam Review*, 15–17.

Hechinger, J. (2008, July 22). *Business schools try palm scans to finger cheats*. Retrieved September 9, 2011, from Wall Street Journal: http://online.wsj.com/article/SB121669545112672811.html

Lavelle, L. (2008, June 23). *Shutting down a GMAT cheat sheet*. Retrieved September 9, 2011, from Business Week: http://www.businessweek.com/bschools/content/jun2008/bs20080623_153722.htm

NCSBN. (2010). 2011 NCLEX *Examination Candidate Bulletin*. Chicago, IL: NCSBN.

NCSBN. (2011, July). *NCLEX Member Boards Manual*. Retrieved September 8, 2011, from NCSBN: https://www.ncsbn.org/NCLEX_Member_Board_Manual.pdf